



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

HOTSPOT -

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

The network contains an on-premises Active Directory domain named adatum.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

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	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 -

ADatum 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 Intune Configuration -

Microsoft Intune 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.

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

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA -

MAM user scope: GroupB -

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1 -

Folder protection: Enable -

List of apps that have access to protected folders: C:\\*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB -

Windows Autopilot Configuration -

ADatum 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 Windows Autopilot.  
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -

ADatum 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.

Deployed a network boundary configuration profile that will have the following settings:

Name: Boundary1 -

Network boundary: 192.168.1.0/24

Scope tags: Tag1 -

Assignments:

Included groups: Group1, Group2 -

Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

Name: Connection1 -

Connection name: VPN1 -

Connection type: L2TP -

Assignments:

Included groups: Group1, Group2, GroupA

Excluded groups: --

Name: Connection2 -

Connection name: VPN2 -

Connection type: IKEv2 -

Assignments:

Included groups: GroupA -

Excluded groups: GroupB -

Technical Requirements -

ADatum 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
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	<input type="radio"/>	<input type="radio"/>
User2 can remove D:\Folder1 from the list of protected folders on Device2.	<input type="radio"/>	<input type="radio"/>
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can remove D:\Folder1 from the list of protected folders on Device2.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	<input type="radio"/>	<input checked="" type="radio"/>

 **volto** Highly Voted 1 year, 4 months ago

1. No - only C:\\*\AppA.exe can create file in this folder.
  2. Yes - Local administrators can delete folder form protected folders list .
  3. No - Global Reader haven't privileges to run something on enrolled computers.
- upvoted 25 times



 **professorStein** 6 days, 3 hours ago

Well, based on my testing correct answers are:

- YES (the setting in ASR policy is only for adding additional trusted programs. Notepad is already trusted by Microsoft. So answer is YES.)

REF: <https://techcommunity.microsoft.com/discussions/analyticsonazurediscussion/all-about-microsoft-endpoint-administrator-md-102/4022853>

upvoted 1 times

  **prBo** 1 year, 2 months ago



Why does the MAM policy apply here?

upvoted 1 times

  **Futfuyfyfj** 1 year, 3 months ago

The global reader could sign in to a device and according to the Autopilot profile he will be a standard user locally. However being a standard user still allows to open a non elevated PS window and create a file, tested this, so should be NYY.

upvoted 8 times

  **FAlie**n 1 year, 1 month ago

No, user 3 cannot create a file on the desktop. the question states that the file is created with a powershellscript. You can only run a powershellscript after the execution policy is changed from restricted to something else.

upvoted 3 times

  **deit**  1 year, 4 months ago

I think it's

1. No - only C:\\*\AppA.exe can create file in this folder.
2. Yes - Local administrators can delete folder form protected folders list .
3. Yes - Desktop is not a folder protected by default. User can log in to computer and create files in his desktop.

upvoted 13 times

  **Futfuyfyfj** 1 year, 3 months ago

I tested this, my situation was not 100% equal, but thuis seems to be right. With non elavated PS I could create a txt file.

upvoted 4 times

  **NoursBear** 11 months, 1 week ago



not with a Powershell script he can't because of execution policy. He can however run a Powershell command from the prompt to create a file or a directory etc..

upvoted 2 times

  **HvD**  3 months, 1 week ago

Question 2: User2 can remove D:\Folder1 from the list of protected folders on Device2. The question is about removing the folder from the list of protected folder, not "remove folder", but "from the list of protected folders", which is in the policy, right? So this user must be able to change the policy in Intune, which he can not. He is only local admin on the devices.

upvoted 1 times

  **Tonsku** 3 months, 1 week ago

N,Y,N

User1: groupA

User2: groupB

User3: GroupA, groupB

Device4: AzureAD Join, group2

Device2: AzureAD Join, group2

All the Azure AD joined devices have an executable file named

C:\AppA.exe and a folder named D:\Folder1.

Folder protection: Enable

List of apps that have access to protected folders: C:\\*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB

upvoted 1 times

  **Tonsku** 1 year ago

MAM user scope: GroupB

upvoted 2 times

🗨️ 👤 **Merrybob** 3 months, 1 week ago

No - A Cloud Device Administrator doesn't have local admin rights. Without Local Admin rights no one can make a change to the folder in question except for C:\\*\AppA.exe

Yes - Tried this on my laptop and it allows me to delete the folder and enable/disable the Controlled Folder feature if needed.

No - Cannot run a script as a Global Reader. Need the execution policy enabled to be able to do that.

upvoted 4 times

🗨️ 👤 **OyYaGotta** 7 months, 1 week ago

The don't need local rights. They are removing the App from the list in Intune, not on a client computer. This whole question is horrendous and doesn't teach anyone anything. It's trick all the way. You would never come across the need to work this out in a real work scenario.

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 3 months, 1 week ago

Well, based on my testing correct answers are:

- YES (the setting in ASR policy is only for adding additional trusted programs. Notepad is already trusted by Microsoft. So answer is YES.)

- YES (Same as before, only custom scripts, programs are prevented from removing files. Exploere.exe is trusted, so answer is YES.)

- YES ( desktop folder is not a system folder like Pictures, Music, Video and Documents. In case this folder needs more protection It should be added in ASR policy. )

upvoted 2 times

🗨️ 👤 **OyYaGotta** 7 months, 1 week ago

- NO - ASR is a disaster recovery service. Nothing to do with this question. You are confusing it with App Protection Policy... which is also incorrect as this is Folder Protection. App list is one app. Notepad is NOT on the list.

Yes - User 2 has Admin rights to change desktop storage options

NO- Global reader can read... nothing else. ASR has, again, nothing to do with the users role rights.

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 9 months, 3 weeks ago

Second one should be NO.

Third one should be NO as well. Because execution policy is enabled by default.

upvoted 1 times

🗨️ 👤 **cruzi** 3 months, 1 week ago

Device4 is a member of Group2 and subject to the Endpoint protection configuration profile Protection1. Protection1 enables folder protection for D:\Folder1. Notepad.exe does not have access to D:\Folder1 and cannot save files in the folder.

Device2 is a member of Group1 and Group2 and subject to the Endpoint protection configuration profile Protection1. Protection1 enables folder protection for D:\Folder1. The protection cannot be removed by a local administrator.

User3 can create a file on his personal desktop using Power Shell, File Explorer, or any other suitable method.

1. No

2. No

3. Yes

upvoted 2 times

🗨️ 👤 **LionelDerBoven** 3 months, 3 weeks ago

Almost.

1 is correct (No). Secured folder.

2 is right (no). MAM configured the secured folder. even local admins can't disable that because it is configured by the MAM.

3 is no because he runs a script. non admin can't run a script or set-executionpolicy command.

upvoted 1 times

🗨️ 👤 **spillb** 3 months, 3 weeks ago

n one device (Device2) to both Groups 1 and 2 that promulgate all 3 policies?

upvoted 1 times

🗨️ 👤 **LionelDerBoven** 3 months, 3 weeks ago

1 (No). Secured folder so user can't do that (not even local admin)

2 (No). MAM configured the secured folder. even local admins can't disable that because it is configured by the MAM.

3 is no because he runs a script. non admin can't run a script or set-executionpolicy command.

upvoted 1 times

🗨️ 👤 **kiik32** 6 months ago

1. Yes note pad is a trusted app by default, I tested this. with a role-less user
  2. Yes
  3. Yes tested as well
- upvoted 2 times

🗨️ 👤 **Blessing\_** 4 months, 3 weeks ago

1. Device 4 is for personally owned
- upvoted 2 times

🗨️ 👤 **kiik32** 6 months ago

3. Yes you dont need a role to create files in unprotected folders from a non elevated power shell script
- upvoted 1 times

🗨️ 👤 **AlSuds** 1 year ago

I'm pretty sure it's N, N, and N.

2. is tricky because User is a local admin and can remove the folder - but cannot remove the policy to 'remove folder from the protected list'.
  3. is tricky too, Restricted Execution Policy allows an interactive PS console session (and the user can quite happily create a .txt file on their own desktop) - but Restricted never allows a user to run a PS script. Answer must be No.
- upvoted 4 times

🗨️ 👤 **lucianosasantos** 1 year, 1 month ago

I think it's

1. No - only C:\\*\AppA.exe can create file in this folder.
2. No - Local administrators can delete folder form protected folders list .
3. Yes - Desktop is not a folder protected by default. User can log in to computer and create

I agree wit @majerzg

2. The question is: user2 can remove D:\Folder1 from the list of protected folders, not - he can remove it from the disk on Device2.
- upvoted 3 times

🗨️ 👤 **majerzg** 1 year, 2 months ago

2. The question is: user2 can remove D:\Folder1 from the list of protected folders, not - he can remove it from the disk on Device2.
- upvoted 2 times



Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

The network contains an on-premises Active Directory domain named adatum.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

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	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 -

ADatum 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 Intune Configuration -

Microsoft Intune 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.

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

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA -

MAM user scope: GroupB -

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1 -

Folder protection: Enable -

List of apps that have access to protected folders: C:\\*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB -

Windows Autopilot Configuration -

ADatum 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 Windows Autopilot.  
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -

ADatum 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.

Deployed a network boundary configuration profile that will have the following settings:

Name: Boundary1 -

Network boundary: 192.168.1.0/24

Scope tags: Tag1 -

Assignments:

Included groups: Group1, Group2 -

Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

Name: Connection1 -

Connection name: VPN1 -

Connection type: L2TP -

Assignments:

Included groups: Group1, Group2, GroupA

Excluded groups: --

Name: Connection2 -

Connection name: VPN2 -

Connection type: IKEv2 -

Assignments:

Included groups: GroupA -

Excluded groups: GroupB -

Technical Requirements -

ADatum must meet the following technical requirements:

Users in GroupA must be able to deploy new computers.

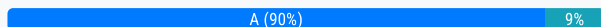
Administrative effort must be minimized.

Which devices are registered by using the Windows Autopilot deployment service?

- A. Device1 only
- B. Device3 only
- C. Device1 and Device3 only
- D. Device1, Device2, and Device3

**Suggested Answer:** C

Community vote distribution



**volto** Highly Voted 3 months, 2 weeks ago

**Selected Answer: A**

It worries me that there is so much irrelevant information in this question. But let's focus on the answer.

"Currently, there are no devices deployed by using Windows Autopilot." But in autopilot profile, they mark option "Convert all targeted devices to Autopilot - yes". It means "register all targeted devices to Autopilot if they are not already registered" "The setting only registers the devices in the assigned group(s) for the Autopilot service"

Autopilot profile is assigned to Group1 exclude Group2 -> Device 1 and Device 3.

But we still have additional requirements:

- Running a supported version of Windows - Device 1 and 3
- Enrolled in an MDM service such as Intune - Device 1 and 3

- A corporate device that's not already registered with Autopilot - only Device 1.


In my opinion, the correct answer is A

upvoted 20 times

 **Tati\_Oliveira** 1 year, 2 months ago


Sorry If, but I could not find where you saw that the only device not yet enrolled was Device 1. Device 1 is a corporate device and makes more sense to be already provisioned than Device 3. But I could find this info on the text "Currently, there are no devices deployed by using Windows Autopilot."

Is it right to say Device 1 and 3 or could be Device 1, Device 2, Device 3 since Device two is part of 2 groups (included and excluded of OOB).  
upvoted 1 times

 **fco168** 1 year, 1 month ago

The setting will register the devices that are not, but will also apply the configuration to the ones that are already.

upvoted 1 times

 **krzysztofbr** Highly Voted 1 year, 4 months ago

**Selected Answer: A**

It's pretty simple. Device 3 is personally owned, can't be in Autopilot.

So is only one possible answer A

upvoted 5 times

 **FemiA55** Most Recent 3 weeks ago

**Selected Answer: A**

Only Device 1 because it is corporate owned and member of Group 1 qualifies for OOB provided by Autopilot. But it still needs a reset for this to happen. A requirement not mentioned in the case study but we have this "All Windows 10 devices are joined to Entra ID and enrolled in Intune"

upvoted 1 times

 **pri27** 3 weeks, 4 days ago

**Selected Answer: A**

Answer A, not C because personal devices cannot be automatically enrolled in Autopilot by default.

upvoted 1 times

 **neothwin** 2 months ago

Answer is D. As in Group 1 is included in Auto pilot assignment.

upvoted 1 times

 **lucianosasantos** 3 months, 1 week ago

In my opinion the correct answer is A because in the link below

<https://learn.microsoft.com/en-us/autopilot/registration-overview>

Note


Don't register to Autopilot the following types of devices:

Microsoft Entra registered, also known as "workplace joined"

Intune MDM-only enrollment

These options are intended for users to join personally-owned devices to their organization's network.

upvoted 1 times

 **Darkfire** 3 months, 1 week ago

**Selected Answer: A**

I think A.

Based on Device 2 which is excluded from the Deployment Profile because it's in Group 2.

Device 3 is a personally owned device which cannot be registered based on:

<https://learn.microsoft.com/en-us/autopilot/windows-autopilot-hybrid#:~:text=If%20you%20want%20all,the%20device%20directly.>

So based on the question, which devices are registered via Deployment?

Only Device 1 ticks all boxes being registered.

But the main question is. Which answer will be right @ the exam?! =0

Anyone recently passed and had this quest? =P

upvoted 1 times

🗳️ 👤 **subbuhotmail** 3 months, 3 weeks ago

Selected Answer: C

Answer is C

Personally owned also can be used to enrol via Autopilot. Main requirement for the Autopilot is the profile and the setup. There is no device restriction mentioned that the personally owned device are restricted.

MDM allowed to register for User 1 & 3,  
Autopilot policy applied to Device 1 and 3.

Refer which devices can be enrolled via Autopilot.

<https://www.systemcenterdudes.com/different-methods-to-intune-windows-devices-enrollment/#:~:text=Windows%20Autopilot%20can%20only%20be,that%20will%20guide%20you%20through.>  
upvoted 2 times

🗳️ 👤 **Ayind3** 2 weeks, 3 days ago

No, a Microsoft Entra registered device, also known as a "workplace joined" device, cannot be enrolled with Windows Autopilot1. Autopilot requires devices to be registered specifically as Autopilot devices, which involves importing the device's hardware ID into the Autopilot service  
upvoted 1 times

🗳️ 👤 **oopspruu** 4 months, 1 week ago

Selected Answer: A

Device 1 Only. Device 3 is personally owned so will be ignored by the "Convert Targeted devices to AP' setting.  
upvoted 1 times

🗳️ 👤 **kiik32** 5 months, 4 weeks ago

Selected Answer: A

including a device group while excluding a device group works so device 2 wont get autopilot, also autopilot will not work with personal devices, so A)

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment>  
upvoted 2 times

🗳️ 👤 **SajjH** 5 months, 2 weeks ago

"The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune." As long as a device is enrolled, it will be assigned the profile even if it is personal. So, Device 1 and 3.

upvoted 1 times

🗳️ 👤 **091095f** 5 months, 4 weeks ago

Selected Answer: A

To those who took the exam recently: Did you encounter this question? What is the correct answer?

Is it C or A?

upvoted 1 times

🗳️ 👤 **kiik32** 6 months ago

Selected Answer: D

inclusion wins over exclusion

upvoted 1 times

🗳️ 👤 **Clauster** 6 months ago

Answer is A

Basically it's all because Device 3 it's a Personally owned device and o tho you can join it to AutPilot it will mark it as a "Corporate Owned" and the problem with this is that now the Coporation will have control over it and if it's a personal device user might not necessarily want that and it's not best practices. I had a lab with personal devices and i joined them to my Tenant using AutoPilot but now they are corp managed and i would have to remove them from Intune to make them Personal devices again. Please see this link: <https://learn.microsoft.com/en-us/autopilot/registration-overview>

upvoted 1 times

🗳️ 👤 **WORKHOLIC** 6 months, 3 weeks ago

Selected Answer: A

Corporate owned devices are covered by Autopilot

upvoted 1 times

🗳️ 👤 **evrybobry** 7 months, 3 weeks ago

Selected Answer: A

Personal devices cannot be covered to Autopilot

upvoted 1 times

  **Irism** 8 months, 1 week ago

**Selected Answer: A**

Only corporated devices can use autopilot

upvoted 1 times

  **AnoG** 9 months ago

If all devices in the assigned groups should automatically register to Autopilot, set Convert all targeted devices to Autopilot to Yes. All corporate owned, non-Autopilot devices in assigned groups register with the Autopilot deployment service. Personally owned devices aren't registered to Autopilot.

Answer is A

upvoted 3 times

HOTSPOT -

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

The network contains an on-premises Active Directory domain named adatum.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

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	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 -

ADatum 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 Intune Configuration -

Microsoft Intune 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.

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

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA -

MAM user scope: GroupB -

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1 -

Folder protection: Enable -

List of apps that have access to protected folders: C:\\*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB -

Windows Autopilot Configuration -

ADatum 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 Windows Autopilot.  
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -

ADatum 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.

Deployed a network boundary configuration profile that will have the following settings:

Name: Boundary1 -

Network boundary: 192.168.1.0/24

Scope tags: Tag1 -

Assignments:

Included groups: Group1, Group2 -

Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

Name: Connection1 -

Connection name: VPN1 -

Connection type: L2TP -

Assignments:

Included groups: Group1, Group2, GroupA

Excluded groups: --

Name: Connection2 -

Connection name: VPN2 -

Connection type: IKEv2 -

Assignments:

Included groups: GroupA -

Excluded groups: GroupB -

Technical Requirements -

ADatum 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
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device4 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device5 marked as compliant.	<input type="radio"/>	<input type="radio"/>

### Answer Area

	Statements	Yes	No
Suggested Answer:	Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
	Device4 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
	Device5 marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>

 **sh123df** Highly Voted 1 year, 4 months ago

No

No

Yes

Answer is correct

upvoted 16 times

 **qw6fzuczyv** 3 weeks, 1 day ago

Can someone explain why Device4 is a "No"

It appears to me that the device is personally owned so the policy will not apply meaning that using these backward settings may be a "Yes". I am under the understanding that compliance policies require devices to be Azure Ad Joined to be able to properly report compliance results. REF: [https://docs.google.com/document/d/1nCz7jJ9Mu-J\\_LfwUmeoPjzrNRZgeyfaeAACSzrBa9k](https://docs.google.com/document/d/1nCz7jJ9Mu-J_LfwUmeoPjzrNRZgeyfaeAACSzrBa9k)

upvoted 2 times

 **kinflaaaa** 1 week, 1 day ago

Device4 is part of Group2, which Policy3 (Require Bitlocker and Secure Boot) applies to, but Device4 only has Secure Boot enabled, so it is not compliant. Compliance policies can be applied to personally-owned (BYOD) devices: <https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment>

upvoted 1 times

 **Tonsku** Highly Voted 3 months, 1 week ago

N,N,Y

device1: bitlocker Y, secureboot N

Device1: group1

group1: policy1 & policy2

compliance policies settings:

Policy1: require bitlocker Only

Policy2: requere secure boot only

mark device with no compliance policy as Compliant

Device1 : Not Compliant

Device4: bitlocker N, secureboot Y

Device4: group2

group2: policy3

compliance policies settings:

Policy3: require bitlocker & secureboot

mark device with no compliance policy as Compliant

Device4 : Not compliance

Device5: bitlocker Y, secureboot N

Device5: group3

Policy3: group2

Policy3: require bitlocker & secureboot

compliance policy: mark device with no compliance as Compliant

Device5 : compliance

upvoted 15 times

 **boxafrica** Most Recent 3 months, 1 week ago

Cela semble correct.Sur le peripherique 1 nous avons deux politiques de conformité policy1 et poliy2 donc peripherique 1est non conforme.peripherique4 appartient au groupe 2 politique appliqué policy 3 qui requiere bitlocker et secure boot activeé;ce qui n'est pas le cas ici donc device 4 non conforme.Device 5 est conforme car il n a aucune poliique de conformité qui s'applique à lui donc oui/e qui nous donne NON;NON;OUI

upvoted 1 times

 **MR\_Eliot** 3 months, 1 week ago

Provided answer is correct:

Device 1

- Group1

Conditional Policy:

-> Policy1, Require bitlocker: YES

-> Policy2, Require SecureBoot: NO

Device 4

- Group2

Conditional Policy:

-> Policy3, Require Bitlocker & SecureBoot: NO

Device 5

- Group3

Conditional Policy:

-> None: Compliant, because of configuration.

upvoted 6 times

🗨️ 👤 **7798da3** 5 months, 3 weeks ago

disregard last post i see the names was looking for the actual policy

upvoted 1 times

🗨️ 👤 **7798da3** 5 months, 3 weeks ago

where is policy2 I see one only

upvoted 1 times

🗨️ 👤 **Cluster** 6 months ago

Provided answer is Correct 100%

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

No, No, Yes is correct.

upvoted 1 times

🗨️ 👤 **b0gdan433** 1 year, 1 month ago

The answer is No, No, Yes, i just took the exam today.

upvoted 1 times

🗨️ 👤 **iTomi** 1 year ago

So...? MS doesnt reveal right answers.

upvoted 2 times

🗨️ 👤 **Merrybob** 11 months ago

No way you could've confirmed this.

upvoted 1 times

🗨️ 👤 **Contactforntish** 1 year, 2 months ago

Device 1 would not be compliant since Policy 2 would fail for that

Device 4 (yes registered device can be checked for compliance, though no profile possible) is not compliant

Device 5 would be compliant since group 3 is getting no policy and no policy means compliant

No, No, yes

upvoted 3 times

🗨️ 👤 **picho707** 1 year, 2 months ago

Can someone explain why Device4 is a "No"

It appears to me that the device is personally owned so the policy will not apply meaning that using these backward settings may be a "Yes".

I am under the understanding that compliance policies require devices to be Azure AD Joined to be able to properly report compliance results.

upvoted 1 times

🗨️ 👤 **NoursBear** 11 months, 1 week ago

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune. Because it is enrolled it receives compliance policies

upvoted 1 times

🗨️ 👤 **Jacob75** 10 months, 3 weeks ago

Group 2 required Policy is Secure boot and Bitlocker and device does not have Bitlocker.

Personal devices can still be compliant and enrolled I think.

upvoted 1 times

🗨️ 👤 **FrenchDuck** 1 year, 3 months ago

So for Device 1 it's a Yes bc the way it's arranged, from my understanding, Group one only needs either or to be marked as compliant. Compared to Device 2\group 2, it explicitly states it needs Bitlocker AND Secure boot, hence why it's a Not Compliant for me. Device 5 \ group 3 however , it's up to interpretation based on what I've read in MS Learn so I'm going with Not Compliant based on here:

<https://learn.microsoft.com/en-us/training/modules/implement-device-compliance/4-deploy-policy>

upvoted 2 times

🗨️ 👤 **Futfuyfyfj** 1 year, 3 months ago

In stead of what you are writing you mean it's a No?  
upvoted 1 times

🗨️ 👤 **picho707** 1 year, 3 months ago

These answers are so backward. I will fire the Intune administrator for configuring something like this.  
upvoted 8 times

🗨️ 👤 **NoursBear** 1 year, 4 months ago

Well I was going for Yes No Yes because a device without a compliant policy is to be marked as compliant, so I don't know now as no one is thinking like me  
upvoted 4 times

🗨️ 👤 **Futfuyfyfj** 1 year, 3 months ago

But device1 is assigned to 2 policies, which makes a No for device 1....  
upvoted 2 times

🗨️ 👤 **NoursBear** 11 months ago

dunno why I came up with this, clearly NNY is correct, I see more clearly now lol  
upvoted 1 times

🗨️ 👤 **ShiftDeL** 1 year, 4 months ago

No  
No

Yes for device 5 as : "Mark devices with no compliance policy assigned as: Compliant" has been configured.  
upvoted 2 times

🗨️ 👤 **VirtualJP** 1 year, 4 months ago

I'm going with:

No  
No  
Yes

upvoted 3 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

Guys, so many wrong answers in the comments below!!  
BossAceVentura: your comment is correct.  
"Yes - Device is part of group 1 which require only Bitlocker  
No - Requires both bitlocker and secure boot  
No - there is no group 3 policy"  
upvoted 3 times

🗨️ 👤 **Futfuyfyfj** 1 year, 3 months ago

Lol, you are wrong: Mark devices with no compliance policy assigned as: Compliant" has been configured.  
upvoted 3 times

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

The network contains an on-premises Active Directory domain named adatum.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

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	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 -

ADatum 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 Intune Configuration -

Microsoft Intune 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.

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

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA -

MAM user scope: GroupB -

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1 -

Folder protection: Enable -

List of apps that have access to protected folders: C:\\*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB -

Windows Autopilot Configuration -

ADatum 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 Windows Autopilot.  
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -

ADatum 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.

Deployed a network boundary configuration profile that will have the following settings:

Name: Boundary1 -

Network boundary: 192.168.1.0/24

Scope tags: Tag1 -

Assignments:

Included groups: Group1, Group2 -

Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

Name: Connection1 -

Connection name: VPN1 -

Connection type: L2TP -

Assignments:

Included groups: Group1, Group2, GroupA

Excluded groups: --

Name: Connection2 -

Connection name: VPN2 -

Connection type: IKEv2 -

Assignments:

Included groups: GroupA -

Excluded groups: GroupB -

Technical Requirements -

ADatum must meet the following technical requirements:

Users in GroupA must be able to deploy new computers.

Administrative effort must be minimized.

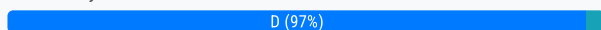
You implement Boundary1 based on the planned changes.

Which devices have a network boundary of 192.168.1.0/24 applied?

- A. Device2 only
- B. Device3 only
- C. Device1, Device2, and Device5 only
- D. Device1, Device2, Device3, and Device4 only

**Suggested Answer: B**

Community vote distribution



**letters1234** Highly Voted 1 year, 4 months ago

**Selected Answer: D**

Both Personal and Corporate devices can be enrolled to Intune, the network boundary can be assigned to enrolled Windows 10/11 devices.

<https://learn.microsoft.com/en-us/mem/intune/configuration/network-boundary-windows>

The Boundary is assigned to Group 1 & 2, Devices 1,2,3 and 4 have membership to these groups. Device 5 is not part of the membership for Group 1 & 2 so doesn't receive the policy.

upvoted 40 times

**iTomi** 1 year ago

When you creating boundary profile there are NO settings for scope tags. So, tags are irrelevant in this question.

upvoted 5 times

**deinth** Highly Voted 1 year, 4 months ago

**Selected Answer: D**

I think it should be D. As the boundary group is assigned to Group 1 and 2

upvoted 7 times

🗨️ 👤 **Joe9011** 1 year, 4 months ago

I read it the same  
upvoted 1 times

🗨️ 👤 **volto** 1 year, 4 months ago

Not only group membership defines assignment, but also scope tags. Device 3 belongs to Group 1 and has the correct scope tag.  
The correct answer is B  
upvoted 9 times

🗨️ 👤 **letters1234** 1 year, 4 months ago

Scope tags are: "You can use role-based access control and scope tags to make sure that the right admins have the right access and visibility to the right Intune objects."  
<https://learn.microsoft.com/en-us/mem/intune/fundamentals/scope-tags>

It isn't used for deployment/assignment to users or devices. Only administration.  
upvoted 12 times

🗨️ 👤 **TC1Labs** 1 year, 1 month ago

When you are creating a Tag, this message explain: "Scope tags define groups of Intune resources that align with specific Intune Role assignments. For example, a "Seattle Office" scope tag could be used to associate policies, profiles or applications with administrators that only apply to the Seattle office locations" I doubt between B or D.  
upvoted 2 times

🗨️ 👤 **JayHall** Most Recent 1 month, 1 week ago

You can assign scope tags to an Intune object type if the tenant can have multiple versions of that object (such as role assignments or apps).  
The following Intune objects are exceptions to this rule and don't currently support scope tags:  
Corp Device Identifiers  
Autopilot Devices  
Device compliance locations  
Jamf devices

Autopilot device deployment do not support the use of scope tags. So D is the only correct answer in this case: :Device1, Device2, Device3, and Device4 only.

See ref: <https://learn.microsoft.com/en-us/mem/intune/fundamentals/scope-tags>  
upvoted 2 times

🗨️ 👤 **AleFCI1908** 2 months ago

Selected Answer: B

B: because tag scope and assignment: only device 3  
upvoted 2 times

🗨️ 👤 **Zachypoo** 5 months, 4 weeks ago

<https://learn.microsoft.com/en-us/mem/intune/configuration/network-boundary-windows>

Point 9. "In Scope tags (optional), assign a tag to filter the profile to specific IT groups, such as US-NC IT Team or JohnGlenn\_ITDepartment."

Indicates given answer B is correct, tags can be used to filter to specific groups of users.  
upvoted 1 times

🗨️ 👤 **c813ce5** 6 months, 3 weeks ago

Device 3 because of the scope tag  
upvoted 3 times

🗨️ 👤 **AnoG** 9 months ago

Answer is B because of the scope tag,, Device 3 only  
upvoted 1 times

🗨️ 👤 **2c57d1c** 6 months, 4 weeks ago

No, you are wrong.  
upvoted 1 times

🗨️ 👤 **AnoG** 9 months ago

Answer is A because of the scope tag..

upvoted 1 times

🗨️ **SanuRockz** 10 months, 2 weeks ago

Answer is correct as per examlab

upvoted 1 times

🗨️ **BigStan82** 10 months, 2 weeks ago

Answer B: Device 3 Only.

It is the only device within the group range and scope range. Tags are used for filtering and scoping.

upvoted 3 times

🗨️ **MR\_Eliot** 10 months, 2 weeks ago

**Selected Answer: D**

I have not tested this to confirm but D seems logical answer. Group tags has nothing to do with assignments, they are just to identify things. nothing more.

upvoted 2 times

🗨️ **MR\_Eliot** 9 months, 3 weeks ago

I stay with D: Policy is applies to all enrolled devices in Intune. You can enroll a device via Company Portal, Autopilot or Hybrid Join.

<https://learn.microsoft.com/en-us/mem/intune/configuration/network-boundary-windows>

upvoted 1 times

🗨️ **onepunchkenshin** 11 months, 4 weeks ago

if the answer is incorrect, why doesn't site administrator update it?

upvoted 5 times

🗨️ **Tonsku** 1 year ago

**Selected Answer: D**

D

Boundary1 has the following assignments:

Included groups: Group1, Group2

Device1 (Group1)

Device2 (Group1, Group2)

Device3 (Group2)

Device4 (Group2)

upvoted 3 times

🗨️ **GeekGizmo** 1 year ago

I chose A. Personal devices can't be azure-ad joined so that would rule out device 3&4. Device 5 is in group 3, so that rules out that one.

upvoted 1 times

🗨️ **OyYaGotta** 10 months ago

Personal devices can be joined, does Azure know it's your computer? No, all it sees is User Groups, devices and policies.

upvoted 1 times

🗨️ **ThePrutser** 1 year, 1 month ago

**Selected Answer: D**

Scope tags are used for delegation of control and has nothing to do with device filtering for configuration profiles. Device 1, 2, 3, 4 are all part of either group 1, 2 or both and Device 5 is not. So it only applies to devices 1 through 4.

upvoted 4 times

🗨️ **Tati\_Oliveira** 1 year, 1 month ago

Network Boundary is applied to Groups 1 and 2 and Tag 1.

The only device that is member of Group 1 and 2 and has Scope Tag 1 is "Device 3" letter B.

upvoted 1 times

🗨️ **madsa** 1 year, 1 month ago

Definitely D.

upvoted 1 times

## HOTSPOT -

You have a Microsoft 365 subscription.

You use Microsoft Intune Suite to manage devices.

You have the iOS app protection policy shown in the following exhibit.

**Access requirements**

PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS8+/iPadOS)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS11+/iPadOS)	Block
PIN reset after number of days	No
Number of days	0
App PIN when device PIN is set	Require
Work or school account credentials for access	Require
Recheck the access requirements after /minutes of inactivity	30

**Conditional launch**

Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access

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.

**Answer Area**

After 30 minutes of inactivity, a user will be prompted for their

- account credentials only
- PIN only
- PIN and account credentials

Entering the wrong PIN five times will

- block access
- reset the app PIN
- reset the device PIN
- wipe company data

**Answer Area**


After 30 minutes of inactivity, a user will be prompted for their

- account credentials only
- PIN only**
- PIN and account credentials


Suggested Answer:

Entering the wrong PIN five times will

- block access
- reset the app PIN
- reset the device PIN**
- wipe company data

 **krzysztofbr** Highly Voted 1 year, 4 months ago

pin and account credentials  
reset app pin NOT device pin  
upvoted 49 times

 **Grg433** 1 year, 3 months ago

yes , it should be 'rest app pin' no ?  
upvoted 3 times

🗨️ **redline13** 10 months, 3 weeks ago

Why pin and account credentials for the first one?

Isn't only pin will be required?

upvoted 2 times

🗨️ **MR\_Eliot** 10 months, 2 weeks ago

Because "Work or school account credentials for access" is set to true.

upvoted 2 times

🗨️ **Temptset** Highly Voted 3 months, 1 week ago

1. PIN and account credentials

2. Reset the app PIN

1. EXPLANATION (PIN and account credentials)

Select Require to require the user to sign in with their work or school account instead of entering a PIN for app access. If you set this to Require, and PIN or biometric prompts are turned on, both corporate credentials and either the PIN or biometric prompts are shown.

SOURCE: <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios#access-requirements>

2. EXPLANATION (Reset the app PIN)

It's an APP protection policy, meaning the settings CAN'T apply to the device layer/level. An app policy is only allowed to utilize services on a device, but can't change device configurations.

upvoted 15 times

🗨️ **Rndadhdman** 1 week, 3 days ago

The question is asking about the App protection policy. So this is correct. Thank you.

upvoted 1 times

🗨️ **xDaveOnFireXx** Most Recent 1 week, 2 days ago

For all of you insisting it is PIN and Account Credentials for the first drop down menu, please allow me to explain why you may be mistaken. Nobody would use their product if we had to re-auth with our 2FA after every 30 min period of inactivity. The PIN alone is sufficient, why else would that be the only thing passed along over to FaceID or other biometric methods? Users in our environment are definitely not prompted to enter their "Work or school account" password when this occurs. FaceID/PIN alone lets you back in and resets the timer. I use corp teams on my MAM enrolled device and I can tell you if I was prompted for a password after using FaceID or entering the Teams PIN manually after 30 mins of inactivity, I would get very annoyed and would consider uninstalling the product altogether. PIN only is indeed the correct answer.

For those of you thinking you are resetting the PIN for the app itself you may be correct on that particular point but as for where that is controlled from, well that is from the device level. From the Intune management portal, you can only "Reset passcode" at the device level which effectively resets the PIN. There is not even anything anywhere else that says "Reset PIN" or even "Reset App Pin" as one would expect it to. After all this is Microsoft we are talking about here. Resetting the device PIN is the same as "reset passcode" in the Intune management portal, see: <https://learn.microsoft.com/en-us/mem/intune/remote-actions/device-passcode-reset> Reset the device PIN is indeed the correct answer.

upvoted 0 times

🗨️ **letters1234** 3 months, 1 week ago

Credential and PIN (or Biometrics if configured) will be required when re-check is done.

Work or school account credentials for access

<https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios#access-requirements>

And yes, just App PIN reset as device is not workplace joined/managed, only app protection policy.

upvoted 4 times

🗨️ **Futfuyfyfj** 1 year, 4 months ago

If you set this to Require, and PIN or biometric prompts are turned on, both corporate credentials and either the PIN or biometric prompts are shown.

upvoted 2 times

🗨️ **NoursBear** 3 months, 1 week ago

For the second question I think Device Pin is correct:

From Microsoft:

Timeout (minutes of inactivity)

Specify a time in minutes after which either a passcode or numeric (as configured) PIN will override the use of a fingerprint or face as method of

access. This timeout value should be greater than the value specified under 'Recheck the access requirements after (minutes of inactivity)'.

It's inactivity of the device not of an app

upvoted 2 times

🗨️ **NoursBear** 1 year, 4 months ago

sorry my bad, App PIN... I misread something

upvoted 7 times

🗨️ **MR\_Eliot** 10 months, 2 weeks ago

Answer:

1> Pin and login using account

2> App pin.

upvoted 5 times

🗨️ **Mattia8** 11 months, 3 weeks ago

Pin and account Credentials is correct

upvoted 1 times

🗨️ **Amir1909** 12 months ago

PIN and account credentials

reset the app PIN

upvoted 3 times

🗨️ **Tonsku** 1 year ago

PIN and account credentials

reset the app PIN

PIN for access: Require

Work or school account credential for access: Require

Max PIN attempts value 5 - action: Reset PIN

upvoted 1 times

🗨️ **Zelda78** 1 year, 2 months ago

pin and account to me. the difference here is that this (Work or school account credentials for access) setting is enabled?

"If required, work or school credentials must be used to access the policy-managed app. If PIN or biometric methods also required for access to the app, the work or school account credentials will be required on top of those prompts."

upvoted 1 times

🗨️ **Suresh\_2411** 1 year, 2 months ago

Pin and account credentials

Reset APP pin (since it is a app protection policy)

upvoted 4 times

🗨️ **VirtualJP** 1 year, 4 months ago

I'm going with krzysztofbr's answer

upvoted 2 times

🗨️ **ansilva** 1 year, 4 months ago

this would reset the app pin not the device pin

upvoted 3 times

🗨️ **Rewound** 1 year, 4 months ago

How would iOS APP protection policy reset DEVICE PIN?

upvoted 6 times

DRAG DROP -

You have a Microsoft 365 E5 subscription and a computer that runs Windows 11.

You need to create a customized installation of Microsoft 365 Apps for enterprise.

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

**Actions**

**Answer Area**

- Run `setup.exe` and specify the `/packager` switch.
- Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.
- Edit the XML configuration file.
- Run `setup.exe` and specify the `/download` switch.
- Run `setup.exe` and specify the `/configure` switch.

- 1
- 2
- 3
- 4



**Answer Area**

Suggested Answer:

- 1 Edit the XML configuration file.
- 2 Run `setup.exe` and specify the `/packager` switch.
- 3 Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.
- 4 Run `setup.exe` and specify the `/download` switch.

**casti** Highly Voted 1 year, 4 months ago

The correct answer is:

1. Download ODT application
2. Create a configuration file (XML)
3. `setup.exe /download` to download the installation files
4. `setup.exe /configure` to deploy the application

<https://learn.microsoft.com/en-us/deployoffice/deploy-microsoft-365-apps-local-source>

1. Download ODT application
2. Create a configuration file (XML)
3. `setup.exe /download` to download the installation files
4. `setup.exe /configure` to deploy the application

<https://learn.microsoft.com/en-us/deployoffice/deploy-microsoft-365-apps-local-source>

<https://learn.microsoft.com/en-us/deployoffice/overview-office-deployment-tool#download-the-installation-files-for-microsoft-365-apps>  
upvoted 82 times

**MR\_Eliot** 10 months, 2 weeks ago



sorry, but the question does not ask to install office. So setup.exe /configure is not needed. We only need to create custom MS Office installation.

upvoted 3 times

 **SajjH** 4 months, 4 weeks ago

There is no requirement for App-V packaging, hence /packager option is irrelevant, and then only option remains is /configure. Therefore the above answer by "casti" is correct.

upvoted 2 times

 **carl\_amadeo** 7 months, 1 week ago


I think the /configure is require as we don't want to distribute the package with /download option

upvoted 1 times

 **OyYaGotta** 10 months ago

Can you explain how, given there is no assumption in the question that you have already deployed non custom 365 apps that you can edit the .xml file without having downloaded ODT?

upvoted 1 times


 **tempelier1975** Highly Voted 1 year, 3 months ago

A mod need to edit this. Shown solution is not right!

The correct answer is:

1. Download ODT app
2. Create a configuration file (XML)
3. setup.exe /download to download the install files
4. setup.exe /configure to install

upvoted 13 times

 **MR\_Eliot** 10 months, 2 weeks ago

sorry, but the question does not ask to install office. So setup.exe /configure is not needed. We only need to create custom MS Office installation.

upvoted 1 times

 **cvos** 1 week ago

If install office is not needed then we only have 3 steps, but the question is asking for 4 steps. So /configure is the only option possible to add to the end

upvoted 1 times

 **laurentiu13** Most Recent 1 month, 1 week ago

1. Download ODT application
2. Create a configuration file (XML)
3. setup.exe /download to download the installation files
4. setup.exe /configure to deploy the application

upvoted 1 times


 **AleFCI1908** 2 months ago

The correct answer is:

1. Download ODT application
2. Create a configuration file (XML)
3. setup.exe /download to download the installation files
4. setup.exe /configure to deploy the application

after some investigations...

upvoted 1 times

 **MR\_Eliot** 3 months, 1 week ago

First: Download ODT Tool

Second: Extrat the files using the exe file.

Third: Edit XML configuration file if needed.

Fourth: Run Setup and specify /download parameter.

Why?

1. Because it should be a sutom installation of office, so you will need to edit the XML configuration file.
2. Setup /configure. Will install the office application. We want to create custom installation of Microsoft Office, not install it.
3. Setup with /download parameter, will pre download Office installation files in a sepearate folder for offline installation.

upvoted 2 times

🗨️ 👤 **OliTakesTests** 10 months, 1 week ago

Your 1st and 2nd are a single option in the answers. Might want to rethink this.

upvoted 3 times

🗨️ 👤 **Innit** 3 months, 1 week ago

The correct answer is:

1. Download ODT application
2. Create a configuration file (XML)
3. setup.exe /download to download the installation files
4. setup.exe /configure to deploy the application

[https://docs.google.com/document/d/1Yxh9Pg5hzlUcv-Hv5x-xUm9LtB6mPI0x\\_o6A4lgQv7l/edit?usp=sharing](https://docs.google.com/document/d/1Yxh9Pg5hzlUcv-Hv5x-xUm9LtB6mPI0x_o6A4lgQv7l/edit?usp=sharing)

upvoted 1 times

🗨️ 👤 **ENGELHENDY** 4 months, 2 weeks ago

The correct answer is:

1. Download ODT application
2. Create a configuration file (XML)
3. setup.exe /download to download the installation files
4. setup.exe /configure to deploy the application

upvoted 3 times

🗨️ 👤 **ushahid** 1 year ago

1. Download ODT application
2. Create a configuration file (XML)
3. setup.exe /download to download the installation files
4. setup.exe /configure to deploy the application

upvoted 4 times

🗨️ 👤 **Tonsku** 1 year ago

1. Download ODT
2. Edit the XML
3. setup.exe /download
4. setup.exe /configure

<https://learn.microsoft.com/en-us/DeployOffice/plan-microsoft-365-apps>

upvoted 1 times

🗨️ 👤 **mohdAj** 1 year, 1 month ago

- 1- Download the Office Deployment Tool (ODT)
- 2- Create a Configuration XML File
- 3- Download Microsoft 365 Apps " setup.exe /download to download the installation files"
- 4- setup.exe /configure config.xml

upvoted 2 times

🗨️ 👤 **HawkieEyes** 1 year, 1 month ago

Is the step to run setup.exe /download required? I thought that running setup.exe /configure will also download the install files first, and then install office?

upvoted 1 times

🗨️ 👤 **ThePrutser** 1 year, 1 month ago

yes the download step is required.

upvoted 1 times

🗨️ 👤 **ZaFletch** 1 year, 2 months ago

The package switch creates an App-V package, which is not mentioned in the question and would in no way be possible before downloading ODT. Are the answers deliberately wrong here? That seems mental.

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 4 months ago

Can't understand how the official answer could be so wrong. The correct way was obvious to everyone here.

upvoted 2 times

🗨️ 👤 **letters1234** 1 year, 4 months ago

casti is right, cant have the xml to edit if you havent got the ODT downloaded (it comes part of the exe unzipping)  
upvoted 2 times

🗨️ 👤 **GaloCO** 1 year, 4 months ago

The order of those steps re wrong  
upvoted 1 times

🗨️ 👤 **GaloCO** 1 year, 4 months ago

1. Download ODT application
  2. Create a configuration file (XML)
  3. setup.exe /download to download the installation files
  4. setup.exe /configure to deploy the application
- upvoted 7 times

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

Name	Platform
Device1	Windows 10
Device2	Windows 11
Device3	Android
Device4	iOS

On which devices can you apply app configuration policies?

- A. Device2 only
- B. Device1 and Device2 only
- C. Device3 and Device4 only
- D. Device2, Device3, and Device4 only
- E. Device1, Device2, Device3, and Device4

**Suggested Answer:** C

Community vote distribution

C (100%)

 **volto** Highly Voted 1 year, 4 months ago

**Selected Answer: C**

iOS and Android only

upvoted 22 times

 **krzysztofbr** 1 year, 4 months ago


app configuration exist also for Windows but in preview. I hope exam measure features not in preview. so i Agree wit You

upvoted 1 times

 **Futfuyfj** 1 year, 3 months ago

No you are referring to app PROTECTION policies. Question is about app CONFIGURATION policies

upvoted 2 times

 **krzysztofbr** Highly Voted 1 year, 4 months ago

was for Android and IOS only not for Windows:)

upvoted 9 times


 **Besxp** Most Recent 2 months ago

From Copilot

I get the confusion: the older answer C was based on the historical use of app configuration policies, which were initially designed for iOS and Android only. As Intune has evolved, so have its capabilities. Nowadays, those policies apply to Windows devices too.

So, given the most recent information, it's not just iOS and Android anymore—it's all platforms Intune can manage, meaning all devices in your list. E is the right call.


upvoted 2 times

 **OigresMG** 2 months, 3 weeks ago

Correct option is E:

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-managed-app>

upvoted 4 times

 **OigresMG** 2 months, 3 weeks ago

I think currently the 4 options may be correct, according to this reference link:

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-managed-app>

upvoted 2 times

 **JGMG** 3 months, 1 week ago

The answer is:

E. Device1, Device2, Device3, and Device4.

App configuration policies can be applied to all managed devices, regardless of the platform. Managed devices are devices that are enrolled in Microsoft Intune and have a management profile installed. In this case, all four devices are managed devices, so app configuration policies can be applied to all of them.

Here is a breakdown of the different platforms and whether they can be managed by Intune:

Windows 10 and Windows 11: Yes

Android: Yes

iOS: Yes

macOS: No

Linux: No


So the correct answer is E.

upvoted 4 times

 **Futfuyfj** 1 year, 3 months ago

Wrong, take a look yourself Intune-Apps-app configuration policies and try to create one , you will see you are wrong


upvoted 2 times

 **Jimix** 3 months ago

That's correct. You only need to read the article below to notice only iOS and Android can be targeted by that policy

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

upvoted 1 times

 **Haider\_Raza** 3 months, 1 week ago


No, App Configuration policies in Microsoft Intune are not only for Android and iOS devices; they can also be used for Windows devices. App Configuration policies allow you to configure settings and features for apps on mobile devices, regardless of the operating system.

With App Configuration policies, you can customize app behavior, configure app settings, and even control app access to corporate resources. These policies are particularly useful for managing settings in line-of-business (LOB) apps or apps developed in-house that support AppConfig standards.

In the case of Windows devices managed by Intune, App Configuration policies can be used to configure settings for Universal Windows Platform (UWP) apps and Win32 apps deployed using Intune. This allows you to tailor the app experience and functionality to meet your organization's specific requirements.

OPTION E IS CORRECT

upvoted 4 times

 **veliyath** 3 months, 1 week ago

**Selected Answer: C**

In Microsoft Intune, app configuration policies can be applied to devices that run mobile operating systems, such as Android and iOS. Based on the provided table:

Device1: Windows 10

Device2: Windows 11


Device3: Android

Device4: iOS

App configuration policies are generally intended for mobile operating systems. Therefore, the correct answer is:

C. Device3 and Device4 only

upvoted 1 times


 **091095f** 5 months, 4 weeks ago

I'm confused. Can you explain why we can apply "app configuration policies" only for mobile (Android and iOS) and not for Windows 10 and 11?



The apps in the Microsoft Store are also called "apps" so why can't we apply these configuration policies to the 'apps' in the Microsoft Store?

Thanks

upvoted 2 times


 **Shawn\_Chen** 9 months, 3 weeks ago

E is correct. From Intune admin center > Apps > App protection policies, it now can choose ios/ipados, android and windows  
upvoted 4 times

  **Friscini** 1 month, 3 weeks ago



You are confusing App PROTECTION policies with App CONFIGURATION policies, the question is about CONFIGURATION policies so correct answer should be C

upvoted 1 times

  **MR\_Eliot** 10 months, 2 weeks ago

Answer is correct. You can only configure App Configuration policy for IOS & Android devices.

upvoted 2 times

  **Darkfire** 10 months, 3 weeks ago

**Selected Answer: C**

C is correct

You can create and use app configuration policies to provide configuration settings for

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> both iOS/iPadOS or Android apps.

upvoted 1 times

  **Tonsku** 1 year ago

**Selected Answer: C**

iOS/iPadOS & Android

upvoted 1 times

  **mohdAj** 1 year, 1 month ago

**Selected Answer: C**

"You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps."

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

upvoted 2 times



  **mohdAj** 1 year, 1 month ago

**Selected Answer: C**

"You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps."

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

upvoted 2 times

  **Praveenm2712** 1 year, 1 month ago

Ans is C. There is option to manage devices or apps.

Managed devices - The device is managed by Intune as the unified endpoint management provider. The app must be pinned to the management profile on iOS/iPadOS or deployed through Managed Google Play on Android devices. In addition, the app supports the desired app configuration.

upvoted 1 times

  **Jacob75** 1 year, 3 months ago

**Selected Answer: C**

The answer is C --

"You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps."

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

upvoted 2 times

HOTSPOT -

You have an 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.

### Answer Area

Policy type:  ▼

- App configuration policy
- App protection policy
- Conditional access policy
- Device compliance policy

Minimum number of policies:  ▼

- 1
- 2
- 3
- 4
- 5

### Answer Area

Suggested Answer:

Policy type:  ▼

- App configuration policy
- App protection policy
- Conditional access policy
- Device compliance policy

Minimum number of policies:  ▼

- 1
- 2
- 3
- 4
- 5

 mohdAj Highly Voted 3 months, 1 week ago

Here's how you can achieve this:

Create an App Protection Policy:

Create a new App Protection Policy in the Microsoft Endpoint Manager admin center.

Configure Data Transfer Settings:

Within the App Protection Policy, configure the settings related to data transfer. In your case, you would likely look for settings related to the clipboard or data sharing.

Assign the Policy:

Assign the App Protection Policy to the specific app (App1) on the targeted platforms (Windows, Android, and iOS).


In this scenario, you should create one App Protection Policy per platform. So, you would create:

One App Protection Policy for Windows.

One App Protection Policy for Android.

One App Protection Policy for iOS.

upvoted 18 times

 **MR\_Eliot** Highly Voted 10 months, 2 weeks ago


Answer is correct. I research all my answers before commenting.

upvoted 13 times

 **PraniIR** Most Recent 3 months, 1 week ago


Policy type: App protection policy Minimum number of policies: 1 Comprehensive Explanation of Correct Answer Only: The correct answer is app protection policy because it allows you to customize the settings of apps for iOS/iPadOS or Android devices<sup>1</sup>. One of the settings you can configure is Restrict cut, copy, and paste between other apps, which lets you prevent users from copying data from App1 and pasting the data into other apps<sup>2</sup>. You only need one policy to apply this setting to all devices that have App1 installed<sup>1</sup>. Reference: 1: App configuration policies for Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> 2: Troubleshoot restricting cut, copy, and paste between applications - Intune | Microsoft Learn <https://learn.microsoft.com/en-us/troubleshoot/mem/intune/app-protection-policies/troubleshoot-cut-copy-paste>

upvoted 2 times

 **iTomi** 1 year, 1 month ago

You are wrong. Minimum number of policies is 3. Each win, android and ios need own policies.

upvoted 2 times

 **veliyath** 3 months, 1 week ago

You need to create separate App Protection Policies for each platform to prevent users from copying data from App1 and pasting it into other apps. Here's the breakdown:

Windows: One App Protection Policy

Android: One App Protection Policy

iOS: One App Protection Policy


So, you need a total of three App Protection Policies.

The correct selections are:

Policy type: App protection policy

Minimum number of policies: 3

upvoted 5 times

 **Zachypoo** 5 months, 4 weeks ago

<https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policies>

3 App protection policies.

You can only target one platform at a time. Check the screenshot, as they don't seem to explicitly state this in the documentation but is visible in the provided screenshot.

upvoted 3 times

 **Murad01** 11 months, 1 week ago

Given answer is correct


upvoted 2 times

 **Tonsku** 1 year ago

prevent copy/paste/cut/print using App protection policy

Minimum of one policy that can be applied across multiple platforms.

upvoted 1 times

 **fco168** 1 year, 2 months ago

- (1) Policy for Android Devices, (1) for iOS devices and (1) for Windows devices which will apply for Windows 10 and 11 simultaneously. 3 policies.

All 3 policies (copy, paste, cut, etc) settings blocked.

upvoted 3 times



🗨️ 👤 **FrenchDuck** 1 year, 3 months ago

Since it mentioned Intune apps, it implies apps possibly managed by Intune, so I am thinking 2 possible scenarios as to why it's 3 policies: 1) for enrolled, un-enrolled, and Windows devices or 2) for the different platforms (even though windows has Windows-Information Protection instead of Intune)

upvoted 2 times

🗨️ 👤 **NoursBear** 1 year, 4 months ago

I think the number of policies is 2 because in the WIP Policy I cannot find an entry to prevent copy/paste between apps, I see this setting only in Android/iOS Policies. I saw other options about receiving data but that was something else. Well that's my take on it.

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 4 months ago

OK I finally found what I was looking for about WIP:

Using protected apps. Managed apps (apps that you've included on the Protected apps list in your WIP policy) are allowed to access your enterprise data and will interact differently when used with unallowed, non-enterprise aware, or personal-only apps. For example, if WIP management is set to Block, your employees can copy and paste from one protected app to another protected app, but not to personal apps. Imagine an HR person wants to copy a job description from a protected app to the internal career website, an enterprise-protected location, but makes a mistake and tries to paste into a personal app instead. The paste action fails and a notification pops up, saying that the app couldn't paste because of a policy restriction. The HR person then correctly pastes to the career website without a problem.

But I just could not find the option within the policy itself. So 3 Policies it is.

upvoted 6 times

🗨️ 👤 **letters1234** 1 year, 4 months ago

Windows Information Protection can be configured under App Protection Policies and has been around for a while, it's going to be replaced with Purview Information Protection though. So three sounds right to me based on the amount of options in protection policies.

<https://learn.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure>

upvoted 3 times

🗨️ 👤 **F3RRY** 1 year, 4 months ago

But why is the minimum 3?

upvoted 1 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

should be two. for Android and IOS only. protection for Windows is something pretty new. still in preview

upvoted 1 times

🗨️ 👤 **Futfuyfyfj** 1 year, 3 months ago

Should be 3, windows information protection is often called app protection policies. The exam isn't already adjusted on the recently released Windows App Protection Policies for Edge only.

upvoted 2 times

🗨️ 👤 **Futfuyfyfj** 1 year, 4 months ago

one for each platform

upvoted 4 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

answer seems be correct. just because We also have protection for Windows but this is in PREVIEW

<https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-windows>

upvoted 1 times

🗨️ 👤 **Futfuyfyfj** 1 year, 4 months ago

They are referring to Windows Information Protection, it is there for quite Some time already and de deprecation was already announced, take a look in your Intune portal under app protection politik

upvoted 1 times

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.  
 You use Microsoft Intune to manage devices.  
 You plan to deploy two apps named App1 and App2 to all Windows devices. App1 must be installed before App2.  
 From the Intune admin center, you create and deploy two Windows app (Win32) apps.  
 You need to ensure that App1 is installed before App2 on every device.  
 What should you configure?

- A. the App1 deployment configurations
- B. a dynamic device group
- C. a detection rule
- D. the App2 deployment configurations

**Suggested Answer:** C

Community vote distribution



**\_WTH\_** Highly Voted 1 year, 4 months ago

correct answer is D. with a detection rule app2 could install before app1, intune would simply call app2 a failed install due to app1 not being detected. the correct answer is app2 deployment configuration (must list app1 as a requirement or dependency) surely?  
 upvoted 30 times

**Ksobier** 10 months, 2 weeks ago

I just check as I have one app that will fail if the another is not installed. I have 4 apps configured this way. As per answer D. 2nd app depends on installation of app1  
 upvoted 3 times

**GarySappig** 1 year, 4 months ago

Think so as well.

Detection rule is only so that Intune know that the application is correctly installed. With SCCM for example, even when the detection rule is configured incorretly the application still installs, you only get a failure to detect if it's installed correctly.

Requirement or a dependency would be a better option to be sure that APP1 is installed.

upvoted 2 times

**MR\_Eliot** 10 months, 2 weeks ago

Agreed.

upvoted 1 times

**ZaFletch** Highly Voted 1 year, 4 months ago

**Selected Answer: D**

Detection rule won't work here. Detection rules are to confirm the app is or is not installed on the machine. If you configured it to detect the prior install then it will mark app2 as installed and take no further action.

You need a dependency on app2 that will detect app1 then install app1

upvoted 11 times

**PraniR** Most Recent 3 months, 1 week ago

The correct answer is D because you can configure the dependencies for a Win32 app in the deployment configurations1. Dependencies are other Win32 apps that must be installed before your Win32 app can be installed1. You can add Win32 app dependencies only after your Win32 app has been added and uploaded to Intune2. In this case, you need to configure the App2 deployment configurations to add App1 as a dependency2. Reference: 1: Microsoft Intune Win32 App Dependencies - MSEndpointMgr <https://msendpointmgr.com/2019/06/03/new-intune-feature-win32-app-dependencies/> 2: Add and assign Win32 apps to Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-add>

upvoted 1 times

🗨️ **LionelDerBoven** 3 months, 3 weeks ago

**Selected Answer: D**

Wrong. You configure dependency's on APP2.

upvoted 1 times

🗨️ **GSBXL** 5 months, 3 weeks ago

But can you explain why a wrong answer is given in Show Solution? I don't get it. IS it on purpose or they just take an exam made by someone and upload here as he/she performed?

upvoted 1 times

🗨️ **veliyath** 6 months ago

**Selected Answer: D**

To ensure that App1 is installed before App2 on every device, you should configure the dependency settings within the deployment configurations of App2. This involves specifying App1 as a dependency for App2, which ensures that App1 is installed before App2.

Therefore, the correct answer is:

D. the App2 deployment configurations

upvoted 2 times

🗨️ **veliyath** 6 months ago

**Selected Answer: D**

o ensure that App1 is installed before App2 on every device, you should configure the dependency settings within the deployment configurations of App2. This involves specifying App1 as a dependency for App2, which ensures that App1 is installed before App2.

Therefore, the correct answer is:

D. the App2 deployment configurations

upvoted 2 times

🗨️ **speedwaymaniac** 6 months, 1 week ago

**Selected Answer: D**

Detection rules are to confirm the app is or is not installed on the machine.

You need a dependency on app2 that will detect app1 then install app1 if not present, before deploying app2

upvoted 1 times

🗨️ **Ruchira007** 7 months, 2 weeks ago

Answer D is the correct answer

upvoted 1 times

🗨️ **kerimnl** 9 months, 1 week ago

**Selected Answer: D**

D. the App2 deployment configurations

upvoted 1 times

🗨️ **Darkfire** 10 months, 2 weeks ago

**Selected Answer: D**

I also vote for D

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-add#:~:text=App%20dependencies%20define,the%20app%20itself.>

upvoted 1 times

🗨️ **Amir1909** 12 months ago

D is correct

upvoted 1 times

🗨️ **Tonsku** 1 year ago

**Selected Answer: A**

You need to ensure that App1 is installed before App2 on every device.

What should you configure?

the App1 deployment configurations.

upvoted 1 times

🗨️ 👤 **Tonsku** 1 year ago

App1 deployment configurations.

To add App1 to all Windows devices before App2, you should configure the App1 deployment configurations. You can create a deployment configuration for App1 in the Microsoft Endpoint Manager admin center by going to Apps > Windows > Add > Line-of-business app for app type > App package file for app package source > App1 for app information > Configure app package settings for deployment settings > Install behavior for installation settings > Install for the user for user experience settings. Then, create a deployment for App2 and assign it to the same group as App1. Since App1 is installed first, App2 will be installed after App1.

upvoted 1 times

🗨️ 👤 **iTomi** 1 year ago

**Selected Answer: D**

App dependencies are applications that must be installed before your Win32 app can be installed. You can require that other apps are installed as dependencies.

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-add#step-5-dependencies>

upvoted 2 times

🗨️ 👤 **Sonia33** 1 year, 1 month ago

**Selected Answer: D**

App1 as a dependency of App2.

upvoted 1 times

🗨️ 👤 **Dieter\_0026** 1 year, 1 month ago

**Selected Answer: D**

list app1 as a dependency?

upvoted 2 times

You have a Microsoft Intune subscription.

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

Name	Operating system
Device1	Android 8.1.0
Device2	Android 9
Device3	iOS 11.4.1
Device4	iOS 12.3.1
Device5	iOS 12.3.2

An app named App1 is installed on each device.

What is the minimum number of app configuration policies required to manage App1?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

**Suggested Answer: B**

Community vote distribution

B (85%)

A (15%)

 **krzysztofbr** Highly Voted 1 year, 4 months ago

**Selected Answer: B**

answer B is correct You need app protection for both platforms, separately

upvoted 14 times

 **Futfuyfj** 1 year, 4 months ago

Correct, although the answer remains the same, the question is about app configuration policies, not app protection policies :-)


upvoted 5 times

 **Carlio2024** Most Recent 3 weeks, 2 days ago

**Selected Answer: B**

The correct answer is B. Based on testing in my tenant, each platform requires its own dedicated policy.

upvoted 1 times

 **PraniIR** 3 months, 1 week ago

The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices1. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices1. The settings are assigned to user groups and applied when the app runs1. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune1. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings2.


Reference: 1: App configuration policies for Microsoft Intune | Microsoft Learn

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> 2: Add

app configuration policies for managed iOS/iPadOS devices | Microsoft Learn

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-ios>

upvoted 1 times

 **ThePrutser** 3 months, 1 week ago

**Selected Answer: A**

Technically it is possible to create one app configuration policy for both IOS and Android; when I go to the 'basics' tab, then set 'target policy to' to 'selected apps' and then 'select public apps', I can select the same app for Android and iOS/iPadOS at the same time.

The question doesn't mention any other requirements regarding different settings or to do it using best practices. So from what technically is possible and the given (or lacking) requirements in the question, I would say you can achieve it with one App Configuration Policy. Thus I vote A.

If someone can clearly explain to me why I need 2 such policies, as that is the most voted answer, please let me know. The current present explanations are not conclusive enough for me.

upvoted 4 times

 **iTomi** 1 year ago

I agree, right answer is A.1.


I dont see any reason why need to create two separate policies. On basic tab you can choose selected apps, all apps, all microsoft apps or core microsoft apps.

upvoted 2 times

 **iTomi** 1 year ago

We were wrong, right answer is 2.

upvoted 3 times

 **iTomi** 3 months, 1 week ago

**Selected Answer: B**

Intune represents these different app configuration policy channels as:

Managed devices. The device is managed by Intune as the unified endpoint management provider.

Managed apps. An app that has either integrated the Intune App SDK or have been wrapped using the Intune Wrapping Tool and supports App Protection Policies (APP).

In this scenario (devices enrolled in Intune):

Choose the Apps - App configuration policies - Add - Managed devices


On basic tab: Select platform iOS/iPad or Android

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-ios>

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-android>

upvoted 1 times

 **RaziLlycas** 3 months, 1 week ago

If you create an APP CONFIGURATION -> MANAGED APPS and in the "selected apps" add the two versions of App1 (android and iOS) you could configure the same App with 1 policy so answer "A". In case of MANAGED DEVICES instead you have to choose iOS or Android and in that case is "B". As usually Microsoft is misleading with the exam questions, assuming that the less is better, I will go with "A"

upvoted 2 times

 **Zoom2020** 4 months ago

YouTube shows you need to choose the Platform first before picking the app. Only one platform can be picked at a time. Thus 2 policies are required.

upvoted 1 times


 **Innit** 3 months, 1 week ago

The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices<sup>1</sup>. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices<sup>1</sup>. The settings are assigned to user groups and applied when the app runs<sup>1</sup>. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune<sup>1</sup>. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings<sup>2</sup>.

Reference: 1: App configuration policies for Microsoft Intune | Microsoft Learn

[https://docs.google.com/document/d/1Yxh9Pg5hziUcv-Hv5x-xUm9LtB6mPI0x\\_o6A4IqQv7l/edit?usp=sharing](https://docs.google.com/document/d/1Yxh9Pg5hziUcv-Hv5x-xUm9LtB6mPI0x_o6A4IqQv7l/edit?usp=sharing)

upvoted 1 times

 **veliyath** 3 months, 1 week ago

**Selected Answer: B**

To manage App1 on the listed devices, you need to create app configuration policies for each platform, not for each version of the operating system. In this case, you have:

Android: Device1 and Device2 (Android 8.1 and Android 9)

iOS: Device3, Device4, and Device5 (iOS 11.4.1, iOS 12.3.1, and iOS 12.3.2)

You need one app configuration policy for Android and one for iOS.

Therefore, the minimum number of app configuration policies required is:

B. 2

upvoted 3 times

🗨️ 👤 **King\_shola** 3 months, 3 weeks ago

**Selected Answer: B**

It's B

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 2 weeks ago

**Selected Answer: B**

You need separate policies for each OS.

upvoted 2 times

🗨️ 👤 **NoursBear** 11 months, 2 weeks ago

Again this is debatable, devices are enrolled so one can presume you will select "managed devices", there you have to choose a platform. With choosing Managed Apps, the policy doesn't care if the devices are enrolled or not, if you select all apps or individual apps, the target will be both platforms together so 1 policy. In this case I place my bet on B

upvoted 1 times

🗨️ 👤 **Tonsku** 1 year ago

**Selected Answer: B**

B.

one app configuration policy for each platform

upvoted 1 times

🗨️ 👤 **mohdAj** 1 year, 1 month ago

**Selected Answer: B**

in this scenario, the minimum number of app configuration policies required is 2 : one for Android devices and one for iOS devices. This assumes that the configuration settings for App1 are the same within each platform.

upvoted 1 times

🗨️ 👤 **Praveenm2712** 1 year, 1 month ago

Correct ans is B For iOS and for Android.

upvoted 1 times

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. .ipa
- C. .apk
- D. .appx

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ **krzysztofbr** Highly Voted 1 year, 4 months ago

**Selected Answer: B**

B correct IPA (like beer:))

<https://learn.microsoft.com/en-us/mem/intune/apps/lob-apps-ios>

upvoted 25 times

🗳️ **veliyath** Most Recent 6 months ago

**Selected Answer: B**

To deploy a custom line-of-business (LOB) app to iOS devices using Microsoft Intune, you should select the app package file with the .ipa extension.

Therefore, the correct answer is:

B. .ipa

upvoted 1 times

🗳️ **MR\_Eliot** 10 months, 2 weeks ago

**Selected Answer: B**

Correct answer is given.

upvoted 1 times

🗳️ **Darkfire** 10 months, 3 weeks ago

**Selected Answer: B**

B is correct

.IPA = iOS > <https://learn.microsoft.com/en-us/mem/intune/apps/lob-apps-ios>

.APK = Android > <https://learn.microsoft.com/en-us/mem/intune/apps/lob-apps-android>

upvoted 3 times

🗳️ **Tonsku** 1 year ago

**Selected Answer: B**

IPA (iOS)

upvoted 1 times

🗳️ **mohdAj** 1 year, 1 month ago

**Selected Answer: B**

When deploying a custom line-of-business (LOB) app to iOS devices using Microsoft Intune, the recommended extension for the app package file is .ipa. The .ipa file is the standard package format for iOS applications.

upvoted 2 times


🗳️ **Gr8Greet** 1 year, 4 months ago

**Selected Answer: B**

correct



upvoted 2 times

 **casti** 1 year, 4 months ago

Seems correct: <https://learn.microsoft.com/en-us/mem/intune/apps/lob-apps-ios>

upvoted 3 times

You have a Microsoft 365 E5 subscription that contains a user named User1 and a web app named App1. App1 must only accept modern authentication requests. You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:

Assignments -

Users or workload identities: User1

Cloud apps or actions: App1 -

Access controls -

Grant: Block access -

You need to block only legacy authentication requests to App1.



Which condition should you add to CAPolicy1?

- A. Filter for devices
- B. Device platforms
- C. User risk
- D. Sign-in risk
- E. Client apps

**Suggested Answer: E**

Community vote distribution

E (100%)

 **Gr8Greet**  1 year, 4 months ago

**Selected Answer: E**

Seems to be correct.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

upvoted 12 times

 **mohdAj**  1 year, 1 month ago

**Selected Answer: E**

Here's a step-by-step guide:

Go to the Microsoft 365 admin center.

Navigate to "Security" and then "Conditional Access."

Create a new Conditional Access policy (CAPolicy1) and configure the following:

Assignments:

Users or workload identities: User1

Cloud apps or actions:

Include App1

Conditions:

Client apps: Modern authentication clients

Access controls:

Grant: Block access

upvoted 7 times

  **Pisces225** Most Recent 1 month, 2 weeks ago

**Selected Answer: E**

This is the correct page to use to self-verify that E is correct:

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-legacy-authentication>

upvoted 1 times

  **veliyath** 6 months ago



**Selected Answer: E**

To block only legacy authentication requests to App1, you need to target the type of client application used in the authentication request. In Conditional Access policies, this is done using the "Client apps" condition.

Therefore, the correct condition to add to CAPolicy1 is:

E. Client apps



upvoted 2 times

  **MR\_Eliot** 9 months, 3 weeks ago

**Selected Answer: E**

E is correct.

upvoted 2 times

  **Darkfire** 10 months, 3 weeks ago



**Selected Answer: E**

E is correct

7. Under Conditions > Client apps, set Configure to Yes

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-block-legacy>

upvoted 1 times

  **ubiquituz** 11 months, 4 weeks ago

E

client apps <https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-block-legacy>

upvoted 1 times

  **Amir1909** 12 months ago

Correct

upvoted 1 times



  **Tonsku** 1 year ago

**Selected Answer: E**

Grant: Block access -

client Apps block only legacy authentication

upvoted 1 times

  **Praveenm2712** 1 year, 1 month ago

E

Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.

Browse to Protection > Conditional Access.

Select Create new policy.

Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

Under Assignments, select Users or workload identities.

Under Include, select All users.

Under Exclude, select Users and groups and choose any accounts that must maintain the ability to use legacy authentication. Exclude at least one account to prevent yourself from being locked out. If you don't exclude any account, you won't be able to create this policy.

Under Target resources > Cloud apps > Include, select All cloud apps.


Under Conditions > Client apps, set Configure to Yes.

Check only the boxes Exchange ActiveSync clients and Other clients.

Select Done.

Under Access controls > Grant, select Block access.

upvoted 3 times

  **mhmyz** 1 year, 2 months ago

Selected Answer: E

Correct


<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-block-legacy>

upvoted 1 times

  **poppinaz** 1 year, 3 months ago

Correct



upvoted 1 times

  **Rocky83** 1 year, 3 months ago

Selected Answer: E

Correct

upvoted 1 times

  **pinda** 1 year, 3 months ago

Selected Answer: E

Correct

upvoted 1 times

## HOTSPOT -

All users have Microsoft 365 apps deployed.

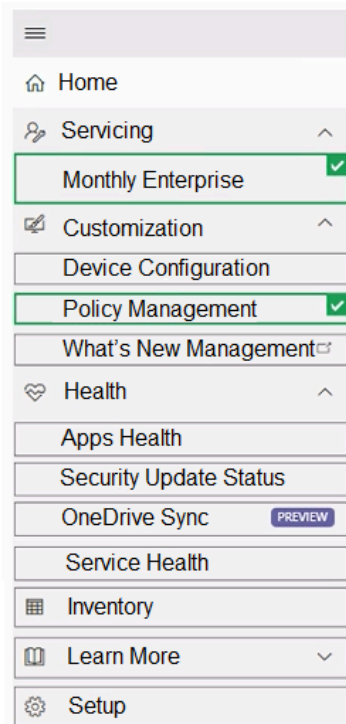
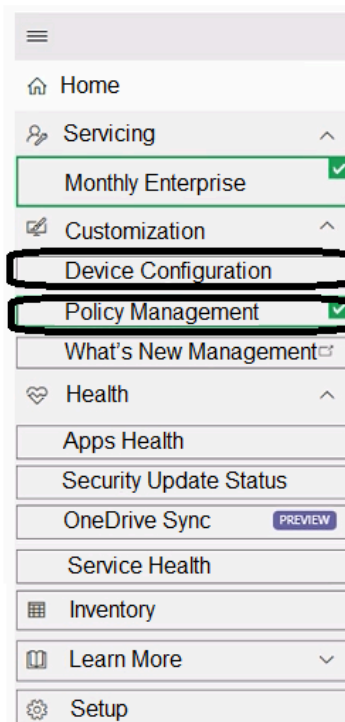
You need to configure Microsoft 365 apps to meet the following requirements:

Enable the automatic installation of WebView2 Runtime.

Prevent users from submitting feedback.

Which two settings should you configure in the Microsoft 365 Apps admin center? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****Answer Area**

Suggested Answer:

Given answer is correct:

Enable the automatic installation of WebView2 Runtime > Device Configuration > Modern Apps Settings

Prevent users from submitting feedback > Policy management

upvoted 10 times

  **Darkfire**  10 months, 3 weeks ago

Answer is correct

You can enable automatic installation in the same setting as where you prevent it from being installed automatically:

To prevent the automatic installation of WebView2 Runtime, sign in to the Microsoft 365 Apps admin center (<https://config.office.com>) with an admin account. Then, go to Customization > Device Configuration > Modern Apps Settings. Select Microsoft Edge WebView2 and then clear the Enable automatic installation of WebView2 Runtime check box.

<https://learn.microsoft.com/en-us/deployoffice/webview2-install>

Prevent users from submitting feedback:

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-feedback-ms-org?view=o365-worldwide>

upvoted 8 times

  **SanuRockz** 10 months, 1 week ago

I agree

Answer : Customization --> Device configuration --> Modern App setting

Policy management also not required here

upvoted 1 times



  **kiik32**  5 months, 3 weeks ago

both are under device configuration now a days.

modern app settings tab for webview



My configurations tab > app preferences to block feedback

upvoted 2 times

  **ten1ton** 4 months, 3 weeks ago

No, You are mistake, WebView2 Runtime > Device Configuration > Modern Apps Settings, Prevent users from submitting feedback > Policy management

upvoted 1 times

  **MR\_Eliot** 10 months, 2 weeks ago

Given answers are correct.

upvoted 3 times

  **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

  **yosry** 1 year ago

correct



upvoted 1 times

  **Tonsku** 1 year ago

configure in the Microsoft 365 Apps admin:

Device Configuration & Policy Management

upvoted 2 times

  **ronct** 1 year, 3 months ago



i verified this in the admin center at [config.office.com](https://config.office.com) and it is correct

upvoted 3 times

  **NoursBear** 1 year, 4 months ago

I don't understand Microsoft 365 apps is not covered anywhere in the MD102 course

upvoted 8 times

  **iTomi** 1 year, 1 month ago


Yes it is, exam ref MD-102 Microsoft Endpoint Administrator book chapter 4, skill 4.1

upvoted 4 times

  **Gbrezy162** 6 months, 2 weeks ago

iTomi, where did you purchase the MD-102 book? Thank you!

upvoted 2 times

  **Roska** 1 month, 3 weeks ago

Microsoft Press Store

upvoted 1 times

You have a Microsoft 365 subscription.

You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM).

You need to deploy the Microsoft 365 Apps for enterprise suite to all the computers.


What should you do?

- A. From the Microsoft Intune admin center, create a Windows 10 device profile.
- B. From Azure AD, add an app registration.
- C. From Azure AD, add an enterprise application.
- D. From the Microsoft Intune admin center, add an app.

**Suggested Answer: A**

Community vote distribution

D (97%)


 **Gr8Greet** Highly Voted 1 year, 4 months ago

**Selected Answer: D**

It should be D.

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-add-office365#select-microsoft-365-apps>

upvoted 30 times

 **ZaFletch** Highly Voted 1 year, 4 months ago

**Selected Answer: D**

Who in the world put A here?


upvoted 12 times

 **yhano** Most Recent 1 month, 2 weeks ago

**Selected Answer: B**

Based on <https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe>. What is related to the question is the personal data. It says that When you use the Retire device action, the user's personal data is not removed from the device.

upvoted 1 times

 **veliyath** 5 months, 4 weeks ago

**Selected Answer: D**

To deploy the Microsoft 365 Apps for enterprise suite to all the computers enrolled in mobile device management (MDM), you should:

D. From the Microsoft Intune admin center, add an app

Here's a step-by-step guide:

Sign in to the Microsoft Intune admin center.

Navigate to "Apps" > "All apps".

Click on "Add".

Select the app type as "Windows 10" and choose "Microsoft 365 Apps".

Configure the app information and settings as required.

Assign the app to the groups or devices you want to deploy it to.

This method leverages Microsoft Intune to manage and deploy applications to your enrolled devices, ensuring they receive the necessary Microsoft 365 Apps for enterprise suite.

upvoted 6 times

 **veliyath** 6 months ago

**Selected Answer: D**

To deploy the Microsoft 365 Apps for enterprise suite to all the computers enrolled in mobile device management (MDM), you should add the app from the Microsoft Intune admin center.

Therefore, the correct answer is:



D. From the Microsoft Intune admin center, add an app.

upvoted 1 times



  **speedwaymaniac** 6 months, 1 week ago

**Selected Answer: D**

Configuration Profiles deploy config settings not apps.

To deploy the suite you need to add an app. Answer is D.

upvoted 1 times

  **CJL324** 7 months, 2 weeks ago

D. From the Microsoft Intune admin center, add an app.

Navigating to the Microsoft Intune admin center.

Selecting Apps > All apps > Add.

Choosing the appropriate app type (in this case, Microsoft 365 Apps for Windows 10).

Configuring the app deployment settings, such as installation context, deployment intent, and assignment to target devices or user groups.


upvoted 1 times

  **proservices** 8 months ago

**Selected Answer: D**

Answer is D

upvoted 1 times

  **Titi150** 8 months, 2 weeks ago

Answer D



upvoted 1 times

  **mestorrent86** 9 months, 3 weeks ago

**Selected Answer: D**

To deploy the Microsoft 365 Apps for enterprise suite to the 10 Windows 10 computers enrolled in mobile device management (MDM), you should follow these steps: From the Microsoft Intune admin center, add an app. This will allow you to deploy the Microsoft 365 Apps for enterprise suite to all the computers efficiently.

upvoted 2 times

  **Dave808** 9 months, 3 weeks ago

**Selected Answer: D**

Always use intune to upload the app

upvoted 1 times

  **SanuRockz** 10 months, 1 week ago

Answer should be D


upvoted 1 times

  **MR\_Eliot** 10 months, 2 weeks ago

**Selected Answer: D**

Answer is D. Device is managed via Intune. So you will need to add a new application. I have done this alot with my work.

upvoted 1 times

  **MR\_Eliot** 10 months, 2 weeks ago

A. From the Microsoft Intune admin center, create a Windows 10 device profile.

- NO, devices are already in MDM.

B. From Azure AD, add an app registration.

- This has nothing to do with the question.

C. From Azure AD, add an enterprise application.

- This has nothing to do with the question.

D. From the Microsoft Intune admin center, add an app.

- This is correct. Since devices are already in MDM, we need to simply create a new app and assing it to all devices.

upvoted 4 times

  **Darkfire** 10 months, 3 weeks ago

**Selected Answer: D**

I think D is correct as well.

Although it says APPS, every app has to be added first before you can deploy it right?

upvoted 1 times

🗨️ 👤 **vijay0715** 11 months, 1 week ago

Sign in to the Microsoft Intune admin center.

Select Apps > All apps > Add.

Select Windows 10 and later in the Microsoft 365 Apps section of the Select app type pane.

Click Select. The Add Microsoft 365 Apps steps are displayed.

upvoted 1 times

🗨️ 👤 **AdamRachel** 11 months, 3 weeks ago

**Selected Answer: A**

i will go for A as in question is you need to deploy Apps not one App. if that will be one App answer D will be correct but that is multiple Apps i think creating Windows 10 will be easy and fast way of deployment all of them at once.

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 2 weeks ago

No, this is not true. With " create a Windows 10 device profile" they mean to create a enrollment profile in Intune. They don't mean Image!

upvoted 1 times

🗨️ 👤 **yosry** 1 year ago

**Selected Answer: D**

correct

upvoted 1 times

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You have a Windows 11 device named Device1 that is enrolled in Intune. Device1 has been offline for 30 days.

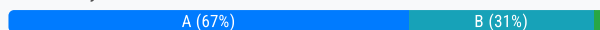
You need to remove Device1 from Intune immediately. The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and OEM-installed apps must be retained.

What should you use?

- A. a Delete action
- B. a Retire action
- C. a Fresh Start action
- D. an Autopilot Reset action

**Suggested Answer:** B

Community vote distribution



**ExamKiller020** Highly Voted 1 year, 3 months ago

**Selected Answer: A**

The clue in this question is: You need to remove Device1 from Intune immediately

So basically the only option that is left is 'delete' as this instantly removes the device from intune and only removes company data.

ref: <https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe#delete-devices-from-the-intune-admin-center>  
upvoted 27 times

**LionelDerBoven** 3 months, 3 weeks ago

Not right:

Delete Action:

Purpose: The Delete action removes the device from Intune's management console, but it does not affect the device itself. This means no data or configurations are removed from the device—it simply stops showing up in Intune's list of managed devices.

upvoted 2 times

**iTomi** 1 year, 1 month ago

This action immediately deletes the device from Intune, and it cannot be undone. However, it does not trigger a wipe of the device.

upvoted 3 times

**ThePrutser** 1 year, 1 month ago

Straight from learn.microsoft.com:

If you want to remove devices from the Intune admin center, you can delete them from the specific device pane. The next time the device checks in, any company data on it will be removed as Intune also retires a device when deleting it from the admin center. So I vote A

upvoted 10 times

**OyYaGotta** 11 months ago

I agree it's a bad question that contradicts its self, but deleting the device leaves the company data and apps on the device. Retire will remove company data and apps as soon as it's next online. Delete will just prevent Intune management /access to Company Portal, but will no longer give you the ability to control data under DLP for example which you likely want to remove. Retire will do this, and as the device is offline anyway, there should be no reason to remove it "immediately" from Intune.

upvoted 2 times

**AppSphere23** 7 months, 4 weeks ago

There is no reason to it but it states in the Question that the device (for whatever reason) needs to be removed so retiring it doesn't fill the requirements, since it then is still in Intune.

upvoted 1 times

**Grimmgore** Most Recent 4 days, 12 hours ago

**Selected Answer: B**

Why "Retire" is the Correct Action:

Behavior of Retire:

Removes Intune-provisioned apps, settings, and data from the device.

Leaves user-installed apps, personal data, and OEM-installed apps intact.

If the device comes online and checks in with Intune later, the retire action will be enforced.

Steps to Perform Retire Action:

Open the Microsoft Intune admin center.

Navigate to Devices > All Devices.

Select Device1 from the device list.

Choose Retire from the list of available actions.

upvoted 1 times

🗨️ **MacWilson** 2 weeks, 1 day ago

**Selected Answer: A**

Answer A

Delete is immediate. It also issues a retire or wipe.

<https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe#delete-devices-from-the-intune-admin-center>

"If you want to remove devices from the Intune admin center, you can delete them from the specific device pane. Intune issues a Retire or Wipe action depending on the OS/Enrollment type. Not all enrollment types support the Retire action. See the following table for the expected behavior based on the device platform and the enrollment type."

upvoted 1 times

🗨️ **OHMSS** 2 weeks, 3 days ago

**Selected Answer: B**

"if the device checks in again, any apps and data provisioned by Intune are removed" only Retire will do that.

upvoted 1 times

🗨️ **Omerozb** 3 weeks, 3 days ago

**Selected Answer: B**

I choose b read closely

You need to remove Device1 from Intune immediately. "The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and OEM-installed apps must be retained."

When the device checks in again, then it needs to be removed

upvoted 2 times

🗨️ **Alboo007\_rs007** 3 weeks, 4 days ago

**Selected Answer: A**

A Delete Action \* remove Device 1 immediately

upvoted 1 times

🗨️ **edo1803** 4 weeks, 1 day ago

**Selected Answer: B**

Delete does not remove corporate data from device, only deletes device from Intune. Correct option is B - Retire.

upvoted 2 times

🗨️ **Sonia33** 1 month ago

**Selected Answer: A**

It is delete action the one that removes immediately the device from the console and also acts as a retire action, based on MS documentation:

<https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe#delete-devices-from-the-intune-admin-center>

upvoted 1 times

🗨️ **Tr619899** 1 month, 2 weeks ago

B. a Retire action

Explanation: The Retire action in Microsoft Intune removes Intune-provisioned apps, settings, and data from the device while keeping user-installed apps, personal data, and OEM-installed apps. This is the recommended action when you want to remove management from a device but

retain personal content, which aligns with your requirement.

- Delete would only remove the device from Intune without affecting the device itself, so if the device checks in again, the settings would still remain.

- Fresh Start removes most apps, settings, and personal files.

- Autopilot Reset resets the device to a business-ready state but does not retain user-installed apps and personal data as required.  
upvoted 3 times

🗨️ 👤 **neothwin** 2 months ago

Answer B: "Delete Action

Purpose: The Delete action permanently removes the device from Intune management.

Outcome: If a device is deleted, it is immediately removed from the Intune portal, and any future check-ins will no longer apply. However, unlike Retire, if the device was managing apps and configurations, the user-installed apps and personal data may still remain on the device, but there won't be any mechanism for Intune to manage or remove those upon future check-ins."

upvoted 1 times

🗨️ 👤 **raduM** 3 months ago

it is b. Retire action removes the corporate data but keeps the personal one, and this is the request. Delete does not remove anything

upvoted 2 times

🗨️ 👤 **RomanV** 3 months, 2 weeks ago

From Microsoft Learn:

The Retire action removes managed app data (where applicable), settings, and email profiles that were assigned by using Intune. The device is removed from Intune management. Removal happens the next time the device checks in and receives the remote Retire action. The device still shows up in Intune until the device checks in. If you want to remove stale devices immediately, use the Delete action instead.

As the question states "immediately", the answer is A)Delete

Source: <https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe#delete-devices-from-the-intune-admin-center>

upvoted 2 times

🗨️ 👤 **King\_shola** 3 months, 3 weeks ago

**Selected Answer: B**

B for retire

upvoted 1 times

🗨️ 👤 **daviis** 3 months, 3 weeks ago

**Selected Answer: B**

The answer is B

Because it said "User-installed apps, personal data, and OEM-installed apps must be retained."

Otherwise, it would've been A.

upvoted 1 times

🗨️ 👤 **LionelDerBoven** 3 months, 3 weeks ago

**Selected Answer: B**

Retire Action:

Purpose: This action removes company data from the device while keeping the user's personal data and apps intact. It's commonly used when a device is no longer needed for corporate use, but the device owner should retain their personal files and apps.

Delete Action:

Purpose: The Delete action removes the device from Intune's management console, but it does not affect the device itself. This means no data or configurations are removed from the device—it simply stops showing up in Intune's list of managed devices.

upvoted 1 times

🗨️ 👤 **dnt91** 4 months ago

**Selected Answer: A**

The Retire action removes managed app data (where applicable), settings, and email profiles that were assigned by using Intune. The device is removed from Intune management. Removal happens the next time the device checks in and receives the remote Retire action. The device still shows up in Intune until the device checks in. If you want to remove stale devices immediately, use the Delete action instead.

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

upvoted 2 times

🗨️ 👤 **Frank9020** 4 months ago

**Selected Answer: B**

Using the RETIRE option:

Immediate Removal: It removes the device from Intune management immediately.

Provisioned Data: Ensures that if the device checks in again, any Intune-provisioned apps and data will be removed.

Retention of Personal and OEM Content: User-installed apps, personal data, and OEM-installed apps are retained, meeting the need to keep these elements.

For this scenario, where you want to ensure that managed apps and data are removed if the device checks in again, but personal data and user-installed apps are retained, the Retire action is the appropriate choice.

upvoted 1 times

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.  
 You use Microsoft Intune to manage devices.  
 You need to review the startup times and restart frequencies of the devices.  
 What should you use?

- A. Azure Monitor
- B. Intune Data Warehouse
- C. Microsoft Defender for Endpoint
- D. Endpoint analytics

**Suggested Answer:** D

Community vote distribution

D (100%)

🗨️ **krzysztofbr** Highly Voted 1 year, 4 months ago

D seems correct  
 upvoted 9 times

🗨️ **Futfuyfj** 1 year, 4 months ago

<https://learn.microsoft.com/en-us/mem/analytics/startup-performance>  
 upvoted 9 times

🗨️ **veliyath** Most Recent 6 months ago

Selected Answer: D

To review the startup times and restart frequencies of the devices managed by Microsoft Intune, you should use:

D. Endpoint analytics

Endpoint analytics provides insights into the health and performance of your devices, including startup performance and restart frequencies.  
 upvoted 3 times

🗨️ **Titi150** 8 months, 2 weeks ago

Answer D  
 upvoted 1 times

🗨️ **Haider\_Raza** 10 months ago

Selected Answer: D

Endpoint analytics aims to improve user productivity and reduce IT support costs by providing insights into the performance of the hardware and software in your organization. Specifically, it can help you review startup times and restart frequencies of devices managed through Microsoft Intune. Endpoint analytics is part of Microsoft Intune and provides valuable metrics and insights about the devices you manage, including proactive remediation scripts, startup performance, and recommended software to help improve user experience and device performance.  
 upvoted 4 times

🗨️ **MR\_Eliot** 10 months, 2 weeks ago

Selected Answer: D

Answer is correct  
 upvoted 2 times

🗨️ **Darkfire** 10 months, 3 weeks ago

Selected Answer: D

D is correct

Endpoint Analytics > <https://learn.microsoft.com/en-us/mem/analytics/>

Startup Performance > <https://learn.microsoft.com/en-us/mem/analytics/startup-performance>

upvoted 1 times

🗨️ **Tonsku** 1 year ago

Selected Answer: D

review the startup times and restart frequencies of the devices.

D. Endpoint analytics

upvoted 2 times

🗨️ **mohdAj** 1 year, 1 month ago

Selected Answer: D

D. Endpoint analytics

upvoted 1 times

🗨️ **iTomi** 1 year, 1 month ago

Selected Answer: D

Endpoint analytics is a feature within Microsoft Endpoint Manager that provides insights into device performance and user experience. It can help you analyze startup times, shutdown times, and restart frequencies of devices. This tool allows you to identify issues affecting device performance and take actions to improve the user experience.

upvoted 3 times

🗨️ **kay000001** 1 year, 1 month ago

Selected Answer: D

D is correct.

upvoted 2 times

🗨️ **zeos\_ucok** 1 year, 1 month ago

D is correct

<https://learn.microsoft.com/en-us/mem/analytics/restart-frequency?source=recommendations>

upvoted 2 times

🗨️ **Gentlemanners** 1 year, 1 month ago

Selected Answer: D

D is the correct answer, you can view the start-up performance in Endpoint Analytics.

<https://learn.microsoft.com/en-us/mem/analytics/startup-performance>

upvoted 2 times

🗨️ **pinda** 1 year, 3 months ago

Selected Answer: D

Correct

upvoted 3 times



HOTSPOT -

You have a Microsoft 365 E5 subscription.

You create a new update rings policy named Policy1 as shown in the following exhibit.

### Update ring settings [Edit](#)

#### Update settings

Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Servicing channel	General Availability channel
<b>User experience settings</b>	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	0
Grace period	0
Auto reboot before deadline	No

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.

### Answer Area

Updates that contain fixes and improvements to existing Windows functionality **[answer choice]**

▼

can be deferred indefinitely

can be deferred for 30 days

will be installed immediately

Updates that contain new Windows functionality will be installed within **[answer choice]** of release

▼

1 day

30 days

60 days

## Answer Area

Updates that contain fixes and improvements to existing Windows functionality [answer choice]

can be deferred indefinitely  
can be deferred for 30 days  
will be installed immediately

Suggested Answer:

Updates that contain new Windows functionality will be installed within [answer choice] of release

1 day  
30 days  
60 days


 **Contactfornitish** Highly Voted 1 year, 2 months ago

It should be immediately and 60 days.

Feature updates are deferred for 30 days so no way those can be installed \*within 30 days\*, even if you take other logic, at best it would have been installed post 30 days but same time below link clearly says, date of publish + any deferral means 30 days plus, only then policy starts countdown.


<https://learn.microsoft.com/en-us/windows/deployment/update/update-policies>

upvoted 19 times

 **HvD** 4 months ago

I guess that the Feature Updates will only be available on the machine 30 days after releasing by MS. After those 30 days, the user can defer them for 30 days. So, strictly, the user itself can only defer them for 30 days. The first 30 days the user doesn't even see the feature update.

upvoted 1 times

 **PranilR** 10 months, 3 weeks ago

quality updates, deadline 0 days, 0 deferral day = immediately

deadline 30 days plus 30 deferral days = 60days

upvoted 9 times

 **veliyath** Most Recent 6 months ago

Updates that contain fixes and improvements to existing Windows functionality:

Given that the "Quality update deferral period (days)" is set to 0, quality updates, which contain fixes and improvements to existing functionality, will be installed immediately.

Answer: will be installed immediately

Updates that contain new Windows functionality:

Given that the "Feature update deferral period (days)" is set to 30, feature updates, which contain new Windows functionality, can be deferred for 30 days.

Answer: can be deferred for 30 days

So, the selected options are:

Updates that contain fixes and improvements to existing Windows functionality will be installed immediately.

Updates that contain new Windows functionality can be deferred for 30 days.

upvoted 4 times

 **slimmerik7** 9 months, 2 weeks ago

30 and 60 are both correct for the second question depending on how you read it.

- up to 30 days when the updates are released to the computer (for the deadline)

- up to 60 days when the updates are released by Microsoft to the public. (30 days waiting until they are available to the pc and then again 30 days for the deadline)

'will be installed within xx days of release' --> Release to that specific computer or release from windows to the public??

upvoted 1 times

🗨️ **Burkidur** 10 months, 1 week ago

"The older policies started enforcing deadlines once the device reached a restart pending state for an update. The new policy starts the countdown for the update installation deadline from when the update is published plus any deferral."

<https://learn.microsoft.com/en-us/windows/deployment/update/update-policies>

"The deadline calculation for both quality and feature updates is based off the time the client's update scan initially discovered the update. Previously, the deadline was based off the release date of the update for quality updates and the reboot pending date for feature updates. The change for deadline calculation was made to improve the predictability of restart."

<https://learn.microsoft.com/en-us/windows/deployment/update/wufb-compliancedeadlines>

upvoted 2 times

🗨️ **MR\_Eliot** 10 months, 2 weeks ago

Answer is correct.

upvoted 2 times

🗨️ **MR\_Eliot** 9 months, 3 weeks ago

Not correct. After further evaluation, the answer should be 60 days.

Update is deferred for 30 days, you also have a deadline of 30 days.

So, the update will install within 60 days. (this is for the second box)

upvoted 1 times

🗨️ **Judith1969** 10 months, 2 weeks ago

It's not 30 + 30

It's 30.

- Feature Updates deferral Period (Days) = if set to 30, updates won't arrive on system before 30 days have past.

- Deadline for feature updates = The deadline behavior is nothing more than when you deploy updates to the machine, it will wait for the number of days specified. For example, if you set the deadline to 30 days, the device will wait for 30 days based on the Automatic update behavior and then restart the device after two days at maintenance time.

upvoted 2 times

🗨️ **Darkfire** 10 months, 3 weeks ago

Answer is correct

<https://learn.microsoft.com/en-us/mem/intune/protect/windows-update-settings>

upvoted 4 times

🗨️ **Merrybob** 11 months, 1 week ago

Got this from ChatGPT 4:

In the provided update rings policy (Policy1), the Feature Update deferral period is set to 30 days, which means that feature updates can be deferred for up to 30 days.

The Deadline for feature updates is also set to 30 days. This means that once the feature update is available, it can be deferred for a maximum of 30 days, but it must be installed within that 30-day period.

The combination of these settings ensures that feature updates will be installed within 30 days of their release. There is no additional 30-day grace period for feature updates in this scenario. Therefore, the correct answer is 30 days of release

upvoted 2 times

🗨️ **Tonsku** 1 year ago

immediately and 60 days

quality update deferral periode 0 day

feature update deferral periode 30 days + deadline for feature update 30 days

upvoted 4 times

🗨️ **Tonsku** 1 year ago

i am wrong, it should be immediately and 30 days deferral periode

upvoted 4 times

🗨️ **iTomi** 1 year, 1 month ago

IMMEDIATELY and 60 DAYS.

The new policy starts the countdown for the update installation deadline from when the update is published plus any deferral.

<https://learn.microsoft.com/en-us/windows/deployment/update/update-policies>

upvoted 2 times

🗨️ 👤 **b0gdan433** 1 year, 1 month ago

It's 30 days, i just took the exam today and got the 2 points.

upvoted 2 times

🗨️ 👤 **iTomi** 1 year, 1 month ago

B...S..., MS / Pearson doesn't reveal how many points you get each question.

upvoted 10 times

🗨️ 👤 **Murad01** 11 months, 1 week ago

MS Pearson exam does not release the answer at all. U will only able to see your total score.

upvoted 2 times

🗨️ 👤 **Kiookr** 1 year, 1 month ago

For the second option "functionality update" meaning (Quality Update for windows ) which I THINK need to be installed "immediately" or if there is no option then (1 day) will do .. I think

upvoted 1 times

🗨️ 👤 **Rocky83** 1 year, 3 months ago

Correct

Feature updates are released as soon as they become available. Feature updates aren't available for LTSC devices. Quality updates: Quality updates are traditional operating system updates, typically released on the second Tuesday of each month (though they can be released at any time)

upvoted 3 times

🗨️ 👤 **NoursBear** 1 year, 3 months ago

The answer is correct. The Quality updates will be published 30 days after market release, Feature Updates can have a value of upto 365 days. For both "This period is in addition to any deferral period that is part of the service channel you select. " In this case it is presumed it is the normal plebs channel.

Both answers are correct.

upvoted 2 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

I think I've changed my mind about this, the second answer is possibly 60 because the key word here is "how many days from release" so they will only start installing after 30 days from release and will take up to 60 days. Had to think a long time on that one

upvoted 3 times

🗨️ 👤 **letters1234** 1 year, 4 months ago

"The new policy starts the countdown for the update installation deadline from when the update is published plus any deferral."

<https://learn.microsoft.com/en-us/windows/deployment/update/update-policies>

The update is available to market, there is then a deferral of 30 days, which then makes it available for a device, once the device has found the update there will be a deadline for 30 days to install and reboot. 60 days total.

Otherwise, the 30 day deadline and 30 day deferral would line up and all devices would be required to install and reboot same day.

upvoted 4 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

answer is correct

upvoted 2 times

🗨️ 👤 **Sprocket10** 1 year, 4 months ago

Immediately and 30 days seems correct to me.

Can be deferred for up to 30 days but must be installed within 30 days

upvoted 3 times

You have computers that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from the Windows event logs.

The computers have the logged events shown in the following table.

Event ID	Log	Type	Computer
1	Application	Success	Computer1
2	System	Information	Computer1
3	Security	Audit Success	Computer2
4	System	Error	Computer2

Which events are collected in the Log Analytics workspace?

- A. 1 only
- B. 2 and 3 only
- C. 1 and 3 only
- D. 1, 2, and 4 only
- E. 1, 2, 3, and 4

**Suggested Answer:** D

Community vote distribution

E (50%) D (50%)

**letters1234** Highly Voted 1 year, 4 months ago

Selected Answer: D

Need to be careful of the wording as well. "Success" is not an event log type. Critical, Warning, Error, Information and Verbose are the event log types. There is Audit Success and Audit Failure in Security event logs (which cant be collected).

But in the scenario, there is no 2 & 4 option, so D.  
upvoted 15 times

**mhmyz** Highly Voted 1 year, 2 months ago

Selected Answer: E

I think answer is E.

Security events can be collected by Azure Monitor Agent and Data Collection rules.

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-rule-azure-monitor-agent?tabs=portal>

upvoted 14 times

**NoursBear** 1 year, 1 month ago

yes that's true but how do we know the Azure Monitor Agent is in use, it could be just the log analytics agent which is being deprecated 2024.  
upvoted 1 times

**NSA\_Poker** 9 months, 2 weeks ago

We know the Azure Monitor is in use by definition of the Log Analytics workspace.

<https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview#:~:text=A%20Log%20Analytics%20workspace%20is%20a%20unique%20environment%20for%20log%20data%20from%20Azure%20Monitor>

upvoted 1 times

**SajjH** 4 months, 4 weeks ago

Should be the key be the statement in the question, " The workspace is configured to collect all available events from the Windows event logs"  
upvoted 1 times

**SajjH** 4 months, 3 weeks ago

My bad, there is no Audit log in Windows Events, so D is correct.  
upvoted 1 times

**SajjH** 4 months, 3 weeks ago

I mean Azure agent doesn't collect that  
upvoted 1 times

🗨️ **TedEx2** Most Recent 3 weeks, 2 days ago

**Selected Answer: D**

The Log Analytics agent is deprecated, but the question requires that. And based on the documentation, it is clear that the Log Analytics agent does not support the collection of security events directly <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events#configure-windows-event-logs>. If the next update talk about Azure Monitor Agent, in this case it is possible.

upvoted 1 times

🗨️ **Alboo007\_rs007** 3 weeks, 4 days ago

**Selected Answer: D**

1. 2 .4 Only

upvoted 1 times

🗨️ **AleFCI1908** 1 month, 4 weeks ago

**Selected Answer: E**

E

can't log sec logs

upvoted 2 times

🗨️ **AleFCI1908** 1 month, 4 weeks ago

sorry, I mean D

upvoted 1 times

🗨️ **AleFCI1908** 2 months ago

**Selected Answer: D**

cannot see security log in log analytics

upvoted 1 times

🗨️ **Nav90** 2 months ago

**Selected Answer: E**

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-windows-events#configure-windows-event-data-source>

upvoted 1 times

🗨️ **Nav90** 2 months, 1 week ago

Answer is E, you can configure Data Collection Rule for Azure monitor to collect all events.

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-windows-events>

upvoted 1 times

🗨️ **TiagoFurtado** 2 months, 2 weeks ago

**Selected Answer: E**

check link <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-windows-events>

upvoted 2 times

🗨️ **Alboo007\_rs007** 2 months, 3 weeks ago

Needs to be updated its: E

upvoted 2 times

🗨️ **martinods** 3 months, 1 week ago

APP, SEC and SYS log can be configured

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-windows-events#configure-windows-event-data-source>

upvoted 1 times

🗨️ **RomanV** 3 months, 2 weeks ago

Shit is deprecated. It's now Azure Monitor Agent.

upvoted 1 times

🗨️ **RomanV** 3 months, 2 weeks ago

Answer is D!

Azure Monitor Agent (AMA) does not directly collect Audit Success and Audit Failure events from Windows Security event logs. Instead, it focuses on collecting broader event log types such as:

Critical

Warning

Error

Information

Verbose

To collect Audit Success and Audit Failure events, you would typically need to use other methods, such as:

Azure Sentinel: For advanced security event collection and analysis, where you can configure data connectors to collect specific security events including audit logs.

upvoted 2 times

🗨️ **LionelDerBoven** 3 months, 3 weeks ago

**Selected Answer: E**

E, Audit logs can be collected. All logs are selected.

upvoted 1 times

🗨️ **Daniel\_G** 3 months, 4 weeks ago

**Selected Answer: E**

The workspace is configured to collect "all" available events.

upvoted 1 times

🗨️ **JayHall** 4 months, 1 week ago

**Selected Answer: D**

1, 2, and 4 only

You can't configure collection of security events from the workspace by using the Log Analytics agent. You must use Microsoft Defender for Cloud or Microsoft Sentinel to collect security events. The Azure Monitor agent can also be used to collect security events.

Collect Windows event log data sources with Log Analytics agent in Azure Monitor - Azure Monitor | Microsoft Learn

upvoted 2 times

🗨️ **Pollosor** 5 months ago

Azure Log Analytics logs all of these types of events except audit events.

upvoted 1 times

🗨️ **veliyath** 6 months ago

**Selected Answer: E**

Since the Azure Log Analytics workspace is configured to collect all available events from the Windows event logs, it will collect events from the Application, System, and Security logs, including all types of events (Success, Information, Audit Success, Error).

Therefore, all the listed events will be collected in the Log Analytics workspace.

The correct answer is:

E. 1, 2, 3, and 4

upvoted 7 times

You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.

You need to configure the devices to run a single app in kiosk mode.

Which Configuration settings should you modify in the device restrictions profile?

- A. Users and Accounts
- B. General
- C. System security
- D. Device experience

**Suggested Answer:** D

Community vote distribution

D (100%)

 **letters1234** Highly Voted 1 year, 4 months ago

**Selected Answer:** D

Currently Intune has

Home > Android > Configuration Profiles > Device Restrictions > Device Experience":

"Enrollment type - Dedicated" and "Kiosk Mode - Single App"

upvoted 34 times

 **krzysztofbr** 1 year, 4 months ago

thanks for this comment i agree

upvoted 6 times

 **MR\_Eliot** Highly Voted 10 months, 2 weeks ago

**Selected Answer:** D

D is correct. I do MDM for a living

upvoted 8 times

 **iamchoy** Most Recent 2 weeks, 4 days ago

**Selected Answer:** D

The correct answer is D. Device experience. This setting allows for granular control over various aspects of the device's user experience, including the ability to restrict it to a single app, which is essential for kiosk mode.

upvoted 1 times

 **veliyath** 6 months ago

To configure Android Enterprise devices to run a single app in kiosk mode using Microsoft Intune, you should modify the device restrictions profile settings under:

D. Device experience

In the Device experience settings, you can configure kiosk mode and specify the app that will run in single-app mode. This setting is designed specifically to manage how the user interacts with the device, including limiting the device to a single app.

upvoted 1 times

 **veliyath** 6 months ago

**Selected Answer:** D

ChatGPT

To configure Android Enterprise devices to run a single app in kiosk mode using Microsoft Intune, you should modify the device restrictions profile settings under:

D. Device experience

In the Device experience settings, you can configure the kiosk mode and specify the app that will run in single-app mode.

upvoted 1 times



🗨️ 👤 **Darkfire** 10 months, 3 weeks ago

**Selected Answer: D**

D is correct

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work#device-experience>

upvoted 2 times

🗨️ 👤 **Amir1909** 12 months ago

Correct

upvoted 1 times

🗨️ 👤 **mohdAj** 1 year, 1 month ago

**Selected Answer: D**

D. Device experience

upvoted 2 times

🗨️ 👤 **NoursBear** 1 year, 3 months ago

I have thought long about this one. Basically initially you need to create an ios app for Defender itself and then deploy a policy for the settings, so you would need to do C and D

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-install-with-intune?view=o365-worldwide&viewFallbackFrom=o365-worldwide%20and%20deploying%20a%20policy>

Another company with sample questions (probably the same as here) on a video also had C but I guess the same answer will always be C wherever ...

upvoted 1 times

🗨️ 👤 **Futfuyfyfj** 1 year, 3 months ago

I guess you are replying to the wrong question? Because what you are writing makes no sense at all.

upvoted 8 times

🗨️ 👤 **NoursBear** 1 year, 3 months ago

D is correct. This is located under "Android Enterprise", maybe some other people missed that this is for Android like me. However I didn't know you would set mobile devices as Kiosk

upvoted 3 times

🗨️ 👤 **Fortind1974** 1 year, 4 months ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work#device-experience>

upvoted 1 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

**Selected Answer: D**

there is no correct answer LOL

under profile restriction, in INTUNE there is a tab called "KIOSK"

the closest answer is D but is still incorrect

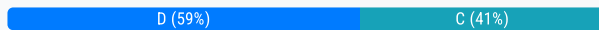
upvoted 2 times

You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune. You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort. What should you do?

- A. Onboard the macOS devices to the Microsoft Purview compliance portal.
- B. From the Microsoft Intune admin center, create a security baseline.
- C. Install Defender for Endpoint on the macOS devices.
- D. From the Microsoft Intune admin center, create a configuration profile.

**Suggested Answer: C**

Community vote distribution



**ronct** Highly Voted 1 year, 3 months ago

The wording of the question is

You need to ensure that you CAN apply Microsoft Defender for Endpoint antivirus policies to the macOS devices.

that suggests you need to make the devices ABLE to receive the policies, not push the policies themselves. Creating a configuration profile alone will not enable you to apply policies, Microsoft Defender for Endpoint needs to be installed and then you CAN apply policies.

upvoted 26 times

**BossAceVentura** Highly Voted 1 year, 4 months ago

C wont minimize admin effort

Answer is D

upvoted 12 times

**Burkidur** 10 months, 1 week ago

Macs don't have Defender pre-installed. You can create and push as many policies as you want -- there's nothing on the client to interpret and enforce them. That is -- until you install Defender (it doesn't say "manually", you can push it through Intune, so not much effort).

upvoted 2 times

**SajjH** 4 months, 3 weeks ago

You can install Defender for Endpoint by using configuration profile.

upvoted 2 times

**vfj** Most Recent 1 week, 1 day ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/defender-endpoint/mac-install-with-intune>

upvoted 1 times

**OHMSS** 2 weeks, 3 days ago

**Selected Answer: C**

You need to install Defender to apply Defender Policys on Mac. On Windows it's already installed.

upvoted 1 times

**Alboo007\_rs007** 3 weeks, 4 days ago

**Selected Answer: C**

Microsoft portals and tests says its C

upvoted 2 times

**Tr619899** 1 month, 2 weeks ago

To ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices enrolled in Microsoft Intune, you need to install Microsoft Defender for Endpoint on the macOS devices. This is a prerequisite for managing antivirus policies for macOS devices through Intune. After installation, the devices can be onboarded to Defender for Endpoint, which allows Intune to enforce antivirus configurations on these devices effectively.

While configuration profiles are used to set specific policies, the Defender for Endpoint client must first be installed to enable these policies to function. This minimizes administrative effort as the installation process and onboarding streamline policy application across devices.

Thus, the correct answer is: C. Install Defender for Endpoint on the macOS devices.

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-advanced-threat-protection-macos>

upvoted 2 times

🗨️ 👤 **AleFCI1908** 2 months ago

**Selected Answer: C**

without defender for endpoint, you can't apply the policy. the policies are there, ms asks to ensure that you can apply them. For me, first of all, you have to install endpoint defender

upvoted 2 times

🗨️ 👤 **elwa1** 3 months ago

For Intune to manage antivirus settings on a device, Microsoft Defender for Endpoint must be installed on that device. See. Microsoft Defender for Endpoint for macOS (In the Microsoft Defender for Endpoint documentation)

<https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-antivirus-policy>

upvoted 1 times

🗨️ 👤 **RomanV** 3 months, 2 weeks ago

Answer is D as Microsoft themselves state:

Create system configuration profiles

The next step is to create system configuration profiles that Microsoft Defender for Endpoint needs. In the Microsoft Intune admin center, open Devices > Configuration profiles.

Source: <https://learn.microsoft.com/en-us/defender-endpoint/mac-install-with-intune>

upvoted 1 times

🗨️ 👤 **Frank9020** 4 months ago

**Selected Answer: C**

A configuration profile in Intune can be used to manage settings and enforce compliance policies across devices. While it can help deploy software or set configurations, it's not typically used for directly installing applications like Microsoft Defender for Endpoint. Instead, configuration profiles are generally used for settings such as VPN configurations, Wi-Fi profiles, or security settings.

What Needs to Happen:

To apply antivirus policies from Microsoft Defender for Endpoint to macOS devices, the Defender software itself must first be installed on the devices. Simply creating a configuration profile in Intune without ensuring that the Defender application is installed won't allow you to enforce these antivirus policies.

upvoted 1 times

🗨️ 👤 **JayHall** 4 months, 1 week ago

**Selected Answer: D**

I vote D: From the Microsoft Intune admin center, create a configuration profile.

Ensure that Microsoft Defender for Endpoint is automatically deployed

Microsoft Defender for Endpoint will implement the security configuration settings it receives from Microsoft Intune. We must first verify that communications are taking place between Defender for Endpoint and Intune. From the Microsoft 365 Defender portal select Settings > Endpoints > Advanced features, and make sure that we switch the connection to Microsoft Intune to On. Next, create a device configuration profile that automatically onboards Intune assets to Defender for Endpoint and assign it to the designated clients.

Source: Hardening Windows Clients with Microsoft Intune and Defender for Endpoint

upvoted 1 times

🗨️ 👤 **veliyath** 6 months ago

**Selected Answer: C**

To ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices and minimize administrative effort, you should:

C. Install Defender for Endpoint on the macOS devices.

Installing Defender for Endpoint on the macOS devices is a prerequisite to applying antivirus policies through Microsoft Intune. Once Defender for Endpoint is installed, you can manage and enforce security policies using Intune.

upvoted 2 times

🗨️ 👤 **Maclouis116** 7 months ago

Answer is D this will minimize administrative effort, imagine installing Defender on 500 devices manually :(

upvoted 3 times

🗨️ 👤 **CJL324** 7 months, 2 weeks ago

D. From the Microsoft Intune admin center, create a configuration profile.

Creating a configuration profile in Intune allows you to configure settings and features on managed devices, including macOS devices. You can use configuration profiles to apply security settings, including antivirus policies provided by Microsoft Defender for Endpoint, ensuring that macOS devices are protected without the need for manual intervention on each device.

upvoted 1 times

🗨️ 👤 **ExamDumpEnjoyer** 8 months, 3 weeks ago

**Selected Answer: D**

You're right to question this. While installing Defender for Endpoint on the macOS devices (option C) is indeed necessary to enable antivirus protection, the question specifically asks for the action that ensures you can apply antivirus policies with minimal administrative effort.

Installing Defender for Endpoint is just the initial step. However, creating a configuration profile (option D) allows you to define and apply antivirus policies centrally to multiple devices at once, which aligns with the requirement to minimize administrative effort. Therefore, option D is the more appropriate choice for achieving the stated objective.

upvoted 5 times

🗨️ 👤 **rcristiano** 9 months ago

Para instalar o Defender em 500 dispositivos macOS você precisa criar um perfil de configuração portanto a resposta e D

upvoted 1 times

🗨️ 👤 **kerimnl** 9 months, 1 week ago

**Selected Answer: C**

Answer is C

upvoted 1 times

You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune. You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.
- B. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.
- C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.
- D. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.
- E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.
- F. To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

**Suggested Answer:** CE

Community vote distribution

DE (67%)

CE (16%)

Other

 **deinth** Highly Voted 1 year, 4 months ago

**Selected Answer: DE**

for firewall E:

<https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/create-windows-firewall-rules-in-intune>

for antivirs D:

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#microsoft-defender-antivirus>  
upvoted 35 times

 **SalonaSahni** 1 year, 4 months ago

DE is the Answer

D:Microsoft Defender Antivirus: Device config-Device Restrictions- It has 28-34 settings for Antivirus.

E: Microsoft Defender Firewall- Device config- Endpoint Protection (Global settings, network settings, Firewall rules)


I have cross checked the lab. The Endpoint Protection does not have the option for MS Defender Antivirus.

upvoted 10 times

 **Futfuyfjfi** 1 year, 3 months ago

Checked this in Intune and DE is the only correct answer!

upvoted 3 times

 **minasamy** Highly Voted 1 year, 4 months ago

**Selected Answer: BC**

B and C are the correct answers :

B. Creating a device configuration profile and configuring the Device restrictions settings allows you to manage the Microsoft Defender Firewall settings on your Azure AD joined Windows 10 devices through Microsoft Intune. This profile can help you configure and manage firewall rules and settings without the need for traditional Group Policy.

C. Creating a device configuration profile and configuring the Endpoint protection settings allows you to manage Microsoft Defender Antivirus settings on your Azure AD joined Windows 10 devices through Microsoft Intune. This profile enables you to configure antivirus settings, exclusions, scanning options, and more, all while minimizing administrative effort.

upvoted 7 times

 **Futfuyfjfi** 1 year, 3 months ago

I just checked in the Intune portal, but there is no Defender firewall component in Device restrictions. However in device restrictions IS a Defender AV option. I consider your answer as wrong. I am still going for DE  
upvoted 3 times

  **OHMSS** Most Recent 2 weeks, 3 days ago

**Selected Answer: CD**

Both in Endpoint security

<https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-policy>

upvoted 1 times

  **RJTW070** 3 weeks, 6 days ago

**Selected Answer: CE**

Explanation:

Since the devices are Azure AD joined and managed by Microsoft Intune, the configurations for both Microsoft Defender Firewall and Microsoft Defender Antivirus should be done through Intune's Endpoint protection settings, as they provide the necessary controls for these security features.

C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings:

Intune's Endpoint protection settings include configurations for Microsoft Defender Antivirus, such as enabling real-time protection, configuring scan schedules, and setting exclusions.

E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings:

Microsoft Defender Firewall settings, such as enabling the firewall, configuring rules, and network security, are also part of the Endpoint protection settings in Intune.

upvoted 2 times

  **Tr619899** 1 month, 2 weeks ago

CE is the Answer

upvoted 2 times

  **SSL2** 2 months, 2 weeks ago

**Selected Answer: CE**

The correct actions are:

C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.

E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.

These two options minimize administrative effort by using Microsoft Intune to centrally manage both Microsoft Defender Antivirus and Microsoft Defender Firewall. The Endpoint protection settings in a device configuration profile allow you to configure both firewall and antivirus settings for Intune-managed devices, streamlining the process and avoiding the need for Group Policy Objects (GPOs).

upvoted 1 times

  **subbuhotmail** 3 months, 3 weeks ago

**Selected Answer: DE**

Yes, FOR AV - Device Restriction and AV

For FW - Endpoint Protection - FW

upvoted 2 times

  **clucks** 5 months, 1 week ago

**Selected Answer: DE**

Just open up intune and you can see for yourself.


Endpoint Protection contains the Firewall configuration. Device restrictions contains MS Antivirus configuration.

upvoted 3 times

  **Pollosor** 5 months ago

That's correct, I had forgotten.

upvoted 2 times

  **veliyath** 5 months, 2 weeks ago

**Selected Answer: DE**

D. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.



Configure Microsoft Defender Antivirus using Device restrictions in Intune

E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.

Configure Microsoft Defender Firewall rules using Endpoint protection in Intune

These selections ensure that the configurations for both Microsoft Defender Antivirus and Microsoft Defender Firewall are managed through Intune, aligning with the goal of minimizing administrative effort.



upvoted 3 times

  **oopspruu** 5 months, 2 weeks ago

**Selected Answer: DE**

D&E are correct options. Tested in lab 2024/07

upvoted 3 times

  **kiik32** 5 months, 3 weeks ago

**Selected Answer: CE**

C and E you can configure both from the endpoint protection template

upvoted 1 times

  **kiik32** 5 months, 3 weeks ago

actually from endpoint protection you enable the antivirus rather than configuring, so for that you will need a device restrictions template.

upvoted 1 times

  **nicholaswildern** 6 months, 1 week ago

Perplexity AI

To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on your Azure AD-joined Windows 10 devices managed by Microsoft Intune, and to minimize administrative effort, you should perform the following actions:

To configure Microsoft Defender Antivirus: Create a device configuration profile and configure the Endpoint protection settings. This allows you to manage antivirus policies directly through Intune, which is streamlined for managing multiple devices in an enterprise environment.



To configure Microsoft Defender Firewall: Create a device configuration profile and configure the Endpoint protection settings. This approach also leverages Intune's capabilities to manage firewall settings across all devices efficiently.

Therefore, the correct answers are:

C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.

E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.

upvoted 1 times

  **keshav80** 7 months, 3 weeks ago

DE is 100% right. I have verified. Be relaxed.

upvoted 1 times

  **Bhuru** 8 months, 1 week ago

**Selected Answer: BC**

BC is the answer Microsoft defender firewall is managed in device restrictions and AV in endpoint protection...the way you guys get lost is disturbing

upvoted 1 times

  **Dave808** 9 months, 2 weeks ago

**Selected Answer: BC**

To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on your Azure AD-joined Windows 10 devices while minimizing administrative effort, you should perform the following actions:

B. To configure Microsoft Defender Firewall:

Create a device configuration profile in Microsoft Intune.

Configure the Device restrictions settings within the profile.

Specify the desired firewall rules and settings for your devices.

C. To configure Microsoft Defender Antivirus:

Create another device configuration profile in Microsoft Intune.

Configure the Endpoint protection settings within the profile.

This allows you to manage antivirus settings, exclusions, and other related configurations.



By following these steps, you can effectively set up both Microsoft Defender Firewall and Microsoft Defender Antivirus without the need for additional Group Policy Objects (GPOs) or manual administrative tasks.

upvoted 1 times

  **Ssssng** 10 months ago

Answer is DE

upvoted 1 times

  **MR\_Eliot** 10 months, 2 weeks ago

**Selected Answer: CE**

Answers are C & E. You can manage both with endpoint security configuration profile. I have confirmed this in my own tenant. Device Restriction is more about what length of password users should have etc.

upvoted 2 times

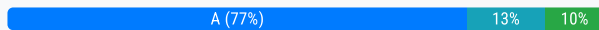


You have an Azure AD group named Group1. Group1 contains two Windows 10 Enterprise devices named Device1 and Device2. You create a device configuration profile named Profile1. You assign Profile1 to Group1. You need to ensure that Profile1 applies to Device1 only. What should you modify in Profile1?

- A. Assignments
- B. Settings
- C. Scope (Tags)
- D. Applicability Rules

**Suggested Answer: C**

Community vote distribution



**krzysztofbr** Highly Voted 1 year, 4 months ago

**Selected Answer: A**

there is no option, You have to modify assignments  
upvoted 18 times

**minasamy** Highly Voted 1 year, 4 months ago

**Selected Answer: A**

I will go for A  
upvoted 10 times

**iamchoy** Most Recent 2 weeks, 4 days ago

**Selected Answer: D**

The correct answer is D. Applicability Rules.

Here's why:

Applicability Rules allow you to define specific conditions under which a configuration profile should apply to devices. In this scenario, you can create an applicability rule that targets Device1 specifically, ensuring that Profile1 only applies to this device. Here's how you can create an applicability rule:

Go to the Applicability Rules tab in your configuration profile.

Click Add.

Choose the appropriate condition, such as Device Name.

Set the condition to match the name of Device1.

Save the rule.

With this rule in place, Profile1 will only be applied to Device1, even though it's assigned to a group that contains both devices.

upvoted 1 times

**SoLZeRa** 1 month, 1 week ago

**Selected Answer: A**

The answer is A.  
upvoted 1 times

**LionelDerBoven** 3 months, 3 weeks ago

**Selected Answer: A**

Scopes is for administrative restriction for configuration NOT for assignment to a device of user (group).  
upvoted 1 times

**subbuhotmail** 4 months ago

**Selected Answer: A**

If you want to filter and assign to specific device/user in the group then need to use filter which is under assignments.  
upvoted 3 times

🗨️ **dnt91** 4 months ago

**Selected Answer: A**

in Assignments we can use filter to exclude some members from groups  
upvoted 2 times

🗨️ **Frank9020** 4 months, 1 week ago

**Selected Answer: D**

The correct answer is D: The question clearly states that the profile1 is only assigned to a group1, that contains 2 windows devices. To ensure that a device configuration profile applies to only one specific device within a group, such as applying Profile1 to Device1 only, you should use "Applicability Rules" - A: Assignments determine which groups receive the configuration profile. If Profile1 is assigned to Group1, both Device1 and Device2 will receive the profile. You cannot use assignments alone to target a single device within a group.  
upvoted 2 times

🗨️ **BurtSmart** 4 months, 1 week ago

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/scope-tags>

Assignments

upvoted 1 times

🗨️ **oopspruu** 4 months, 3 weeks ago

**Selected Answer: A**

The "Filter" option in Assignment section can be used to accomplish what the question is asking.  
upvoted 1 times

🗨️ **kiik32** 5 months, 3 weeks ago

applicability rules would not make it.

upvoted 1 times

🗨️ **7798da3** 5 months, 3 weeks ago

Applicability rules

Applies to:

Windows 11

Windows 10

Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10/11 devices group. And, you only want the profile assigned to devices running Windows Enterprise.  
upvoted 1 times

🗨️ **veliyath** 5 months, 4 weeks ago

**Selected Answer: A**

To ensure that Profile1 applies only to Device1 within Group1, you need to modify the assignments to target only Device1. This can be done by creating a separate Azure AD group that contains only Device1 and then assigning Profile1 to that new group.

Therefore, the correct answer is:

A. Assignments

upvoted 1 times

🗨️ **CJL324** 7 months, 2 weeks ago

A. Assignments

By modifying the assignments, you can target specific devices or groups. In this case, you can remove the assignment of Profile1 from Group1 and directly assign it to Device1. This way, Profile1 will only apply to Device1 and not Device2.  
upvoted 2 times

🗨️ **24438aa** 9 months ago

A is correct answer

Sign in to the Microsoft Intune admin center.

Navigate to Devices > Configuration profiles.

Select Profile1 and go to Properties > Assignments > Edit.



upvoted 1 times

🗨️ **slimmerik7** 9 months, 2 weeks ago

**Selected Answer: A**

In the assignments you can choose "filter" and filter devices out of it.

Be aware: exclusions is not an option since you can only exclude groups and we can't assume there is a group made for the device itself.  
upvoted 3 times

  **suman95** 9 months, 4 weeks ago

Applicability Rules:

Intune allows you to define applicability rules within a configuration profile. These rules act as filters to determine which devices in an assigned group actually receive the profile.

upvoted 2 times

DRAG DROP -

You have a Microsoft 365 subscription that includes Microsoft Intune.

You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:

Enforces compliance for Defender for Endpoint by using Conditional Access

Prevents suspicious scripts from running on devices

What should you configure? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

### Features

### Answer Area

A device restriction policy

A security baseline

An attack surface reduction (ASR) rule

An Intune connection

Enforces compliance:

Prevents suspicious scripts:

**Answer Area**

**Suggested Answer:**

Enforces compliance:

Prevents suspicious scripts:

 **JP1900** Highly Voted 1 year, 4 months ago

Without an Intune connection, how can the policies apply? The original answer is correct.


upvoted 9 times

 **SaiK1234** Most Recent 10 months, 1 week ago

The original answer is correct. Establish a connection and then you can enforce.

second is ASR

upvoted 1 times

 **MR\_Eliot** 10 months, 2 weeks ago

Enforces compliance for Defender for Endpoint by using Conditional Access

- A Device Restriction policy. After which you can configure compliance policu, and conditional access policy to disallow non-compliant devices.

Prevents suspicious scripts from running on devices

- An attack surface reduction.

Trust me on this. I do this a lot!

upvoted 4 times

 **Rylz** 4 months, 2 weeks ago

I've searched for the "Device Restriction policy" in intune and i did not find anything related to that name so i think that this answare is incorrect

upvoted 1 times

 **7798da3** 5 months, 3 weeks ago

I believe your logic but the Microsoft practice tests do the same thing connection before policy these exams are so convoluted. LOL

upvoted 1 times

 **MR\_Eliot** 10 months, 2 weeks ago

Btw, intune connection is required for Microsoft Defender integration and Intune. So that answer is totally not correct!

upvoted 2 times

 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

Configure Microsoft Defender for Endpoint in Intune

Sign-in to the Microsoft 365 Defender portal – <https://security.microsoft.com/>

Select Settings > Endpoints > Advanced features > enable Microsoft Intune connection.

<https://support.blackpointcyber.com/article/125-microsoft-intune-defender-for-endpoint-setup-guide>

upvoted 3 times

🗨️ 👤 **OyYaGotta** 10 months ago

This comment explains the vague "an Intune Connection" answer. It's within the 365 Defender Portal. Unusual that the answers are this vague so best to take the literally.

upvoted 1 times

🗨️ 👤 **iTomi** 1 year, 1 month ago

This is strange and tricky question, but I would choose "an intune connection" and ASR.

If you go to Intune -> Endpoint security -> Microsoft Defender for Endpoint -> Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations

You need to create connection between Intune and Defender before you can use it.

upvoted 1 times

🗨️ 👤 **iTomi** 1 year ago

<https://learn.microsoft.com/fi-fi/mem/intune/protect/advanced-threat-protection-configure>

Use the information and procedures in this article to configure integration of Microsoft Defender for Endpoint with Intune. CONFIGURATION INCLUDES THE FOLLOWING GENERAL STEPS:

- Establish a service-to-service connection between Intune and Microsoft Defender for Endpoint.
- Use Intune policy 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 Intune device compliance policies to set the level of risk you want to allow. Microsoft Defender for Endpoint reports a devices risk level.
- Use a conditional access policy to block users from accessing corporate resources from devices that are noncompliant.
- Use app protection policies for Android and iOS/iPadOS, to set device risk levels.

upvoted 1 times

🗨️ 👤 **VirtualJP** 1 year, 3 months ago

I believe this answer to be correct

upvoted 3 times

🗨️ 👤 **mail2bala3011** 1 year, 4 months ago

Seems like the answer is correct:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-conditional-access?view=o365-worldwide>

upvoted 3 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

You are wrong Intune connection doesn't enforce anything

upvoted 1 times

🗨️ 👤 **iTomi** 1 year ago

Question is "what should you configure?"

Based on this you start configuration creating connections between defender and intune.

<https://learn.microsoft.com/fi-fi/mem/intune/protect/advanced-threat-protection-configure>

upvoted 1 times

🗨️ 👤 **Futfuyfj** 1 year, 3 months ago

No you are wrong compliance policy checks are device checkin dependent. Although this answer is not very well specified, its still the best one:

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot>

upvoted 1 times

  **krzysztofbr** 1 year, 4 months ago

the second part about ASR seems correct but enforces compliance "intune connection"

it should be security baseline i guess. this is set off settings relevant for compliance requirements

upvoted 3 times

  **Futfuyfj** 1 year, 4 months ago

I agree the answer is vague, but Intune enforces online compliance checks. Therefore an active intune connection is required. So Intune connection here is the best of the worst I guess.

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot>

upvoted 4 times

Your network contains an on-premises Active Directory domain and an Azure AD tenant.  
The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

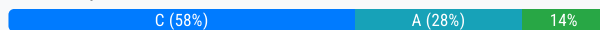
Name	GPO value
LockoutBadCount	0
MaximumPasswordAge	42
MinimumPasswordAge	1
MinimumPasswordLength	7
PasswordComplexity	True
PasswordHistorySize	24

You need to migrate the existing Default Domain Policy GPO settings to a device configuration profile.  
Which device configuration profile type template should you use?

- A. Administrative Templates
- B. Endpoint protection
- C. Device restrictions
- D. Custom

**Suggested Answer:** C

Community vote distribution



**volto** Highly Voted 1 year, 4 months ago

Selected Answer: C

Answer C is correct

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#password>

upvoted 23 times

**RomanV** 3 months, 2 weeks ago

You are so wrong. Read between the lines please or don't respond here... Answer is A!

The question states: "You need to MIGRATE the existing Default Domain Policy GPO settings to a device configuration profile."

So according to Microsoft and myself, as an Intune administrator, after you Import and analyze your on-premises GPOs using Group Policy analytics in Microsoft Intune, you CREATE the template. Which profile type? Administrative Templates!

upvoted 3 times

**krzysztofbr** 1 year, 4 months ago

You are correct! so many wrong answers again! inside device restrictions, You have password settings. your link shows everything regarding password

upvoted 5 times

**LionelDerBoven** 3 months, 3 weeks ago

The correct answer is A. Administrative Templates.

Explanation:

To migrate the existing Default Domain Policy GPO settings (like password policies, lockout settings, etc.) to Intune as a device configuration profile, Administrative Templates is the correct template type to use.


Administrative Templates in Intune mirror many Group Policy Object (GPO) settings, making it the right choice for applying these specific configurations (like password length, complexity, and history).

The settings shown in the image (such as MaximumPasswordAge, PasswordComplexity, etc.) are commonly found in Group Policies, which can be replicated in Intune via Administrative Templates.

Other options such as Device Restrictions, Endpoint Protection, or Custom profiles do not cover the breadth of traditional GPO settings like password policies as well as Administrative Templates do.


Thus, Administrative Templates is the correct profile type for this scenario.

upvoted 2 times

 **vijay0715** 11 months, 1 week ago

Password setting usually reflect on accounts know?

upvoted 1 times

 **iTomi** Highly Voted 1 year ago

Selected Answer: A

In this question you are MIGRATING the EXISTING GPO settings from AD to Intune, not creating new one.

Steps are:

Import and analyze your on-premises GPOs using Group Policy analytics in Microsoft Intune

<https://learn.microsoft.com/en-us/mem/intune/configuration/group-policy-analytics>


Create a Settings Catalog policy using your imported GPOs in Microsoft Intune (public preview)

<https://learn.microsoft.com/en-us/mem/intune/configuration/group-policy-analytics-migrate>

Use Windows 10/11 templates to configure group policy settings in Microsoft Intune

<https://learn.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows>


upvoted 9 times

 **Grimmgore** Most Recent 4 days, 12 hours ago

Selected Answer: A

<https://learn.microsoft.com/en-us/mem/intune/configuration/administrative-templates-import-custom#create-a-profile-using-your-imported-files>

upvoted 1 times

 **vfnj** 1 week, 1 day ago

Selected Answer: A

<https://learn.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows?tabs=template>

upvoted 1 times

 **Moot2** 1 month ago

Selected Answer: A

A use admin templates

upvoted 1 times

 **yaktownboii** 1 month, 1 week ago

Selected Answer: A

Answer A is correct. <https://learn.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows?tabs=template>

upvoted 1 times

 **AleFCI1908** 2 months ago

Selected Answer: A

it's a migration, vote for A

upvoted 2 times

 **d3a3d8a** 2 months ago

Password policy settings are not in the Administrative Templates part of Group Policies. they are in the Computer>Windows Settings. only

Administrative Templates (which are represented as xml text files) can be "migrated" from GPOs. The correct answer is C. The word "migrate" in the question is there to fool you.

upvoted 1 times

 **59c6be3** 1 month ago

Exactly. Therefor the answer remains C.

upvoted 1 times

 **AleFCI1908** 2 months ago

Selected Answer: A

migrate, so A

upvoted 1 times

 **Nav90** 2 months, 1 week ago

Selected Answer: A

We are migrating GPO here not creating new policy to have same settings.

upvoted 1 times

 **SSL2** 2 months, 2 weeks ago



**Selected Answer: A**

The correct answer is **A. Administrative Templates**.

Here's why:

\* **Administrative Templates** device configuration profile type template is used to configure settings related to user and computer policies, similar to Group Policy Objects (GPOs).

\* The settings in the Default Domain Policy GPO are related to user and computer policies (password complexity, lockout policy, etc.), which aligns with the Administrative Templates template.

\* **Endpoint protection** is used for configuring antivirus and firewall settings.

\* **Device restrictions** is used for configuring device-level restrictions, such as blocking specific apps or websites.

\* **Custom** is used for creating custom profiles with specific settings not covered by other templates.

Therefore, the Administrative Templates template is the most appropriate choice for migrating the Default Domain Policy GPO settings to a device configuration profile.

upvoted 1 times

 **King\_shola** 3 months, 3 weeks ago

**Selected Answer: C**

C - Over complicating it using A

upvoted 1 times

 **King\_shola** 3 months, 3 weeks ago

C - Over complicating it using A

upvoted 1 times

 **LionelDerBoven** 3 months, 3 weeks ago

**Selected Answer: A**

The correct answer is A. Administrative Templates.

Explanation:

To migrate the existing Default Domain Policy GPO settings (like password policies, lockout settings, etc.) to Intune as a device configuration profile, Administrative Templates is the correct template type to use.

Administrative Templates in Intune mirror many Group Policy Object (GPO) settings, making it the right choice for applying these specific configurations (like password length, complexity, and history).

The settings shown in the image (such as MaximumPasswordAge, PasswordComplexity, etc.) are commonly found in Group Policies, which can be replicated in Intune via Administrative Templates.

Other options such as Device Restrictions, Endpoint Protection, or Custom profiles do not cover the breadth of traditional GPO settings like password policies as well as Administrative Templates do.

Thus, Administrative Templates is the correct profile type for this scenario.


upvoted 1 times

 **Frank9020** 4 months, 1 week ago

**Selected Answer: A**

By using the Administrative Templates profile type, you can more effectively replicate and manage the settings from the Default Domain Policy GPO in Intune.

upvoted 2 times

 **Vlado123** 4 months, 2 weeks ago

A

<https://learn.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows?tabs=template#create-the-template>

upvoted 2 times

 **Maclouis116** 6 months, 1 week ago

**Selected Answer: A**

You migrate your AD GPO's to administrative templates using the ADMX file

upvoted 2 times

You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace.

Which three types of data can you collect from the computers by using Log Analytics? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. failure events from the Security log
- B. the list of processes and their execution times
- C. the average processor utilization
- D. error events from the System log
- E. third-party application logs stored as text files

**Suggested Answer:** CDE

Community vote distribution



**HvD** Highly Voted 1 year, 2 months ago

Answer id BCD:

- A: No security-event loggings in LogAnalytics Agent (MMA)

- B: the list of processes and their execution times: Yes, try it if you want in LogAnalytics: Perf

| where ObjectName == "Process" and CounterName == "% Processor Time"

You will see all processes of all the computers and their run time.

- C: the average processor utilization: Yes, run: InsightsMetrics

| where Origin == "vm.azm.ms"

| where Namespace == "Processor" and Name == "UtilizationPercentage"

D: Yes, Systemlogs are collected.

E: Log files apart from Application and System logs are NOT collected. For sure not if they are text-based log files. Only Eventlogs. No textfiles.

upvoted 26 times

**Rubends** 1 year, 2 months ago

I think it's correct, E: you must configure it.

upvoted 1 times

**MR\_Eliot** 10 months, 2 weeks ago

Totally agree with you. BCD is the answer.

upvoted 4 times

**TedEx2** Most Recent 3 weeks, 2 days ago

**Selected Answer: CDE**

The Log Analytics agent itself does not natively collect detailed process information, such as a list of processes and their execution times, without additional configuration. B is wrong.

upvoted 1 times

**c4e009c** 1 month, 1 week ago

**Selected Answer: CDE**

C: <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-performance-counters#log-queries-with-performance-records>

D: <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-syslog>

E: <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-custom-logs>

upvoted 1 times

**KBMS** 4 months ago

Security Log Events: Log Analytics can collect various types of events from the Security log, which includes failure events. This is useful for monitoring security-related incidents on your devices.

Processor Utilization: Performance data, such as average processor utilization, can be collected to monitor the performance and health of your

devices.

System Log Events: Error events from the System log can be collected to help diagnose and troubleshoot issues on your devices.

Options B and E are not correct because Log Analytics does not natively collect detailed process execution times or third-party application logs stored as text files without additional configuration or custom log collection setups.

correct answers are: A, C, D

upvoted 2 times

 **CJL324** 7 months, 2 weeks ago

B. the list of processes and their execution times

C. the average processor utilization

E. third-party application logs stored as text files

upvoted 1 times

 **sace** 8 months, 3 weeks ago

**Selected Answer: BCD**

The three types of data that you can collect from the computers using Azure Log Analytics are:

B. the list of processes and their execution times: Log Analytics can collect process-related information, including details about running processes and their resource consumption.

C. the average processor utilization: Log Analytics can capture performance-related data, such as CPU utilization metrics, which can include averages over time.

D. error events from the System log: Log Analytics can gather events from Windows Event Logs, including error events from the System log, providing insights into system-level issues and errors.

Therefore, the correct selections are:

B. the list of processes and their execution times

C. the average processor utilization

D. error events from the System log

upvoted 3 times

 **Burkidur** 10 months, 1 week ago

It's probably outdated and you won't see those exact answers on the exam. MMA is being replaced with AMA and it does collect custom text logs ([https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-text-log?WT.mc\\_id=AZ-MVP-5000120&tabs=portal](https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-text-log?WT.mc_id=AZ-MVP-5000120&tabs=portal)).


upvoted 3 times

 **MR\_Eliot** 10 months, 2 weeks ago

**Selected Answer: BCD**

See comment from HvD.

upvoted 2 times

 **Merrybob** 11 months, 1 week ago

**Selected Answer: BCD**

BCD

List of processes and their execution times

Average processor utilization (these are performance metrics and easily captured by Log Analytics)

Error events from System log

upvoted 1 times

 **Merrybob** 11 months, 1 week ago

BCD - I've set this up in a Log Analytics Workspace and tried it myself.

upvoted 1 times

 **ubiquituz** 11 months, 4 weeks ago

CDE

Windows Event logs Information sent to the Windows event logging system

Syslog Information sent to the Linux event logging system

Performance Numerical values measuring performance of different aspects of operating system and workloads

IIS logs Usage information for IIS websites running on the guest operating system

Custom logs Events from text files on both Windows and Linux computers

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent>

upvoted 1 times

🗨️ 👤 **yosry** 1 year ago

Selected Answer: BCD

seems correct

upvoted 1 times

🗨️ 👤 **belyo** 1 year ago

Selected Answer: BCD

not sure that 3rd party logs can be collected by default, you need SIEM integration / Sentinel

Log Analytics documentation dont say much about 3rd party log collection

i would go with BCD

upvoted 1 times

🗨️ 👤 **NoursBear** 11 months, 2 weeks ago

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-custom-logs>

upvoted 1 times

🗨️ 👤 **cpaljchc4** 1 year, 1 month ago

1. Performance Data: This includes information like the average processor utilization, memory usage, disk performance, and network metrics.
2. Event Log: These logs contain information about system, security, and application events. This includes error events from the System log, failure events from the Security log, and other event logs captured by the operating system.
3. Custom Logs: You can also collect logs from third-party applications or services. These could be stored as text files or in a specific format, enabling monitoring and analysis within the Log Analytics workspace.

I think I will go with CDE.

upvoted 1 times

🗨️ 👤 **BlackCat9588** 1 year, 2 months ago

Why B is not?

upvoted 1 times

🗨️ 👤 **VirtualJP** 1 year, 2 months ago

Selected Answer: BDE

Personally I think I'd have to go with BDE

upvoted 1 times

🗨️ 👤 **VirtualJP** 1 year, 2 months ago

Correction, I go with BCD

upvoted 4 times

🗨️ 👤 **yingo20** 1 year, 3 months ago

CDE it's a correct answers

upvoted 1 times

You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

- A. an attack surface reduction (ASR) policy
- B. a security baseline
- C. an endpoint detection and response (EDR) policy
- D. an account protection policy
- E. an antivirus policy

**Suggested Answer:** C

Community vote distribution

C (85%)

E (15%)

 **krzysztofbr** Highly Voted 1 year, 4 months ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-configure?view=o365-worldwide>  
upvoted 10 times

 **Futfuyfjij** 1 year, 4 months ago

Direct link:

<https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure#onboard-windows-devices>  
upvoted 3 times

 **veliyath** Most Recent 5 months, 4 weeks ago

**Selected Answer: C**

To onboard devices to Microsoft Defender for Endpoint using Microsoft Intune, you should create an endpoint detection and response (EDR) policy. This policy is specifically designed to configure and manage endpoint detection and response capabilities, including onboarding devices to Microsoft Defender for Endpoint.

Therefore, the correct answer is:


C. an endpoint detection and response (EDR) policy  
upvoted 3 times

 **KakTak** 6 months ago

**Selected Answer: E**

It should be E

upvoted 1 times

 **Haider\_Raza** 9 months, 4 weeks ago


**Selected Answer: C**

To onboard the Windows 11 computers to Microsoft Defender for Endpoint using Microsoft Intune, you should create an Antivirus policy. This policy helps manage the antivirus protection settings on the devices, which includes configuring Microsoft Defender Antivirus settings. This is essential for ensuring that the devices are protected and that Defender for Endpoint can monitor and respond to threats effectively.  
upvoted 1 times

 **MR\_Eliot** 10 months, 2 weeks ago

**Selected Answer: C**

C is correct. When you configure Defender for Endpoint, it will also create a default policy to onboard Windows devices in Defender for Endpoint. This currently only works for Windows. For MacOS it's a different story.  
upvoted 2 times

 **Darkfire** 10 months, 3 weeks ago

**Selected Answer: C**

C is correct

When you integrate Microsoft Defender for Endpoint with Intune, you can use endpoint security policies for endpoint detection and response (EDR) to manage the EDR settings and onboard devices to Microsoft Defender for Endpoint.

<https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-edr-policy>

upvoted 1 times

🗨️ **Merrybob** 11 months, 1 week ago

**Selected Answer: E**

E - While creating an Endpoint Detection and Response (EDR) policy in Microsoft Defender for Endpoint is essential for advanced threat detection and response capabilities, the initial onboarding process specifically involves creating an antivirus policy for managing settings related to Microsoft Defender Antivirus.

The antivirus policy helps ensure that antivirus protection is configured correctly on enrolled devices. It includes settings related to real-time protection, cloud-delivered protection, automatic sample submission, and more.

upvoted 1 times

🗨️ **Merrybob** 11 months, 1 week ago

C - Would also work because it is required to create an EDR. Creating an Antivirus policy and an EDR are both required steps according to this. Scroll through the steps and see: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboarding-endpoint-manager?view=o365-worldwide>

upvoted 1 times

🗨️ **Merrybob** 11 months ago

Checked this again and can confirm it's C that's correct.

When you integrate Microsoft Defender for Endpoint with Intune, you can use endpoint security policies for endpoint detection and response (EDR) to manage the EDR settings and onboard devices to Microsoft Defender for Endpoint.

<https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-edr-policy>

upvoted 1 times

🗨️ **NoursBear** 11 months, 3 weeks ago

The answers do not match the question, the question says:

You need to onboard the devices to Microsoft Defender for Endpoint.

First you need to turn Onboarding under settings under Microsoft Defender for Endpoint, plus download the package scripts to run on devices, or under Advanced Features, turn on the Intune Connector AND turn on the Defender for Endpoint Connection in Endpoint Manager (2x ways). From the question the computers are not onboarded yet. Then you configure the various ASR, EDR etc.... I guess if I get this on the exam 1:1 I will answer as per the answers here

upvoted 1 times

🗨️ **onepunchkenshin** 11 months, 3 weeks ago

ChatGPT tells E is the correct answer

upvoted 1 times

🗨️ **RomanV** 3 months, 2 weeks ago

GPT wants you to fail for the test and pay again to redo it. The correct answer is C! I onboarded so thousands of devices and the first thing you start with is EDR policy.

upvoted 1 times

🗨️ **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗨️ **chandravamsi** 1 year, 1 month ago

**Selected Answer: E**

Option: E

upvoted 1 times

🗨️ **Daveazure** 1 year, 2 months ago

In many cases, organizations will have existing endpoint security products in place. The bare minimum being an antivirus solution, but in some cases, an organization might have existing endpoint detection and response solution. Note "bare minimum".

upvoted 1 times

 **Rocky83** 1 year, 3 months ago

**Selected Answer: C**

Correct

upvoted 1 times

Your company uses Microsoft Intune to manage devices.

You need to ensure that only Android devices that use Android work profiles can enroll in Intune.

Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From Platform Settings, set Android device administrator Personally Owned to Block.
- B. From Platform Settings, set Android Enterprise (work profile) to Allow.
- C. From Platform Settings, set Android device administrator Personally Owned to Allow.
- D. From Platform Settings, set Android device administrator to Block.

**Suggested Answer:** BD

Community vote distribution

BD (100%)

🗨️ 👤 **RJTW070** 3 weeks, 6 days ago

**Selected Answer:** AB

Why these configurations?

A. From Platform Settings, set Android device administrator Personally Owned to Block:

The Android device administrator method is an older, less secure management framework.

Blocking Personally Owned Android Device Administrator ensures that only Android devices enrolled using modern methods like Android Enterprise work profiles can be enrolled.

B. From Platform Settings, set Android Enterprise (work profile) to Allow:

Android Enterprise (work profile) is the modern management method for managing BYOD (Bring Your Own Device) Android devices.

Allowing this ensures that Android devices with work profiles can be enrolled in Intune.

upvoted 3 times

🗨️ 👤 **dragzz07** 2 weeks, 1 day ago

You want to block the entire Android Device Administrator platform.... not just the personally owned portion of the device Android Device Administrator platform.

upvoted 1 times

🗨️ 👤 **veliyath** 5 months, 4 weeks ago

**Selected Answer:** BD

To ensure that only Android devices using Android work profiles can enroll in Intune, you should:

D. From Platform Settings, set Android device administrator to Block.

B. From Platform Settings, set Android Enterprise (work profile) to Allow.

This configuration ensures that only devices using Android work profiles can enroll while blocking other Android devices managed by the older device administrator method.

upvoted 3 times

🗨️ 👤 **Cheban** 9 months, 2 weeks ago

you can control which devices are allowed to enroll by setting device enrollment restrictions. To ensure that only Android devices that use Android work profiles can enroll in Intune, you should:

Block Android device administrator Personally Owned devices: This prevents Android devices that are not using work profiles from enrolling.

Allow Android Enterprise (work profile) devices: This allows Android devices that are using work profiles to enrol. A and B are the right answers.

upvoted 1 times

🗨️ 👤 **Savior99** 10 months ago

**Selected Answer:** BD

There's no "android Personally owned" option, only Work profile and Admin

upvoted 1 times



MR\_Eliot 10 months, 2 weeks ago

Selected Answer: BD

BD agreed. Also device administrator will be out of support by Microsoft very soon.

upvoted 2 times

Merrybob 11 months ago

Selected Answer: BD

BD

Ref for D: <https://learn.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#blocking-personal-android-devices>

upvoted 1 times

Rocky83 1 year, 3 months ago

Selected Answer: BD

In groups where both Android platforms are allowed, devices that support work profile will enroll with a work profile. Devices that don't support work profile will enroll on the Android device administrator platform. Neither work profile nor device administrator enrollment will work until you complete all prerequisites for Android enrollment.

upvoted 3 times

mirak123 1 year, 3 months ago

why is it D?

upvoted 3 times

NoursBear 11 months, 2 weeks ago

Because Android Device Admin may not enroll at all so when blocking Android Device Admin under the platform setting, the personally owned device is greyed out automatically so you don't set the "block" there

upvoted 2 times

Futfuyfj 1 year, 4 months ago

Answers are 100% correct

upvoted 2 times

krzysztofbr 1 year, 4 months ago

Selected Answer: BD

<https://learn.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set>

upvoted 4 times

HOTSPOT -

You have the device configuration profile shown in the following exhibit.

### Kiosk

Windows 10 and later

- 1 Basics
- 2 Configuration settings**
- 3 Assignments

Configure your devices to run in kiosk mode. Before you select a kiosk mode, review your app assignments in the Mobile Apps blade. Apps that you want to run in kiosk mode should be assigned to a Windows device. [Learn more about Windows kiosk mode.](#)

Select a kiosk mode \* ⓘ

User logon type \* ⓘ

Application type \* ⓘ

This kiosk profile requires Microsoft Edge version 87 and later with Windows 10 version 1909 and later. [Learn more about Microsoft Edge kiosk mode.](#)

Edge Kiosk URL \* ⓘ

Microsoft Edge kiosk mode type ⓘ

Refresh browser after idle time ⓘ

Specify Maintenance Window for App Restarts \* ⓘ  Require  Not configured

Maintenance Window Start Time

Maintenance Window Recurrence ⓘ

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.

### Answer Area

Users [answer choice]

- can access any URL
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com

Windows 10 and later devices can have [answer choice]

- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has multiple tabs
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

**Answer Area**

**Suggested Answer:**

Users [answer choice]

- can access any URL
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com

Windows 10 and later devices can have [answer choice]

- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has multiple tabs
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

answers are correct

<https://learn.microsoft.com/en-us/mem/intune/configuration/kiosk-settings-windows>

upvoted 14 times

  **letters1234**  1 year, 4 months ago

<https://learn.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode#overview>

Would require Digital/Interactive Signage experience instead of Public-Browsing to be limited to one site.



Multiple tabs are also part of PBE

upvoted 5 times

  **7798da3**  5 months, 3 weeks ago


I have seen it show multiple browser single tab

upvoted 1 times

  **MR\_Eliot** 10 months, 2 weeks ago



Answers are correct!

upvoted 4 times

  **MR\_Eliot** 10 months, 2 weeks ago

<https://learn.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode#overview>

upvoted 2 times

  **yosry** 1 year, 1 month ago

Seems Correct

upvoted 2 times

  **Rocky83** 1 year, 3 months ago

Correct

upvoted 3 times

## HOTSPOT -

You have 100 Windows 10 devices enrolled in Microsoft Intune.

You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.

Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Delivery Optimization setting:

- Bandwidth optimization type
- Download mode
- VPN peer caching

Intune object:

- A configuration profile
- App configuration policies
- Windows 10 and later quality updates
- Windows 10 and later update rings

### Answer Area

Suggested Answer:

Delivery Optimization setting:

- Bandwidth optimization type
- Download mode
- VPN peer caching

Intune object:

- A configuration profile
- App configuration policies
- Windows 10 and later quality updates
- Windows 10 and later update rings

**letters1234** Highly Voted 1 year, 4 months ago

LAN (1 - Default): This default operating mode for Delivery Optimization enables peer sharing on the same network.

The Delivery Optimization cloud service finds other clients that connect to the Internet using the same public IP as the target client. These clients then try to connect to other peers on the same network by using their private subnet IP.

<https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference#download-mode>

And yes, done through configuration profile.

upvoted 10 times

**oopspruu** Most Recent 5 months, 2 weeks ago

Provided answers are correct. Update Rings doesn't have delivery optimization settings.

upvoted 1 times

**MR\_Eliot** 10 months, 2 weeks ago

Answer is correct.

upvoted 3 times

**Darkfire** 10 months, 3 weeks ago

Answer is correct

upvoted 1 times

**yosry** 1 year, 1 month ago

seems correct

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

Correct, Download mode, Configuration Profile>Templates>Delivery optimization.  
upvoted 1 times

🗨️ 👤 **ExamKiller020** 1 year, 3 months ago

Answer is correct, just checked in my own tenant  
upvoted 4 times

🗨️ 👤 **NoursBear** 1 year, 3 months ago

Hmm ok fair enough but now it should be done via the newer options Update rings for W10, Feature Updates for W10 etc....  
upvoted 1 times

🗨️ 👤 **ExamKiller020** 1 year, 3 months ago

You cant config that in Update rings...  
upvoted 4 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

hmmm, download mode? 99%

100% device profile.

answers are correct hope so 99%

<https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization>

upvoted 2 times

## HOTSPOT -

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

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

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

From Intune, you create and send a custom notification named Notification1 to Group1.

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


NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
User1 receives Notification1 on Device1.	<input type="radio"/>	<input type="radio"/>
User2 receives Notification1 on Device2.	<input type="radio"/>	<input type="radio"/>
User1 receives Notification1 on Device3.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> User1 receives Notification1 on Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 receives Notification1 on Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User1 receives Notification1 on Device3.	<input checked="" type="radio"/>	<input type="radio"/>

 **Futfuyfj** Highly Voted 1 year, 3 months ago

The answer is here: <https://learn.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications>

-> When sending a notification to a group, messages target only the users in the group and are sent to each iOS/iPadOS or Android device that the user has registered. Devices in the group will be ignored when targeting the notification.

Answer is correct.

upvoted 27 times

 **Friscini** 3 weeks, 1 day ago

On the Assignments tab, select the groups to which you'd like to send this custom notification, and then select Next to continue. Sending a notification to a group will target only the users of that group; the notification will go to all iOS/iPadOS and Android devices enrolled by that user.

upvoted 1 times

 **Casticod** 1 year, 3 months ago

From the same link: "Use Microsoft Intune to send custom notifications to the users of managed iOS/iPadOS and Android devices"

So I think:

No Its Windows

YES Its Android an device in Group 1

NO Its IOS but not In group 1

upvoted 7 times

 **onepunchenshin** 11 months, 3 weeks ago

user takes precedence, so Futfuyfj is right

upvoted 2 times

 **LionelDerBoven** 3 months, 3 weeks ago

But what I don't understand in 2 is the device is in group 1, but the user is not. So what has the highest priority? is it not a OR? if Device OR user is in notification group: send? make more sense.

upvoted 1 times

  **krzysztofbr** Highly Voted 1 year, 4 months ago

so many wrong answers again:)

custom doesn't work for Windows and MacOS

DEVICE 1 (Windows) NO

Device 2 (Android) YES

Device 3 (IOS) but group 2 - NO



upvoted 18 times

  **OyYaGotta** 10 months ago

It's IOS not MacOS. Question states IOS not OSX operating system.

Windows device will not receive the notification. IOS and Android will. Push notifications are not designed for Windows based machines only Mobile OS machines.

upvoted 2 times

  **BJS78** 1 year, 3 months ago

Well, not entirely true. You CAN create custom Notifications (Toast) on Windows via PS and deploy, but not "send" them

upvoted 1 times

  **krzysztofbr** 1 year, 4 months ago

I was wrong!

NO, NO, YES!

upvoted 25 times

  **AdamRachel** 11 months, 3 weeks ago

Device 1 NO - does not affect Windows and MacOS

Device 2 No because it is from User2 not User1 -please check

Device3 I need an explanation why YES if that device is in Group2 where the notification was sent to Group1...

upvoted 4 times

  **captainspork** 3 months, 1 week ago

device 3 is yes because it is sent to the user, not the device. The user is part of the group and receives it on the phone because of that.

upvoted 3 times

  **Tr619899** Most Recent 1 month, 2 weeks ago

Answer is: NO, YES, NO

The device's group membership, not the user's, determines whether the device will receive a custom notification in Intune. User precedence does not apply in this case. This behavior aligns with Intune's design for targeting devices rather than users in notification scenarios.

upvoted 1 times

  **KOUKI21** 2 months ago

To answer this question, let's analyze the groups and devices involved:

Notification1 is sent to Group1.

Group1 includes the following members based on the tables:

Users: User1

Devices: Device1 (Windows 10) and Device2 (Android)

Let's go through each statement in the "Answer Area":

Statement 1: User1 receives Notification1 on Device1.

Yes. Since User1 is in Group1 and Device1 is also in Group1, User1 would receive the notification on Device1.

Statement 2: User2 receives Notification1 on Device2.

No. User2 is a member of Group2, not Group1. Thus, User2 will not receive Notification1 on any device.

Statement 3: User1 receives Notification1 on Device3.

No. Device3 is a member of Group2, not Group1. Therefore, User1 will not receive the notification on Device3.

Final Answers:

User1 receives Notification1 on Device1: Yes

User2 receives Notification1 on Device2: No

User1 receives Notification1 on Device3: No

upvoted 1 times

🗨️ 👤 **King\_shola** 3 months, 3 weeks ago

NO, NO, YES

"You can send notifications to users in groups. When sending notifications to groups, each notification can be targeted directly to up to 25 groups.

Nested groups do not count toward this total. ""When a notification is sent to a group, messages are targeted only to users in the group and

sent to each iOS/iPadOS or Android device that the user has registered. When targeting the notification, devices in the group will be ignored.""

upvoted 1 times

🗨️ 👤 **93831b0** 4 months ago

Answer is correct. Tenant admin > custom notifications

Select groups to send this notification to. If a group contains users and devices, only users will be targeted. iOS and Android support only.

upvoted 1 times

🗨️ 👤 **Pollosor** 4 months, 2 weeks ago

NO: Windows devices do not support custom notifications.

YES: Device2 is compatible because it is an Android device and belongs to Group1.

NO: Device3 is compatible but is not part of Group1.

<https://learn.microsoft.com/es-es/mem/intune/remote-actions/custom-notifications>

upvoted 3 times

🗨️ 👤 **oopspruu** 4 months, 2 weeks ago

NNY

The key here is to understand how Custom Notifications work in Intune and not just guess based on your general understanding. as per the custom notification Assignments section:

"Select groups to send this notification to. If a group contains users and devices, only users will be targeted. iOS and Android support only."

1. The notification targets only users, and not devices. So it doesn't matter which group a device is in, what matters is the user in the group.
2. only iOS and Android support.

So User 2 will not receive any notification anywhere and User 1 will always get notification on an iOS and Android device.

upvoted 1 times

🗨️ 👤 **SasaBond** 5 months, 2 weeks ago

Its NNN

User1 and DEVICE 1 (Windows) NO - Does not support Send Custom Notification

User2 and Device 2 (Android) NO - Question is mentioning to GROUP1. User2 is GROUP2

User1 and Device 3 (IOS) - NO - User1 is not part of GROUP2, hence not part of Device3.

upvoted 2 times

🗨️ 👤 **carl\_amadeo** 7 months, 1 week ago

Notification 1was assigned to Group 1 where only User1 is member of.

User1 logs in to Device1 (Windows not supported) - no notification

User2 logs in to Device2(Android supported but User2 is not a member of group1) - no notification

User1 logs in to Device3 (iOS supported) - Yes notification will be sent

upvoted 2 times

🗨️ 👤 **kerimnl** 9 months, 1 week ago

NO

NO

YES

1- NO: Intune custom notifications aren't supported by macOS and Windows devices.

Link: <https://learn.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications#:~:text=the%20device%20appear.,intune%20custom%20notifications%20aren%27t%20supported%20by%20macOS%20and%20Windows%20d>

Custom%20notification%20messages



2-NO: Sending a notification to a group will target only the users of that group; the notification will go to all iOS/iPadOS and Android devices enrolled by user. User 2 is not a member of Group1.

3- YES: User1 is a member of Group1. Sending a notification to a group will target only the users of that group; the notification will go to all iOS/iPadOS and Android devices enrolled by that user.

upvoted 6 times

  **slimmerik7** 9 months, 2 weeks ago

No, No, Yes

1) Windows so no

2) Android but user is in wrong group and notifications are user based.

3) IOS and correct user/group; IOS is supported and user is in correct group. Device does not matter since it only looks at users in the group (see article below).

<https://learn.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications#send-a-custom-notification-to-groups>

"On the Assignments tab, select the groups to which you'd like to send this custom notification, and then select Next to continue. Sending a notification to a group will target only the users of that group; the notification will go to all iOS/iPadOS and Android devices enrolled by that user."

upvoted 2 times

  **MJFT** 9 months, 4 weeks ago

no, custom notification available windows devices

No. only sent to group1

Yes . sent to group1. IOS and android devices are allowed.

Sending a notification to a group will target only the users of that group; the notification will go to all iOS/iPadOS and Android devices enrolled by that user.

<https://learn.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications>


upvoted 1 times

  **MJFT** 9 months, 4 weeks ago

mistake here it should be:



no, custom notification not available windows devices

upvoted 1 times

  **Sergey42** 10 months, 1 week ago

But device 3 is in group 2, how did the user 1 receive that notification?

upvoted 1 times



  **MR\_Eliot** 10 months, 2 weeks ago

Answer is correct.

On the Assignments tab, select the groups to which you'd like to send this custom notification, and then select Next to continue. Sending a notification to a group will target only the users of that group; the notification will go to all iOS/iPadOS and Android devices enrolled by that user.

<https://learn.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications#send-a-custom-notification-to-groups>

upvoted 3 times

  **Softeng** 10 months, 2 weeks ago

N-N-Y

Notifications only apply to Android/iOS devices:

<https://learn.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications#:~:text=Use%20Microsoft%20Intune%20to%20send%20custom%20n>

Notifications only target users in group, not devices:

<https://learn.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications#:~:text=Sending%20a%20notification%20to%20a%20group%20will%20target%20only%20the%20users%20of%20that%20group%3B%20the%20>

upvoted 2 times

  **Darkfire** 10 months, 3 weeks ago

Answer is correct

When sending a notification to a group, messages target only the users in the group and are sent to each iOS/iPadOS or Android device that the user has registered. Devices in the group will be ignored when targeting the notification.

<https://learn.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications>

upvoted 1 times

You use Microsoft Intune and Intune Data Warehouse.  
You need to create a device inventory report that includes the data stored in the data warehouse.  
What should you use to create the report?

- A. the Company Portal app
- B. Endpoint analytics
- C. the Azure portal app
- D. Microsoft Power BI

**Suggested Answer:** D

*Community vote distribution*

D (100%)

MR\_Eliot 4 months, 1 week ago

Selected Answer: D

<https://learn.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports>  
upvoted 1 times

Darkfire 4 months, 1 week ago

Selected Answer: D

D is correct

<https://learn.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi#load-the-data-and-reports-using-the-power-bi-intune-compliance-data-warehouse-app~:text=BI%20Desktop-,Load%20the%20data%20and%20reports%20using%20the%20Power%20BI%20Intune%20Compliance%20Data%20Warehouse%20The%20Power%20BI>  
upvoted 2 times

Krayzr 4 months, 2 weeks ago

Selected Answer: D

correct  
upvoted 1 times

pinda 8 months, 4 weeks ago

Selected Answer: D

correct  
upvoted 3 times

krzysztofbr 10 months, 2 weeks ago

Microsoft Power BI  
upvoted 4 times

Futfuyfj 10 months, 1 week ago

<https://learn.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi>  
upvoted 6 times

You have a Microsoft 365 E5 subscription and 25 Apple iPads.  
You need to enroll the iPads in Microsoft Intune by using the Apple Configurator enrollment method.  
What should you do first?

- A. Configure an Apply MDM push certificate.
- B. Add your user account as a device enrollment manager (DEM).
- C. Modify the enrollment restrictions.
- D. Upload a file that has the device identifiers for each iPad.

**Suggested Answer: A**

Community vote distribution

A (100%)

letters1234 **Highly Voted** 10 months, 2 weeks ago

**Selected Answer: A**

Pre-requisites - <https://learn.microsoft.com/en-us/mem/intune/enrollment/apple-configurator-enroll-ios>  
upvoted 9 times

5bd2675 **Most Recent** 2 months, 3 weeks ago

A is correct, but shouldn't it say "Apple" not "Apply"  
upvoted 4 times

Haider\_Raza 3 months, 3 weeks ago

**Selected Answer: A**

To enroll the Apple iPads in Microsoft Intune using the Apple Configurator enrollment method, you should first configure an Apple MDM push certificate. This certificate is required to establish trust between the iPads and the Intune service, enabling them to enroll and be managed through Intune. After obtaining the MDM push certificate, you can proceed with the enrollment process using the Apple Configurator tool.  
upvoted 3 times

MR\_Eliot 4 months, 1 week ago

**Selected Answer: A**

A is correct.  
upvoted 1 times

Darkfire 4 months, 1 week ago

**Selected Answer: A**

A is correct

<https://learn.microsoft.com/en-us/mem/intune/enrollment/apple-configurator-enroll-ios#:~:text=An%20Apple%20MDM%20push%20certificate>  
upvoted 1 times

Tonsku 6 months, 2 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-ios-ipados>  
upvoted 1 times

VirtualJP 9 months, 2 weeks ago

**Selected Answer: A**

Pre-reqs  
upvoted 2 times

krzysztofbr 10 months, 2 weeks ago

A. Configure an Apply MDM push certificate.  
from MS website  
Prerequisites  
Physical access to iOS/iPadOS devices  
Set MDM authority

An Apple MDM push certificate

Device serial numbers (Setup Assistant enrollment only)

USB connection cables

macOS computer running Apple Configurator 2.0

upvoted 2 times

## HOTSPOT -

You have 100 computers that run Windows 10. You have no servers. All the computers are joined to 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.

**Answer Area**

Windows Update technology to use:

- Windows Server Update Services (WSUS)
- Microsoft Configuration Manager
- Windows Update for Business

Manage the configuration by using:

- A Group Policy object (GPO)
- Microsoft Configuration Manager
- Microsoft Intune

Manage the traffic by using:

- Delivery Optimization
- BranchCache
- Peer cache

**Answer Area**

Windows Update technology to use:


- Windows Server Update Services (WSUS)
- Microsoft Configuration Manager
- Windows Update for Business**

Suggested Answer: Manage the configuration by using:


- A Group Policy object (GPO)
- Microsoft Configuration Manager
- Microsoft Intune**

Manage the traffic by using:


- Delivery Optimization**
- BranchCache
- Peer cache

 **krzysztofbr** Highly Voted 1 year, 4 months ago

"you have no servers" so it must be Intune and Windows update for bussiness  
upvoted 16 times

 **sh123df** Highly Voted 1 year, 4 months ago

Answers seems correct out  
upvoted 7 times

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

Windows Update for Business  
Microsoft Intune  
Delivery Optimization.

Keyword sentence is "you have no servers" and also Microsoft tries to push very hard for full cloud, so it's logical that they will not advertise on-prem solutions in their exams.

Cloud services = generating business for MSFT.

upvoted 3 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

The key to this question is "You have NO SERVERS".

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 2 weeks ago

answer is correct.

upvoted 1 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

Answers are correct.

upvoted 1 times

🗨️ 👤 **Murad01** 11 months ago

Given answers are correct

upvoted 1 times

🗨️ 👤 **WilliamsNL** 11 months, 1 week ago

For more information about managing the traffic: <https://learn.microsoft.com/en-us/windows/deployment/do/waas-optimize-windows-10-updates>

BranchCache is not available at Windows Update (for Business)

upvoted 2 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

answers are correct

upvoted 4 times

You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices. All the devices are enrolled in Microsoft Intune.

You need to configure Delivery Optimization on the devices to meet the following requirements:

Allow downloads from the internet and from other computers on the local network.

Limit the percentage of used bandwidth to 50.

What should you use?

- A. a configuration profile
- B. a Windows Update for Business Group Policy setting
- C. a Microsoft Peer-to-Peer Networking Services Group Policy setting
- D. an Update ring for Windows 10 and later profile

**Suggested Answer:** C

Community vote distribution

A (100%)

- 🗨️ **krzysztofbr** Highly Voted 1 year, 4 months ago  
 answer is wrong should be A "delivery Optimization"  
<https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference>  
 upvoted 25 times
- 🗨️ **Buzl** Highly Voted 1 year, 4 months ago  
 A Configuration profile using the "Delivery Optimization" template will allow you to specify the percentage of bandwidth (max) to be used  
 upvoted 12 times
- 🗨️ **FemiA55** Most Recent 2 weeks, 6 days ago  
Selected Answer: B  
 I had thought that since these machines are in azure hybrid relationship, Windows Update for Business Group Policy settings would be the way to go. Azure AD or Entra id would not have required administrative rights to configure these machines. Only the users.  
 upvoted 1 times
- 🗨️ **LionelDerBoven** 3 months, 3 weeks ago  
Selected Answer: A  
 A is right from experiance.  
 upvoted 2 times
- 🗨️ **CJL324** 7 months, 2 weeks ago  
 To configure Delivery Optimization on hybrid Azure AD joined Windows devices enrolled in Microsoft Intune, meeting the specified requirements, you should use a configuration profile.
- A. a configuration profile
- Using a configuration profile in Microsoft Intune allows you to centrally configure settings on devices, including those related to Delivery Optimization. You can specify the Delivery Optimization settings to allow downloads from the internet and other computers on the local network, as well as limit the percentage of used bandwidth to 50%.
- upvoted 2 times
- 🗨️ **AVN1711** 5 months, 3 weeks ago  
 Peer-To-Peer policy can be used as fine tuning for delivery optimization  
 "Policies to prioritize the use of peer-to-peer and cache server sources  
 When Delivery Optimization client is configured to use peers and Microsoft Connected Cache (MCC), to achieve the best possible content delivery experience, the client connects to both MCC and peers in parallel. If the desired content can't be obtained from MCC or peers, Delivery Optimization will automatically fall back to the HTTP source to get the requested content. There are four settings that allow you to prioritize peer-to-peer or MCC sources by delaying the immediate fallback to HTTP source, which is the default behavior."  
 upvoted 1 times



🗨️ **mestorrent86** 9 months, 4 weeks ago

Selected Answer: A

A it's the correct answer just read the documentation  
upvoted 1 times

🗨️ **OyYaGotta** 10 months ago

Selected Answer: A

A is definitely right and C is 100% wrong. Peer to Peer networking services are not designed in any way for Delivery Optimization which is specifically mentioned in the question. Configuration Profiles have multiple settings for this including bandwidth control. It is very frustrating and time consuming when a question like this is definitely wrong.  
upvoted 1 times

🗨️ **MR\_Eliot** 10 months, 2 weeks ago

Selected Answer: A

A is correct. You can create a configuration for delivery optimization settings.  
upvoted 3 times

🗨️ **Darkfire** 10 months, 3 weeks ago

Selected Answer: A

A is correct

<https://learn.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-settings#bandwidth>

upvoted 1 times

🗨️ **Merrybob** 11 months, 1 week ago

Selected Answer: A

A. a configuration profile  
upvoted 1 times

🗨️ **Amir1909** 11 months, 4 weeks ago

A is correct  
upvoted 1 times

🗨️ **onepunchkenshin** 12 months ago

ChatGPT tells you A is correct  
upvoted 1 times

🗨️ **OyYaGotta** 10 months ago

So does Copilot.  
upvoted 1 times

🗨️ **yosry** 1 year, 1 month ago

Selected Answer: A

configuration profile > Delivery Optimization > bandwidth optimization type = percentage  
then select set "Maximum foreground download bandwidth " and "Maximum background download bandwidth " to 50  
upvoted 1 times

🗨️ **madsa** 1 year, 1 month ago

This answer is correct, Microsoft Questions can be a bit tricky but with this information, the answer is correct.  
upvoted 1 times

🗨️ **chandravamsi** 1 year, 1 month ago

Selected Answer: A

Option A: Configuration Profile  
upvoted 1 times

🗨️ **Gentlemanners** 1 year, 1 month ago

Selected Answer: A

The Answer is A.  
You need a Configuration profile that allows you to configure the delivery optimization and its settings.

<https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference>

upvoted 1 times

🗨️ **fco168** 1 year, 1 month ago

**Selected Answer: A**

A Configuration Profile allows you to configure Delivery Optimization and its settings.  
upvoted 1 times

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10.

You have the groups shown in the following table.

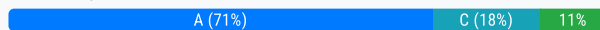
Name	Type	Location
Group1	Universal distribution group	Contoso.com
Group2	Global security group	Contoso.com
Group3	Group	Computer1
Group4	Group	Computer1

Which groups can you add to Group4?

- A. Group2 only
- B. Group1 and Group2 only
- C. Group2 and Group3 only
- D. Group1, Group2, and Group3

**Suggested Answer:** D

Community vote distribution



**picho707** Highly Voted 1 year, 2 months ago

**Selected Answer: A**

The correct answer is A.

Group 4 is a local group therefore Universal Distribution Groups cannot be nested.

Group 4 is a local group therefore other local Groups cannot be nested.

upvoted 26 times

**93831b0** 4 months ago

I get why the majority here will choose A. But because the key difference here is that the question is not about group nesting in an Entra tenant but about on-site AD. And on-site AD allows more complex nesting scenarios compared to Azure AD. Therefore I lean towards D.

upvoted 1 times

**OyYaGotta** 10 months ago

That's not right at all. Global Administrators have permission control of local Groups and Universal Distribution Groups distribute all sorts of GPO's to local machines, even across domains. It's possible but not necessary, to nest a GA in a local Group. GA has permissions to all forested Groups in the Domain.

upvoted 1 times

**Temptset** 1 year, 2 months ago

This is correct!

upvoted 3 times

**OyYaGotta** 10 months ago

It's not actually.

upvoted 2 times

**volto** Highly Voted 1 year, 4 months ago

**Selected Answer: C**

Answer D is wrong. Unable to add local security group, universal distribution group. Just another local computer group or domain security group.

The correct answer is C.

upvoted 10 times

**picho707** 1 year, 3 months ago

The correct answer is "C". A universal distribution group cannot be added to a local group however a security group can be nested to a local group.

upvoted 1 times

**picho707** 1 year, 2 months ago

I am withdrawing this answer after further research.

upvoted 2 times

 **TedEx2** Most Recent 3 weeks, 1 day ago

**Selected Answer: C**

it' C - you can add a global security group, but not a universal distribution group to a local group


upvoted 1 times

 **Pisces225** 1 month, 1 week ago

**Selected Answer: C**

Read for yourself, it's laid out clear as day in the table at the top of the page: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>

upvoted 1 times

 **LionelDerBoven** 3 months, 3 weeks ago

**Selected Answer: A**


After extensive research:

Group 1 Universal type group can't be added to group 4 (local). Universal type groups can't be added to local groups.

Group 2 (global) can be added to a local group (group 4)

Group 3 can't be added to group 4 because local groups can not be nested (even on the same device).

upvoted 3 times

 **dnt91** 4 months ago

**Selected Answer: D**

Domain Local Possible members : Accounts from any domain or any trusted domain

Global groups from any domain or any trusted domain


Universal groups from any domain in the same forest

Other Domain Local groups from the same domain

Accounts, Global groups, and Universal groups from other forests and from external domains

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>

upvoted 4 times

 **93831b0** 4 months, 3 weeks ago


An AD computer, a local group can include:

- Local users and groups from the same computer.

- Domain users and groups (including domain local, global, and universal groups) from the same domain or trusted domains.

It looks as the given answer is correct

upvoted 1 times

 **HellfireZA** 4 months, 3 weeks ago

**Selected Answer: A**

Lab tested on company tenant. Only security groups can be added to other groups.

upvoted 2 times

 **Cezt** 5 months ago

**Selected Answer: A**

group nesting is not supported for local groups

upvoted 2 times

 **Jt909** 5 months, 3 weeks ago

**Selected Answer: A**

Correct Answer is A - Lab-tested. Only Domain Security groups (universal, global and domain local ) can be added. Any kind of Domain

Distribution groups(Uni/Glob/Dloc) is not selectable by the picker. Computer1 local group cannot be added. Confusion is probably due to Domain

Local groups and Computer Local groups...

upvoted 4 times

 **CJL324** 7 months, 2 weeks ago

A

Group3 is a local group specific to Computer1. Local groups can contain users, global groups, and other local groups from the same computer.

However, they cannot be added to groups from other domains or computers.

Since Group4 is also a local group on Computer1, it cannot contain Group3 because local groups cannot be nested within each other. Therefore, Group3 cannot be added to Group4.

upvoted 2 times

MR\_Eliot 9 months, 3 weeks ago

Selected Answer: A

A is correct. I have tested this in my lab.

upvoted 4 times

zeos\_ucok 9 months, 4 weeks ago

Selected Answer: D

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755692\(v=ws.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755692(v=ws.10)?redirectedfrom=MSDN)

Group 4 is domain local group which can include any groups

upvoted 3 times

flc 9 months, 4 weeks ago

I just tried in a lab environment to create two groups (Security Group and Universal Distribution) on a domain and two other local groups (group3 and group4) on the Win10 device that is joined to the domain. I attempted to add group3 and the 'Universal Distribution' group to group4, but it wouldn't allow me to do so. Then I tried adding the 'Security Group', and it was successfully added to group4 without any issues. Therefore, I can confirm with 100% certainty that the correct answer is 'A: Group2 only.'

upvoted 1 times

VLAG 10 months ago

Selected Answer: D

Given answer D is correct.

Based on following link

<https://learn.microsoft.com/en-us/windows/win32/ad/nesting-in-native-mode#:~:text=A%20domain%20local%20group,other%20domain%20or%20forest>

"A domain local group can contain universal groups, global groups and accounts from any domain or forest.

A domain local group can also contain other domain local groups from the same domain that the group belongs to.

A domain local group cannot contain other domain local groups from any other domain or forest."

So, a Domain Local Group (Group4 in question) can nest:

1. other Domain Local Group from the same domain (Group3 is from the same Location: Computer1)
2. Global Security Groups (Group2)
3. Universal distribution Groups (Group1)

Any helpful comment is welcome.

upvoted 1 times

Maclouis116 6 months, 2 weeks ago

Distribution groups cannot be added to computer groups

upvoted 1 times

Darkfire 10 months, 2 weeks ago

Selected Answer: A

A seems right

<https://learn.microsoft.com/en-us/windows/win32/ad/nesting-in-native-mode>

<https://learn.microsoft.com/en-us/windows/win32/ad/group-objects>

<https://ss64.com/nt/syntax-groups.html#:~:text=Nesting%20one%20Group%20within%20another%20with%20a%20different%20scope>

upvoted 2 times

Softeng 10 months, 2 weeks ago

Selected Answer: C

You can't nest Universal Distribution Group into a local group.

upvoted 1 times

Maclouis116 6 months, 2 weeks ago

You also cannot nest local groups so answer is A

upvoted 1 times

DRAG DROP -

You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a compliance policy that meets the following requirements:

Requires BitLocker Drive Encryption (BitLocker) on each device

Requires a minimum operating system version

Which setting of the compliance policy should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

### Settings

### Answer Area

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Requires BitLocker:

Requires a minimum operating system version:

### Answer Area

**Suggested Answer:**

Requires BitLocker:

Requires a minimum operating system version:

 **krzysztofbr** Highly Voted 1 year, 4 months ago

answers are correct

<https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows>

upvoted 24 times

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

Device health:

To ensure devices boot to a trusted state, Intune utilizes Microsoft device attestation services. Devices across Intune commercial, US Government GCC High, and DoD services running Windows 10 use the Device Health Attestation (DHA) service.

Device Properties:

To discover build versions for all Windows 10/11 Feature Updates and Cumulative Updates (to be used in some of the fields below), see Windows release information. Be sure to include the appropriate version prefix before the build numbers, like 10.0 for Windows 10 as the following examples illustrate.

upvoted 1 times

 **MR\_Eliot** 10 months, 2 weeks ago

Answers are correct.

upvoted 3 times

 **Darkfire** 10 months, 2 weeks ago

Answers are correct idd


<https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows>

upvoted 1 times

 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

 **Richard\_rex** 1 year, 1 month ago

The Answer is correct, Lab tested

upvoted 1 times

🗨️ 👤 **Rocky83** 1 year, 3 months ago

Correct

upvoted 1 times

🗨️ 👤 **maggie22** 1 year, 3 months ago

it should be system security for bitlocker

upvoted 4 times

🗨️ 👤 **gv\_myra** 1 year, 3 months ago

It's not. It is Device Health. <https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows#device-health>

upvoted 1 times

🗨️ 👤 **Casticod** 1 year, 3 months ago

Correct: <https://www.anoopcnair.com/bitlocker-compliance-policy-using-intune/>

upvoted 1 times

🗨️ 👤 **Casticod** 1 year, 3 months ago

My comment should be generate dudes Correct With the option posted by Maggie22

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

no, check it in your Tenant

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You have the Windows 11 devices shown in the following table.

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

You deploy the device compliance policy shown in the exhibit. (Click the Exhibit tab.)

**Basics** [Edit](#)

Name	Policy1
Description	--
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

**Compliance settings** [Edit](#)

**Device Health**

Require BitLocker Require

**Actions for noncompliance** [Edit](#)

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

**Scope tags** [Edit](#)

Default

**Assignments** [Edit](#)

Included groups

**Group**

Group1

Group3

Excluded groups

**Group**

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.

**Answer Area**

Statements	Yes	No
Device1 will have Policy assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 will have Policy assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 will have Policy assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
<b>Suggested Answer:</b> Device1 will have Policy assigned and will be marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 will have Policy assigned and will be marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 will have Policy assigned and will be marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>



🗨️ 👤 **Kiookr** Highly Voted 👍 1 year, 3 months ago

YNN , \*\*\* Excluded Groups \*\*\* group 2, and per Microsoft "exclusion" take precedence over "inclusion "  
upvoted 33 times

🗨️ 👤 **665d390** 3 months, 4 weeks ago

correct  
upvoted 1 times

🗨️ 👤 **riccardo1999** 1 year ago

if the exclusion win the device has not compliance policy and so is compliance  
upvoted 2 times

🗨️ 👤 **OyYaGotta** 9 months, 4 weeks ago

No, that makes no sense. Exclusion policy takes precedence. Device is excluded from policy all together. If a device has no compliance policy it will be marked as NOT compliant by default.  
upvoted 5 times

🗨️ 👤 **ubiquituz** 1 year ago

the question is device 3 will have a policy assigned...so the answer is NO because of the exclusion...yes it will be excluded and marked as compliant but wont have a policy assigned...so as per the question the answer is YNN  
upvoted 6 times

🗨️ 👤 **letters1234** Highly Voted 👍 1 year, 4 months ago

Y - Applies and Bitlocker enabled  
N - Applies and Bitlocker disabled  
Y - Compliance check doesn't apply

Mark devices with no compliance policy assigned as:

This setting determines how Intune treats devices that haven't been assigned a device compliance policy. This setting has two values:  
"Compliant (default): This security feature is off. Devices that aren't sent a device compliance policy are considered compliant."

<https://learn.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#compliance-policy-settings>

upvoted 10 times

🗨️ 👤 **WORKHOLIC** 7 months ago

Y - Applies and Bitlocker enabled  
N - Applies and Bitlocker disabled  
N - Applies and Bitlocker disabled  
upvoted 2 times

🗨️ 👤 **cserra** 1 year, 4 months ago

The third question starts with "Device 3 will have a policy assigned" and as it belongs to Group2, the policy will not be assigned to it.  
Therefore it is no.  
The correct answer would be YNN  
upvoted 10 times

🗨️ 👤 **TheWiz** 1 year, 4 months ago

Correct. Device 3 is in both an included and excluded group. In that case, exclusion wins. Policy will not be assigned.  
<https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments>  
upvoted 5 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

Very good point but tricky though  
upvoted 1 times

🗨️ 👤 **AdamRachel** 11 months, 3 weeks ago

Yes but policy will be not assigned to that device. And in question you have Device3 will have "Policy Assigned" (which is no) and marked as compliant  
upvoted 4 times

🗨️ 👤 **Kiookr** 1 year, 2 months ago

Device 3 is part of Group 2 "Excluded" , and per Microsoft "exclusion" take precedence over "inclusion " thus is NO not compliant  
upvoted 1 times

🗨️ 👤 **93831b0** Most Recent 🕒 4 months, 3 weeks ago

Yes, NO, NO

Excluded groups take precedence over included groups when applying policies. This means if a device or user is part of both an included and an excluded group, the policy will not be applied to them. <https://techcommunity.microsoft.com/t5/microsoft-intune/device-in-include-and-exclude-group/td-p/1191297>

upvoted 2 times

🗨️ 👤 **veliyath** 5 months, 4 weeks ago

To determine whether each device will have the policy assigned and be marked as compliant, let's analyze the provided information:

Device1:

Member of Group1

BitLocker is enabled

Group1 is included in the policy assignment

Not excluded

Device2:

Member of Group1 and Group3

BitLocker is disabled

Group1 and Group3 are included in the policy assignment

Not excluded

Device3:

Member of Group1 and Group2

BitLocker is enabled

Group1 is included in the policy assignment

Group2 is excluded

Given these details, the answers are:

Device1 will have Policy1 assigned and will be marked as compliant: Yes

Device2 will have Policy1 assigned and will be marked as compliant: No (BitLocker is disabled)

Device3 will have Policy1 assigned and will be marked as compliant: No (Member of excluded Group2)

upvoted 1 times

🗨️ 👤 **RaziLlycas** 9 months, 3 weeks ago

the last device will be complaint because for default if no policy is assigned device is marked compliant, but the question ask if the policy will be assigned and it will be marked complaint, so the final answer is NO, due it will be marked complaint but because NO POLICY will be assigned

upvoted 2 times

🗨️ 👤 **MR\_Eliot** 10 months, 2 weeks ago

Answers are correct

upvoted 2 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

I think answers are correct

Y - Applies and Bitlocker enabled

N - Applies and Bitlocker disabled

N - Least rights count for Group2 because its excluded from the policy. So marked as NON compliant immediately.

upvoted 2 times

🗨️ 👤 **kaushik07** 10 months, 3 weeks ago

Even though the option says policy is assigned to the device3 it won't apply to it as exclusion takes precedence and eventually makes the device compliant, because in case of not applicable or targeted, Intune marks it as compliant. This helps avoid unnecessarily marking devices non-compliant due to missing policies that don't apply to them

upvoted 1 times

🗨️ 👤 **Frobenius** 11 months ago

You can't really know if the given answer is correct, this is purely based on your default Compliance Policy Settings, if no changes have been made, Device3 will be marked compliant.

upvoted 4 times

🗨️ 👤 **Engr001** 11 months, 2 weeks ago

I dont understand the answers here. It should be NNN ???

When the policy is applied the device will be set as non-compliant. So every answer will be no??

upvoted 1 times

🗨️ 👤 **Engr001** 11 months, 2 weeks ago

Man, i should really read better. Or not try to study when i'm tired. It is YNN

upvoted 1 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **Tonsku** 1 year ago

Y, N, N

Device1 group1 enabled bitlocker

device2 group1 & 3 disabled bitlocker

device3 group1 & 2 enabled bitlocker

bitlocker: require

include group1 & group3

exclude group2

upvoted 1 times

🗨️ 👤 **jbuexamtopics** 1 year ago

YNN

Device 1: Already have bitlocker enabled.

Device 2: Didnt have bitlocker enabled

Device 3: Configured on excluded group therefor policy will not apply

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

Yes No Yes I agree with letters, for otherwise the question would have to state that devices with no policy aren't compliant.

upvoted 2 times

🗨️ 👤 **b0gdan433** 1 year, 1 month ago

Yes,No,No correct answ, took the exam today and all the points from the question.

upvoted 1 times

🗨️ 👤 **NTNT** 12 months ago

Sure, you must be the first one that gets the score points of the questions. Do not tell usnonsense.

upvoted 2 times

🗨️ 👤 **iamforksu** 1 year, 2 months ago

Yes

No

No

upvoted 2 times

🗨️ 👤 **Suresh\_2411** 1 year, 2 months ago

Y - policy assigned and compliant

N - policy assigned and not compliant

N - policy not assigned

N

upvoted 4 times

DRAG DROP -

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

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system builds can access network resources.

Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

### Settings

### Answer Area

Require BitLocker	Device1:	<input type="text"/>
Prevent jailbroken devices from having corporate access.	Device2:	<input type="text"/>
Prevent rooted devices from having corporate access.	Device3:	<input type="text"/>
Require Secure Boot to be enabled on the device.		

### Answer Area

#### Suggested Answer:

Device1:	Require Secure Boot to be enabled on the device.
Device2:	Prevent jailbroken devices from having corporate access.
Device3:	Prevent rooted devices from having corporate access.

 **krzysztofbr** Highly Voted 1 year, 4 months ago


answers are correct  
upvoted 14 times

 **Crismo** Highly Voted 1 year, 3 months ago

rooted is the term used for modified Androids, jailbroken for iOS  
upvoted 8 times

 **MR\_Eliot** Most Recent 10 months, 2 weeks ago

Correct!  
upvoted 2 times

 **Darkfire** 10 months, 3 weeks ago

Answers are correct

<https://learn.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

Keywords:

Secure Boot = for Windows = Device1

Jailbroken = iOS modified = Device2

Rooted = Android modified = Device3

upvoted 2 times

 **sunil\_pal12051989** 1 year ago

why not require bitlocker

upvoted 3 times

🗨️ **RomanV** 3 months, 2 weeks ago

"access network resources." Read between the lines.

Correct answers are:

Secure Boot --> Windows

Jailbreak --> iOS

Root -> Android

upvoted 1 times

🗨️ **Dennizje** 6 months, 1 week ago

It's about accessing (being able to connect to) resources.

Bitlocker doesn't necessarily prevent a connection from happening, it just encrypts data.

upvoted 1 times

🗨️ **NoursBear** 11 months, 2 weeks ago

you need to ensure that only devices running trusted firmware or operating system builds can access network resources.

upvoted 2 times

DRAG DROP -

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.

You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices.

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

**Actions**

**Answer Area**

Review the compliance dashboard for results.

Create and assign a compliance policy that has System Security settings configured.

Review the Conditional Access Insights and Reporting workbook for results.

Create a PowerShell discovery script and a JSON file.

Upload the PowerShell script to Intune.

Upload the JSON file to Azure AD.

Create and assign a custom compliancy policy.

1

2

3

4



**Answer Area**

Suggested Answer:

1 Create a PowerShell discovery script and a JSON file.

2 Upload the PowerShell script to Intune.

3 Create and assign a custom compliancy policy.

4 Review the compliance dashboard for results.

🗨️ 👤 **krzysztofbr** Highly Voted 👍 10 months, 2 weeks ago

answers are corect

<https://learn.microsoft.com/en-us/mem/intune/protect/compliance-use-custom-settings#prerequisites>

upvoted 16 times

🗨️ 👤 **MR\_Eliot** Most Recent 🕒 4 months, 1 week ago

Answers are correct

upvoted 2 times

🗨️ 👤 **Darkfire** 4 months, 1 week ago

Answers correct idd

<https://learn.microsoft.com/en-us/mem/intune/protect/compliance-use-custom-settings#prerequisites>

upvoted 1 times

🗨️ 👤 **Amir1909** 5 months, 3 weeks ago

- create a powershell discovery script and a JSON file

- upload the powershell script to intune

- Create and assign a custom compliance policy

- upload the JSON file to Azure AD

upvoted 1 times

🗨️ 👤 **Alscoran** 9 months ago

Don't you have to upload the JSON file ?

<https://learn.microsoft.com/en-us/mem/intune/protect/create-compliance-policy>

For Windows:

On the Compliance settings page, expand Custom Compliance and set Custom compliance to Require.

For Select your discovery script, select Click to select, and then specify a script that's been previously added to the Microsoft Intune admin center. This script must have been uploaded before you begin to create the policy.

For Upload and validate the JSON file with your custom compliance settings, select the folder icon and then locate and add the JSON file for Windows that you want to use with this policy.

upvoted 2 times

🗨️ 👤 **Temptset** 9 months ago

Based on the URL you've provided you can find a hyperlink "Custom compliance JSON files" under the header Prerequisites, subhead JSON, which leads to:

<https://learn.microsoft.com/en-us/mem/intune/protect/compliance-custom-json>

"You'll upload the JSON file when you create a compliance policy that includes custom compliance settings."

This means the given answers are correct as you upload the JSON-file DURING the creation of a new policy, you don't upload it upfront as is needed for a PS script.

upvoted 4 times

🗨️ 👤 **FemiA55** 4 days, 5 hours ago

"The scripts must be uploaded to the Microsoft Intune admin center before you create a compliance policy. You select the script when you're configuring a policy to support custom settings."

<https://learn.microsoft.com/en-us/mem/intune/protect/compliance-use-custom-settings#prerequisites>

upvoted 1 times

DRAG DROP -

You have a computer that runs Windows 10 and contains two local users named User1 and User2.

You need to ensure that the users can perform the following actions:

User1 must be able to adjust the date and time.

User2 must be able to clear Windows logs.

The solution must use the principle of least privilege.

To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

### Groups

Administrators

Event Log Readers

Performance Log Users

Power Users

System Managed Accounts Group

### Answer Area

User1:

User2:

### Answer Area

#### Suggested Answer:

User1:

User2:

 **letters1234** Highly Voted 1 year, 4 months ago

As a twist, in Windows 11 a standard user can change the time without elevation. Make sure to read that this question says Windows 10.  
upvoted 13 times

 **volto** Highly Voted 1 year, 4 months ago

Answers are wrong

User1: "By default, only users with administrator rights in Windows 10 can change time and date settings."

User 2: "Restricting the Manage auditing and security log user right to the local Administrators group is the default configuration."

upvoted 13 times

 **Futfuyfyjfj** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/clear-eventlog?view=powershell-5.1>

upvoted 2 times

 **Garrick98** 1 year, 2 months ago

That is correct, "you must be a member of the Administrators group on the affected computer."

upvoted 2 times

 **Futfuyfyjfj** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/change-the-system-time#default-values>

upvoted 3 times

 **yhano** Most Recent 1 month, 2 weeks ago

User1: To adjust the date and time, User1 should be added to the Power Users group. This group has the necessary permissions to change the system time without granting full administrative rights1.

User2: To clear Windows logs, User2 should be added to the Administrators group. Only administrators have the rights to manage and clear event logs2.

upvoted 1 times

 **larry\_derby** 2 months ago

on my test Windows 10, hyper-v, works fine only Admin, account.

Power User, can't change time, Performance user can't clean events.



upvoted 2 times

🗨️ 👤 **Faceless\_Void** 5 months, 1 week ago

You have a computer that runs Windows 10 and contains two local users named User1 and User2.

You need to ensure that the users can perform the following actions:

User1 must be able to adjust the date and time.

User2 must be able to clear Windows logs.

The solution must use the principle of least privilege.

To which group should you add each user? what permission will you give to user1 and user2?

Copilot

Sent by Copilot:

To ensure that User1 and User2 can perform their respective tasks while adhering to the principle of least privilege, you should assign them to the appropriate groups and permissions:

User1 (Adjust the date and time):

Group: Add User1 to the Power Users group.

Permission: Grant the Change the system time permission through Local Security Policy or Group Policy.

User2 (Clear Windows logs):

Group: Add User2 to the Event Log Readers group.

Permission: Grant the Manage auditing and security log permission through Local Security Policy or Group Policy.

upvoted 2 times

🗨️ 👤 **Jt909** 5 months, 3 weeks ago

Administrators for both. Lab tested on Windows 10 22H2 domain-joined. With Power Users and Performance Log Users always access denied .

upvoted 8 times

🗨️ 👤 **LukeXtreme** 7 months, 1 week ago

Looks like the below is correct:

User1: Administrator; you need this for changing time and date however there is GPO policy you could set to go around it but that's not a possible answer here

User2 : Administrator; By default, only members of the Administrators group are able to clear the system logs. Workaround? You would need to change the Security Descriptor to allow users to clear the logs; however, this is a security-sensitive operation and should be done with caution.

upvoted 3 times

🗨️ 👤 **mail2bala3011** 9 months, 1 week ago

I just tested on my lab

User1: Administrator

User2 : Administrator

Administrator can perform both action

upvoted 7 times

🗨️ 👤 **sergioandreslq** 10 months, 1 week ago

User1: The Power Users group is able to install software, manage power and time-zone settings, and install ActiveX controls, actions that limited Users are denied.

User 2: Only administrator

upvoted 2 times

🗨️ 👤 **MR\_Eliot** 10 months, 2 weeks ago

In Windows 10 & 11 you can change the timezone without any admin privileges. However when you want to change the date and time settings, it will ask you for admin permissions.

So my answers:

1: Administrators

2: Administrators. Performance log users can only schedule collection of logs. Not remove the system logs.

upvoted 2 times

🗨️ 👤 **Softeng** 10 months, 2 weeks ago

- User 1: Administrator

- User 2: Administrator

<https://community.spiceworks.com/topic/2244141-power-users-vs-local-admins>

upvoted 1 times

🗨️ 👤 **Darkfire** 10 months, 3 weeks ago

User1: Administrator

User2: Administrator

Change system time = <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/change-the-system-time#default-values>

Clear eventlog = <https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/clear-eventlog?view=powershell-5.1>

Only Administrators can. The other user groups are not administrators.

upvoted 3 times

🗨️ 👤 **Judith1969** 10 months, 2 weeks ago

You are talking about domain joined in this case. I don't see any reference to that in this question. I am thing user 1: Power Users and user 2: Administrators.

upvoted 1 times

🗨️ 👤 **Merrybob** 11 months, 1 week ago

User 1: Power Users (they use the principle of least privilege and can change Time/Date settings and are still available in Windows 10)

User 2: Administrators (only the local administrators group members can delete Windows logs) Ref: <https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/clear-eventlog?view=powershell-5.1#description>

upvoted 1 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

- Administrators

- Administrators

upvoted 1 times

🗨️ 👤 **Tonsku** 1 year ago

user1: power users

user2: administrators

upvoted 3 times

🗨️ 👤 **belyo** 1 year ago

Power Users is a deprecated group since Vista, but according to some research they can change date & time | not sure why is present in tests...

<https://superuser.com/questions/241092/difference-between-power-user-and-administrator>

Performance Log Users is correct for clearing the event log

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#performance-log-users>

upvoted 1 times

🗨️ 👤 **yosry** 1 year, 1 month ago

answers should be :

User1: Administrator

User2: Administrator

User1: "By default, only users with administrator rights in Windows 10 can change time and date settings."

User 2: "Restricting the Manage auditing and security log user right to the local Administrators group is the default configuration."

upvoted 5 times

## HOTSPOT -

You have an Azure AD tenant named contoso.com.

You have the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	Ubuntu Linux

Which devices can be Azure AD joined, and which devices can be registered in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Azure AD joined:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2, and Device3 only
- Device1, Device2, Device3, and Device4

Registered in contoso.com:

- Device1 and Device2 only
- Device2 and Device3 only
- Device3 and Device4 only
- Device2, Device3, and Device4 only
- Device1, Device2, Device3, and Device4

### Answer Area


Suggested Answer:

Azure AD joined:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2, and Device3 only
- Device1, Device2, Device3, and Device4

Registered in contoso.com:

- Device1 and Device2 only
- Device2 and Device3 only
- Device3 and Device4 only
- Device2, Device3, and Device4 only
- Device1, Device2, Device3, and Device4

 **krzysztofbr** Highly Voted 10 months, 2 weeks ago

answers are correct

upvoted 13 times

 **Futfuyfj** 10 months ago

Azure AD join capable Devices: <https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-directory-join>

Azure AD registered Devices: <https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-device-registration>


upvoted 7 times

 **MR\_Eliot** Most Recent 4 months, 1 week ago

Answers are correct. You can only join Windows devices to Azure AD. You are also able to join Linux devices by installing Intune agent.

<https://learn.microsoft.com/en-us/entra/identity/devices/concept-device-registration>

upvoted 3 times

 **Darkfire** 4 months, 1 week ago

Answers are correct

Azure AD join capable Devices: <https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-directory-join>

Azure AD registered Devices: <https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-device-registration>

upvoted 2 times

🗨️ 👤 **Merrybob** 5 months, 1 week ago

Correct

upvoted 1 times

🗨️ 👤 **Amir1909** 5 months, 3 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **yosry** 6 months ago

seems correct

upvoted 1 times

🗨️ 👤 **kay000001** 7 months, 2 weeks ago

Answer are correct.

Can only AD join windows devices.

Can register any device.

upvoted 1 times

🗨️ 👤 **krzysztofbr** 10 months, 2 weeks ago

ad join win10 and 11

Ad registered all platforms including linux

upvoted 3 times

🗨️ 👤 **mirak123** 9 months, 3 weeks ago

shouldnt be opposite then

ad join is contoso.com (Directory name) so only 1 and 2

and Azure AD all devices so 1234

upvoted 1 times

HOTSPOT -

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

Name	Role
Admin1@contoso.com	Security Administrator
Admin2@contoso.com	Cloud Device Administrator
User1@contoso.com	None

You have a computer named Computer1 that runs Windows 10. Computer1 is in a workgroup and has the local users shown in the following table.

Name	Member of
Administrator1	Network Configuration Operators
Administrator2	Power Users
UserA	Administrators

UserA joins Computer1 to Azure AD by using user1@contoso.com.

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

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	<input type="radio"/>	<input type="radio"/>
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	<input type="radio"/>	<input type="radio"/>
Admin2@contoso.com can install software on Computer1.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> User1@contoso.com is a member of the local Administrators group on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2@contoso.com can install software on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>

**letters1234** 1 year, 4 months ago

Should be YNN, CDA is admin within azure portal. SA is also azure role and doesn't have local admin rights to make changes.  
upvoted 31 times

**Futfuyfj** 1 year, 3 months ago

Wat not YNY.

(Cloud) Device administrator role :

<https://techcommunity.microsoft.com/t5/microsoft-intune/as-a-device-admin-global-admin-how-can-i-install-software/m-p/2025358>

upvoted 4 times

**SajjH** 4 months, 3 weeks ago

Cloud Device Admin and Device/Global Admin are not same.

upvoted 1 times

**Alscoran** 1 year, 3 months ago

I don't think they can install anything on the local machine:

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

upvoted 2 times

**ExamKiller020** 1 year, 3 months ago


The link you provided doesnt clarify anything. In the article is probably referred to the 'Azure AD Joined Device Local Administrator' role and not the Cloud device Administrator role

upvoted 3 times

  **NoursBear** 11 months, 2 weeks ago

This article does not make sense, the person says they are global admin and device admin, the global admin group would be automatically inserted in the local admin group

upvoted 1 times

  **JP1900** Highly Voted 1 year, 4 months ago

letters1234 is correct, it is YNN.

upvoted 14 times

  **Tr619899** Most Recent 1 month, 1 week ago

YNN is the answer

upvoted 2 times

  **LionelDerBoven** 3 months, 3 weeks ago

Y

N



N

When device is joined in AAD it wil get local admin rights (for now).

Security admin is for administration of security feature in entra etc.. No local admin rights.

Same with cloud device administrator.

upvoted 2 times

  **oopspruu** 4 months, 2 weeks ago

YNN

As of now, user performing Join will become an admin. This can be managed in future with a preview setting currently rolling out.

Cloud Device Admin has only permission for Entra Device section and not the actual device.



Security Admin has no permission to any device management.

upvoted 1 times

  **mail2bala3011** 9 months ago

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#security-administrator>

upvoted 1 times



  **Softeng** 10 months, 2 weeks ago

YNN

Cloud Device Administrator role does not grant permissions to manage any other properties on the device:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#cloud-device-administrator>

upvoted 3 times

  **kaushik07** 10 months, 3 weeks ago

User1 have no roles assigned, but part of local "users" group, when UserA join the device1 using the user1 account it doesn't automatically elivate the user1's roles, user1 will still be an local user, will not become a member of local admins group.

upvoted 5 times

  **Merrybob** 11 months, 1 week ago

NYN is correct

upvoted 5 times

  **NoursBear** 11 months, 2 weeks ago

Manage regular users

By default, Microsoft Entra ID adds the user performing the Microsoft Entra join to the administrator group on the device. If you want to prevent regular users from becoming local administrators, you have the following options:

Windows Autopilot - Windows Autopilot provides you with an option to prevent primary user performing the join from becoming a local administrator by creating an Autopilot profile.

Bulk enrollment - a Microsoft Entra join that is performed in the context of a bulk enrollment happens in the context of an autogenerated user.

Users signing in after a device has been joined aren't added to the administrators group.

answers are correct

upvoted 2 times

🗨️ 👤 **NoursBear** 11 months, 2 weeks ago

I didn't mean the answers are correct from the question, but with YNN above  
upvoted 4 times

🗨️ 👤 **NoursBear** 11 months, 3 weeks ago

After further research, I have read that a cloud device administrator gets admin rights on the devices that are joined but NOT if they are hybrid joined. So now I don't know anymore about the 3rd answer. When reading about the role itself, it's not mentioning any of this.  
upvoted 1 times

🗨️ 👤 **NoursBear** 11 months, 3 weeks ago

I am now convinced that there is a confusion with the 2 roles "Microsoft Entra Joined Device Local Administrator" which is automatically added to the local devices and "Cloud Device Administrator" and I think this confusion is also on Microsoft community blogs, some MS employees are answering wrong stuff so I am now satisfied with a No for 3rd answer  
upvoted 1 times

🗨️ 👤 **belyo** 1 year ago

i would vote for NO,NO,NO

during the join operation security principals of the user are temporary added to local admin group, not the user itself, even if not so thats temporary

security admin cannot configure firewall & defender on that computer

cloud device admin cant install anything

upvoted 2 times

🗨️ 👤 **yosry** 1 year, 1 month ago

the first answer is NO:

tested it on my tenant (joining a device using a user profile does not add it to the Administrators Group)

Proof that the second answer is YES:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#security-administrator>

this is proof that the third answer is NO:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#cloud-device-administrator>

upvoted 12 times

🗨️ 👤 **iTomi** 1 year, 1 month ago

YES

At the time of Microsoft Entra join, we add the following security principals to the local administrators group on the device:

\* The Microsoft Entra Global Administrator role

\* The Microsoft Entra Joined Device Local Administrator role

\* The user performing the Microsoft Entra join

<https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin>

NO

Question is "Admin1@contoso.com can configure the firewall and Microsoft Defender ON COMPUTER1." Security administrator doesn't have local admin rights to modify firewall and defender settings ON COMPUTER1.

NO

This is a privileged role. Users in this role can enable, disable, and delete devices in Microsoft Entra ID and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#cloud-device-administrator>

upvoted 5 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

Cloud Device Administrator:

With Cloud Device administrator role, you can Delete/Disable/Enable devices in Azure Active Directory but you cannot Add/Remove Users in the directory.

With User administrator role, you can Add/Remove users in Azure AD but cannot Delete/Disable/Enable the devices.

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

Security Administrator

Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.

It is a Privileged role, but unable to understand what that actually means

upvoted 1 times

  **benpatto** 1 year, 1 month ago

By default, Microsoft Entra ID adds the user performing the Microsoft Entra join to the administrator group on the device. If you want to prevent regular users from becoming local administrators, you have the following options:

upvoted 2 times

  **benpatto** 1 year, 2 months ago

You have to be assigned to the local admin group, it doesn't come as default once you join to azure. <https://learn.microsoft.com/en-us/answers/questions/1300903/azure-ad-joined-device-local-administrator-role-to>

upvoted 1 times




Your network contains an Active Directory domain. The domain contains a user named Admin1. All computers run Windows 10. You enable Windows PowerShell remoting on the computers. You need to ensure that Admin1 can establish remote PowerShell connections to the computers. The solution must use the principle of least privilege. To which group should you add Admin1?

- A. Access Control Assistance Operators
- B. Remote Desktop Users
- C. Power Users
- D. Remote Management Users

**Suggested Answer: B**

Community vote distribution

D (97%)

 **letters1234** Highly Voted 1 year, 4 months ago

**Selected Answer: D**

Remote Management Users Group provides the effective rights for PS remote/remote connection. Remote Desktop Users doesn't, would also require also having local Administrator permission, not least privilege having two roles where one defined role will do.

[https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about\\_remote\\_requirements?view=powershell-7.3](https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_requirements?view=powershell-7.3)

User permissions - To create remote sessions and run remote commands, by default, the current user must be a member of the Administrators group on the remote computer or provide the credentials of an administrator. Otherwise, the command fails.

upvoted 16 times

 **SajjH** Most Recent 5 months, 1 week ago

From: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#remote-management-users>

Use the Remote Management Users group to allow users to manage servers through the Server Manager console. Use the "WinRMRemoteWMIUsers\" group to allow users to remotely run Windows PowerShell commands.

As such using "Remote Management Users" group is not an option. However, to allow execution of Powershell commands, administrator privilege on the remote desktop is required. So I'm confused. I don't think it's a well thought question, I couldn't find anything that relates Powershell to Remote Desktop Users group.


upvoted 1 times

 **CJL324** 7 months, 2 weeks ago

D. Remote Management Users

This group specifically grants users the ability to connect to the computer using PowerShell remoting. Adding Admin1 to this group will provide the necessary permissions for remote PowerShell connections without granting unnecessary privileges.

upvoted 2 times

 **Haider\_Raza** 9 months, 3 weeks ago

**Selected Answer: D**

To ensure that Admin1 can establish remote PowerShell connections to the computers using the principle of least privilege, you should add Admin1 to the D. Remote Management Users group. This group is specifically designed to give users the necessary permissions to manage the computer remotely without granting them more permissions than necessary, which aligns with the principle of least privilege.

upvoted 1 times

 **zeos\_ucok** 9 months, 4 weeks ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#remote-management-users>

upvoted 1 times

 **mestorrent86** 9 months, 4 weeks ago

**Selected Answer: D**

D. Remote Management Users: This group is designed for remote management tasks and is the correct choice for our scenario. It grants the necessary permissions for PowerShell remoting without granting full administrator rights.


Therefore, to ensure that Admin1 can establish remote PowerShell connections with the principle of least privilege, we should add Admin1 to the Remote Management Users group.

Correct answer is D

Documentation

<https://4sysops.com/archives/powershell-remoting-without-administrator-rights/>


<https://helpcenter.gsx.com/hc/en-us/articles/202447926-How-to-Configure-Windows-Remote-PowerShell-Access-for-Non-Privileged-User-Accounts>  
upvoted 1 times

 **MR\_Eliot** 10 months, 2 weeks ago

**Selected Answer: D**

D for sure

upvoted 1 times

 **Darkfire** 10 months, 2 weeks ago

**Selected Answer: D**

D is correct.

See Letters1234 comment..


upvoted 1 times

 **yafeci5971** 11 months ago

D is right answer

Get up-to-date <https://www.pinterest.com/pin/937522847419269960/>

upvoted 1 times

 **Krayzr** 11 months ago

**Selected Answer: D**

D. Remote Management Users

upvoted 1 times

 **Merrybob** 11 months, 1 week ago

D is right.

upvoted 1 times

 **Amir1909** 11 months, 4 weeks ago

D is correct

upvoted 1 times

 **onepunchkenshin** 12 months ago

ChatGPT tells D

upvoted 1 times

 **Tonsku** 1 year ago

**Selected Answer: D**

D. remote management users

upvoted 1 times

 **belyo** 1 year ago

**Selected Answer: D**

its about PowerShell remoting, not about RDP connections

definitely D

upvoted 1 times

 **NoursBear** 1 year, 1 month ago

I finally found the article proving D



<https://4sysops.com/archives/powershell-remoting-without-administrator-rights/>

upvoted 1 times

  **NoursBear** 1 year, 1 month ago



What is trick with this question the user is called Admin1, you'd expect it is an admin already, but where. A domain admin will have the privileges already and will not need group membership, they'll just have to give their admin credentials

upvoted 2 times

  **madsa** 1 year, 1 month ago

Answer is correct, it does not say less management it says least privilege.

upvoted 2 times

  **iTomi** 1 year, 1 month ago

Not quite.. Remote DESKTOP User doesn't give rights to use PowerShell Remote. Two different thing.

upvoted 1 times

## 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.

## Create profile

Windows PC

✓ Basics **2 Out-of-box experience (OOBE)** 3 Assignments 4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode * ⓘ	User-Driven
Join to Azure AD as * ⓘ	Azure AD joined
Microsoft Software License Terms ⓘ	Show Hide
<p><b>i</b> Important information about hiding license terms</p>	
Privacy settings ⓘ	Show Hide
<p><b>i</b> The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11</p>	
Hide change account options ⓘ	Show Hide
User account type ⓘ	Administrator Standard
Allow pre-provisioned deployment ⓘ	No Yes
Language (Region) ⓘ	Operating system default
Automatically configure keyboard ⓘ	No Yes
Apply device name template ⓘ	No Yes

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.

### 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

## Answer Area

Users who deploy a device by using Profile 1  
[answer choice].

Suggested Answer:

Users can configure the [answer choice]  
during the deployment.

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

computer name  
Cortana settings  
keyboard layout

 **fco168** Highly Voted 1 year, 1 month ago


I think for the second one should be the computer name.

- As the Apply Device Name Template is set to 'No'.

- The Keyboard Layout is set to 'automatically configure' and it does so from the Default System Language.

- Cortana is dead.

upvoted 13 times


 **LionelDerBoven** 3 months, 3 weeks ago

The second statement cannot be "computer name" because in the provided Autopilot profile, the option to "Apply device name template" is set to No. This means that users will not be able to configure or customize the computer name during the deployment process.

If the option "Apply device name template" were set to Yes, then the device might be configured with a specific naming convention, and users may or may not have the ability to modify it depending on the policy. But since it is set to No, the computer name will be automatically assigned, and users cannot modify it during the deployment.


Therefore, "keyboard layout" is the correct choice because users can configure the keyboard layout during the deployment, as the "Automatically configure keyboard" option is set to Yes, allowing for flexibility in keyboard layout selection during the setup process.

upvoted 1 times

 **F3RRY** 1 year, 1 month ago

RIP Cortana, they should make a new AI that can make powershell scripts with voice commands lol

upvoted 3 times

 **OyYaGotta** 9 months, 4 weeks ago

They should call it Copilot.

upvoted 9 times

 **Valavanchandran** 10 months, 4 weeks ago


if computer name template is not declared it takes name like DESKTOP-ADCDEFG or LAPTOP-ABCDEFG. Computername declaration is admin task. 1 is correct, 2 close one is keyboard otherwise question is dodgy

upvoted 2 times

 **picho707** Highly Voted 1 year, 3 months ago

On the second question, the deployment is user-driven so the user may be able to provide the computer name during the enrollment. This is a really bogus question.

upvoted 7 times

 **OyYaGotta** 9 months, 4 weeks ago

No deployment in config results in automatic name being applied. Does not give the user right to change, just doesn't apply a name set in Intune.

upvoted 1 times

 **Tr619899** Most Recent 1 month, 1 week ago

1. Users who deploy a device by using Profile1:

Answer: Users can modify the desktop settings only for themselves

Reason: The "User account type" in the Autopilot profile is set to Standard, meaning that users are not granted administrative privileges. This restricts them from modifying system-wide settings or creating additional local users. However, they can still modify their own user-specific desktop settings.

2. Users can configure the [answer choice] during the deployment:

Answer: Keyboard layout

Reason: The profile is configured to automatically configure the keyboard setting to "Yes." However, since "Language (Region)" is set to "Operating System Default," users may still have the option to confirm or adjust the keyboard layout during deployment, even though other settings (like Cortana or computer name) are not configurable during this process.

upvoted 1 times

🗨️ 👤 **yhano** 1 month, 2 weeks ago

for the 2nd question: Computer name, given that you did not set a device name in the autopilot registration. If "Apply device name template" is set to "No": You will be prompted to manually enter a device name during the Out-of-Box Experience (OOBE), provided you haven't set a name in the Autopilot registration.

upvoted 1 times

🗨️ 👤 **LionelDerBoven** 3 months, 3 weeks ago

The second statement cannot be "computer name" because in the provided Autopilot profile, the option to "Apply device name template" is set to No. This means that users will not be able to configure or customize the computer name during the deployment process.

If the option "Apply device name template" were set to Yes, then the device might be configured with a specific naming convention, and users may or may not have the ability to modify it depending on the policy. But since it is set to No, the computer name will be automatically assigned, and users cannot modify it during the deployment.

Therefore, "keyboard layout" is the correct choice because users can configure the keyboard layout during the deployment, as the "Automatically configure keyboard" option is set to Yes, allowing for flexibility in keyboard layout selection during the setup process.

upvoted 1 times

🗨️ 👤 **oopspruu** 4 months ago

I don't think there is any cortana setting in the Windows 11 setup. I hope the questions clarifies if its windows 10 OOBE or 11 OOBE.

upvoted 1 times

🗨️ 👤 **RomanV** 3 months, 2 weeks ago

There is.

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 2 weeks ago

I agree with the first one. Second one should be keyboard layout since cortana is dead and language setting are not configured

upvoted 2 times

🗨️ 👤 **Burkidur** 10 months, 1 week ago

But it says right there on the screenshot "Automatically configure keyboard: Yes"

upvoted 7 times

🗨️ 👤 **Merrybob** 11 months, 1 week ago

Can modify the desktop settings only for themselves - Unless there was a policy restricting this, it should work for a typical user

Keyboard Layout - Users can change that during the setup process.

upvoted 1 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

- can modify the Desktop settings only for themselves

- Computer Name

upvoted 5 times

🗨️ 👤 **Greatone1** 1 year ago

Correct answers is only for themselves and keyboard layout.

<https://www.examttopics.com/discussions/microsoft/view/64041-exam-md-101-topic-2-question-51-discussion/>

upvoted 3 times

🗨️ 👤 **madsa** 1 year, 1 month ago

Even if keyboard is set, while on the OOBE you can modify the Keyboard, as it just highlights it. So prevented from modifying any desktop settings and Keyboard.

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

The keyboard selection will appear to the user if the language is NOT set to a particular country, if OS Default is set, the user has a chance to change it there and then. In the profile creation you can check the little info thing against it

upvoted 1 times

🗨️ 👤 **LiamAzure** 1 year, 2 months ago

What a bunch are rubbish  
upvoted 2 times

🗨️ 👤 **ExamKiller020** 1 year, 3 months ago

Second answer: Keyboard layout  
Cortana is dead <https://support.microsoft.com/nl-nl/topic/end-of-support-for-cortana-d025b39f-ee5b-4836-a954-0ab646ee1efa>  
upvoted 2 times

🗨️ 👤 **NoursBear** 1 year, 3 months ago

There is no correct answer for the second one  
"If the Automatically configure keyboard is set to Yes, you won't be seeing the keyboard layout selection prompt in OOBE during deployment.  
Firstly you need to make the automatically configured keyboard set to No, and then select language if you make the selection to User Select."  
upvoted 1 times

🗨️ 👤 **BJS78** 1 year, 3 months ago

This is true only if you set the Region above fixed and not the using the default.  
upvoted 2 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

yes indeed I found out later that if the language is set to OS, then the user has a chance to change the keyboard layout again.....  
upvoted 2 times

🗨️ 👤 **letters1234** 1 year, 4 months ago

Agree with prevented from modifying any desktop settings.

Apply device name template: No

Doesn't create a template or pattern when naming your devices. The device will have the OEM name, such as DESKTOP-, followed by some random characters.

<https://learn.microsoft.com/en-us/autopilot/windows-autopilot-scenarios>

In Windows 10, version 1903 and later, Cortana voiceover and speech recognition during OOBE is DISABLED by default.

Old Intune Setting: Skip Cortana, OneDrive, and OEM registration setup pages.

On the above, most likely keyboard is correct. This question may not be in the final version of this exam as it doesn't reflect the current Intune settings. (Exam goes from beta to live from 6 Sept 2023).

upvoted 2 times

🗨️ 👤 **JP1900** 1 year, 4 months ago

Correct answers: are prevented from modifying any desktop settings  
and Keyboard Layout  
upvoted 2 times

🗨️ 👤 **HvD** 1 year, 2 months ago

Why would a normal user not be able to change any setting, like desktop background, volume, default printer, etc?  
upvoted 1 times

## HOTSPOT -

You have a server named Server1 and computers that run Windows 10. Server1 has the Microsoft Deployment Toolkit (MDT) installed. You plan to upgrade the Windows 10 computers to Windows 11 by using the MDT deployment wizard.

You need 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.

## 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 11 image and package only
- Windows 11 image and task sequence only
- Windows 11 image only
- Windows 11 image, task sequence, and package

**Answer Area**

**Suggested Answer:**

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 11 image and package only
- Windows 11 image and task sequence only**
- Windows 11 image only
- Windows 11 image, task sequence, and package

**650afa5** Highly Voted 6 months, 3 weeks ago

I took the exam yesterday June 11th. This question was on there.  
upvoted 6 times

**RomanoSmooth81** 5 months, 4 weeks ago

How did it go?  
upvoted 1 times

**Tr619899** Most Recent 1 month, 1 week ago

1. On Server1:  
Install the Windows Assessment and Deployment Kit (Windows ADK)

2. Add to the MDT deployment share:  
Windows 11 image and task sequence only  
upvoted 1 times

**Zoom2020** 4 months ago

ADK is pre-requisites to MDT. Since MDT is already installed, that means ADK is already on the server. Thus WDS should be the answer.  
upvoted 2 times

**ExamDumpEnjoyer** 8 months, 3 weeks ago

MDT is being deleted as of 26 April 2024. Question no longer relevant.  
upvoted 4 times

**Pollosor** 4 months, 3 weeks ago

What is your source?  
  
You can't say something so delicate like that out of nowhere.  
upvoted 1 times

**Dave808** 9 months, 1 week ago

Install the Windows Deployment Services (WDS) role on Server1. WDS is required for network-based deployments and is an essential component for MDT. It allows you to boot and deploy operating systems over the network.  
upvoted 1 times



🗨️ 👤 **OyYaGotta** 9 months, 4 weeks ago

WDS is not a pre-requisite for ADK. Answer is correct.  
upvoted 2 times

🗨️ 👤 **MR\_Eliot** 10 months, 2 weeks ago

Correct!  
upvoted 3 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

Answers are correct.  
upvoted 2 times

🗨️ 👤 **Softeng** 10 months, 2 weeks ago

ADK:

<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit#packages:~:text=MDT%20builds%20on%20top%20of%20the%20core%20deployment%20tools%20in%20the%20Windows%20Assessment%20and%2>

Image and task sequence only:

<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit#task-sequences> the 'Task sequence' section below 'Packages').

upvoted 3 times

🗨️ 👤 **Pisces225** 1 month, 1 week ago

This is the only correct answer in this discussion. ADK is a pre-req, WDS is also pre-req, but MSFT docs specify to start with ADK. MSFT docs also say to use language package, but they recommend to deploy those types of packages via WSUS. The dude saying WDS isn't a pre-req is wrong, and people saying that about the task sequence, "Task sequences are the heart and soul of the deployment solution."

Open both of these links, read this stuff for yourself, and you will also call BS on every other ignorant discussion here.

upvoted 1 times

🗨️ 👤 **Merrybob** 11 months, 1 week ago

Correct answers are:

Install the Windows ADK (Ref: <https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment-with-mdt#install-the-windows-adk>)

Windows 11 Image and Package Only - Only the Windows image and Application/Driver packages are needed. A task sequence will be used to deploy the OS, Apps, and Drivers. Ref: <https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit#deployment-shares>

upvoted 1 times

🗨️ 👤 **Anonymouse1312** 10 months, 2 weeks ago

Incorrect:

Windows ADK is a toolset containing : WCD, Win PE, DISM, SIM, USMT, VAMT, Windows Assessment Toolkit, and Windows Performance Toolkit. In order to deploy an image you need WDS, which is a server role.

Windows 11 image and task sequence are at the very minimum required.

A package is just extras.

upvoted 2 times

🗨️ 👤 **caskolo** 1 year ago

As I know Windows 11 not supported the MDT, Windows 11 deployment need Configuration Manager, so the Question might is wrong

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

Answer is correct.

upvoted 1 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

seems to be ok. not 100% sure

upvoted 3 times

🗨️ 👤 **Futfuyfyfj** 1 year, 3 months ago

Agreed:

ADK required in order to create a deployment share; <https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment-with-mdt#install-the-windows-adk>

upvoted 3 times

🗨️ 👤 **Futfuyfyfj** 1 year, 3 months ago

Win11 image and task sequence seems to be correct as well:

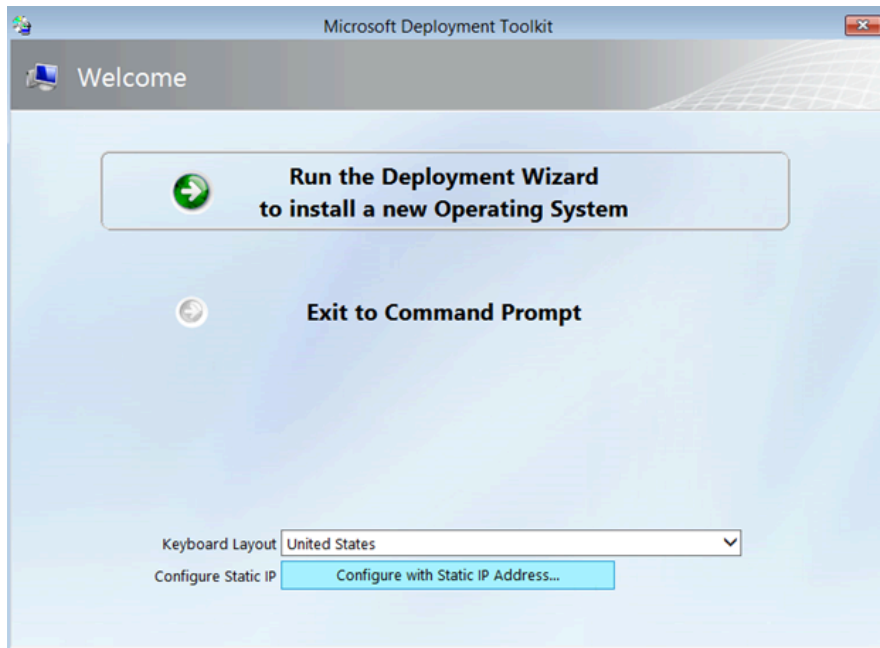
<https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference-image#create-the-reference-image-task-sequence>

upvoted 2 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.

**Actions**

**Answer Area**

- Modify the task sequence.
- Replace the ISO image.
- Modify the CustomSettings.ini file
- Modify the Bootstrap.ini file
- Update the deployment share.

1

2

3

Navigation arrows: right, left, up, down.

**Answer Area**

Suggested Answer:

- 1 Modify the CustomSettings.ini file
- 2 Modify the task sequence.
- 3 Update the deployment share.

JP1900 Highly Voted 1 year, 4 months ago

- Modify Bootstrap.ini
- Modify CustomSettings.ini
- Update deployment share

The CustomSettings.ini is a rules file processed by ZTIGather.wsf after the Bootstrap.ini is processed

The rules (CustomSettings.ini and Bootstrap.ini) make up the brain of MDT. The rules control the Windows Deployment Wizard on the client.

upvoted 31 times

iamchoy 2 weeks, 2 days ago

- Modify the Bootstrap.ini file
- Modify the CustomSettings.ini file

Replace the ISO image

Modifying the Bootstrap.ini file and the CustomSettings.ini file, and then replacing the ISO image with these changes will effectively prevent the welcome screen from appearing during the PXE boot process.

The steps to modify the task sequence and update the deployment share are not directly necessary to achieve this specific goal.

upvoted 1 times

🗨️ 👤 **SaiK1234** 10 months, 1 week ago

<https://www.examttopics.com/discussions/microsoft/view/80401-exam-md-101-topic-2-question-98-discussion/>

upvoted 1 times

🗨️ 👤 **Valavanchandran** 10 months, 4 weeks ago

incorrect bootstrap.ini is baked into ISO. Customsettings parses the variables for TS actions , correct answer, Modify bootstrap, update dep share and replace the iso by recreating it

upvoted 4 times

🗨️ 👤 **letters1234** Highly Voted 1 year, 4 months ago

<https://learn.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#SkipBDDWelcome>

-Configure Bootstrap

-Configure CustomSettings.ini

-Update Deployment Share (which updates the image used for MDT).

upvoted 18 times

🗨️ 👤 **Futfuyfyfj** 1 year, 3 months ago

Your reference proves your answer is correct!

upvoted 3 times

🗨️ 👤 **Tr619899** Most Recent 1 month, 1 week ago

1. Modify the Bootstrap.ini file

2. Update the Deployment Share

3. Replace the ISO Image

upvoted 2 times

🗨️ 👤 **LionelDerBoven** 3 months, 3 weeks ago

Modify the Bootstrap.ini file

The Bootstrap.ini file controls the initial settings that the computer uses when it first connects to the MDT server. To skip the welcome screen, you need to set the proper configurations here. You can add or modify settings such as SkipBDDWelcome=YES to bypass the welcome screen.

2. Modify the CustomSettings.ini file

The CustomSettings.ini file contains rules that MDT uses during the deployment process. These settings further customize the deployment experience and can also be used to control aspects like skipping screens. Adding entries like SkipWizard=YES can help prevent unnecessary user input during the deployment.

3. Update the Deployment Share

After making changes to the configuration files, you must update the deployment share so that the new settings are applied when computers connect to the MDT server. This step ensures the settings in the modified .ini files are applied in the LiteTouch PE environment.

upvoted 4 times

🗨️ 👤 **ExamDumpEnjoyer** 8 months, 3 weeks ago

MDT being deleted from the exam as of 26 April 2024. Question not relevant.

upvoted 9 times

🗨️ 👤 **LionelDerBoven** 3 months, 3 weeks ago

Only after september 17 2024

upvoted 2 times

🗨️ 👤 **Burkidur** 10 months, 1 week ago

It needs to be modified in both .ini files -- <https://www.reddit.com/media?url=https%3A%2F%2Fi.redd.it%2F301bxkpqsu221.png>

However, the order shouldn't matter. Normally for the questions where more than one order is valid, they make a note stating that fact and it's missing here.

upvoted 1 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

Incorrect.

1. Modify Bootstrap.ini

2. Modify CustomSettings.ini
3. Update deployment share

<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt#:~:text=The%20Bootstrap.ini%20file>

upvoted 2 times

🗨️ 👤 **Merrybob** 11 months, 1 week ago

Bootstrap.ini

CustomSettings.ini

Update Deployment Share

In that order.

"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."

Ref: <https://learn.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#SkipBDDWelcome>

upvoted 3 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

- Modify the CustomSettings.ini file

- Modify the BootStrap.ini file

- update the deployment Share

upvoted 3 times

🗨️ 👤 **yosry** 1 year, 1 month ago

Modify the bootstrap.ini file

Modify the CustomStettings.ini file

Update the deployment Share

upvoted 1 times

🗨️ 👤 **Contactfornitish** 1 year, 2 months ago

Need to modify both files bootstrap.ini and CustomSettings.ini since SkipBDDWelcome need to updated in both and since you updating bootstrap.ini, you would need to update deployment share. (would not have required if you updated only customsettings.ini

upvoted 1 times

🗨️ 👤 **RabbitB** 1 year, 3 months ago

1. Modify the Bootstrap.ini file

2. Update the deployment share

3. Replace the ISO image

upvoted 4 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

answer seems to be wron

should be

Modify the task sequence

Modify the bootstrap ini file (inside thsi file is seeting about Welcome Sreen)

Update the deployment share


<https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt>

upvoted 2 times

You use Windows Admin Center to remotely administer computers that run Windows 10.  
When connecting to Windows Admin Center, you receive the message shown in the following exhibit.

## This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

 [Go to your Start page](#)

Details

The website's security certificate is not yet valid or has expired.

Error Code:  
DLG\_FLAGS\_INVALID\_CA

[Go on to the webpage](#) (Not recommended)


You need to prevent the message from appearing when you connect to Windows Admin Center.  
To which certificate store should you import the certificate?

- A. Client Authentication Issuers
- B. Personal
- C. Trusted Root Certification Authorities


**Suggested Answer:** C

Community vote distribution

C (100%)


 **Vlado123** 4 months, 2 weeks ago

Correct answer is B, check on your device after installing Admin Center where is the certificate  
upvoted 1 times

 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: C**

Agreed  
upvoted 1 times


 **Darkfire** 10 months, 2 weeks ago

**Selected Answer: C**

C is correct.

<https://learn.microsoft.com/en-us/windows-hardware/drivers/install/trusted-root-certification-authorities-certificate-store>

upvoted 1 times


 **Amir1909** 11 months, 4 weeks ago

C is correct  
upvoted 1 times

 **fco168** 1 year, 1 month ago

**Selected Answer: C**

C it is!  
upvoted 1 times

 **ZaFletch** 1 year, 2 months ago

**Selected Answer: C**

Error references CA  
upvoted 3 times

🗨️ 👤 **letters1234** 1 year, 4 months ago

Selected Answer: C

Trusted Root

upvoted 2 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

You need "Certification Authorities"

answer C

upvoted 2 times

HOTSPOT -

You have an 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 11	Registered	None
Device2	Windows 10	Joined	None
Device3	Windows 10	Joined	Microsoft Intune

Contoso.com contains the Azure AD 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.

## Create profile

Windows PC

Basics
  Out-of-box experience (OOBE)
  Assignments
  **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	Self-Deploying (preview)
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	--

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 Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>



## Answer Area

	Statements	Yes	No
Suggested Answer:	If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
	If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
	If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input checked="" type="radio"/>	<input type="radio"/>

 **Crismo** Highly Voted 1 year, 3 months ago

NNY seems correct to me. Since device 1 and 2 are not enrolled in Intune, the deployment profile will have no effect on them.  
upvoted 20 times

 **airmancompsci** 1 year, 2 months ago

However, they are all in Azure AD, which is the requirement to use Autopilot. Part of the Autopilot process is to enroll in Intune per Microsoft as well as join it to AD (so device1 will switch from registered to joined is my guess - if anyone can test this I am curious).

Additionally, the big thing for Microsoft seems to be the hardware address. They don't seem to refer to device names at all, so I am guessing it shouldn't matter if they change?

<https://learn.microsoft.com/en-us/autopilot/user-driven>

My guess for the answer would be:

Yes - Device1 is part of Group1.

No - Device2 is part of Group2 which is nested in Group1. Autopilot doesn't work apply to nested groups.

Yes - Device3 is part of Group1.

I haven't been able to test this though, so if someone has a different answer please let me know.

upvoted 5 times

 **93831b0** 4 months ago

Device1 is registered = private in Entra (AAD).

upvoted 1 times

 **cpaljhc4** 1 year, 1 month ago

Windows Autopilot depends on specific capabilities available in Windows client and Microsoft Entra ID. "It also requires an MDM service such as Microsoft Intune."

Found this here: <https://learn.microsoft.com/en-us/autopilot/licensing-requirements>

upvoted 4 times

 **Drainev** 1 year ago

It surely requires an MDM service such as Microsoft Intune - To be set up!

It doesn't mean that devices have to be enrolled in Intune at all.

Since Autopilot enroll the device in Intune while the deployment, that would be weird for it not to work with unenrolled devices.

Tried it on Lab and it worked properly.

YNY!

upvoted 3 times

 **d3a3d8a** Most Recent 2 months ago

Nested groups work within Intune, but Device 2 will still not be converted. the reason Device 2 won't work here is because a device needs to be enrolled with Intune in order for it's Hardware Hash to be extracted. Entra cannot do that on its own. The answers are correct.

upvoted 2 times

 **Huffancs00** 3 months, 2 weeks ago

YNY:

guys if you check YES on "Convert all targeted devices to Autopilot" then: "Select Yes to register all targeted devices to Autopilot if they are not already registered. The next time registered devices go through the Windows Out of Box Experience (OOBE), they will go through the assigned Autopilot scenario." so it does not matter whether the device is already registered in MDM or not, all the devices targeted by the deployment

profile will start with the autopilot OOB. It basically says "yo idc if the devices in this group are MDM enrolled, just let them go through the assigned Autopilot scenario"

upvoted 3 times

🗨️ **Bart\_Hofstede** 4 months ago

You need an MDM. So it's no, no, yes

upvoted 3 times

🗨️ **MJFT** 8 months, 3 weeks ago

An existing device can automatically register if it's:

Running a supported version of Windows

Enrolled in an MDM service such as Intune

A corporate device that isn't already registered with Autopilot

<https://learn.microsoft.com/en-us/autopilot/automatic-registration#windows-autopilot-for-existing-devices>

upvoted 2 times

🗨️ **OyYaGotta** 9 months, 4 weeks ago

This is a tricky question. Windows Autopilot deployment profiles are configured as part of Mobile Device Management (MDM) in Intune, therefore, for this question, Autopilot doesn't deploy to devices without a deployment profile. Answer is correct N,N,Y.

upvoted 3 times

🗨️ **Darkfire** 10 months, 3 weeks ago

I also think its YNY

<https://learn.microsoft.com/en-us/autopilot/automatic-registration#windows-autopilot-for-existing-devices>

upvoted 1 times

🗨️ **kaushik07** 10 months, 3 weeks ago

Feature Azure AD Joined Azure AD Registered

Full OOTB experience with Intune Autopilot Yes No

Zero-touch deployment Yes Limited

Microsoft Account sign-in Yes No (Requires domain join)

Automatic company resource access Yes Requires additional steps

Given answer stands true

upvoted 1 times

🗨️ **Merrybob** 11 months ago

YNY

Using the setting Convert all targeted devices to Autopilot in the Autopilot profile doesn't automatically convert existing hybrid Microsoft Entra device in the assigned group(s) into a Microsoft Entra device. The setting only registers the devices in the assigned group(s) for the Autopilot service.

Ref: <https://learn.microsoft.com/en-us/autopilot/existing-devices>

Ref: <https://learn.microsoft.com/en-us/autopilot/existing-devices#register-the-device-for-windows-autopilot>

upvoted 1 times

🗨️ **mp34** 11 months, 2 weeks ago

I think the question here is has the device details been uploaded by .csv file, that is the requirement for Autopilot to work...

So, any device that is already in Intune will be deployed by Autopilot...any device that isn't, won't....

upvoted 3 times

🗨️ **mp34** 11 months, 2 weeks ago

So then the given answer is correct....

upvoted 2 times

🗨️ **NoursBear** 11 months, 3 weeks ago

OK this question is still annoying after the 3rd visit. I believe the information which is missing is whether Intune is configured for "automatic enrollment" I think we probably have assume that yes. In this case the computers assigned the profile but have MDM to No in the info, would still

get enrolled provided they are not personally owned

upvoted 1 times

🗨️ **tktk** 11 months, 4 weeks ago

YNY!!!

upvoted 1 times

🗨️ **frack** 11 months, 4 weeks ago

YNY

as long as the device is Autopilot-registered / Corporate ready image (SN uploaded/registered to intune), it is possible to run Autopilot enrollment.

upvoted 1 times

🗨️ **AdamRachel** 11 months, 3 weeks ago

device one it is not register in Intune.

upvoted 2 times

🗨️ **BJS78** 11 months, 4 weeks ago

First and seconds devices are private devices quite likely, so we DON'T want them managed by Autopilot.

Also suggested by MS:

"Don't register to Autopilot the following types of devices:

Microsoft Entra registered, also known as "workplace joined"

Intune MDM-only enrollment

These options are intended for users to join personally-owned devices to their organization's network."

Based on this fine article - <https://call4cloud.nl/2020/05/intune-auto-mdm-enrollment-for-devices-already-azure-ad-joined/> - it seems you MUST have MDM-coverage for the device to be able to use with Autopilot. (Not only Intune could be used)

upvoted 1 times

🗨️ **belyo** 1 year ago

one of the benefits of autopilot is to automatically join azure ad & automatically enroll to intune

so here the status of registered/joined/enrolled makes totally no sense

really not sure does it support nesting in assignments so i vote

Y N Y

upvoted 1 times

🗨️ **mhmyz** 1 year ago

YNY

Device1 & Device3 are part of Group1.

"Convert all targeted devices to Autopilot"=Yes,so current device status is not concerned.

<https://learn.microsoft.com/en-us/autopilot/automatic-registration#windows-autopilot-for-existing-devices>

upvoted 3 times

🗨️ **ckmay** 10 months, 3 weeks ago

Device 1 is in group 1 but.... it is only entra registered (workplace joined), and not entra joined. devices that are entra registered are marked as personally owned and if automatic enrollment to intune is turned on, it will not enroll personally owned devices into intune, only corporate.

I can't find it now but I'm pretty sure a self-deploying enrollment profiles will not apply to personally owned devices.

Honestly our speculation is basically worthless without knowing whether or not these devices even have had their HWID hashes uploaded to Intune and are registered for autopilot. If they are not Autopilot registered, then the answer is NNN.



Otherwise, I am going with NYY.

upvoted 2 times

🗨️ **ckmay** 10 months, 3 weeks ago

For device 2, I can find NO evidence that being in a nested group would prevent it from being targeted. I have actually read some articles from microsoft employees that actually said the opposite. The article was about optimizing intune performance by not making tons of different groups when 1 or a few would achieve the same thing and require less reprocessing for Intune. This was in reference to groups with 10,000 plus devices. A better practice that was suggested was to create an empty group and over the period of 3 days add 3 different groups in the empty group that each had 30k+ devices. this was to spread the workload out and they had 0 concern for devices not getting targeted because of the nesting.

upvoted 1 times

  **ckmay** 10 months, 2 weeks ago

Nesting: I see no mention of autopilot or device profiles behind not supported for group nesting. I found the following listed limitations.

(<https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-groups#add-or-remove-a-group-from-another-group>)

"We currently don't support:

Adding groups to a group synced with on-premises Active Directory.

Adding security groups to Microsoft 365 groups.

Adding Microsoft 365 groups to security groups or other Microsoft 365 groups.

Assigned membership to shared resources and apps for nested security groups.

Applying licenses to nested security groups.

Adding distribution groups in nesting scenarios.

Adding security groups as members of mail-enabled security groups.

Adding groups as members of a role-assignable group."

upvoted 1 times

  **Tati\_Oliveira** 1 year ago

YNY

When a Windows device starts in Out-of-Box (OOB) Mode, it means the device is in its initial state, ready for setup. What makes difference is if the device is registered on the Windows Autopilot via Hardware ID. That info is not provided, and I believe they are trying to make us getting mistakes when providing info that is registered to AAD. Considering that the device is registered with Windows Autopilot and will start in OOB Mode, initial state, what was provisioned is ignored and will start again. Device 1 and 3 are part of Group 1 which is assigned to Windows Autopilot Profile. Then for me will be Yes, No, Yes.

upvoted 3 times

HOTSPOT -

Your network contains an Active Directory domain. The domain contains 1,000 computers that run Windows 11.

You need to configure the Remote Desktop settings of all the computers. The solution must meet the following requirements:

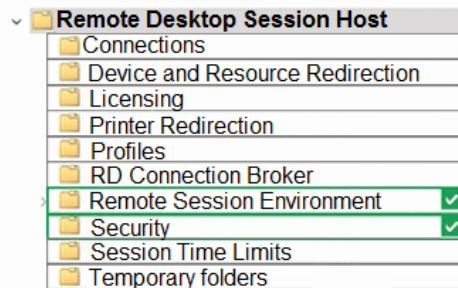
Prevent the sharing of clipboard contents.

Ensure that users authenticate by using Network Level Authentication (NLA).

Which two nodes of the Group Policy Management Editor should you use? To answer, select the appropriate nodes in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area



**Suggested Answer:**

A screenshot of the Group Policy Management Editor, similar to the one above. The 'Remote Desktop Session Host' folder is expanded. The 'Device and Resource Redirection' and 'Security' folders are highlighted with red boxes, indicating they are the suggested answers. The 'Remote Session Environment' folder also has a green checkmark in the right margin.

**letters1234** Highly Voted 1 year, 4 months ago

Device and Resource Re-direction and Security are the two answers

From GPO (Allow users to connect remotely by using Remote Desktop Services):

You can limit which clients are able to connect remotely by using Remote Desktop Services by configuring the policy setting at Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require user authentication for remote connections by using Network Level authentication.

upvoted 22 times

**BJS78** Highly Voted 1 year, 3 months ago

Clipboard --> Device and Resource Redirection \ Do not allow Clipboard redirection

NLA --> Security \ Require user authentication for remote connections by using NLA

upvoted 13 times

**Temptset** 1 year, 2 months ago

This is the correct answer. You can double check it yourself when opening Local Group Policy Editor in Windows: expand Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> (Device and Resource Redirection / Security)

upvoted 2 times

**Tr619899** Most Recent 1 month, 1 week ago

Answer is: Device and Resource Re-direction and Security

upvoted 1 times

**Merrybob** 11 months, 1 week ago

Device and Resource Redirection (Clipboard Redirection)

Security (NLA)



upvoted 2 times

**Amir1909** 11 months, 4 weeks ago

- Device and Resource Redirection

- Security

upvoted 1 times

  **Krayzr** 12 months ago

Device and Resource Re-direction

Security

upvoted 2 times

  **cpaljchc4** 1 year, 1 month ago

1. Prevent Clipboard Sharing:

• Navigate to: Computer Configuration → Policies → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Device and Resource Redirection.

• Look for the policy "Do not allow clipboard redirection" and set it to Enabled. This prevents the sharing of clipboard contents during Remote Desktop sessions.

2. Network Level Authentication (NLA):

• Navigate to: Computer Configuration → Policies → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Security.

• Find the policy "Require user authentication for remote connections by using Network Level Authentication" and set it to Enabled. This ensures users authenticate via Network Level Authentication (NLA) for remote connections.

This the answer by got

upvoted 4 times

## HOTSPOT -

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

Azure AD joined Windows devices enroll automatically in Intune.

You have the devices shown in the following table.

Name	Operating system	Azure AD joined	Line-of-business (LOB) apps installed
Device1	64-bit version of Windows 10 Pro	Yes	No
Device2	32-bit version of Windows 10 Pro	No	Yes
Device3	64-bit version of Windows 10 Pro	No	Yes

You are preparing to upgrade the devices to Windows 11. All the devices are compatible with Windows 11.

You need to evaluate Windows Autopilot and in-place upgrade as deployment methods to implement Windows 11 Pro on the devices, while retaining all user settings and applications.

Which devices can be upgraded by using each method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Windows Autopilot:

In-place upgrade:

**Answer Area**

Suggested Answer:

Windows Autopilot:

In-place upgrade:


 **Casticod** Highly Voted 1 year, 3 months ago

someone explain me how to upgrade From Windows 11 from autopilot?

In the first option I think None of the devices

In the second 1 & 3 (2 it's 32 beats)

upvoted 30 times

 **ExamKiller020** Highly Voted 1 year, 3 months ago

Bit of a vague question. The question states: while retaining all user settings and applications.

Windows autopilot is possible on all devices (upload hash) but it will wipe all data. So is the answer then 'non of the devices'?

The inplace update is only possible on device 1 and 3 because there doesnt exist a 32bit version of W11



Correct me if im wrong

upvoted 12 times

 **cpaljchc4** 1 year, 1 month ago



It says all devices is compatible with Win 11 but there is a 32 bit machine..

upvoted 3 times

  **iTomi** 1 year, 1 month ago

Win10 OS can be 32-bit or 64-bit version, even device is 64-bit. Win11 offer only 64-bit version and always need 64-bit device.

upvoted 4 times

  **Casticod** 1 year, 2 months ago

With windows autopilot we cannot update Windows versions.

To update to Windows 11 we would need to configure the updates but that section is no longer within autopilot. Your question would be well posed, if instead of Autopilot, in the question, put Intune.

(at least I think so)

upvoted 3 times

  **Tr619899** Most Recent 1 month, 1 week ago

1. None of the Devices

2. Device 1 and 3 only

upvoted 1 times

  **AleFCI1908** 2 months ago

autopilot: none, only dev1 can, but only with wipe because autopilot, so: no

in place: 32 bit need a wipe, so dev1 no. dev1 and dev3 yes

upvoted 1 times

  **dnt91** 4 months ago



Answer is correct because you have the sentence "Azure AD joined Windows devices enroll automatically in Intune." so Device1 is the only registered in intune and then it will get the autopilot deployment Profile. As there is no Windows 11 32 bit version in place upgrade is not possible for Device 2

upvoted 1 times

  **TempestWithin** 4 months ago

If I read the question correctly it states that all the devices are compatible with Windows 11. Which could be true if you reinstall the OS software with 64-bit (as long as the hardware can install 64-bit which it states saying they are compatible with Windows 11). Even though installing a in-place upgrade on a 32-bit wouldn't work because windows 11 doesn't accept 32-bit workstation, so a re-installation should be needed to do that. So yeah Device 1, and Device 2 are able to do a in-place upgrade.

upvoted 1 times

  **oopspruu** 5 months, 2 weeks ago

There is no Windows 11 32-bit so upgrade to 32Bit OS is not possible. Upgrade to 64-bit would need a wipe which won't work with the question.



Also you can upload the device hash but to truly make them autopilot devices, they'll need a wipe.

Hence:

None

Device 1 and 3

upvoted 1 times

  **Raziellucas** 9 months, 3 weeks ago

- None (Autopilot doesn't upgrade windows versions, it leverage existing OEM installed)

- Device1 and Device3 only due the 32 bit of device 2



upvoted 3 times

  **Merrybob** 11 months ago

Windows Autopilot: None of the devices. [User settings and app will not be retained using any Autopilot scenarios]

In-place Upgrade: Device 1 & 3 only [Device 2 is 32-bit and not eligible]

upvoted 8 times

  **St\_Ives** 10 months, 2 weeks ago

it took me a few times to re-read the part on AutoPilot, but I go for this answer.

upvoted 1 times

  **Pugmohone** 11 months, 1 week ago

The answer is correct as is.

The questions asks how to upgrade. Autopilot will only run on a device that is enrolled in Autopilot (i.e. - the hardware hash has been uploaded.) All devices enrolled in Autopilot have an Entra Joined entry.



Without knowing anything else, my assumption is that Device 1 will run autopilot and upgrade to Windows 11. There is no line of business app preventing it. Users settings will hopefully be saved in cloud. (That is my only concern with this question). Otherwise the other two devices are not entra joined so we cannot assume they are enrolled in autopilot. The second part of the question will in place upgrade both and retain user info for sure, 32 bit not supported as already discussed.

upvoted 1 times

🗨️ 👤 **AdamRachel** 11 months, 3 weeks ago

Only device 1 can be upgrade by using Autopilot as only this device is automatically enrolled in Intune. Autopilot require MDM service such as Intune. Device 2 and 3 are not enrolled in Intune so they can not be upgrade by Autopilot.

upvoted 1 times

🗨️ 👤 **[Removed]** 11 months, 3 weeks ago

Also Device 2 is 32 bit.

upvoted 1 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

- None

- Device1 and Device3 only

upvoted 4 times

🗨️ 👤 **mp34** 1 year ago

according to this link you can update via Autopilot, but only after you login and Feature updates are installed - <https://learn.microsoft.com/en-us/mem/intune/protect/windows-10-feature-updates#limitations-for-feature-updates-for-windows-10-and-later-policy>

upvoted 1 times

🗨️ 👤 **Tati\_Oliveira** 1 year ago

Windows Autopilot is a powerful tool for deploying and managing Windows devices in an efficient and streamlined manner. However, it's essential to clarify that Windows Autopilot primarily focuses on device provisioning, which includes tasks like device registration, configuration, and deployment. Here are some key points related to your question:

Device Deployment and Configuration:

Windows Autopilot simplifies the initial setup of Windows devices by automating tasks such as domain join, app installation, and policy enforcement.

It doesn't directly handle Windows upgrades (upgrading from Windows 10 to Windows 11) as its primary purpose is to get devices ready for use.

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

The answer is correct due to the line of business app, I overlooked that.

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

The only possible answer here is 1 and 3 only on both

upvoted 1 times

🗨️ 👤 **Tr1v** 1 year, 1 month ago

Autopilot: None of the devices > Autopilot doesn't upgrade OS, and doesn't retain user data.

"You need to evaluate Windows Autopilot and in-place upgrade as deployment methods to implement Windows 11 Pro on the devices, while retaining all user settings and applications."

upvoted 4 times

DRAG DROP -

You have 100 computers that run Windows 10.

You plan to deploy Windows 11 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.

### Actions

Configure known folder redirection in Microsoft OneDrive.

Run `scanstate.exe`.

Run `loadstate.exe`.

Enable Enterprise State Roaming.

Create a system image Backup.

Deploy Windows 11.

Restore a system image backup.

### Answer Area

1



2



3



### Answer Area

Suggested Answer:

1

Run `scanstate.exe`.

2

Deploy Windows 11.

3

Run `loadstate.exe`.

**krzysztofbr** Highly Voted 1 year, 4 months ago

answers are correct

<https://learn.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax>

upvoted 7 times

**benpatto** Highly Voted 1 year, 2 months ago

This is yet another annoying one, yes the answers are theoretically correct but in ANY workplace known to man, you ALWAYS take a backup / snapshot of a device with user data on. Does Microsoft not actually deal with anything like this themselves for such vague questions?

upvoted 7 times

**oopspruu** Most Recent 5 months, 2 weeks ago

MDT is not even supposed to be on the exam anymore so I don't know how relevant these questions are. But given answers are correct, however weird they may be.

upvoted 2 times

**veliyath** 6 months ago

To retain user settings and user data while performing a wipe and load installation of Windows 11 on 100 computers, you should follow these steps in sequence:

Run `scanstate.exe`. This will capture the user state from the existing Windows 10 installations.

Deploy Windows 11. This will perform the wipe and load installation of the new operating system.

Run loadstate.exe. This will restore the user state to the new Windows 11 installations.

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

Provided answer is correct.

upvoted 2 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

Answer is correct

Run scanstate.exe

<https://learn.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax>

Deploy Windows 11

Run loadstate.ex

<https://learn.microsoft.com/en-us/windows/deployment/usmt/usmt-loadstate-syntax>

upvoted 2 times

🗨️ 👤 **Merrybob** 11 months ago

Sounds about right!

upvoted 2 times

🗨️ 👤 **frack** 11 months, 4 weeks ago

considering known folder redirection to onedrive was already configured, this is correct

upvoted 1 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

Letters is right, but the point here is not the use of KFM, as the combination of it with ESR will do the job the question is stating Wipe and Load installation, meaning the use of USM tool, and the answer is correct.

upvoted 1 times

🗨️ 👤 **letters1234** 1 year, 4 months ago

Reason it isnt KFM for data is that it only backs up specific folders and not all users Appdata folder etc.

upvoted 3 times

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.  
You use Microsoft Intune to manage devices.  
You use Windows Autopilot to deploy Windows 11 to devices.  
A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device.  
You need to ensure that when a deployment fails, the deployment logs can be collected.  
What should you configure?

- A. the automatic enrollment settings
- B. the Windows Autopilot deployment profile
- C. the enrollment status page (ESP) profile
- D. the device configuration profile

**Suggested Answer:** C

Community vote distribution

C (100%)

🗨️ **oopspruu** 5 months, 2 weeks ago

**Selected Answer: C**

"Turn on log collection and diagnostics page for end users" set to YES in ESP settings.  
upvoted 1 times

🗨️ **veliyath** 6 months ago

ChatGPT

To ensure that deployment logs can be collected when a Windows Autopilot deployment fails, you should configure the enrollment status page (ESP) profile.

The enrollment status page (ESP) in Windows Autopilot allows you to track the progress of the device provisioning process and can be configured to collect logs if the deployment fails.

Therefore, the correct answer is:

C. the enrollment status page (ESP) profile  
upvoted 2 times

🗨️ **MR\_Eliot** 10 months, 1 week ago

Answer is correct.  
upvoted 1 times

🗨️ **Darkfire** 10 months, 3 weeks ago

**Selected Answer: C**

Answer is correct

To deploy the ESP to devices, you have to create an ESP profile in Microsoft Intune. Within the profile, you can configure the ESP settings that control:

Visibility of installation progress indicators.

Device access during provisioning.

Time limits.

Allowed troubleshooting operations.

<https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status>

upvoted 2 times

🗨️ **Merrybob** 11 months, 1 week ago

**Selected Answer: C**

C

ESP allows users to collect troubleshooting logs

upvoted 1 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

Turn on log collection and diagnostics page for end users

Yes, the answer is correct.

upvoted 1 times

🗨️ 👤 **cpaljchc4** 1 year, 1 month ago

This is what I got from Chat GPT:

To enable the collection of deployment logs when a Windows Autopilot deployment fails, you'll want to adjust settings withing Microsoft Intune:

1. Enable Diagnostic Settings in Intune:

Go to Microsoft Endpoint Manager admin center

Navigate to Devices>Windows.Windows enrollment> Deployment profiles.

Choose the specific Autopilot deployment profile used for the deployments.

Within the profile settings, ensure that "Collect diagnostic logs" or similar options are enabled.

upvoted 1 times

🗨️ 👤 **frack** 11 months, 4 weeks ago

the premise is there's a support engineer. So manually collecting the log in ESP is the way to do it

upvoted 1 times

🗨️ 👤 **cpaljchc4** 1 year, 1 month ago

According to ChatGPT, setting up ESP is beneficial before deploying through Autopilot.

However, specifically for the purpose of collecting deployment logs when deployment fails, the critical aspects configuring the diagnostic settings within the Autopilot deployment profile. The ESP enhances the deployment process but might not directly influence the collection of logs during a failed deployment.

Configuring the diagnostic settings within the deployment profile is more directly linked to the collection of logs in case of a failed deployment.

upvoted 1 times

🗨️ 👤 **letters1234** 1 year, 4 months ago

**Selected Answer: C**

Also, here "Allow users to collect troubleshooting logs".

<https://learn.microsoft.com/en-us/autopilot/enrollment-status#esp-profiles>

upvoted 4 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

**Selected Answer: C**

the question is wrong.

because You have logs without any action

but If You would like give end user logs yes You have to setup ESP

<https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status>

\

upvoted 3 times

You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite.  
You use Microsoft Intune to manage devices.  
You have a device named Device1 that is enrolled in Intune.  
You need to ensure that User1 can use Remote Help from the Intune admin center for Device1.  
Which three actions should you perform? Each correct answer presents part of the solution.  
NOTE: Each correct selection is worth one point.

- A. Deploy the Remote Help app to Device1.
- B. Assign the Help Desk Operator role to User1.
- C. Assign the Intune Administrator role to User1.
- D. Assign a Microsoft 365 E5 license to User1.
- E. Rerun device onboarding on Device1.
- F. Assign the Remote Help add-on license to User1.

**Suggested Answer:** ABE

Community vote distribution

ABF (80%) ABD (16%) 4%

  **rmac** Highly Voted 1 year, 4 months ago

From my point of view, the solution is:

A,B,F

upvoted 13 times

  **SajjH** 5 months, 1 week ago

The question states Intune Suite is used, so the license for Remote Help add-on not required, so F is not correct.

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons#available-add-ons>

upvoted 2 times

  **SajjH** 5 months, 1 week ago

I'm not sure what Rerun device onboarding means, but if it is assigning a profile to the Device1 then 3rd answer could be E. Any thoughts?

upvoted 1 times

  **SajjH** 4 months, 3 weeks ago

There is difference in device name, in the first place it is called Devic1 and 2nd time it is called Device1. Should we consider it a typo or another device?



upvoted 1 times

  **rmac** 1 year, 4 months ago

reference:



<https://learn.microsoft.com/en-us/mem/intune/fundamentals/remote-help#prerequisites>

upvoted 2 times

  **fco168** 1 year, 1 month ago

The license is already assigned in the statement of the question.

upvoted 1 times

  **fco168** 1 year, 1 month ago

Disregard my previous comment. The license assigned is the O365, not the Intune Remote Help!

upvoted 1 times

  **Twindragon** Most Recent 4 weeks ago

Selected Answer: ABF

i will go with ABF

upvoted 1 times

  **Tr619899** 1 month, 1 week ago

- A. Deploy the Remote Help app to Device1
  - B. Assign the Help Desk Operator role to User1
  - F. Assign the Remote Help add-on license to User1
- upvoted 2 times

🗨️ 👤 **King\_shola** 3 months, 2 weeks ago

Selected Answer: ABF

This is the only correct answer  
upvoted 1 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

Selected Answer: ABF

1. The Remote Help add-on license is needed for both the user and admin.  
2. The Remote Help app needs to be installed on the device.  
3. The admin or user taking access needs appropriate role before doing so. MS goes by principle of least privilege so we go for F.  
upvoted 2 times

🗨️ 👤 **veliyath** 6 months ago

Selected Answer: ABF

To ensure that User1 can use Remote Help from the Intune admin center for Device1, you should perform the following actions:

Deploy the Remote Help app to Device1. The Remote Help app needs to be installed on the device to enable remote assistance.  
Assign the Help Desk Operator role to User1. This role provides the necessary permissions to perform remote assistance operations.  
Assign the Remote Help add-on license to User1. The Remote Help add-on license is required for using the Remote Help feature.  
Therefore, the three actions you should perform are:

- A. Deploy the Remote Help app to Device1.
  - B. Assign the Help Desk Operator role to User1.
  - F. Assign the Remote Help add-on license to User1.
- upvoted 3 times

🗨️ 👤 **veliyath** 6 months ago

To ensure that User1 can use Remote Help from the Intune admin center for Device1, you should perform the following actions:

Deploy the Remote Help app to Device1. The Remote Help app needs to be installed on the device to enable remote assistance.  
Assign the Help Desk Operator role to User1. This role provides the necessary permissions to perform remote assistance operations.  
Assign the Remote Help add-on license to User1. The Remote Help add-on license is required for using the Remote Help feature.  
Therefore, the three actions you should perform are:

- A. Deploy the Remote Help app to Device1.
  - B. Assign the Help Desk Operator role to User1.
  - F. Assign the Remote Help add-on license to User1.
- upvoted 2 times

🗨️ 👤 **Haider\_Raza** 9 months, 3 weeks ago

Selected Answer: ABF

CORRECT ANSWER  
upvoted 2 times

🗨️ 👤 **mestorrent86** 9 months, 3 weeks ago

Selected Answer: ABE

the correct actions are:

- \*\*B. Assign the Help Desk Operator role to User1.\*\*
- \*\*E. Rerun device onboarding on Device1.\*\*
- (Additional information: \*\*A. Deploy the Remote Help app to Device1\*\* is not explicitly required for User1 to use Remote Help, but it's a good practice to have the app installed on the device.)

Please note that assigning the Intune Administrator role or a Microsoft 365 E5 license is not directly related to enabling Remote Help specifically for User1 and Device1.

upvoted 1 times



🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

Correct answer is ABF:

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control-reference#help-desk-operator>

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/remote-help-windows>

upvoted 1 times

  **OyYaGotta** 9 months, 3 weeks ago



E5 includes the Remote help license. You don't need an additional license for remote help. A,B,E is correct.

upvoted 1 times

  **LionelDerBoven** 3 months, 3 weeks ago

The Remote Help add-on license is essential to unlock the feature for the user, even if they already have a Microsoft 365 E5 license. So no.

upvoted 1 times

  **Merrybob** 11 months, 1 week ago

**Selected Answer: ABF**

ABF

F because adding an Intune Remote Help add on is required as part of the pre-req (Ref: <https://learn.microsoft.com/en-us/mem/intune/fundamentals/re>

upvoted 1 times

  **Merrybob** 11 months ago

Ref: <https://www.prajwaldesai.com/intune-remote-help/>



upvoted 1 times

  **Merrybob** 11 months ago

Ref: [https://learn.microsoft.com/en-us/mem/intune/fundamentals/remote-](https://learn.microsoft.com/en-us/mem/intune/fundamentals/remote-help#:~:text=Enable%20Remote%20Help%20for%20your%20tenant%3A%20By%20default%2C%20Intune%20tenants%20aren%27t%20enabled%20for%2)

[help#:~:text=Enable%20Remote%20Help%20for%20your%20tenant%3A%20By%20default%2C%20Intune%20tenants%20aren%27t%20enabled%20for%2](https://learn.microsoft.com/en-us/mem/intune/fundamentals/remote-help#:~:text=Enable%20Remote%20Help%20for%20your%20tenant%3A%20By%20default%2C%20Intune%20tenants%20aren%27t%20enabled%20for%2)

upvoted 1 times

  **GlobalS** 11 months, 2 weeks ago

I read the question that User1 needs help rather than will be assisting others?

upvoted 1 times

  **Amir1909** 11 months, 4 weeks ago

A and B and F is correct

upvoted 1 times

  **kilat** 1 year ago

**Selected Answer: ABF**

ABF - looks good for me

upvoted 1 times

  **NoursBear** 1 year, 1 month ago

In case this helps anyone

<https://ctsdemos.azureedge.net/microsoft/Intune/remotehelp/RemoteHelpDemo.html>



upvoted 3 times

  **mks\_academy** 1 year, 1 month ago

**Selected Answer: ABD**

I think A,B,D. A and B are correct, nothing to say. The D answer better fit in the scenario because we don't need Administrator role, there is no need to rerun device onboarding and the add-on license is no needed cause we use intune suite

upvoted 2 times

  **madsa** 1 year, 1 month ago

AB and F is correct, here you have the full deployment <https://www.prajwaldesai.com/intune-remote-help/>

upvoted 1 times

  **mks\_academy** 1 year ago

Great guide! But we don't need the add-on license because the Intune Suite unifies all the features, as Remote Help.

Also in the guide says "To use Intune Remote Help, both the helper and the sharer must sign in with an Azure AD account", so we need to assign E5 license to User1

upvoted 2 times



You have a Windows 11 capable device named Device1 that runs the 64-bit version of Windows 10 Enterprise and has Microsoft Office 2019 installed.

You have the Windows 11 Enterprise images shown in the following table.

Name	Platform	Description
Image1	x64	Custom Windows 11 image that has Office 2021 installed
Image2	x64	Default Windows 11 image created by Microsoft


Which images can be used to perform an in-place upgrade of Device1?

- A. Image1 only
- B. Image2 only
- C. Image1 and Image2

**Suggested Answer: B**

Community vote distribution

B (100%)

 **letters1234** Highly Voted 1 year, 4 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios>

Existing applications are preserved through the process. So, the upgrade process uses the standard Windows installation media image (Install.wim). Custom images aren't needed and can't be used because the upgrade process is unable to deal with conflicts between apps in the old and new operating system.

upvoted 18 times

 **oopspruu** Most Recent 5 months, 2 weeks ago

**Selected Answer: B**

From: <https://learn.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios#in-place-upgrade>

Existing applications are preserved through the process. The upgrade process uses the standard Windows installation media image (Install.wim). "Custom images not only aren't needed, but they also can't be used. Custom images can't 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 10 and Contoso Timecard 3.0 in the Windows 11 image.

upvoted 1 times

 **veliyath** 6 months ago

**Selected Answer: B**

it is clear that custom images cannot be used for an in-place upgrade because the upgrade process cannot handle conflicts between apps in the old and new operating systems.

Therefore, only the default Windows 11 image created by Microsoft (Image2) can be used for the in-place upgrade of Device1.

The correct answer is:

B. Image2 only

upvoted 2 times

 **MR\_Eliot** 10 months, 1 week ago

You can perform in-place upgrade, only with the default Windows image. Anything else is not supported.

upvoted 4 times

 **Darkfire** 10 months, 2 weeks ago

**Selected Answer: B**

B is correct

Custom images not only aren't needed, but they also can't be used.

<https://learn.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios#:~:text=Existing%20applications%20are,Windows%2011%20image>.


upvoted 1 times

  **Merrybob** 11 months, 1 week ago

**Selected Answer: B**

Ref: <https://learn.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios#in-place-upgrade>

upvoted 1 times

  **Amir1909** 11 months, 4 weeks ago

B is correct

upvoted 1 times

  **poppinaz** 1 year, 2 months ago

Totally agree with you. Tried it in my Lab

upvoted 3 times

## HOTSPOT -

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant by using Azure AD Connect.

You use Microsoft Intune and Configuration Manager to manage devices.

You need to recommend a deployment plan for new Windows 11 devices. The solution must meet the following requirements:

Devices for the marketing department must be joined to the AD DS domain only. The IT department will install complex applications on the devices at build time, before giving the devices to the marketing department users.

Devices for the sales department must be Azure AD joined. The devices will be shipped directly from the manufacturer to the homes of the sales department users.

Administrative effort must be minimized.

Which deployment method should you recommend for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth point.

### Answer Area

Sales:

- Configuration Manager
- Windows Autopilot with automatic registration
- Windows Autopilot with manual registration
- Windows Autopilot with OEM registration

Marketing:

- Configuration Manager
- Windows Autopilot with automatic registration
- Windows Autopilot with manual registration
- Windows Autopilot with OEM registration

**Answer Area**

Sales:

- Configuration Manager
- Windows Autopilot with automatic registration
- Windows Autopilot with manual registration
- Windows Autopilot with OEM registration

Marketing:

- Configuration Manager
- Windows Autopilot with automatic registration
- Windows Autopilot with manual registration
- Windows Autopilot with OEM registration

**Suggested Answer:**

**letters1234** Highly Voted 10 months, 2 weeks ago

Correct, Configuration manager doesn't require AAD connectivity and Autopilot with OEM registration means you can send the devices direct to user.

upvoted 22 times

**Futfuyfyfj** 9 months, 3 weeks ago

Agreed

upvoted 1 times

**Rocky83** 9 months ago

Agreed

upvoted 1 times

**b3c32d7** Most Recent 1 month, 3 weeks ago

If all agree then..

upvoted 1 times

**MR\_Eliot** 4 months, 1 week ago

Answer is correct. Also the Marketing team computers, will also be able to join Entra ID with hybrid enrollment.

upvoted 1 times

🗨️ 👤 **Darkfire** 4 months, 2 weeks ago

Answers are correct

<https://learn.microsoft.com/en-us/autopilot/registration-overview>

upvoted 2 times

🗨️ 👤 **Merrybob** 5 months ago

Correct.

Marketing requires SCCM because it can be run using on-prem AD (AD DS) only. Intune needs Azure AD

Sales: OEM Registration - The manufacturer will provide the Hardware IDs for Autopilot to run effectively. The users will receive the device and be asked to log-in with their credentials before they can start the initialization of the device.

upvoted 2 times

🗨️ 👤 **Amir1909** 5 months, 3 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **Krayzr** 6 months ago

55. Given answer is Correct

upvoted 1 times

🗨️ 👤 **cpaljchc4** 7 months, 3 weeks ago

ChatGPT agreed too

upvoted 2 times



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. Import an OS package.
- B. Create a selection profile.
- C. Add a Gather task to the task sequence.
- D. Add a Validate task to the task sequence.


**Suggested Answer: B**


Community vote distribution

B (100%)



 **da\_terminator**  6 months, 3 weeks ago  
MDT was removed from the Exam in April 2024. Irrelevant to the exam  
upvoted 6 times


 **GreenJPGSandRAM**  8 months, 2 weeks ago  
MDT will be removed from the exam on Apr 26, 2024, so this question is no longer relevant  
upvoted 5 times



 **LionelDerBoven** 3 months, 3 weeks ago  
September 17 it wil.  
upvoted 2 times

 **CJL324**  7 months, 2 weeks ago  
B. Create a selection profile



A selection profile allows you to specify which drivers should be injected during the deployment process based on criteria such as hardware models. By creating a selection profile, you can ensure that only the necessary drivers for the targeted hardware model are installed during deployment, utilizing PnP detection  
upvoted 1 times

 **rcristiano** 10 months, 1 week ago  
  
B esta correto. Adicionar um novo perfil de seleção permite que você selecione a pasta com os novos drivers durante a configuração do compartilhamento de implantação do MDT. A implantação fará referência ao perfil de seleção para instalar os drivers.  
upvoted 1 times

 **MR\_Eliot** 10 months, 1 week ago  
Question is so vague, but answer is correct.  
You can use selection profile in MDT workbench.  
upvoted 1 times

 **Darkfire** 10 months, 3 weeks ago  
  
Answer is correct

Create folder structures in the Out-of-Box Drivers node in the Deployment Workbench to provide the level of control you want for deploying device drivers to target computers. The folder structure groups or categorizes device drivers so that you can select specific groupings or categories of drivers using selection profiles.  
<https://learn.microsoft.com/en-us/mem/configmgr/mdt/use-the-mdt>  
upvoted 1 times

 **Merrybob** 11 months ago  


B. Create a selection profile.

Ref: <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit#:~:text=Control%20which%20drivers%20are%20injected%20during%20the%20task%20sequence>.

upvoted 1 times

🗨️ 👤 **Tonsku** 1 year ago

**Selected Answer: B**

B. Create a selection profile.

<https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit>

upvoted 3 times

🗨️ 👤 **iamforksu** 1 year, 2 months ago

**Selected Answer: B**

B is correct I believe

upvoted 1 times

🗨️ 👤 **krzysztofbr** 1 year, 4 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt>

upvoted 2 times

You have an on-premises server named Server1 that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1. You need to ensure that MDT1 supports multicast deployments. What should you install on Server1?

- A. Multipath I/O (MPIO)
- B. Multipoint Connector
- C. Windows Deployment Services (WDS)
- D. Windows Server Update Services (WSUS)

**Suggested Answer:** C

Community vote distribution

C (100%)

 **GreenJPGSandRAM** Highly Voted 8 months, 2 weeks ago

MDT will be removed from the exam on Apr 26, 2024, so this question is no longer relevant  
upvoted 7 times

 **letters1234** Highly Voted 1 year, 4 months ago

**Selected Answer: C**

C as Windows Deployment Services is able to serve PXE requests. Couldn't find an exact article, but PowerShell cmdlet for WDS includes Get-WDSMulticastClient and other commands showing it is a feature of WDS.

<https://learn.microsoft.com/en-us/powershell/module/wds/get-wdsmulticastclient?view=windowsserver2022-ps>

upvoted 7 times

 **Futfuyfjfi** 1 year, 3 months ago

This is the article: <https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt#multicast-deployments>

upvoted 6 times

 **veliyath** Most Recent 6 months ago

To ensure that your MDT deployment share (MDT1) supports multicast deployments, you need to install Windows Deployment Services (WDS) on Server1. WDS provides the necessary multicast functionality to MDT.

Therefore, the correct answer is:

C. Windows Deployment Services (WDS)


upvoted 2 times

 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: C**

Answer is correct.

upvoted 1 times

 **Darkfire** 10 months, 3 weeks ago

**Selected Answer: C**

C is correct

Multicast requires that Windows Deployment Services (WDS) is running on Windows Server 2008 or later. In addition to the core MDT setup for multicast, the network needs to be configured to support multicast. In general, this configuration means involvement of the organization networking team to ensure that Internet Group Management Protocol (IGMP) snooping is turned on and that the network is designed for multicast traffic. The multicast solution uses IGMPv3.

<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt>

upvoted 1 times


 **Merrybob** 11 months ago

Selected Answer: C

C. Windows Deployment Services (WDS)

Ref: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831764\(v=ws.11\)#:~:text=Transmits%20data%20and%20images%20by%20using%20multicast%20functionality.](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831764(v=ws.11)#:~:text=Transmits%20data%20and%20images%20by%20using%20multicast%20functionality.)

upvoted 1 times



  **Tonsku** 1 year ago

Selected Answer: C

C. Windows Deployment Services (WDS)

<https://learn.microsoft.com/en-us/mem/configmgr/osd/deploy-use/use-multicast-to-deploy-windows-over-the-network>

upvoted 1 times

  **krzysztofbr** 1 year, 4 months ago

the answer is correct. multicast in this case requires WDS

upvoted 2 times



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 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. Windows Autopilot
- B. Microsoft Deployment Toolkit (MDT)
- C. a Windows Configuration Designer provisioning package
- D. Windows Deployment Services (WDS)

**Suggested Answer: C**

Community vote distribution

C (69%)

A (31%)

 **letters1234**  1 year, 4 months ago

**Selected Answer: C**

Autopilot would require resetting the device, provisioning package can be loaded during normal use of the OS. Doesn't require resetting/wiping etc.

upvoted 12 times

 **MR\_Eliot** 10 months, 1 week ago

In my experience all the new devices use out-of-box experience. From out-of-box experience you should be able to enroll the device in Intune by using Autopilot.

upvoted 1 times

 **benpatto** 1 year, 1 month ago

Agree with letters1234, every Auto-pilot case requires a full reset. If you sysprepped a device beforehand, it would allow to then auto-pilot after using MDT's task sequences but not needed here.

upvoted 1 times

 **Rylz** 4 months, 2 weeks ago

That is not correct, Sysprep doesn't delete apps, it's only preparing your computer by unregistering and cleaning some registry keys. Autopilot is the best way to go and has the least administrative effort.

upvoted 1 times

 **Tr619899**  1 week, 1 day ago

**Selected Answer: C**

A Windows Configuration Designer provisioning package is the best solution because it:

Upgrades Windows 10 Pro to Windows 10 Enterprise via subscription activation.

Joins the device to Azure AD.

Installs Microsoft Store apps.

Retains user-installed applications and settings.

Requires minimal user intervention, as the provisioning package can be deployed via USB, email, or other methods.

upvoted 1 times

 **458184c** 1 week, 3 days ago

**Selected Answer: A**

Intune Autopilot is an ideal solution for upgrading a retailer-bought Windows Pro laptop to Windows Enterprise while retaining existing applications. It streamlines the process through zero-touch provisioning, automatically upgrading the OS via Intune without reimaging the device. Autopilot ensures compliance with organizational policies, enables centralized management, and enhances security by enrolling the device into Azure Active Directory and Intune. This approach saves time, preserves user data and apps, and delivers a consistent, secure, and personalized setup aligned with corporate standards.

upvoted 1 times

🗨️ 👤 **Omerozb** 3 weeks, 3 days ago

**Selected Answer: C**

Ensure any application from user is retained, must be C, as autopilot requires full reset

upvoted 1 times

🗨️ 👤 **Tr619899** 1 month, 1 week ago

A. Windows Autopilot

upvoted 1 times

🗨️ 👤 **Alboo007\_rs007** 1 month, 1 week ago

**Selected Answer: A**

"The best" solution is Autopilot

upvoted 1 times

🗨️ 👤 **AleFCI1908** 2 months ago

**Selected Answer: A**

if intune joined, can do this with minimal effort

upvoted 1 times

🗨️ 👤 **Nav90** 2 months ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provision-pcs-for-initial-deployment>

upvoted 1 times

🗨️ 👤 **SSL2** 2 months, 1 week ago

**Selected Answer: A**

Windows Autopilot allows you to upgrade the computers to Windows 10 Enterprise, join them to Azure AD, and install Microsoft Store apps with minimal user intervention. It also ensures that any applications installed by the users are retained. This solution is designed to streamline the deployment process and provide a seamless experience for end users.

upvoted 1 times

🗨️ 👤 **Frank9020** 4 months, 1 week ago

**Selected Answer: A**

Windows Autopilot is the best choice for achieving the goal of upgrading from Windows 10 Pro to Windows 10 Enterprise, joining the computers to Azure AD, installing Microsoft Store apps, retaining user-installed applications, and minimizing user intervention.

upvoted 1 times

🗨️ 👤 **veliyath** 6 months ago

The best recommendation to achieve the goal of upgrading the computers to Windows 10 Enterprise, joining the computers to Azure AD, and installing several Microsoft Store apps while ensuring that any applications installed by the users are retained and minimizing user intervention is:

A. Windows Autopilot

Windows Autopilot is specifically designed for this type of scenario. It allows for the configuration and deployment of devices in a way that minimizes user intervention, retains user-installed applications, and can handle the upgrade to Windows 10 Enterprise and the joining of devices to Azure AD.

upvoted 3 times

🗨️ 👤 **SajjH** 5 months, 1 week ago

The question didn't mention anything about availability of Intune whereas Autopilot requires Intune. Based on this, using Autopilot is not a solution.

upvoted 1 times

🗨️ 👤 **rcristiano** 10 months, 1 week ago

**Selected Answer: C**

Resposta C. Use a ferramenta Designer de Configuração do Windows para criar pacotes de provisionamento para configurar facilmente dispositivos que executam o cliente Windows. O Designer de Configuração do Windows é usado principalmente por departamentos de TI para instituições empresariais e educacionais que precisam provisionar dispositivos BYOD (bring-your-own-device) e fornecidos por empresas.


upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: C**

Answer is C. Autopilot requires full device reset. Autopilot is not the same as Intune. It's the process of enrolling the device in Intune. C is a better solution, since it doesn't require device reset.

upvoted 2 times

  **Darkfire** 10 months, 3 weeks ago

**Selected Answer: C**

Definitely C

<https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages>

upvoted 1 times

  **Merrybob** 11 months ago

**Selected Answer: C**

C. a Windows Configuration Designer provisioning package

Ref: <https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages>

upvoted 1 times

  **Tonsku** 1 year ago

**Selected Answer: A**

More than one answer choice may achieve the goal. Select the BEST answer.

A & C

upvoted 1 times

  **belyo** 1 year ago

**Selected Answer: C**

a provisioning package would do an excellent job here - minimal user intervention & ability to upgrade versions  
autopilot can also make it work

upvoted 1 times

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 AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you modify the User settings and the Device settings.

Does this meet the goal?


A. Yes

B. No

**Suggested Answer: B**

Community vote distribution

B (100%)

 **letters1234** Highly Voted 1 year, 4 months ago

Entra Portal only has information around MFA/ESR/BitLocker/UserJoin-Register/LocalAdmin. To configure PIN would require Configuration Profile from Intune or GPO for AD / HAADJ devices.

upvoted 12 times

 **iTomi** Highly Voted 1 year, 1 month ago

**Selected Answer: B**

NO!

Intune > Devices > Configuration profiles > Create > New Policy > Windows 10 or later > Settings Catalog > Create > Windows Hello for Business.

upvoted 6 times

 **veliyath** Most Recent 6 months ago

No, modifying the User settings and Device settings in the Microsoft Entra admin center does not directly address the requirement to ensure users are prompted to set up a six-digit PIN. The PIN length and complexity settings are typically managed through Windows Hello for Business policies, which are configured using Group Policy or Intune.

Therefore, the correct answer is:

B. No

upvoted 1 times

 **Rogo86** 10 months ago

**Selected Answer: B**

B for sure

upvoted 1 times

 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: B**

Easy no.

upvoted 1 times

 **krzysztofbr** 1 year, 4 months ago

**Selected Answer: B**

agree with letters1234

upvoted 1 times

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 AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you create and assign a device restrictions profile.

Does this meet the goal?

A. Yes

B. No

**Suggested Answer: B**

Community vote distribution

B (75%)

A (25%)

 **MR\_Eliot** Highly Voted 10 months, 1 week ago

**Selected Answer: B**

Answer is NO. In device restriction policy, you can only configure password policy. There is nothing about the pin settings. For pin settings, you will need to configure Windows Hello for Business.

upvoted 5 times

 **veliyath** Most Recent 6 months ago

The device restrictions profile in Intune primarily manages password policies and does not include specific settings for PIN configuration. For configuring PIN settings, you need to use Windows Hello for Business policies.

Therefore, the correct answer is:

B. No

upvoted 4 times

 **Merrybob** 11 months ago

**Selected Answer: B**

B. No

You'd need a Windows Hello for Business config profile.

<https://learn.microsoft.com/en-us/mem/intune/protect/windows-hello#:~:text=In%20the%20Anniversary%20Update%2C%20these%20two%20PINS%20were%20merged%20into%20one%20single%20device%20PIN.%20Any>

upvoted 3 times


 **yosry** 1 year ago

**Selected Answer: B**

No

the answer is B

upvoted 1 times

 **iTomi** 1 year, 1 month ago

**Selected Answer: B**

NO!

Intune > Devices > Configuration profiles > Create > New Policy > Windows 10 or later > Settings Catalog > Create > Windows Hello for Business.

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

I also agree A yes is correct  
upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

Nope.. the correct way is in question 61. So this is a No now  
upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

This answer is wrong as to perform this action via Intune you need "Device Configuration Profiles - Identity protection", that is the way I have it setup for the company I work for. So correct answer is No.  
upvoted 3 times

🗨️ 👤 **frack** 11 months, 4 weeks ago

device configuration profile not restriction profile, correct. I agree, the answer is No.  
upvoted 1 times

🗨️ 👤 **Krayzr** 1 year, 1 month ago

**Selected Answer: B**

This is what Bing AI provided.

After further research, I found that to ensure users are prompted to set up a six-digit PIN when they join the Windows 10 devices to contoso.com, you need to configure the PIN complexity settings in the Intune policy1.

Here are the steps to do it:

Sign in to the Microsoft Intune admin center.

Go to Devices > Enroll devices > Windows enrollment > Windows Hello for Business.

The Windows Hello for Business pane opens.

Select from the following options for Configure Windows Hello for Business: Enabled. Select this setting if you want to configure Windows Hello for Business settings. When you select Enabled, other settings for Windows Hello are visible and can be configured for devices1.

The default PIN length is six characters, but you can enforce a minimum length of four characters. The maximum PIN length is 127 characters.

So, you can set the minimum length to six characters to ensure a six-digit PIN.

upvoted 1 times

🗨️ 👤 **Krayzr** 1 year, 1 month ago

Correction, Question says Intune admin center.

Answer "A"

upvoted 2 times

🗨️ 👤 **sbermejor** 1 year, 1 month ago

**Selected Answer: B**

I think answer is B. In device restriction profile you can configure password not pin. You can force the password to be only numbers but it's still a pin as it's not the same.

<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password>

upvoted 1 times

🗨️ 👤 **fco168** 1 year, 1 month ago

**Selected Answer: B**

Technically, the answer is B.

Because creating a Restrictions Profile does not meet the end. You can create an empty Restrictions profile and assign it or configure it for something else.

upvoted 1 times

🗨️ 👤 **benpatto** 1 year, 1 month ago

MDM Enrollment allows for Intune to then take over, which would allow for device config or even windows enrollment.

upvoted 1 times

🗨️ 👤 **Suresh\_2411** 1 year, 2 months ago

**Selected Answer: A**

should be Yes



upvoted 1 times

🗨️ 👤 **suresh08** 1 year, 3 months ago

Selected Answer: A

Yes, we can achieve it from device restriction.

upvoted 3 times

  **iTomi** 1 year, 1 month ago

NO!

Intune > Devices > Configuration profiles > Create > New Policy > Windows 10 or later > Settings Catalog > Create > Windows Hello for Business.

upvoted 1 times

  **letters1234** 1 year, 4 months ago

Correct, would need to be Enroll Devices \ Windows Enrollment \ Windows Hello for Business \ Minimum PIN Length. Or possibly a Device Configuration Policy.



upvoted 4 times

  **Futfuyfj** 1 year, 3 months ago

You are right it can be achieved with a WHfB config, but you can do it with a device restriction as well:

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#password>

upvoted 2 times

  **BJS78** 1 year, 3 months ago

Wrong. You can set PIN for iOS/Android, but for Windows only the password (not the PIN) can be controlled via Device restrictions.

upvoted 1 times

  **Futfuyfj** 1 year, 3 months ago

I guess you didn't read the article nor you checked Intune itself? Article says:

Required password type: Choose the type of password. Your options:

Not configured: Intune doesn't change or update this setting. By default, the OS might allow the password to include numbers and letters.

Alphanumeric: Password must be a mix of numbers and letters.

Numeric: Password must only be numbers.

So numeric is a PIN.....

upvoted 3 times

  **sbermejor** 1 year ago

Password and pin are different, regardless a password contains only numbers it's still a password. <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password>

upvoted 2 times

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 AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you configure the Windows Hello for Business enrollment options.

Does this meet the goal?

A. Yes

B. No

**Suggested Answer: A**


Community vote distribution

A (100%)

 **letters1234**  10 months, 2 weeks ago

Correct, confirmed Intune 2308 environment.

upvoted 8 times

 **Hadilsa** 3 months, 2 weeks ago

yes is correct

upvoted 1 times

 **Jeff777**  3 months ago

A is correct


upvoted 2 times

 **Haider\_Raza** 3 months, 2 weeks ago

**Selected Answer: A**

YES, IT is correct


upvoted 1 times

 **Haider\_Raza** 3 months, 2 weeks ago

**Selected Answer: A**

ANSWER IS CORRECT

upvoted 1 times

 **MR\_Eliot** 4 months, 1 week ago

**Selected Answer: A**

Yess. Answer is correct.

upvoted 1 times

 **ckmay** 5 months ago

**Selected Answer: A**

Only Windows Hello for Business allows changing this configuration and in order to apply a WHfB configuration, the device must be enrolled in Intune. In order to ensure devices are enrolled in Intune and configurations applied to it when joining AAD, Automatically Enroll Azure joined devices to Intune option must be enabled in the Intune admin center

upvoted 1 times

 **Krayzr** 5 months, 3 weeks ago

**Selected Answer: A**

A is Good

upvoted 1 times



🗨️ 👤 **NoursBear** 7 months, 1 week ago  
OK so the previous question with No was correct  
upvoted 2 times

🗨️ 👤 **fco168** 8 months ago  
**Selected Answer: A**  
YES.....  
upvoted 2 times

🗨️ 👤 **yosry** 8 months ago  
**Selected Answer: A**  
allah yarhmou walla rabi m3ah  
upvoted 2 times

Case study -

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 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 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 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	<i>Not applicable</i>	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	<i>None</i>
Policy2	Group2	Group3
Policy3	Group1	<i>None</i>

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.
- 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.
- 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 meet the technical requirements for the iOS devices.

Which object should you create in Intune?

- A. a deployment profile
- B. an app protection policy
- C. a device configuration profile
- D. a compliance policy

**Suggested Answer: C**

*Community vote distribution*

C (100%)

A: NO, because it just deployment profile.

B: NO

C: Correct

D: easy no. It's just for compliancy. does nothing else.

upvoted 1 times

🗨️ 👤 **Darkfire** 4 months, 2 weeks ago

**Selected Answer: C**

Answer is correct.

Block sending diagnostic and usage data to Apple: Yes prevents devices from sending diagnostic and usage data to Apple. When set to Not configured (default), Intune doesn't change or update this setting. By default, the OS might allow this data to be sent.

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-ios#settings-apply-to-all-enrollment-types-4>

upvoted 2 times

🗨️ 👤 **Merrybob** 5 months ago

**Selected Answer: C**

C. a device configuration profile

Ref: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-ios#settings-apply-to-all-enrollment-types-4>:~:text=Block%20sending%20diagnostic%20and%20usage%20data%20to%20Apple%3A%20Yes%20prevents%20devices%20from%20sending%20diagnosti

4:~:text=Block%20sending%20diagnostic%20and%20usage%20data%20to%20Apple%3A%20Yes%20prevents%20devices%20from%20sending%20diagnosti

upvoted 3 times

🗨️ 👤 **Tonsku** 6 months, 2 weeks ago

**Selected Answer: C**

C. a device configuration profile

upvoted 1 times

🗨️ 👤 **iamforksu** 8 months, 2 weeks ago

**Selected Answer: C**

Seem like C

upvoted 1 times

🗨️ 👤 **Futfuyfyfj** 10 months ago

C is correct, however telemetry is a bit of vague wording in relation to iOS

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-ios#settings-apply-to-all-enrollment-types-4>

upvoted 2 times

## HOTSPOT

-

## Case study

-

## 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 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 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 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	<i>Not applicable</i>	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	<i>Not applicable</i>	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	<i>Not applicable</i>	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	<i>None</i>
Policy2	Group2	Group3
Policy3	Group1	<i>None</i>

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.
- 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.
- 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 are evaluating which devices are compliant.

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

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is compliant.	<input type="radio"/>	<input type="radio"/>
Device4 is compliant.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device4 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

**Suggested Answer:**

**MR\_Eliot** Highly Voted 10 months, 1 week ago

Answers are correct:

Device 1:

Groups: Group1

Policies: Policy3

Result: Not compliant.

Device 3:

Groups: Group2, Group3

Policies: Policy1

Result: Compliant.

Device 4:

Groups: Group 2

Policies: Policy2

Result: Compliant

upvoted 14 times

**Tr619899** Most Recent 1 month, 1 week ago

Answer is: No, Yes, Yes

upvoted 1 times

**Engr001** 10 months, 1 week ago

I will go with N, N, Y

Device 3 will be a NO because it is an android device. Policy 2 will be applied because of group 2 (group 3 is excluded) but policy 2 goes for iOS devices. Because Group 3 isn't used and Group 2 is for iOS then device 3 will not be compliant. Am i wrong?

upvoted 1 times

**b47afda** 7 months, 2 weeks ago

Device 3 is in group 2 and 3, Policy 2 applies to group 2 but excludes group 3, therefore policy 2 will not apply to Device 3. Policy 1 applies only to group 3 so it will apply to Device 3 and be marked compliant.

upvoted 5 times

**Darkfire** 10 months, 2 weeks ago

Answer is correct. (NYY)

Device3 > member of group 2 & 3. Least privileges override, so Group3 = Policy1 > Is compliant  
upvoted 4 times

🗨️ 👤 **Tonsku** 1 year ago

N, Y, Y

The device compliance policies:

Policy1: Android. Require encryp Not configured

Policy2: iOS. Require encryp Not applicable

Policy3: Android. Require encryp Require

Device1: Android. Disable Encryp

Device1: Group1

Policy3: Android. Require encryp: Require

Policy3: Group1. Exclude None

Device3: Android. Disable Encryp

Device3: Group2 & Group3

Policy1: Group3. Exclude None

Policy1: Android. Require encryp: Not configured

Device4: iOS. Not applicable Encryp

Device4: Group2

Policy2: Group2. Exclude Group3

Policy2: iOS. Require encryp: Not applicable

upvoted 4 times

🗨️ 👤 **madsa** 1 year, 1 month ago

No Yes Yes is correct, sorry, Futfuyfyfj is 100% correct, this device will be affected by policy 1.

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

No No Yes or No Yes Yes, all comes down to the fact that devices are to be or not to be compliant if they have not policy assigned, in early questions someone was saying he did the exam and he got all points in questions were this argument is present, is devices with no policy are to be flagged as no compliant the answer is No Yes Yes otherwise is No No Yes.

upvoted 1 times

🗨️ 👤 **Suresh\_2411** 1 year, 2 months ago

NO

YES

YES

upvoted 2 times

🗨️ 👤 **picho707** 1 year, 2 months ago

Question 1:

Device1 belongs to Group1

Policy3 is assigned to Group1

Policy3 Settings = Android = Require = Assigned

Device1 Settings = Android = Disabled

The Policy requires encryption and Device encryption is disabled therefore the device is not compliant so answer is NO

upvoted 4 times

🗨️ 👤 **picho707** 1 year, 2 months ago

Question 2

Device3 belongs to group2 and group3

Policy1 and Policy2 are assigned to Groups2 and Groups3

Policy1 Settings = Android = Not Configured = Assigned

Policy2 Settings = IOS = Not Applicable = Assigned = Exclude Group3 so it will not apply.

Device3 Settings = Android = Disabled

The effective Policy requires encryption "Not Applicable" and Device encryption is "Disabled" therefore the device is compliant so answer is

Yes

upvoted 3 times



🗨️ 👤 **picho707** 1 year, 2 months ago

Question 3

Device4 belongs to Group2

Policy2 is assigned to Group2 and Group3

Policy2 Settings = IOS = Not Applicable = Assigned = Exclude Group3 but device does not belong to group 3.

Device4 Settings = IOS = Not Applicable

The Policy requires encryption "Not Applicable" and Device encryption is "Not Applicable" therefore the device is compliant so answer is Yes

upvoted 4 times

🗨️ 👤 **ExamKiller020** 1 year, 3 months ago

NO

YES

YES

upvoted 4 times

🗨️ 👤 **sh123df** 1 year, 3 months ago

No

? = Will the exclude or include over ride?

Yes

upvoted 1 times

🗨️ 👤 **Futfuyfj** 1 year, 3 months ago

Doesn't matter, the policy (2) is for iOS, the Devices is Android. So policy is not applicable

upvoted 3 times

🗨️ 👤 **BJS78** 1 year, 3 months ago

Wrong. Device 3 will be excluded from Policy2 due to ex: Group3 setting. The device will receive. N-Y-Y, answer is correct

upvoted 1 times

🗨️ 👤 **Futfuyfj** 1 year, 3 months ago

You need to learn and watch. Device 3 will be compliant because of the assignment on policy 1... policy 2 has nothing to do with device regardless exclusion or not.

upvoted 3 times

🗨️ 👤 **BJS78** 1 year ago

Never said, device3 is non-compliant. You are right, that policy 2 has no business here (I missed the iOS vs Andoird compliance), but your arrogance blinded you to see the - still correct - answer I wrote: N-Y-Y

upvoted 1 times

Case study -

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 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 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 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	<i>None</i>	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	<i>Not applicable</i>	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	<i>Not applicable</i>	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	<i>Not applicable</i>	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	<i>None</i>
Policy2	Group2	Group3
Policy3	Group1	<i>None</i>

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.
- 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.
- 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?

- Generalize the computers and configure the Device settings from the Microsoft Entra admin center.
- Extract the serial number of each computer to an XML file and upload the file from the Microsoft Intune admin center.
- Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune admin center.
- Generalize the computers and configure the Mobility (MDM and MAM) settings from the Microsoft Entra admin center.
- Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Intune admin center.

**Suggested Answer:** C

Community vote distribution

C (100%)

🗨️ 👤 **Krayzr** 3 months, 3 weeks ago

Selected Answer: C

C it is

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 4 months, 1 week ago

Answer is correct.

upvoted 1 times

🗨️ 👤 **Darkfire** 4 months, 2 weeks ago

Selected Answer: C

C is correct

<https://learn.microsoft.com/en-us/autopilot/add-devices>

upvoted 1 times

🗨️ 👤 **ckmay** 5 months ago

Selected Answer: C

C. Devices are already purchased so are not coming from OEM so in order for devices to pickup a Autopilot deployment profile when they are in the OOBE, they need to have their hardware IDs already registered with intune and since there is no mention of the OEMs or Vendors doing this step, it has to be done manually

upvoted 1 times

🗨️ 👤 **Tonsku** 6 months, 2 weeks ago

Selected Answer: C

office in Phoenix. Most of the users in the Phoenix office will work from home.

C. Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune admin center.

upvoted 1 times

🗨️ 👤 **fco168** 8 months ago

Selected Answer: C

Get the Hash IDs to provision using Autopilot.

upvoted 1 times

🗨️ 👤 **Kiookr** 9 months, 2 weeks ago

I think there is typo or wrong word "upload the file from the Microsoft Intune

Should be ==> "upload the file to the Microsoft Intune admin center."

Is "to" not "from" because you already downloaded the hash or hardware ID from the computer.

upvoted 3 times

🗨️ 👤 **Futfuyfyfj** 9 months, 2 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **Oslaf\_PSN** 8 months, 3 weeks ago

The wording on these questions is always debatable...

I think they mean "upload the file" (and where do you do this from?) "from the Intune Admin Center."

upvoted 2 times

🗨️ 👤 **Futfuyfyfj** 9 months, 2 weeks ago

Answer is correct.

upvoted 2 times

## HOTSPOT

-

## Case study

-

## 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 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 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 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	<i>Not applicable</i>	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	<i>Not applicable</i>	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	<i>Not applicable</i>	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	<i>None</i>
Policy2	Group2	Group3
Policy3	Group1	<i>None</i>

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.
- 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.
- 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.

What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

User1 can enroll a maximum of:

- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

User2 can enroll a maximum of:

- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

### Answer Area

Suggested Answer:

User1 can enroll a maximum of:

- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

User2 can enroll a maximum of:

- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

**Fortind1974** Highly Voted 1 year, 3 months ago

User 1: 10 devices

User 2: 1000

User2 is a device enrollment manager (DEM) in Intune, so device limit restrictions won't work on them.

<https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll#device-limit-restrictions>

upvoted 29 times

**Savior99** 10 months ago

Correct: "Device limit restrictions

DEM enrolls Windows 10/11 devices in shared device mode, so device limit restrictions won't work on them" . Source:

<https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll>

upvoted 1 times

**picho707** 1 year, 3 months ago

Device enrollment managers are affected by device limit restrictions in Intune. Device limit restrictions let you restrict the number of devices a user can enroll in Intune. Each restriction type comes with one default policy that you can edit and customize as needed. Intune applies the default policy to all user and userless enrollments until you assign a higher-priority policy. Therefore, if a device enrollment manager is also a user, they will be subject to the device limit restrictions set by the administrator.

upvoted 2 times

**Futfufyfj** 1 year, 3 months ago

Source?

upvoted 3 times



**picho707** 1 year, 3 months ago

Azure AD

Applying an Azure AD maximum device limit of less than 1,000 to a DEM account will prevent you from reaching the 1,000 device limit that the DEM account can enroll.



<https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll>

upvoted 5 times

  **Burkidur** 10 months, 1 week ago

That's Entra device limit restrictions, not Intune. The question says nothing about Entra restrictions, so it's safe to assume it's unlimited.

upvoted 2 times

  **fco168** 1 year, 1 month ago

The device enrollment restriction takes precedence over the privileges granted by the DEM role.

upvoted 5 times

  **Tr619899** Most Recent 1 month, 1 week ago

Answer is:

User1 can enroll a maximum of: 10 devices

- User1 is a member of GroupA, which has a device limit set by Restriction2 at 10 devices. The priority of Restriction2 (10 devices) takes precedence over the default restriction (5 devices).

User2 can enroll a maximum of: 1,000 devices

- User2 is a Device Enrollment Manager (DEM), and DEM accounts can enroll up to 1,000 devices regardless of other restrictions. This is a unique capability of DEM accounts to allow bulk device enrollment.

upvoted 2 times

  **bubbab** 1 month, 1 week ago

Applying a Microsoft Entra maximum device limit of less than 1,000 to a DEM account prevents you from reaching the 1,000 device limit that the DEM account can enroll. The answer is correct

<https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll>

upvoted 1 times

  **AleFCI1908** 1 month, 3 weeks ago

user 1: 10 , device limit is applied to intune admin too

user 2 : 1000 , dem is a special account, the limitation doesn't apply

upvoted 1 times

  **LionelDerBoven** 3 months, 3 weeks ago

1000

Unlimited.

In Microsoft Intune, a Device Enrollment Manager (DEM) is a special user account used for enrolling and managing multiple devices. The primary purpose of a DEM account is to enable scenarios where a single user needs to enroll and manage several devices, such as shared devices in a retail or educational setting.

Device Enrollment Manager (DEM) Limit:

A Device Enrollment Manager can enroll up to 1,000 devices in Intune.

Intune Administrator: No set limit on the number of devices they can manage or enroll. Administrators manage devices, policies, and configurations in Intune, and their role primarily involves overseeing enrollment and device management but does not impose enrollment restrictions on themselves.

upvoted 1 times

  **dnt91** 4 months ago



I think

User1 (Intune Admin) : Unlimited devices

User2 (DEM) : 1000 devices

Documentation says a NON ADMIN USER is limited to 15 and a DEM is a non admin user with a limit of 1000. This implicitly says that an admin user is (probably) not limited. I can't find a limit for an intune admin.

upvoted 2 times

  **rcristiano** 8 months, 3 weeks ago

Usuário 1: 15 dispositivos e usuário 2: 1000 - DEM (gerenciador de registro de dispositivos) no Intune

upvoted 1 times



🗨️ 👤 **Jeff777** 9 months ago

User1: 10

User2: 15

User1 GroupA

User2 GroupB & DEM

Device limit 15 GroupB

Device limit 10 GroupA

upvoted 1 times

🗨️ 👤 **ckmay** 10 months, 1 week ago

The question: What is the maximum number of devices that User1 and User2 can enroll in Intune? is based on the planned changes which include: 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.

It seems the question is essentially asking "In order to perform the planned changes, what will the limitations of this be based on the configured policies"

Because Enrollment restrictions do not count towards DEM when enrolling Windows devices in shared modes, the answer is 1000 devices for user 2

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

Co-managed enrollments

Group Policy (GPO) enrollments

Microsoft Entra joined enrollments, including bulk enrollments

Windows Autopilot enrollments

Device enrollment manager enrollments

<https://learn.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set>)

User 1: 15 devices

User 2: 1000 devices

upvoted 4 times

🗨️ 👤 **ckmay** 10 months, 1 week ago

CORRECTION-

User 1: 10 Devices

User 2: 1000

upvoted 3 times

🗨️ 👤 **sergioandreslq** 10 months, 1 week ago

User 1: 10 Devices because, user 1 belong to group A which has a restriction of device limit 10.

upvoted 2 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

Partly correct.

User1: 10 devices

User2: 1000

User2 is a device enrollment manager (DEM) in Intune, so device limit restrictions won't work on them.

<https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll#device-limit-restrictions>

upvoted 4 times

🗨️ 👤 **Merrybob** 11 months ago

User 1 - 10 Devices (Based on policy)

User 2 - 15 Devices

(Ref: <https://learn.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure#:~:text=Intune%20device%20limit%20restrictions%20set%20the%20maximum%20number%20of%20devices%20that%20a%20user%20can%20enroll.>

upvoted 1 times

🗨️ **Anymouse1312** 10 months, 2 weeks ago

Wrong according to your own link:

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

(...)

Device enrollment manager enrollments

Answer definitely is 1000.

upvoted 3 times

🗨️ **onepunchkenshin** 11 months, 3 weeks ago

I will vote 1000 devices for User2 as Windows devices are being deployed

upvoted 2 times

🗨️ **Tonsku** 1 year ago

User1: 10

User2: 15

User1 GroupA

User2 GroupB & DEM

Device limit 15 GroupB

Device limit 10 GroupA

upvoted 4 times

🗨️ **iTomi** 1 year, 1 month ago

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

This scenario is only INTUNE device limit restriction. No mentions of Azure device limit restriction, so right answers are 10 and 1000.

Stop making things up and creating your own scenarios. Follow the given task.

upvoted 3 times

🗨️ **mks\_academy** 1 year ago

But the question asked is "What is the maximum number of devices that User1 and User2 can enroll in INTUNE", so to me the answers are correct (User1 10 - User2 15).

upvoted 2 times

🗨️ **NoursBear** 1 year, 1 month ago

This may help:

<https://learn.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure>

but here it says DEM are not affected by restrictions for WINDOWS devices, so which is it ?

Windows devices

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

Co-managed enrollments

Group policy object (GPO) enrollments

Microsoft Entra joined enrollments

Bulk Microsoft Entra joined enrollments

Autopilot enrollments

Device enrollment manager enrollments

upvoted 1 times

🗨️ **NoursBear** 1 year, 1 month ago

OK here we are working with mobile devices, where die DEM would be limited

upvoted 1 times

🗨️ **madsa** 1 year, 1 month ago

The correct answer is 10 and 15. Restrictions overrule DEM.

upvoted 2 times

🗨️ **NoursBear** 1 year, 1 month ago

OK here we are working with mobile devices, where die DEM would be limited

upvoted 1 times

  **NoursBear** 1 year, 1 month ago

Comment in wrong place

upvoted 1 times

  **kay000001** 1 year, 1 month ago

I did some research and reached the following conclusion based on: <https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll>

DEM offers max of 1000, and do not succumb to restrictions, however, you can configure a hard limit manually which has been done so under restrictions 2 (device limit 10) of the case study.

So...

User 1: Is an Intune Administrator who by default can enrol upto 1000 devices, but he is in Group A that has a manual restriction (Restriction2) of 10 devices. So answer should be: 10.

User 2: Has a non-administrator role, so his limit is 15.

Correct me if I am wrong.

upvoted 1 times

  **kay000001** 1 year, 1 month ago

Apolgies, User 2: is also under Restriction1 (15 devices), so their limit will be 15 anyway.

upvoted 1 times

## HOTSPOT

-

## Case study

-

## 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 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 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 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	<i>Not applicable</i>	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	<i>Not applicable</i>	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	<i>Not applicable</i>	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	<i>None</i>
Policy2	Group2	Group3
Policy3	Group1	<i>None</i>

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.
- 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.
- 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.

To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Policy1:  ▼

- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device3

Policy2:  ▼

- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device3

### Answer Area

Suggested Answer:

Policy1:  ▼

- Device1 only
- Device2 only
- Device3 only**
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device3

Policy2:  ▼

- Device1 only
- Device2 only
- Device3 only
- Device4 only**
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device3

**Futfuyfjfi** Highly Voted 1 year, 3 months ago

A lot to walkthrough but the answer is correct. Remember excludes takes precedence and Android policies won't apply to iOS of course (and vice versa)  
upvoted 18 times

**DiligentSam** Most Recent 1 month, 3 weeks ago

Given Answer is correct.  
upvoted 1 times

**Darkfire** 10 months, 2 weeks ago

Answer is correct.  
upvoted 4 times

**Tonsku** 1 year ago

Device3: Group2 & Group3  
Policy1: Group3. Exclude None

Device4: Group2  
Policy2: Group2. Exclude Group3  
upvoted 1 times

**yosry** 1 year ago

seems correct

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

The given answer is correct.

upvoted 1 times

🗨️ 👤 **sh123df** 1 year, 2 months ago

Policy 1=device 3

Policy 2=device 2 and 4

upvoted 2 times

🗨️ 👤 **HawkieEyes** 1 year, 2 months ago

Device2 is in Group3, which is excluded by Policy2, so Policy2 is Device4 only

upvoted 6 times

🗨️ 👤 **fco168** 1 year, 1 month ago

Policy 2 = Device 4 Only. Device 2 is in group 3 as well and Policy 2 excludes that group.

upvoted 4 times

Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10.

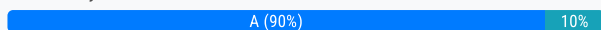
On Computer1, you need to run the Invoke-Command cmdlet to execute several PowerShell commands on Computer2.

What should you do first?

- A. On Computer2, run the Enable-PSRemoting cmdlet.
- B. On Computer2, add Computer1 to the Remote Management Users group.
- C. From Active Directory, configure the Trusted for Delegation setting for the computer account of Computer2.
- D. On Computer1, run the New-PSSession cmdlet.

**Suggested Answer: A**

Community vote distribution



**Darkfire** 4 months, 2 weeks ago

**Selected Answer: A**

A is correct

<https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-7.4>  
upvoted 3 times

**Tonsku** 6 months, 2 weeks ago

**Selected Answer: A**

A. On Computer2, run the Enable-PSRemoting cmdlet.  
upvoted 1 times

**belyo** 6 months, 3 weeks ago

**Selected Answer: A**

1] Enable-PSRemoting  
2] To verify that remoting is configured correctly use New-PSSession which creates a remote session on the local computer  
upvoted 1 times

**VirtualJP** 8 months, 3 weeks ago

**Selected Answer: A**

Answer is correct  
upvoted 2 times

**Temptset** 9 months ago

**Selected Answer: A**

"PowerShell remoting is enabled by default on Windows Server platforms. You can use Enable-PSRemoting to enable PowerShell remoting on other supported versions of Windows and to re-enable remoting if it becomes disabled."

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-6>

The key is "enabled by default on SERVER...", not the client (Windows 10/11). You have to enable it first.  
upvoted 2 times

**Aiscoran** 9 months ago

**Selected Answer: A**

As Futfuyfujfj says... [https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about\\_remote\\_requirements?view=powershell-7.3](https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_requirements?view=powershell-7.3)  
upvoted 1 times



🗨️ 👤 **Rocky83** 9 months ago

**Selected Answer: D**

According to this article:

To run a single command on a remote computer, use the ComputerName parameter. To run a series of related commands that share data, use the New-PSSession cmdlet to create a PSSession (a persistent connection) on the remote computer, and then use the Session parameter of Invoke-Command to run the command in the PSSession. To run a command in a disconnected session, use the InDisconnectedSession parameter. To run a command in a background job, use the AsJob parameter.

upvoted 1 times

🗨️ 👤 **picho707** 9 months ago

You do not need to run the New-PSSession cmdlet before running the Invoke-Command cmdlet. The Invoke-Command cmdlet will automatically create a new PowerShell session if one does not already exist.

upvoted 3 times

🗨️ 👤 **Futfuyfyfj** 10 months ago

Not 100% sure but looks correct:

[https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about\\_remote\\_requirements?view=powershell-7.3](https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_requirements?view=powershell-7.3)

upvoted 3 times

🗨️ 👤 **Rocky83** 9 months ago

same here

upvoted 1 times

You have an Azure AD tenant that contains the devices shown in the following table.

Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered


Which devices can be activated by using subscription activation?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device2, Device3, and Device4

**Suggested Answer:** C

Community vote distribution

C (100%)

 **Futfuyfjfi** Highly Voted 1 year, 3 months ago

Answer is correct:

<https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#requirements>


upvoted 9 times

 **Twindragon** Most Recent 4 weeks ago

**Selected Answer: C**

Agree with C

upvoted 1 times

 **Tr619899** 1 month, 1 week ago

**Selected Answer: C**

Agrees with the WORKHOLIC answer

upvoted 2 times

 **Pollosor** 6 months ago


Automatic subscription?

upvoted 1 times

 **WORKHOLIC** 7 months, 2 weeks ago

Devices must be Microsoft Entra joined or Microsoft Entra hybrid joined. Workgroup-joined or Microsoft Entra registered devices aren't supported.

upvoted 3 times

 **Darkfire** 10 months, 2 weeks ago


**Selected Answer: C**

C is correct

Devices must be Microsoft Entra joined or Microsoft Entra hybrid joined. Workgroup-joined or Microsoft Entra registered devices aren't supported.

<https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation>

upvoted 2 times

 **smart008** 10 months, 3 weeks ago

When you say device must be Entra joined, then how do you justify the following question in which I presume the devices are not joined to Azure?

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains 100 client computers that run Windows 10.

Currently, your company does NOT have a deployment infrastructure.

The company purchases Windows 11 licenses through a volume licensing agreement.

You need to recommend how to upgrade the computers to Windows 11. The solution must minimize licensing costs.

What should you include in the recommendation?

- A. Windows Autopilot
- B. Configuration Manager
- C. subscription activation (Correct Answer)
- D. Microsoft Deployment Toolkit (MDT)

upvoted 1 times

🗨️ 👤 **Tonsku** 1 year ago

**Selected Answer: C**

C. Device1 and Device3 only

upvoted 1 times

🗨️ 👤 **iTomi** 1 year ago

**Selected Answer: C**

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.

Devices must be Microsoft Entra joined or Microsoft Entra hybrid joined. Workgroup-joined or Microsoft Entra registered devices aren't supported.

<https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#subscription-activation-for-enterprise>

upvoted 2 times

🗨️ 👤 **fco168** 1 year, 1 month ago

**Selected Answer: C**

Devices 1 and 3 are joined to the azure AD domain. Therefore, can be activated. vs 2 and 4 which are only registered and can be BYOD devices.

upvoted 1 times

🗨️ 👤 **Rocky83** 1 year, 3 months ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#requirements>

Devices must be Azure AD-joined or hybrid Azure AD joined. Workgroup-joined or Azure AD registered devices aren't supported.

upvoted 2 times

You have 25 computers that run Windows 10 Pro.

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You need to upgrade the computers to Windows 11 Enterprise by using an in-place upgrade. The solution must minimize administrative effort.

What should you use?

- A. Microsoft Deployment Toolkit (MDT) and a default image of Windows 11 Enterprise
- B. Microsoft Configuration Manager and a custom image of Windows 11 Enterprise
- C. Windows Autopilot
- D. Subscription Activation

**Suggested Answer:** D

Community vote distribution



**Sas2003** Highly Voted 1 year, 3 months ago

**Selected Answer: A**

Autopilot does not upgrade Windows version. The only approach listed to perform upgrade in-place is MDT with DEFAULT image  
upvoted 21 times

**Cheban** 8 months, 2 weeks ago

The answers is B - Configuration manager  
upvoted 1 times

**OyYaGotta** 9 months, 3 weeks ago

Autopilot does upgrade to Win 11, and there is no MDT in Azure AD, but the least Administrative effort is Subscription Activation, so the answer is D.  
upvoted 4 times

**pxdPhil2** 9 months ago

Subscription activation cannot upgrade between versions, ie 10 to 11  
upvoted 2 times

**oopspruu** Highly Voted 5 months, 2 weeks ago

**Selected Answer: D**

The question doesn't say anywhere that they have on-premise infrastructure setup which is needed for MDT and Config Manager. so both options A & B are gone.

Windows Autopilot can upgrade your computer from Windows 10 Pro to Windows 11 Pro, but to upgrade Pro to Windows Enterprise edition, a Subscription is needed.

So correct answer is D.

upvoted 5 times

**458184c** Most Recent 1 week, 3 days ago

**Selected Answer: D**

The correct answer is D. Subscription Activation.

upvoted 1 times

**BigTone** 4 weeks, 1 day ago

**Selected Answer: A**

The answer cannot be B, you cannot use a custom image to do an in-place upgrade

The answer cannot be D, Subscription activation can't be used to upgrade to a newer version of Windows <https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivots=windows-10>

So that leaves A or C as potential correct answers.

According to this article you would need configuration manager to deploy an OS upgrade with Windows Autopilot <https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivots=windows-10>

us/autopilot/existing-devices

So for me, the only possible correct answer is A

upvoted 2 times

🗨️ **Abitek007** 1 month, 1 week ago

**Selected Answer: D**

Subscription activation can upgrade from pro to enterprise. hence D is right

upvoted 1 times

🗨️ **Tr619899** 1 month, 1 week ago

**Selected Answer: D**

Microsoft's Subscription Activation feature allows you to seamlessly upgrade Windows 10 Pro devices to Windows 11 Enterprise without requiring reimaging or an in-place upgrade process. When you assign a Microsoft 365 E5 license to a user signed into a Windows 10 Pro or Windows 11 Pro device, it automatically upgrades the operating system to Windows 10 Enterprise or Windows 11 Enterprise.

upvoted 1 times

🗨️ **1655b71** 2 months ago

The correct answer, based on the requirement for minimal administrative effort and the availability of Microsoft Intune, is:

C. Windows Autopilot

Explanation:

Windows Autopilot is designed for automating device setup and provisioning with minimal intervention, making it ideal for upgrading and configuring multiple devices through cloud-based services like Intune. Since the organization has Microsoft Intune, Windows Autopilot allows a streamlined process to upgrade to Windows 11 Enterprise without the need to manage complex deployment images or on-premises tools like MDT or Configuration Manager.

Subscription Activation (Option D) is typically used for license activation, not for performing upgrades.

upvoted 3 times

🗨️ **AleFCI1908** 2 months ago

**Selected Answer: D**

minimal effort

upvoted 1 times

🗨️ **AleFCI1908** 2 months ago

**Selected Answer: D**

minimal administrative effort

upvoted 2 times

🗨️ **d3a3d8a** 2 months ago

"Subscription activation can't be used to upgrade to a newer version of Windows" From <https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivot=windows-11#subscription-activation-for-enterprise>

upvoted 2 times

🗨️ **SSL2** 2 months, 1 week ago

**Selected Answer: D**

To upgrade your 25 Windows 10 Pro computers to Windows 11 Enterprise with minimal administrative effort, you should use D. Subscription Activation.

Subscription Activation allows you to upgrade eligible Windows 10 Pro devices to Windows 11 Enterprise automatically, leveraging your Microsoft 365 E5 subscription. This method is seamless and requires minimal intervention, as it uses the existing subscription to activate the Enterprise features.

upvoted 1 times

🗨️ **RomanV** 3 months, 2 weeks ago

Do people not study before commenting here? C & D are not for upgrading purposes and cannot do upgrades... Seriously guys, you are making it very hard for people on ExamTopics...

You have 2 options: A or B. The answer here should be A, as you need a DEFAULT image. But... MDT is DEPRECATED so this will not be an option anymore. I would go for B, the MCM solution but the answer should have been "MCM and a DEFAULT image".

So for now, it's A.

upvoted 2 times

🗨️ **EUC\_PRO** 3 months, 3 weeks ago

**Selected Answer: A**

Answer is A. You can only upgrade Windows with a DEFAULT image. In-place upgrade is not supported with a custom image.

upvoted 1 times

🗨️ 👤 **LionelDerBoven** 3 months, 3 weeks ago

**Selected Answer: D**

Since you are upgrading Windows 10 Pro to Windows 11 Enterprise and minimizing administrative effort is the key requirement, Subscription Activation is the easiest and most efficient way to accomplish this. Here's why:

Subscription Activation allows you to upgrade devices from Windows 10 Pro to Windows 11 Enterprise without reinstalling the operating system or using custom images.

You already have a Microsoft 365 E5 subscription, which includes the necessary license for Windows 11 Enterprise.

With Subscription Activation, when a device running Windows 10 Pro is linked to the user's Azure AD account, the license is automatically upgraded to Windows 11 Enterprise without any complex configurations or custom images.

upvoted 1 times

🗨️ 👤 **BurtSmart** 4 months, 1 week ago

<https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivot=windows-11>

This may lessen the confusion.

upvoted 2 times

🗨️ 👤 **Zoom2020** 3 months, 4 weeks ago

This only update the Windows edition on th same OS level, it does not IPU the device!

upvoted 1 times

🗨️ 👤 **ergacharsk** 5 months, 2 weeks ago

**Selected Answer: D**

Subscription Activation allows you to seamlessly upgrade Windows 10 Pro devices to Windows 10 Enterprise or Windows 11 Enterprise without reimaging. Since you already have a Microsoft 365 E5 subscription, which includes licensing for Windows Enterprise, you can utilize this feature. This method is the most efficient and requires the least administrative effort because it leverages existing subscriptions and does not require reimaging or deploying custom images.

upvoted 3 times

🗨️ 👤 **Maclouis116** 7 months ago

**Selected Answer: D**

Should be D. Subscription Activation

Explanation: With a Microsoft 365 E5 subscription, you can leverage Subscription Activation to automatically upgrade your Windows 10 Pro devices to Windows 11 Enterprise without needing to re-deploy or create custom images. This process is streamlined and integrated with Microsoft Intune, which you are already using, making it a convenient and efficient solution for in-place upgrades

upvoted 5 times

You use the Microsoft Deployment Toolkit (MDT) to manage Windows 11 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 Deployment Shares node, update the deployment share.
- B. From the Advanced Configuration node, create new media.
- C. From the Packages node, import a new operating system package.
- D. From the Operating Systems node, import a new operating system.

**Suggested Answer: A**

*Community vote distribution*

A (71%)

B (29%)

 **GreenJPGSandRAM** Highly Voted 8 months, 2 weeks ago

MDT is being removed from the exam on Apr 26, 2024. This question is no longer relevant  
upvoted 5 times

 **Tr619899** Most Recent 1 month, 1 week ago

**Selected Answer: A**

When you modify WinPE settings in the Microsoft Deployment Toolkit (MDT), such as adding PowerShell support, you need to generate updated WinPE boot images that include those changes. This is done by updating the deployment share. Here's why:

Why Update the Deployment Share?


The "Update Deployment Share" process in MDT regenerates the necessary files, including the WinPE boot image files, with the new settings. This action rebuilds the LiteTouch boot images (LiteTouchPE\_x86.wim and LiteTouchPE\_x64.wim) located in the deployment share's Boot folder.  
upvoted 2 times

 **Capzn** 4 months, 1 week ago

Answer is A  
upvoted 1 times

 **Ruchira007** 7 months, 1 week ago

A is correct  
upvoted 1 times

 **mestorrent86** 9 months, 3 weeks ago

**Selected Answer: B**

B. From the Advanced Configuration node, create new media. This will regenerate the WinPE boot image files with the updated settings, ensuring compatibility with Windows 11  
upvoted 1 times


 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: B**

B is correct. Trust me on this one.  
upvoted 2 times

 **RomanV** 3 months, 2 weeks ago

In a world of anonymity, trust is absent; only proof and evidence matter.  
upvoted 1 times

 **ten1ton** 8 months, 2 weeks ago

Thanks, I trust you  
upvoted 2 times

🗨️ **Darkfire** 10 months, 2 weeks ago

**Selected Answer: A**

A is correct

<https://learn.microsoft.com/en-us/windows/deployment/customize-boot-image?tabs=powershell#updating-the-boot-image-and-boot-media-in-mdt>  
upvoted 3 times

🗨️ **Tonsku** 1 year ago

**Selected Answer: B**

B. From the Advanced Configuration node, create new media.

Option A is incorrect because updating the deployment share will not create new WinPE boot image files with the updated settings.

upvoted 1 times

🗨️ **yosry** 1 year ago

**Selected Answer: A**

seems correct

upvoted 1 times

🗨️ **NoursBear** 1 year, 1 month ago

According to this question in MD 101 everyone voted the same "update deployment share"

<https://www.examttopics.com/discussions/microsoft/view/86938-exam-md-101-topic-2-question-97-discussion/>

upvoted 2 times

🗨️ **Linkin27** 1 year, 1 month ago

**Selected Answer: B**

I think it's B

upvoted 1 times

🗨️ **fco168** 1 year, 1 month ago

**Selected Answer: A**

A is correct. And then replace the image in WDS.

upvoted 4 times

🗨️ **LiamAzure** 1 year, 2 months ago

**Selected Answer: A**

Right click deployment share -> Update

upvoted 3 times

🗨️ **Dropkick** 1 year, 2 months ago

A

In Deployment Workbench, right click MDT Deployment Share and click Update Deployment Share. Select "Completely regenerate the boot images" and press next, next, finish. This will start a process that will generate boot images and built the ISO file. Just drink some coffee and come back later.

upvoted 4 times

🗨️ **VirtualJP** 1 year, 3 months ago

**Selected Answer: A**

I believe A to be correct, as per: <https://learn.microsoft.com/en-us/windows/deployment/customize-boot-image?tabs=powershell#updating-the-boot-image-and-boot-media-in-mdt>

upvoted 1 times

🗨️ **Support\_Compu** 1 year, 3 months ago

To generate a new set of WinPE boot image files with the updated settings in the Microsoft Deployment Toolkit (MDT), you should:

B. From the Advanced Configuration node, create new media.

Here's how you can do it:

Open the Deployment Workbench.

In the left pane, expand the "Advanced Configuration" node.



Right-click on "Media" and select "New Media."

Follow the wizard to create new media. During this process, you can customize the WinPE settings and add PowerShell support as needed.

After the media creation is complete, you can use the generated media to boot and deploy Windows 11 with the updated WinPE settings.

Option A (updating the deployment share) is used to update the deployment share itself but does not create new WinPE boot images with updated settings.



Option C (importing a new operating system package) and Option D (importing a new operating system) are related to importing and managing operating system packages and images but are not the steps required to create new WinPE boot images with customized settings.

upvoted 4 times

  **cpaljhc4** 1 year, 1 month ago

Agreed

upvoted 1 times

  **BJS78** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/windows/deployment/customize-boot-image?tabs=powershell#updating-the-boot-image-and-boot-media-in-mdt>

upvoted 1 times

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. Standard Client Task Sequence
- B. Standard Client Replace Task Sequence
- C. Litetouch OEM Task Sequence
- D. Sysprep and Capture

**Suggested Answer:** B

Community vote distribution


B (100%)

 **GreenJPGSandRAM** 2 months, 1 week ago

MDT is being removed from the exam on Apr 26, 2024. This question is no longer relevant  
upvoted 4 times

 **mestorrent86** 3 months, 2 weeks ago


B. Standard Client Replace Task Sequence. This template is designed for replacing an existing computer. It backs up the user state from the old computer, wipes and installs the operating system on the new computer, and then restores the user state. This process minimizes administrative effort as it automates the tasks of backing up and restoring user data, as well as securely wiping and decommissioning the devices.  
upvoted 4 times

 **MR\_Eliot** 4 months, 1 week ago

**Selected Answer: B**

B is correct.

<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit#task-sequence-templates>  
upvoted 2 times

 **Darkfire** 4 months, 2 weeks ago

B is correct

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.

<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit>  
upvoted 2 times

 **Tonsku** 6 months, 2 weeks ago

**Selected Answer: B**

B. Standard Client Replace Task Sequence  
upvoted 1 times

 **Wonder55** 7 months, 3 weeks ago

**Selected Answer: B**

B, 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.

<https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit#task-sequence-templates>

upvoted 1 times

🗨️ 👤 **kj2021** 8 months ago

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 2 times

🗨️ 👤 **Fortind1974** 9 months, 3 weeks ago

**Selected Answer: B**

B. Standard Client Replace Task Sequence

<https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit#task-sequence-templates>

upvoted 4 times

🗨️ 👤 **cserra** 9 months, 4 weeks ago

I think the right response is the A

The "Standard Client Replace Task Sequence" don't preserve the user state.

upvoted 1 times

🗨️ 👤 **Futfuyfj** 9 months, 2 weeks ago

Documentation says you are wrong?

<https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit#task-sequence-templates>

upvoted 2 times

🗨️ 👤 **4rk4n4** 8 months, 3 weeks ago

Option A ("Standard Client Task Sequence") is used for clean installations, not for replacing existing devices or migrating user data.

upvoted 1 times

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 11.

You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:

- For the WinRM service, set Startup type to Automatic.
- Create a listener that accepts requests from any IP address.
- Enable a firewall exception for WS-Management communications.

Which PowerShell cmdlet should you use?

- A. Connect-WSMan
- B. Enable-PSRemoting
- C. Invoke-WSManAction
- D. Enable-PSSessionConfiguration

**Suggested Answer:** B

Community vote distribution

B (100%)

 **neki99** Highly Voted 1 year, 2 months ago

The Enable-PSRemoting cmdlet performs the following operations:

Runs the Set-WSManQuickConfig cmdlet, which performs the following tasks:

Starts the WinRM service.

Sets the startup type on the WinRM service to Automatic.

Creates a listener to accept requests on any IP address.

Enables a firewall exception for WS-Management communications.

Creates the simple and long name session endpoint configurations if needed.

Enables all session configurations.

Changes the security descriptor of all session configurations to allow remote access.

Restarts the WinRM service to make the preceding changes effective.


upvoted 8 times

 **ergacharsk** Most Recent 5 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

 **MR\_Eliot** 10 months, 1 week ago

Selected Answer: B

Correct

upvoted 1 times

 **Darkfire** 10 months, 2 weeks ago

Selected Answer: B

B is correct

The Enable-PSRemoting cmdlet performs the following operations:

Runs the Set-WSManQuickConfig cmdlet, which performs the following tasks:

Starts the WinRM service.

Sets the startup type on the WinRM service to Automatic.

Creates a listener to accept requests on any IP address.



Enables a firewall exception for WS-Management communications.

Creates the simple and long name session endpoint configurations if needed.

Enables all session configurations.

Changes the security descriptor of all session configurations to allow remote access.  
Restarts the WinRM service to make the preceding changes effective.

<https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-7.4>  
upvoted 1 times

  **BJ578** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-7.3>  
upvoted 1 times

HOTSPOT

-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The tenant contains the users shown in the following table.

Name	Member of	On-premises sync
User1	Group1	Disabled
User2	Group2	Enabled

You assign Windows 10/11 Enterprise E5 licenses to Group1 and User2.

You deploy the devices shown in the following table.

Name	Operating system	Joined to
Device1	Windows 11 Pro	Azure AD
Device2	Windows 11 Pro	AD DS
Device2	Windows 10 Pro	Azure AD

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 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input checked="" type="radio"/>

 **Grg433** Highly Voted 1 year, 3 months ago

Ans : Y,N,N

When a user with a Windows 11 Enterprise E5 license signs in to a Windows 11 Pro device that is Azure AD-joined, it can unlock specific Windows 11 Enterprise features via the licensing. However, if the device is AD DS-joined (Active Directory Domain Services-joined) and not Azure AD-joined, it may not automatically upgrade to Windows 11 Enterprise based solely on the user's licensing.

upvoted 23 times

 **[Removed]** 1 year, 3 months ago

Device 3 is Azure AD Joined, and User 2 have the assignment of E5 license. It will be upgraded to Windows 11 Enterprise.

upvoted 3 times

 **picho707** 1 year, 3 months ago

Subscription Upgrade does not apply to version upgrade from Windows 10 to Windows 11

upvoted 11 times

🗨️ 👤 **F3RRY** 1 year, 1 month ago

Device 3 has windows 10 pro, so the os licensing wont work  
upvoted 6 times

🗨️ 👤 **[Removed]** 1 year ago

No,No,No,

1: User1 is not synced to Azure AD

2: The device is not Azure AD joined (otherwise it would state hybride joined)

3: Not possible to upgrade Windows 10 pro to Windows 11 Enterprise via subscription upgrades.

upvoted 10 times

🗨️ 👤 **Anonymouse1312** 10 months, 2 weeks ago

Y,N,N

User 1 is not synced meaning it is cloud only. User1 is in group1 and only in entra you can assign licenses to groups.

upvoted 3 times

🗨️ 👤 **HvD** 3 months, 3 weeks ago

Or User1 is AD-onprem only and thus not available in AzureAD.

upvoted 1 times

🗨️ 👤 **FemiA55** 2 weeks, 4 days ago

Windows 10/11 Enterprise E5 licenses to Group1 and User2. User 1 is member of Group 1. User 1 is in Entra.

Y

N

N

upvoted 1 times

🗨️ 👤 **Stuckbear** 1 year, 3 months ago

until User1 is synced it is not licensed with the E5 license and therefore the device is not upgraded to W11

N,N,N

upvoted 11 times

🗨️ 👤 **Krayzr** 1 year ago

The first line of Q says the users are in Entra. So....?

upvoted 3 times

🗨️ 👤 **Vlad99** Highly Voted 1 year, 2 months ago

This is what I consider:

1. NO (missing on-premises sync)

If you have an on-premises Active Directory Domain Services (AD DS) domain, you need to synchronize the identities in the on-premises AD DS domain with Azure AD. This synchronization is required for users to have a single identity that they can use to access their on-premises apps and cloud services that use Azure AD. An example of a cloud service is Windows Enterprise E3 or E5.

<https://learn.microsoft.com/en-us/windows/deployment/deploy-enterprise-licenses>

2. YES (hybrid domain joined supported)

Requirements on devices :Devices must also be joined to Azure AD, or hybrid domain joined with Azure AD Connect. Customers who are federated with Azure AD are also eligible.

<https://learn.microsoft.com/en-us/windows/deployment/deploy-enterprise-licenses>

3. NO

Active subscription supports upgrade only from Pro to Enterprise.

upvoted 15 times

🗨️ 👤 **LiamAzure** 1 year, 1 month ago

For number 2, the device is already in Azure AD, so it doesnt matter if the sync is disabled?

upvoted 1 times

🗨️ 👤 **LiamAzure** 1 year, 1 month ago

For number 1 I mean

upvoted 1 times

🗨️ 👤 **Tr619899** Most Recent 1 month, 1 week ago

Answer is:

No - For Windows Subscription Activation, sync is required. In this case, sync is disabled.

No - The Device has to be Azure AD or Hybrid AD Joined. In this case, it is only joined to AD DS.

Yes - User 2 is licensed, and Device3 is joined to Azure AD, which meets the requirement for Windows Subscription Activation to upgrade to Win 11 Enterprise.

upvoted 1 times

🗨️ 👤 **1655b71** 2 months ago

Y = This statement should be Yes because User1's licensing and device Azure AD join status support an automatic upgrade to Windows 11 Enterprise.

N= This statement should be No because Device2 is only joined to AD DS without Azure AD involvement, which does not meet the criteria for automatic upgrade to Enterprise

Y = : This statement should be Yes because Device3 is Azure AD joined, which satisfies the requirement for an automatic upgrade when licensed correctly.

upvoted 2 times

🗨️ 👤 **AleFCI1908** 1 month, 2 weeks ago

the 3rd is win10, you can't upgrade win 10 to 11 wind subs activation, so NO

upvoted 1 times

🗨️ 👤 **Cezt** 5 months ago

Microsoft Entra available for identity management. is a requirement to upgrada

upvoted 1 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

Y N N

Subscription will simply upgrade Windows 10 Pro to Windows 10 Enterprise. You have to do the upgrade from Windows 10 to 11 manually.

upvoted 1 times

🗨️ 👤 **CJL324** 7 months, 2 weeks ago

Yes - Doesn't matter user is cloud only device is still joined to Azure AD, fyi the license is assigned in the cloud

Yes - Well depends if this is Hybrid which I am assuming

No - In Place Upgrade or other method needs to be performed,

upvoted 1 times

🗨️ 👤 **Murad01** 11 months, 1 week ago

I think correct answer should be YNN.

upvoted 2 times

🗨️ 👤 **mertak** 11 months, 1 week ago

YYN: 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>

see also; <https://www.examttopics.com/discussions/microsoft/view/52384-exam-md-101-topic-2-question-48-discussion/>

upvoted 2 times

🗨️ 👤 **Mattia8** 11 months, 1 week ago

Seems correct

upvoted 1 times

🗨️ 👤 **belyo** 1 year ago

1.NO user not synced

2.YES [it looks to me like a hybrid joined device, given the question statements]

3.NO definitely

upvoted 1 times

🗨️ 👤 **arsh807** 11 months ago

1. User not synced BUT Device1 is already joined to Azure AD

Y Y N



upvoted 1 times

🗨️ 👤 **Krayzr** 1 year ago

Y, Y, N

Most of the people missed line one of the question.

""Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The tenant contains the users shown in the following table.""

It says users are on the (Azure) Tenant (already). And the AD Syncs with Azure Tenant. So the given answer is correct IMHO

upvoted 4 times

🗨️ 👤 **madsa** 1 year, 1 month ago

Yes Yes No, come ON Guys the second device has no syn, and it makes no difference as it is Azure AD Joined, the user is available on the company tenancy so it as a license assigned, the device will upgrade to Enterprise, as per device 3 it will go to Win10 enterprise first so No.

upvoted 2 times

🗨️ 👤 **madsa** 1 year, 1 month ago

Actually, the answer is correct.

upvoted 1 times

🗨️ 👤 **kay000001** 1 year, 1 month ago

1. No, user is not sync'd to get the benefits of the license.

2. Yes, if the ADDS identities are sync'd with Azure AD.

3. Yes, Win10 Pro can be upgraded to Win11 Enterprise (if the device is running 'supported' versions of Win10 Pro).

Please correct me if I am wrong.

upvoted 1 times

🗨️ 👤 **Krayzr** 1 year ago

Read the question line one. It says users are on the (Azure) Tenant (already)

upvoted 1 times

🗨️ 👤 **fco168** 1 year, 1 month ago

If device 3 was Windows 11 pro, then it'll be YYY.

A device can be azure ad joined only, or on premise only. And both users are in Azure AD. The only difference is that user1 is not local on Active Directory. But if both users log into any of those devices, they will upgrade to Enterprise edition. Howeeveeeeeer, Device3 is windows 10 pro, CANNOT UPGRADE TO WINDOWS 11 ENT. Only to Win10 Ent.

That was the trick.

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

I think the user itself also needs to be synced and the device Entra ID joined.

<https://www.teamas.co.uk/2022/06/assigning-windows-1011-enterprise.html>

upvoted 1 times

HOTSPOT

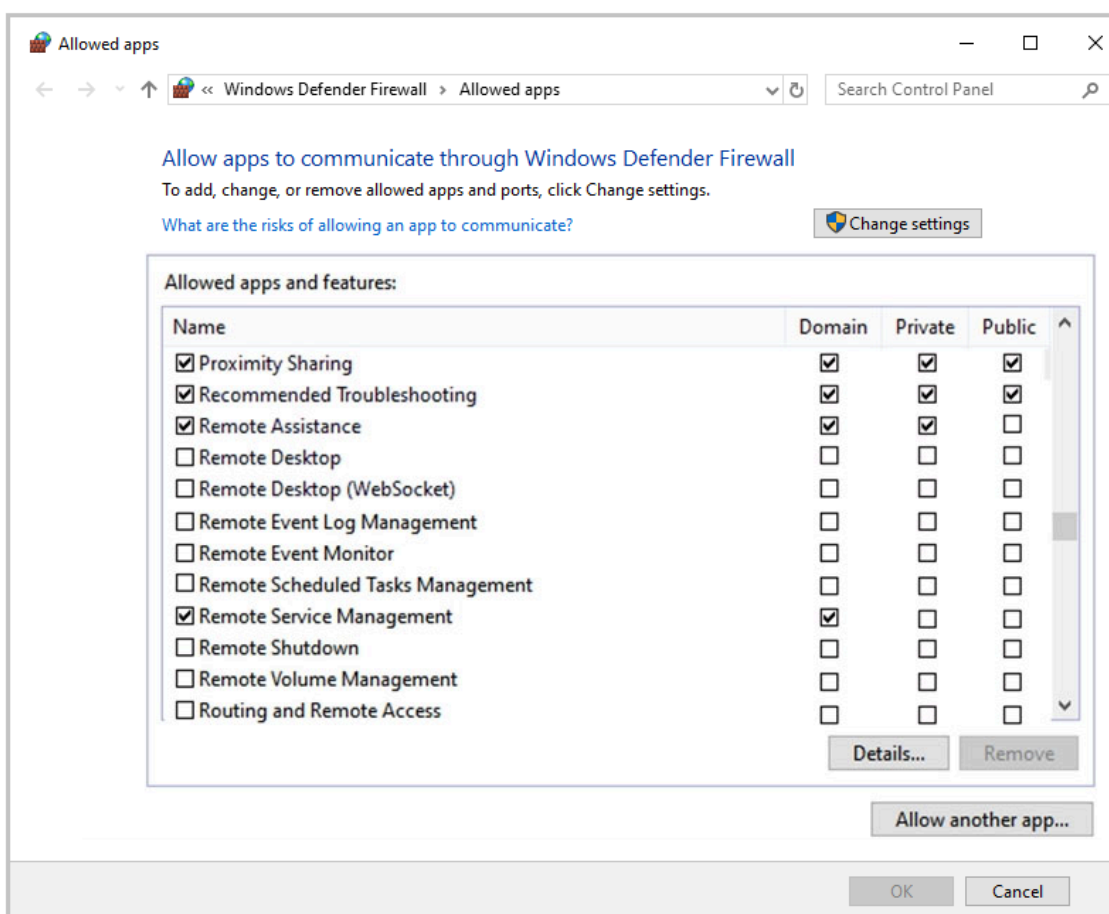
-

Your network contains an Active Directory domain named adatum.com, a workgroup, and computers that run Windows 10. The computers are configured as shown in the following table.

Name	Member of	Active Windows Defender Firewall profile
Computer1	Adatum.com	Domain
Computer2	Adatum.com	Domain
Computer3	Workgroup	Public

The local Administrator accounts on Computer1, Computer2, and Computer3 have the same user name and password.

On Computer1, Windows Defender Firewall is configured as shown in the following exhibit.



The services on Computer1 have the following states.

Status	Name	DisplayName
Stopped	RasAuto	Remote Access Auto Connection Manager
Running	RasMan	Remote Access Connection Manager
Stopped	RemoteAccess	Routing and Remote Access
Stopped	RemoteRegistry	Remote Registry
Stopped	RetailDemo	Retail Demo Service
Running	RmSvc	Radio Management Service
Running	RpcEptMapper	RPC Endpoint Mapper
Stopped	RpcLocator	Remote Procedure Call (RPC) Locator
Running	RpcSs	Remote Procedure Call (RPC)

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
From Computer2, you can use Disk Management to manage Computer1 remotely.	<input type="radio"/>	<input type="radio"/>
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	<input type="radio"/>	<input type="radio"/>
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> From Computer2, you can use Disk Management to manage Computer1 remotely.	<input type="radio"/>	<input checked="" type="radio"/>
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	<input type="radio"/>	<input checked="" type="radio"/>
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.	<input type="radio"/>	<input checked="" type="radio"/>

**fco168** Highly Voted 1 year, 1 month ago

You need Remote Registry Service to be running for Disk Management, Performance Monitor and Registry itself. That's required.

N

N

N

upvoted 11 times

**ckmay** 11 months ago

But because Remote Service Management is enabled for the domain profile, doesn't that mean computer 2 could start the remote registry service and therefore be able to remotely manage the disks?

if so, seems like it should be YNN

upvoted 1 times

**ckmay** 11 months ago

Actually YNN because in both scenarios 1&2, computer 2 could start the remote registry service and then could manage disk management and the registry.

Scenario 3 would still be no because computer 3 not being joined to the domain would be subject to the public firewall settings on computer 1 which does not allow remote service management to be managed

upvoted 1 times

**Tr619899** Most Recent 1 month, 1 week ago

Answer is: NO, NO, NO

upvoted 1 times

**Engr001** 10 months, 1 week ago

Remote Access Service is stopped. So no remote access is available? Therefore it's N, N, N ?

upvoted 3 times

**yosry** 1 year ago

seems correct

upvoted 2 times

**pirate84** 1 year, 1 month ago

No,No,No

upvoted 1 times

**NoursBear** 1 year, 1 month ago



About remote disk management

<https://techcommunity.microsoft.com/t5/windows-management/getting-to-the-bottom-of-it-remote-computer-management-storage/m-p/1603930>  
upvoted 1 times

  **NoursBear** 1 year, 1 month ago

To set up remote monitoring with PerfMon, you need to follow a few steps. First, you need to enable the Remote Registry service on the remote computer, and make sure that the local and remote computers have the same user account and password

upvoted 3 times

  **BJ578** 1 year, 3 months ago

<https://techcommunity.microsoft.com/t5/windows-management/getting-to-the-bottom-of-it-remote-computer-management-storage/m-p/1603930>  
<https://www.serverbrain.org/solutions-2003/monitoring-performance-remotely.html>

upvoted 1 times

You have a Hyper-V host that contains the virtual machines shown in the following table.

Name	Generation	Virtual processors	Memory
VM1	1	4	16 GB
VM2	2	1	8 GB
VM3	2	2	4 GB

On which virtual machines can you install Windows 11?

- A. VM1 only
- B. VM3 only
- C. VM1 and VM2 only
- D. VM2 and VM3 only
- E. VM1, VM2, and VM3

**Suggested Answer:** B

Community vote distribution

B (100%)

🗨️ 👤 **Twindragon** 3 weeks, 6 days ago

Selected Answer: B

Answer B is correct windows 11 is not supported by generation1.  
upvoted 1 times

🗨️ 👤 **Tr619899** 1 month, 1 week ago

Selected Answer: B

Answer seems correct.  
upvoted 2 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

Selected Answer: B

<https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/should-i-create-a-generation-1-or-2-virtual-machine-in-hyper-v#windows-guest-operating-system-support>

Generation 1 doesn't support Windows 11.  
Windows 11 needs at least 2 cores and 4GB RAM.  
upvoted 3 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

Selected Answer: B

Answer seems correct based on Microsoft documentation.

<https://learn.microsoft.com/en-us/windows/whats-new/windows-11-requirements#virtual-machine-support>

It seems that's right  
upvoted 1 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

Selected Answer: B

B is correct

Windows 11 cannot be installed in VM1 because it is generation 1.  
Windows 11 cannot be installed in VM2 because it only has 1 vCPU.  
VM3 is the only available option.

<https://techcommunity.microsoft.com/t5/itops-talk-blog/how-to-run-a-windows-11-vm-on-hyper-v/ba-p/3713948>

<https://www.microsoft.com/en-us/windows/windows-11-specifications?r=1>

upvoted 2 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **yosry** 1 year ago

**Selected Answer: B**

seems correct

upvoted 1 times

🗨️ 👤 **fco168** 1 year, 1 month ago

**Selected Answer: B**

Win11 minimum requirements, 2 cores and 4GB Ram

upvoted 3 times

🗨️ 👤 **Casticod** 1 year, 3 months ago

**Selected Answer: B**

Picho707 Right

upvoted 1 times

🗨️ 👤 **Grg433** 1 year, 3 months ago

**Selected Answer: B**

I think B is right

o install Windows 11, the virtual machines must meet specific hardware requirements, including having a 64-bit processor with at least two cores, 4 GB or more of RAM, and 64 GB or more of storage. Additionally, they must support certain virtualization features like Second Level Address Translation (SLAT).

upvoted 2 times

🗨️ 👤 **picho707** 1 year, 3 months ago

Windows 11 cannot be installed in VM1 because it is generation 1.

Windows 11 cannot be installed in VM2 because it only has 1 vCPU.

VM3 is the only available option.

upvoted 6 times

🗨️ 👤 **warrior\_404** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/windows/whats-new/windows-11-requirements#virtual-machine-support>

It seems that's right

upvoted 2 times

HOTSPOT

-

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

Name	Member of	License
User1	Group1	None
User2	Group1	Microsoft 365 E3
User3	Group2	Microsoft 365 E5

Group2 has been assigned in the Enrollment Status Page.

You have the devices shown in the following table.

Name	Operating system	Department
Device1	Windows 10 Pro	Marketing
Device2	Windows 10 Home	Research
Device3	Windows 10	Marketing

You capture and upload the hardware IDs of the devices in the marketing department.

You configure Windows Autopilot.

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


NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
User1 can complete the Autopilot process on Device1.	<input type="radio"/>	<input type="radio"/>
User2 can complete the Autopilot process on Device1.	<input type="radio"/>	<input type="radio"/>
User3 can view device setup information during the enrollment phase of Device1.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> User1 can complete the Autopilot process on Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can complete the Autopilot process on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can view device setup information during the enrollment phase of Device1.	<input checked="" type="radio"/>	<input type="radio"/>

 **ExamKiller020** Highly Voted 1 year, 3 months ago

N Y Y

Given answers are correct.

1. no license
  2. MS E3 and if no ESP config is assigned the default ESP will take place
  3. MS E5 And ESP has been configured
- upvoted 18 times

 **rcristiano** 8 months ago

N,N,Y O dispositivo 02 não pertence ao departamento de marketing, ID de hardware não foi carregado.

upvoted 1 times



  **Casticod**  1 year, 3 months ago

option 2, Its Windows HOME.

For me should Be: N N Y



<https://techcommunity.microsoft.com/t5/microsoft-intune/autopilot-windows-10-home/m-p/1438719>

upvoted 11 times

  **c54796e** 7 months, 3 weeks ago

Correct. Windows Autopilot is not available for Windows 10 Home edition. It requires Windows 10 Pro, Enterprise, or Education editions to utilize Autopilot.

upvoted 2 times

  **RomanV** 3 months, 2 weeks ago

You do realize it's talking about DEVICE 1 right? So answer is YES.

upvoted 4 times

  **Savior99** 10 months ago



All 3 questions refer to Device1, so N Y Y is correct

upvoted 3 times

  **Casticod** 1 year, 3 months ago

I correct NYY and the second question talks about device 1 (not 2)

upvoted 6 times

  **Kiookr** 1 year, 1 month ago

Very true option 2, Its Windows HOME. ==> Thus NO

upvoted 2 times

  **HvD** 3 months, 3 weeks ago

Question 2 also is about Device1, Windows Pro. Not Home.

upvoted 1 times

  **VLAG** 10 months ago

Fully Agree !!

answer 2 is NO because Windows HOME is not supported by Autopilot

N

Y

Y

upvoted 1 times

  **VLAG** 10 months ago

mistyped sorry


correct answers are

N

N

Y

upvoted 1 times

  **[Removed]** 9 months, 2 weeks ago

Read the question again. 2 refers to User 2 on Device 1 not Device 2. User 2 has the correct license and Device is Windows 10 Pro.

upvoted 1 times

  **Tr619899**  1 month, 1 week ago

Answer is: No, Yes, Yes



upvoted 1 times

  **Xillar** 1 month, 3 weeks ago

NYY is correct.

All questions about Device 1

upvoted 1 times

  **EUC\_PRO** 3 months, 3 weeks ago

NYY is correct

upvoted 1 times



- 🗨️ 👤 **oopspruu** 5 months, 2 weeks ago  
People here don't really pay attention to the question. Device 2 which has HOME isn't even listed in the question so I am not sure where all this HOME discussion is coming from. The questions are being asked for Device 1. So NYY is correct.  
upvoted 4 times
- 🗨️ 👤 **KakTak** 6 months ago  
Guys, keep in mind that all 3 questions are regarding device 1. So exclude device 2 and 3 from the scope here and you will find the answer.  
No, Yes, Yes  
upvoted 1 times
- 🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago  
NYY  
  
<https://learn.microsoft.com/en-us/autopilot/software-requirements>  
upvoted 4 times
- 🗨️ 👤 **nlnick** 10 months, 3 weeks ago  
User 2 isn't a member of group so should be N-N-Y  
upvoted 1 times
- 🗨️ 👤 **[Removed]** 9 months, 2 weeks ago  
The Group has nothing to do with answer 2. User 2 has the correct license and Device 1 is able to upgrade with said license. Answers are N Y Y.  
upvoted 1 times
- 🗨️ 👤 **Murad01** 11 months, 1 week ago  
It is definitely NYY.  
upvoted 1 times
- 🗨️ 👤 **abill** 1 year, 1 month ago  
NYY - Windows home is not supported for autopilot  
upvoted 1 times
- 🗨️ 👤 **AdamRachel** 11 months, 3 weeks ago  
it is device1 Windows 10 Pro not device 2.  
upvoted 1 times
- 🗨️ 👤 **abill** 1 year, 1 month ago  
Sorry it's NYY - no mention of device 2  
upvoted 2 times
- 🗨️ 👤 **LiamAzure** 1 year, 1 month ago  
N N Y  
Windows 10 Home edition is not supported for autopilot  
upvoted 1 times
- 🗨️ 👤 **LiamAzure** 1 year, 1 month ago  
Sorry, it doesn't mention device 2, only device 1  
upvoted 2 times
- 🗨️ 👤 **LiamAzure** 1 year, 1 month ago  
So it's N Y Y  
upvoted 1 times
- 🗨️ 👤 **sh123df** 1 year, 3 months ago  
Correct answer  
upvoted 3 times

QUESTION NO: 77 -

You have a Microsoft 365 subscription that contains a user named User1. User1 is assigned a Windows 10/11 Enterprise E3 license.

You use Microsoft Intune Suite to manage devices.

User1 activates the following devices:

- Device1: Windows 11 Enterprise
- Device2: Windows 10 Enterprise
- Device3: Windows 11 Enterprise

How many more devices can User1 activate?

- A. 2
- B. 3
- C. 7
- D. 8

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗨️ **Xillar** 1 month, 3 weeks ago

Answer is correct. You can activate a total of 5 devices.

So the question is "How many More" So far we have three so we can activate 2 more.

upvoted 1 times

🗨️ **oopspruu** 5 months, 2 weeks ago

**Selected Answer: A**

"How many more" is they key pointer in the question. Given answer is correct.

upvoted 1 times

🗨️ **Pollosor** 7 months ago

By default, we can activate up to 5 devices. The question mentions 'how many more'. So far, 3 have already been activated, so there are 2 more to go to reach the limit of 5.

upvoted 2 times

🗨️ **kerimnl** 9 months, 1 week ago

**Selected Answer: A**

Total 5, Answer is 2

upvoted 1 times

🗨️ **Haider\_Raza** 9 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

🗨️ **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: A**

A is correct.

<https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation#licenses>

upvoted 2 times

🗨️ **vijay0715** 11 months, 1 week ago

Read question carefully its how may MORE, so total 5 already 3 devices activated 2 more left answer is 2

upvoted 2 times

🗨️ 👤 **Krayzr** 1 year ago

Selected Answer: A

Normal user's limit is 5 devices

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

It seems with an E5 license it is also 5

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

Another link with info and confirming the license type and number of devices:

[https://www.skilllocation.com/Public/Windows\\_10\\_Enterprise\\_E3\\_in\\_CSP\\_TechnicalGuide.pdf](https://www.skilllocation.com/Public/Windows_10_Enterprise_E3_in_CSP_TechnicalGuide.pdf)

upvoted 1 times

🗨️ 👤 **fco168** 1 year, 1 month ago

Selected Answer: A

With this subscription you obtain a license to activate up to 5 devices.

upvoted 2 times

🗨️ 👤 **Casticod** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure#azure-device-limit-restriction>

The question is poorly worded, and we have to understand that it asks how many Windows devices, if so, the answer is correct, 2 (5 in total)

upvoted 3 times

🗨️ 👤 **Kiookr** 1 year, 3 months ago

Why not 3 , there are 3 devices and maximum is 5 , it doesn't matter 2 of them are Win 11..

upvoted 1 times

🗨️ 👤 **Kiookr** 1 year, 3 months ago

Disregard please.. I see \_ how many more \_

upvoted 1 times

🗨️ 👤 **picho707** 1 year, 3 months ago

The answer is correct a user-assigned windows 10/11 enterprise E3 license can activate 5 devices therefore the answer needs to be 2.

upvoted 4 times

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.

**Actions**

**Answer Area**

Upload the file by using Microsoft Intune.

Generate a CSV file that contains the computer information.

Reset the computer.

Generate a JSON file that contains the computer information.

Upload the file by running `azcopy.exe`.

1

2

3

Navigation arrows: > < ^ v

**Answer Area**

Suggested Answer:

- Generate a CSV file that contains the computer information.
- Upload the file by using Microsoft Intune.
- Reset the computer.

**Moot2** 1 month, 2 weeks ago

Answer is correct  
upvoted 3 times

**Xillar** 1 month, 3 weeks ago

Given answer is the correct one.  
upvoted 2 times

**Josete1106** 3 months, 1 week ago

The answer are correct:

Generate a CSV file that contains the computer information

Upload the file by using Microsoft Intune

Reset the computer

upvoted 1 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

Given answer is correct.

1. Collect Hardware hash from Computer in csv format.
2. Upload hash to Device > Enrollment > Windows Autopilot > Devices > Import
3. Reset the device, connect it to Internet and it'll automatically grab the autopilot profile.

upvoted 2 times

🗨️ 👤 **den5\_pegito83** 8 months, 4 weeks ago

Reset Computer

Create CSV File

Import CSV into Intune

upvoted 2 times

🗨️ 👤 **3661de6** 8 months, 2 weeks ago

NO

1. Create
2. Import
3. Reset

upvoted 4 times

🗨️ 👤 **captainspork** 3 months, 2 weeks ago

I think the person above you was thinking from the perspective of an enterprise environment. Usually you aren't able to log into the account without breaking privacy policies so you are expected to wipe it before importing the hash, but in this case the hash would normally already be imported and you don't have to import hash after each use. Your answer is correct but the way they wrote the question both could be correct. If the hash still needs to be imported, you wouldn't even be able to get past the login screen since there is no way you can log in as admin onto the device.

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

coorect

upvoted 1 times

🗨️ 👤 **abill** 1 year, 1 month ago

Correct

upvoted 1 times

🗨️ 👤 **HawkieEyes** 1 year, 1 month ago

Answer is correct

upvoted 2 times

🗨️ 👤 **fco168** 1 year, 1 month ago

That's correct.

upvoted 1 times

🗨️ 👤 **Casticod** 1 year, 3 months ago

Ja Ja Ja, I have repeated this operation more than 1000 times, its correct

upvoted 4 times

🗨️ 👤 **Sherpa23** 4 months, 3 weeks ago

The device detail should already be in Intune if it is used by a past employee so why repeat it again? Why is there not an option to wipe the device and login using new user details?

upvoted 2 times

🗨️ 👤 **ExamKiller020** 1 year, 3 months ago

Given answer is correct.

ref: <https://learn.microsoft.com/en-us/autopilot/add-devices>

upvoted 3 times

You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 11.

You create a new task sequence by using the Standard Client Task Sequence template to deploy Windows 11 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. Initialization
- B. State Restore
- C. Preinstall
- D. Postinstall

**Suggested Answer:** C

*Community vote distribution*

C (100%)

 **Grg433** Highly Voted 1 year, 3 months ago


**Selected Answer: C**

To modify the task sequence to create a system volume and a data volume when deploying Windows 11, you should make changes in the:

C. Preinstall phase

The Preinstall phase is where you can customize the disk partitions and create system and data volumes before the operating system is installed. You can use the "Format and Partition Disk" task in the Preinstall phase to create the desired partitions and volumes according to your requirements.


upvoted 6 times

 **Twindragon** Most Recent 3 weeks, 6 days ago

**Selected Answer: C**

C is the correct answer.


upvoted 1 times

 **ergacharsk** 5 months, 2 weeks ago

**Selected Answer: C**

preinstall


upvoted 2 times

 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: C**

Just checked this. C is correct.

upvoted 1 times

 **fco168** 1 year, 1 month ago

**Selected Answer: C**

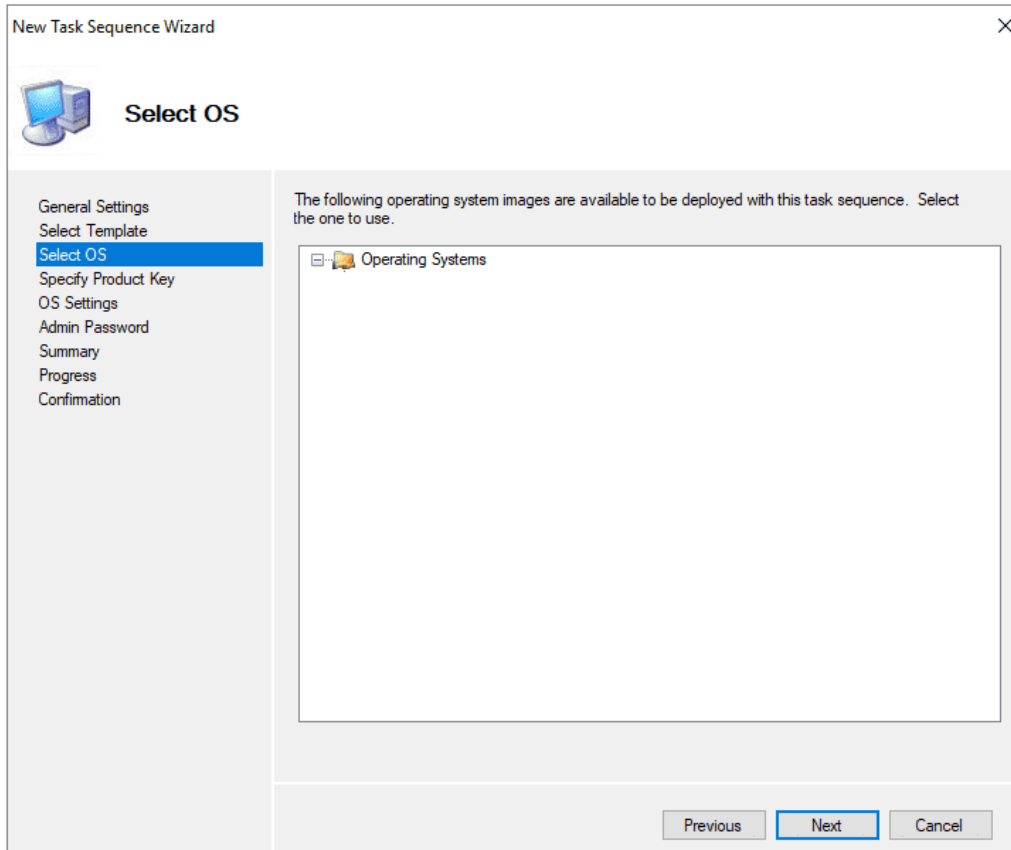
Correct!

upvoted 2 times

You have a Microsoft Deployment Toolkit (MDT) deployment share.

From the Deployment Workbench, you open the New Task Sequence Wizard and select the Standard Client Upgrade Task Sequence task sequence template.

You discover that there are no operating system images listed on the Select OS page as shown in the following exhibit.



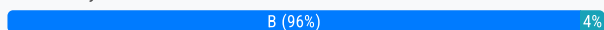
You need to be able to select an operating system image to perform a Windows 11 in-place upgrade.

What should you do?

- A. Enable monitoring for the deployment share.
- B. Import a full set of source files.
- C. Import a custom image file.
- D. Run the Update Deployment Share Wizard.

**Suggested Answer:** C

Community vote distribution



**Krayzr** Highly Voted 10 months, 4 weeks ago

**Selected Answer: B**

The correct answer is B. Import a full set of source files.

Here's why:

Enabling monitoring (A) won't resolve the issue of missing operating system images. It only collects information about deployments.

Importing a custom image file (C) is only necessary if you have a specific, pre-created image you want to use. In this case, the task requires a full

set of source files to build the image.

Running the Update Deployment Share Wizard (D) updates the share with changes made elsewhere, but it won't add new images unless they are already available in the source files.

Importing a full set of source files (B) provides the necessary components for MDT to create the installation media, including the Windows 11 image. This is the standard way to add new operating systems to MDT deployment shares.

Therefore, importing a full set of source files, which contains the Windows 11 installation files, will address the issue of missing images and allow you to proceed with the Windows 11 in-place upgrade task sequence.

upvoted 9 times

  **Jt909** Most Recent 5 months, 3 weeks ago

**Selected Answer: B**

Upgrade with custom image can't be done. Only vanilla full source files

upvoted 3 times

  **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: B**

B is correct

upvoted 3 times

  **Anonymouse1312** 10 months, 2 weeks ago

**Selected Answer: B**

The keyword here is "perform a Windows 11 in-place upgrade"

Cannot upgrade using custom images

upvoted 2 times

  **yosry** 1 year ago

**Selected Answer: B**

B is the correct answer

upvoted 3 times

  **NoursBear** 1 year, 1 month ago

I think this question may be missing something, this is what I found from one of the links below, this particular bit is important:



Add Windows 10 Enterprise x64 (full source)

Note

If you have already have a Windows 10 reference image in the MDT Build Lab deployment share, you can use the deployment workbench to copy and paste this image from the MDT Build Lab share to the MDT Production share and skip the steps in this section.

It says if there was already an image created then add this so you don't need to import the entire source. So we could presume there was already an image, so really B and C could be correct

upvoted 2 times

  **Tr1v** 1 year, 1 month ago

**Selected Answer: B**

- Obtain the Windows 11 installation media or ISO.

- Use the "Import Operating System" wizard in MDT to import the source files.

After importing the source files, you should be able to see the operating system images listed when creating a task sequence for a Windows 11 in-place upgrade.



upvoted 1 times

  **chandravamsi** 1 year, 1 month ago

**Selected Answer: C**

Import custom image file, Although option B is Correct as Windows is not Open source it is not viable

upvoted 2 times

  **fco168** 1 year, 1 month ago

**Selected Answer: B**

Agree with VirtualJP

upvoted 2 times



🗨️ 👤 **VirtualJP** 1 year, 2 months ago

**Selected Answer: B**

Here's why:

Importing a full set of source files into the Deployment Workbench is necessary to have an operating system image available for the in-place upgrade task sequence.

The in-place upgrade task sequence requires access to the Windows 11 source files to perform the upgrade.

Options A, C, and D are not directly related to the availability of operating system images in the task sequence. Enabling monitoring (Option A) is for tracking deployment progress, importing a custom image file (Option C) is for using a custom image (not needed for an in-place upgrade), and running the Update Deployment Share Wizard (Option D) is for updating the deployment share but doesn't specifically address the lack of operating system images.

upvoted 1 times

🗨️ 👤 **Zelda78** 1 year, 3 months ago

indeed B to me.

upvoted 1 times

🗨️ 👤 **Kiookr** 1 year, 3 months ago

Thank you for your confidence, BUT can you back up your choice with documentation?

upvoted 1 times

🗨️ 👤 **Nozuka** 1 year, 3 months ago

**Selected Answer: B**

Pretty sure it should be B.

<https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit#add-windows-10-enterprise-x64-full-source>

upvoted 4 times

Your company implements Azure AD, Microsoft 365, Microsoft Intune, and Azure Information Protection. The company's security policy states the following:

- Personal devices do not need to be enrolled in Intune.
- Users must authenticate by using a PIN before they can access corporate email data.
- Users can use their personal iOS and Android devices to access corporate cloud services.
- Users must be prevented from copying corporate email data to a cloud storage service other than Microsoft OneDrive for Business.

You need to configure a solution to enforce the security policy.


What should you create?

- A. a device configuration profile from the Microsoft Intune admin center
- B. a data loss prevention (DLP) policy from the Microsoft Purview compliance portal
- C. an insider risk management policy from the Microsoft Purview compliance portal
- D. an app protection policy from the Microsoft Intune admin center

**Suggested Answer:** D

Community vote distribution

D (100%)

 **ergacharsk** 5 months, 2 weeks ago


**Selected Answer:** D

D is correct  
upvoted 1 times

 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer:** D

D is correct. done this many times  
upvoted 1 times

 **Darkfire** 10 months, 2 weeks ago

**Selected Answer:** D

D is correct

App protection policies also help separate personal data from organization data. For example, you can create policies that block copy-and-paste between apps, require a PIN when opening an app, block backups to personal cloud services, and more.

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-apps>

upvoted 2 times

 **Merrybob** 11 months ago


**Selected Answer:** D

D. an app protection policy from the Microsoft Intune admin center  
upvoted 1 times

 **Tonsku** 1 year ago

**Selected Answer:** D

D. an app protection policy from the Microsoft Intune admin center  
upvoted 1 times

 **Nivla** 1 year, 2 months ago

**Selected Answer:** D

Answer is : D. App protection policies also help separate personal data from organization data. For example, you can create policies that block copy-and-paste between apps, require a PIN when opening an app, block backups to personal cloud services, and more.

source : <https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-apps>

upvoted 4 times

 **picho707** 1 year, 3 months ago

The answer is: D. an app protection policy from the Microsoft Intune admin center

App protection policies (APPs) allow you to manage and protect corporate data within managed apps. For example, you can use APPs to prevent users from copying corporate email data to a cloud storage service other than Microsoft OneDrive for Business.

upvoted 4 times

You have a Microsoft 365 subscription that contains 500 Android Enterprise devices.

All the devices are enrolled in Microsoft Intune.

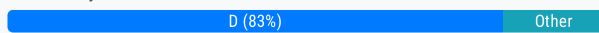
You need to deliver bookmarks to the Chrome browser on the devices.

What should you create?

- A. a compliance policy
- B. a configuration profile
- C. an app protection policy
- D. an app configuration policy

**Suggested Answer:** C

Community vote distribution



**Nozuka** Highly Voted 1 year, 3 months ago

**Selected Answer: D**

I don't agree with sh123df, since his answer is for Windows devices and this question states Android. Answer should be D.

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android#add-app-configuration-for-managed-ae-devices>  
upvoted 15 times

**edo1803** Most Recent 4 weeks, 1 day ago

**Selected Answer: D**

D is correct  
upvoted 1 times

**Pollosor** 5 months, 2 weeks ago

**Selected Answer: D**

The answer is D because it is the most direct method, I suppose.  
upvoted 1 times

**MR\_Eliot** 10 months, 1 week ago

**Selected Answer: D**

D is correct.  
upvoted 1 times

**BigStan82** 10 months, 2 weeks ago

**Selected Answer: D**

For delivering bookmarks to the Chrome browser on Android Enterprise devices, an app configuration policy (D) is actually the more appropriate choice if the goal is to specifically configure settings within the Chrome app itself. This allows for the direct management of app settings like bookmarks, homepage configurations, and other browser-specific preferences.

upvoted 1 times

**Darkfire** 10 months, 2 weeks ago

**Selected Answer: D**

Should be D

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android#add-app-configuration-for-managed-ae-devices>  
upvoted 1 times

**Krayzr** 10 months, 3 weeks ago

**Selected Answer: D**

D. an app configuration policy

Here's why:

Compliance policies define security and access requirements for devices, not specific configurations like bookmarks.

Configuration profiles are used for general device settings, not app-specific configurations.


App protection policies mainly focus on data security and access control within an app, not directly delivering bookmarks.

App configuration policies allow customizing specific settings within an app, making them ideal for delivering pre-defined bookmarks to Chrome on your managed devices.

Here's the reasoning for each option:

you would like to block or allow.

upvoted 3 times

  **Krayzr** 10 months, 3 weeks ago

D. an app configuration policy

Here's the reasoning for each option:

Compliance policies: These policies enforce security and access regulations on devices. They don't define app-specific configurations like adding bookmarks.

Configuration profiles: These profiles configure general device settings like Wi-Fi, passwords, or security, not app-specific features like bookmarks.

App protection policies: These policies manage data security and access within an app, controlling how users interact with app data. While they might control access to web content, they don't directly manage bookmarks.

App configuration policies: These policies let you tailor specific settings within an app. In this case, you can use an app configuration policy for Chrome to define the desired bookmarks structure and content.

upvoted 1 times



  **Krayzr** 10 months, 3 weeks ago

By creating an app configuration policy for Chrome, you can specify the exact bookmarks you want to add to the browser on your managed devices. This ensures consistency and provides easy access to important resources for your users.

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android>

"You can use an Intune app configuration policy to configure Google Chrome for Android devices. The settings for the app can be automatically applied. For example, you can specifically set the bookmarks and the URLs that you would like to block or allow."

upvoted 1 times

  **Krayzr** 11 months, 3 weeks ago

**Selected Answer: C**

Answer D:

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android>

Credit to Tonsku

upvoted 1 times

  **Hamouda1** 1 year ago

**Selected Answer: D**

Is correct

upvoted 1 times

  **Tonsku** 1 year ago

**Selected Answer: C**

C. an app protection policy

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android>

upvoted 2 times

  **Tonsku** 1 year ago

my mistake, D. an app configuration policy

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android>

upvoted 3 times

🗨️ 👤 **belyo** 1 year ago

Selected Answer: D

i have been doing this for 4+ years in enterprise environment and its always app config profile, not app protection policy  
upvoted 1 times

🗨️ 👤 **kay000001** 1 year, 1 month ago

Selected Answer: D

Answer is D:  
<https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android>  
upvoted 1 times

🗨️ 👤 **chandravamsi** 1 year, 1 month ago

Selected Answer: D

Option : D  
upvoted 1 times

🗨️ 👤 **fco168** 1 year, 1 month ago

Selected Answer: D

agree with VirtualJP  
upvoted 1 times

🗨️ 👤 **LiamAzure** 1 year, 2 months ago

Selected Answer: D

Its android so app configuration  
upvoted 1 times

🗨️ 👤 **4rk4n4** 1 year, 2 months ago

Selected Answer: D

Answer is D.  
upvoted 1 times

🗨️ 👤 **iamforksu** 1 year, 2 months ago

Selected Answer: D

Answer is D  
upvoted 1 times

You have a Microsoft 365 E5 subscription and 100 computers that run Windows 10.

You need to deploy Microsoft Office Professional Plus 2019 to the computers by using Microsoft Office Deployment Tool (ODT).

What should you use to create a customization file for ODT?

- A. the Microsoft 365 admin center
- B. the Microsoft Intune admin center
- C. the Microsoft Purview compliance portal
- D. the Microsoft 365 Apps admin center

**Suggested Answer: D**

Community vote distribution

D (100%)

06152f0 5 months ago

This is now both B and D.

I configured this in Intune admin>apps>policies for office apps and the policies I made here are duplicated in 365 app admin portal.

upvoted 2 times

MR\_Eliot 10 months, 1 week ago

Selected Answer: D

Correct.

upvoted 1 times

Darkfire 10 months, 2 weeks ago

Selected Answer: D

D is correct

<https://learn.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options>

upvoted 1 times

Mattia8 11 months, 3 weeks ago

D is the correct one

upvoted 1 times

Tonsku 1 year ago

Selected Answer: D

D. the Microsoft 365 Apps admin center

upvoted 1 times

fco168 1 year, 1 month ago

Selected Answer: D

Microsoft 365 APPS admin center is different from Microsoft 365(no apps) Admin Center. (I used to get confused). And it allows you to create a customized .xml file for O365 Installation.

upvoted 3 times

ExamKiller020 1 year, 3 months ago

Selected Answer: D

Given answer is correct.

<https://config.office.com/>

upvoted 3 times

picho707 1 year, 3 months ago

To create a customization file for ODT, you should use the Microsoft 365 Apps admin center.



The other options are incorrect:

The Microsoft 365 admin center: The Microsoft 365 admin center does not provide a tool for creating customization files for ODT.

The Microsoft Intune admin center: The Microsoft Intune admin center is used to manage mobile devices, not desktop computers.

The Microsoft Purview compliance portal: The Microsoft Purview compliance portal is used to manage compliance for Microsoft 365 and other Microsoft products. It does not provide a tool for creating customization files for ODT.

upvoted 4 times

  **NoursBear** 1 year, 1 month ago

the Microsoft Intune admin center can manage all devices including desktop devices however

upvoted 1 times



You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.

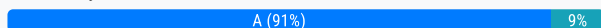
You plan to use Intune to deploy an application named App1 that contains multiple installation files.

What should you do first?

- A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.
- B. Create an Android application package (APK).
- C. Upload the contents of App1 to Intune.
- D. Install the Microsoft Deployment Toolkit (MDT).

**Suggested Answer:** C

Community vote distribution



**Nozuka** Highly Voted 1 year, 3 months ago

**Selected Answer: A**

Should be A.

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-prepare>

upvoted 11 times

**edo1803** Most Recent 4 weeks, 1 day ago

**Selected Answer: A**

It's A. With win32 apps you are able to package applications with custom scripts, config files, multiple .msi and .exe files and whatever you did like in SCCM or MDT.

upvoted 1 times

**oopspruu** 5 months, 2 weeks ago

**Selected Answer: A**

You can upload LOB apps directly with the msi or msix or msixbundle etc extensions. But you cannot upload .exe files in that option.

Since the question doesn't really say what type of files there are, I'd package all files in a intunewim format and execute the script command to install it using a script.

upvoted 2 times

**Michael\_010** 8 months, 1 week ago

so many discussable questions.. not stated correctly as MS always does.

what do they mean with installation files... are that for example dll files or MSI?

In case of any files except msi you should give answer A.

if they mean multiple msi files it must be C in order to proceed (without the need of scripting).

In my opinion this should not make it to the final exam questions, to many room for assumptions

I do have several years experience in working with Intune

upvoted 2 times

**650afa5** 6 months, 3 weeks ago

had this one on the exam yesterday. I went with A. Still scored a 662, but obviously not sure if A was correct

upvoted 1 times

**Michael\_010** 8 months, 1 week ago

reviewed Microsoft Learn, now the Answer is 100% A

Use the Microsoft Win32 Content Prep Tool to preprocess Windows classic (Win32) apps. The tool converts application installation files into the .intunewim format.

upvoted 1 times

**MR\_Eliot** 10 months, 1 week ago

Selected Answer: A

its A.

upvoted 1 times

BigStan82 10 months, 2 weeks ago

Selected Answer: A

For deploying an application that contains multiple installation files to Windows 11 devices enrolled in Microsoft Intune, the first step is:

A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.

The Microsoft Win32 Content Prep Tool is used to prepare complex applications, including those with multiple files and dependencies, for deployment via Microsoft Intune. This tool packages the application into a format (.intunewin) that is suitable for uploading to Intune and deploying across your managed devices. This process is necessary for applications that cannot be directly uploaded in their original format due to their complexity or the presence of multiple installation files. After preparing the app with the tool, you can then upload the packaged file to Intune for deployment.

upvoted 2 times

ckmay 10 months, 2 weeks ago

Selected Answer: A

A. As previously mentioned, you can't upload to intune until all the app files are wrapped with the .intunewin app wrapper

upvoted 1 times

Darkfire 10 months, 2 weeks ago

Selected Answer: C

C is correct

Win32 app is not mentioned in the question. So it's an normal app.

upvoted 2 times

OyYaGotta 9 months, 3 weeks ago

Darkfire is technically correct. Although the question is badly worded. It doesn't mention the app is a line of business app. Win32 Prep tool is only needed for LOB apps.

upvoted 1 times

Krayzr 10 months, 3 weeks ago

Selected Answer: A

A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.

Here's why:

Microsoft Win32 Content Prep Tool specifically prepares Windows applications for deployment with Microsoft Intune. It converts the installation files into the format required by Intune (.intunewin) and gathers information about the application for proper management.

Android application package (APK) wouldn't be relevant since you're dealing with Windows 11 devices and App1.

Uploading the contents directly without preparation can lead to deployment failures in Intune.

Microsoft Deployment Toolkit (MDT) focuses on creating Windows images, not preparing existing applications for Intune deployment.

upvoted 2 times

Merrybob 11 months ago

Selected Answer: A

A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.

upvoted 2 times

Pugmohone 11 months ago

Selected Answer: A

Multiple files. Must be A. Need to wrap all the files as an intunewin

upvoted 2 times

Tonsku 1 year ago

Selected Answer: A

What should you do first?

A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool

upvoted 1 times

belyo 1 year ago

**Selected Answer: A**

The Microsoft Win32 Content Prep Tool zips all files and subfolders when it creates the .intunewin file.  
this will solve the requirement with multiple installation files  
next step is to upload to intune  
upvoted 1 times

🗨️ 👤 **CyberBuck\_92** 1 year ago

It doesn't mention at all that we are deploying a legacy application; how did people get to that conclusion?  
upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

**Selected Answer: C**

nowhere in the question does it say anything about win32 apps preferably would use app wrapping tool first but c is most correct  
upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Sign in to the Microsoft Intune admin center.  
Select Apps > All apps > Add.  
In the Select app type pane, under the Other app types, select Line-of-business app.  
Click Select. The Add app steps are displayed.  
<https://learn.microsoft.com/en-us/mem/intune/apps/lob-apps-windows>  
upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

A would be correct if it were a win32 app which it is not  
upvoted 2 times

🗨️ 👤 **ZaFletch** 1 year, 2 months ago

**Selected Answer: A**

Answer is A, uploading apps to intune requires them to be in the correct format. Cannot upload until the prep tool has been run.  
upvoted 1 times

🗨️ 👤 **picho707** 1 year, 2 months ago

**Selected Answer: A**

The answer is: A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.  
The other answer choices are incorrect:

B. An Android application package (APK) is used to deploy Android apps, not Win32 apps.

C. You cannot upload the contents of App1 to Intune until you have prepared the app content by using the Microsoft Win32 Content Prep Tool.

D. The Microsoft Deployment Toolkit (MDT) is used to deploy Windows operating systems and other software to computers, not to manage mobile devices.

upvoted 3 times

## HOTSPOT

-

You have groups that use the Dynamic Device membership type as shown in the following table.

Name	Syntax
Group1	(device.deviceOwnership -eq "Company")
Group2	(device.deviceOwnership -eq "Personal")

You are deploying Microsoft 365 apps.

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

Name	Ownership	Platform
LT1	Company	Windows 10 Enterprise x64
LT2	Personal	Windows 10 Enterprise x64
LT3	Company	MacOS Big Sur

In the Microsoft Intune admin center, you create a Microsoft 365 Apps app as shown in the exhibit. (Click the Exhibit tab.)

### App information

Name: Microsoft 365 Apps for Windows 10

Description: Microsoft 365 Apps for Windows 10

Publisher: Microsoft

Category: Productivity

Show this as a featured app in the Company Portal: No


Information URL: <https://products.office.com/en-us/explore-office-for-home>

Privacy URL: <https://privacy.microsoft.com/en-US/privacystatement>

Developer: Microsoft

Owner: Microsoft

Notes: --

Logo: 

### App suite configuration [Edit](#)

Apps to be installed as part of the suite: Access Excel, OneNote, Outlook, PowerPoint, Publisher, Skype for Business, Teams, Word

Architecture: 64-bit

Update channel: Current Channel

Remove other versions: Yes

Version to install: Latest

Use shared computer activation: No

Accept the Microsoft Software License Terms on behalf of users: No

Install background service for Microsoft Search in Bing: Yes

Apps to be installed as part of the suite: 1 language(s) selected

### Assignments [Edit](#)

Group mode	Group
<input checked="" type="checkbox"/> Required	
<input type="checkbox"/> Included	Group1
<input type="checkbox"/> Available for enrolled devices	

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

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
LT1 will have Microsoft 365 apps installed.	<input type="radio"/>	<input type="radio"/>
LT2 will have Microsoft 365 apps installed.	<input type="radio"/>	<input type="radio"/>
LT3 will have Microsoft 365 apps installed.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> LT1 will have Microsoft 365 apps installed.	<input checked="" type="radio"/>	<input type="radio"/>
LT2 will have Microsoft 365 apps installed.	<input type="radio"/>	<input checked="" type="radio"/>
LT3 will have Microsoft 365 apps installed.	<input type="radio"/>	<input checked="" type="radio"/>

- BJ578** Highly Voted 1 year, 3 months ago  
Group1: Company, Group2: Any private devices.  
App is for W10, assigned to Group1, where we have only 1 W10, which is LT1  
--> YNN  
upvoted 12 times
- Casticod** 1 year, 3 months ago  
I'm Agree  
upvoted 1 times
- benpatto** Highly Voted 1 year, 1 month ago  
Just on another note which can be important, MacOS is only support on version 12-14 so this wouldn't work anyways. BigSur is version 11.\*\*  
upvoted 7 times
- Cezt** Most Recent 5 months, 1 week ago  
YNN this portal only supports w10/11 and some wserver  
upvoted 1 times
- Haider\_Raza** 9 months, 2 weeks ago  
Answer correct...  
upvoted 1 times
- MR\_Eliot** 10 months, 1 week ago  
YNN.  
  
for mac you will need to create another application.  
upvoted 3 times
- Darkfire** 10 months, 2 weeks ago  
Answer is correct.  
upvoted 1 times
- Tonsku** 1 year ago  
LT1: Y, LT2: N, LT3: N  
Device:  
LT1: Company - W10 Ex64 - Group1  
LT2: Personal - W10 Ex64 - Group2

LT3: Company - MacOS BigSur - Group1

App Information:

for Windows10 & Include Group1

upvoted 2 times

  **LiamAzure** 1 year, 2 months ago

Its correct, it will install only on Corporate Windows Devices

upvoted 1 times

  **Rocky83** 1 year, 3 months ago

I think the answer is correct

upvoted 1 times

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 Microsoft Intune admin center? Each correct answer is a complete solution.

NOTE: Each correct selection is worth one point.

- A. a device restrictions device configuration profile
- B. an app configuration policy
- C. a Windows 10 and later security baseline
- D. a custom device configuration profile
- E. a Windows 10 and later update ring

**Suggested Answer:** DE

Community vote distribution



**ExamKiller020** Highly Voted 1 year, 3 months ago

**Selected Answer:** DE

Given answers are correct.

Ref: <https://learn.microsoft.com/en-us/windows-insider/business/manage-builds#set-up-insider-preview-builds-using-intune>

Ref: [https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-Update?WT.mc\\_id=Portal-fx#managepreviewbuilds](https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-Update?WT.mc_id=Portal-fx#managepreviewbuilds)  
upvoted 10 times

**Grg433** Highly Voted 1 year, 3 months ago

**Selected Answer:** AD

I think it should be A and D.

A. Device restrictions device configuration profile: You can use this profile to enforce specific settings on Windows 10 devices, including preventing enrollment in the Windows Insider Program.

D. Custom device configuration profile: Creating a custom device configuration profile allows you to define specific settings and restrictions for your Windows 10 devices, including preventing enrollment in the Windows Insider Program.

upvoted 8 times

**458184c** Most Recent 1 week, 2 days ago

**Selected Answer:** AE

To prevent users from enrolling devices in the Windows Insider Program, you can use a combination of a device restrictions configuration profile and a Windows 10 and later update ring in Microsoft Intune. The device restrictions profile allows you to explicitly disable access to features like the Windows Insider Program, ensuring users cannot enable pre-release builds. Additionally, the update ring policy can enforce update settings that block devices from downloading and installing Insider builds. These two configurations work together to provide comprehensive control over update management and prevent unauthorized enrollment in pre-release Windows programs, minimizing administrative effort and ensuring compliance with organizational policies.

upvoted 1 times

**Tr619899** 1 month, 1 week ago

**Selected Answer:** AE

A device restrictions device configuration profile (Option A): Create a device restrictions policy targeting Windows 10.

In the settings, navigate to General and set Enable Preview Builds to Blocked to prevent devices from being enrolled in the Windows Insider Program.

A Windows 10 and later update ring (Option E): Create a Windows 10 update ring policy.

In the Settings section, under Update Settings, set Enable Preview Builds to Not Allowed to ensure that devices do not install preview builds from the Windows Insider Program.

upvoted 2 times

🗨️ 👤 **1655b71** 2 months ago

A and E

To prevent access to the Windows Insider Program, the most appropriate configurations are likely:

A. A device restrictions device configuration profile: This can be used to set device restrictions, including blocking access to certain system settings that could allow users to enroll in the Insider Program.

E. A Windows 10 and later update ring: This can be configured to control the type of updates that devices receive, including limiting updates to stable releases and excluding Insider builds.

So, the correct answers should be: A. A device restrictions device configuration profile and E. A Windows 10 and later update ring.

upvoted 1 times

🗨️ 👤 **EUC\_PRO** 3 months, 3 weeks ago

Selected Answer: AE

A and E are correct

upvoted 1 times

🗨️ 👤 **Cezt** 5 months, 1 week ago

A, E proven, update ring can set to not configured in case someone already enrolled device restrictions. to block access to update settings

upvoted 2 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

Selected Answer: AE

A : If you set Telemetry to required in Device Restrictions, they cannot get preview builds as it needs Optional Telemetry.

E: Use update ring to block preview builds.

Source:

I just implemented this last week.

upvoted 2 times

🗨️ 👤 **Prasis** 5 months, 3 weeks ago

A and E.

To prevent users from enrolling their devices in the Windows Insider Program using Microsoft Intune, you can perform the following configurations:

Device Restrictions Device Configuration Profile: This configuration allows you to set up restrictions on the devices. You can create a device restrictions profile in Intune to control features on enrolled devices.

Windows 10 and Later Update Ring: This configuration allows you to manage when Windows 10 updates are received by devices in your organization. You can create an update ring in Intune to specify how and when updates are delivered to devices

upvoted 2 times

🗨️ 👤 **SaiK1234** 10 months, 1 week ago

DE.

It is not in Device Restrictions. It is Configuration -> Setting Catalog -> Windows Update for Business -> Manage Preview Builds. This option is not there. So its D and E.

upvoted 2 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

Selected Answer: DE

DE is correct.

upvoted 2 times

🗨️ 👤 **[Removed]** 10 months, 2 weeks ago

Selected Answer: AE

A device restrictions device configuration profile allows you to control various settings on Windows 10 devices, including preventing users from enrolling in the Windows Insider Program.

A Windows 10 and later update ring allows you to control the update behavior of Windows 10 devices, including specifying which updates and builds are installed on the devices. By configuring this, you can prevent users from accessing preview builds, which are part of the Windows Insider Program.



upvoted 1 times

🗨️ 👤 **Krayzr** 10 months, 3 weeks ago

**Selected Answer: AE**

A. Device restrictions device configuration profile:

This profile allows you to restrict access to specific features and settings on devices.

Under "Windows Feature Experience", configure "Allow access to diagnostic data in the Windows Insider Program" to "Block".

E. Windows 10 and later update ring:

Update rings control which updates devices receive through Intune.

Create a new update ring with the "Update channel" set to "None (security updates only)".

Assign this update ring to the devices you want to prevent from joining the Insider Program.

upvoted 1 times

🗨️ 👤 **NoursBear** 11 months ago

The 30 days represents an upgrade of Windows Version through a feature update not a standard feature update

upvoted 1 times

🗨️ 👤 **Merrybob** 11 months ago

**Selected Answer: DE**

DE

Ref: <https://www.petervanderwoude.nl/post/managing-windows-insider-preview-builds-within-the-organization/>

upvoted 1 times

🗨️ 👤 **Murad01** 11 months, 1 week ago

I would go for A and D.

upvoted 1 times

🗨️ 👤 **frack** 11 months, 3 weeks ago

**Selected Answer: AE**

custom is almost legacy as it requires OMA-URI, always the last resort

upvoted 1 times

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune.

You plan to use Endpoint analytics.

You need to create baseline metrics.

What should you do first?

- A. Modify the Baseline regression threshold.
- B. Onboard 10 devices to Endpoint analytics.
- C. Create a Log Analytics workspace.
- D. Create an Azure Monitor workbook.

**Suggested Answer: B**

Community vote distribution

B (70%)

C (30%)

 **picho707** Highly Voted 1 year, 3 months ago

To create baseline metrics in Endpoint analytics, you should start by:

C. Create a Log Analytics workspace.

upvoted 14 times

 **oopspruu** Highly Voted 5 months, 2 weeks ago

**Selected Answer: B**

Some very inexperienced answers have been given here and people just go by the default "tick log analytics workspace for any question that says logs".

That will not work here unfortunately. The question has nothing to do with Log Analytics workspace. Endpoint analytics is built into Intune already to start getting analytics, you just need to enroll devices into it. To start a baseline to compare with other orgs, you need minimum 10 devices onboarded to Endpoint Analytics. So option B is absolutely correct.

upvoted 9 times

 **JayHall** Most Recent 1 month ago


**Selected Answer: B**

Answer is Correct: Onboard 10 devices to Endpoint analytics.

Endpoint analytics is built into Intune already to start getting analytics, you just need to enroll devices into it. To start a baseline to compare with other orgs, you need minimum 5 devices onboarded to Endpoint Analytics. So uploading 10 devices definitely satisfies this requirement

[https://learn.microsoft.com/en-us/mem/analytics/enroll-intune#bkmk\\_onboard](https://learn.microsoft.com/en-us/mem/analytics/enroll-intune#bkmk_onboard)

upvoted 1 times

 **GyanPoudyal** 4 months, 2 weeks ago

Before you can create baseline metrics, you need to ensure that devices are onboarded to Endpoint analytics. By onboarding devices, you enable data collection, which is necessary for generating baseline metrics. Starting with onboarding a few devices, like 10, is a common initial step to ensure that everything is set up correctly.

The other options are related to more advanced configurations and monitoring, but they are not the first step in creating baseline metrics.

B. Onboard 10 devices to Endpoint analytics.

upvoted 1 times

 **GreenJPGSandRAM** 8 months, 2 weeks ago

**Selected Answer: C**

You need a Log Analytics Workspace before you can start collecting information

upvoted 1 times

🗨️ **Rastova** 9 months, 3 weeks ago

**Selected Answer: B**

Therefore, you should onboard 10 devices to Endpoint Analytics first. This initial onboarding allows Endpoint Analytics to start collecting data, which is essential for establishing baseline metrics. After you have some devices onboarded and data is being collected, you can then proceed with analyzing that data and setting up baseline metrics for your organization's devices.

upvoted 2 times

🗨️ **Raziellucas** 9 months, 3 weeks ago

**Selected Answer: C**

I don't use that tool, but from several other question before, the first step is usually create the workspace, then the minimum devices onboard is a requirements but probably you can't onboard them if you don't have the workspace, am I right? someone that has endpoint analytics could check this?

upvoted 1 times

🗨️ **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: C**

c is the answers. you need log analytics workspace before you can collect the informaion. question also asls for what should you do first!

upvoted 1 times

🗨️ **RomanV** 3 months, 2 weeks ago

Answer is B.

This is about ENDPOINT ANALYTICS!!! The score Microsoft gives your environment and the improvements you need to do etc. to get a higher score.

<https://learn.microsoft.com/en-us/mem/analytics/scores>

upvoted 1 times

🗨️ **ckmay** 10 months, 2 weeks ago

**Selected Answer: B**

B. as there is definitely a minimum requirement for getting a baseline in endpoint analytics

upvoted 1 times

🗨️ **Darkfire** 10 months, 2 weeks ago

**Selected Answer: B**

B is correct

A status of insufficient data means you don't have enough devices reporting to provide a meaningful score. Currently, at least five devices are required.

<https://learn.microsoft.com/en-us/mem/analytics/scores>

upvoted 1 times

🗨️ **frack** 11 months, 3 weeks ago

**Selected Answer: B**

If I plan to use Endpoint analytics, need to upload at least 5 devices as a requirement.

[https://learn.microsoft.com/en-](https://learn.microsoft.com/en-us/mem/analytics/scores#:~:text=A%20status%20of%20insufficient%20data%20means%20you%20don%27t%20have%20enough%20devices%20reporting)

[us/mem/analytics/scores#:~:text=A%20status%20of%20insufficient%20data%20means%20you%20don%27t%20have%20enough%20devices%20reporting](https://learn.microsoft.com/en-us/mem/analytics/scores#:~:text=A%20status%20of%20insufficient%20data%20means%20you%20don%27t%20have%20enough%20devices%20reporting)

upvoted 2 times

🗨️ **Tonsku** 1 year ago

**Selected Answer: B**

B. Onboard 10 devices to Endpoint analytics.

<https://learn.microsoft.com/en-us/mem/analytics/scores>

upvoted 1 times

🗨️ **GeekGizmo** 1 year ago

B is wrong. It says onboard "10 devices". The question stated 100 Windows '10' devices. So it's not 10 devices, it's 100 devices. Trick of the wording. So the answer is C

upvoted 1 times

🗨️ **frack** 11 months, 3 weeks ago

Endpoint analytics will show you insufficient data. It needs at least 5 devices to have an enough devices reporting.

<https://learn.microsoft.com/en-us/mem/analytics/scores>

upvoted 1 times

  **Krayzr** 1 year ago

**Selected Answer: B**

B seems to correct

upvoted 1 times

  **iTomi** 1 year ago

**Selected Answer: B**

B is right answer

[https://learn.microsoft.com/en-us/mem/analytics/enroll-configmgr#bkmk\\_onboard](https://learn.microsoft.com/en-us/mem/analytics/enroll-configmgr#bkmk_onboard)

upvoted 1 times

  **iTomi** 1 year ago



Onboarding from the Endpoint analytics portal is required for both Configuration Manager and Intune managed devices. For more information about common issues, see Troubleshooting device enrollment and startup performance.

upvoted 1 times

  **yosry** 1 year ago

B seems correct

upvoted 3 times

  **madsa** 1 year, 1 month ago

Before enrolling you need to Create a Log Analytics workspace.

upvoted 2 times

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

Community vote distribution

B (100%)

oopspruu 5 months, 2 weeks ago

Selected Answer: B

Intune allows a value of 2-60 days. Unfortunately I wasn't able to find any official MS source that says its 10 but if you create a new policy, the pre-filled value is 10 so I'd stick with that answer.

upvoted 1 times

MR\_Eliot 10 months, 1 week ago

default it's 10. you can extend this to 60 days by configuring it in intune.

<https://learn.microsoft.com/en-us/mem/intune/protect/windows-update-settings#update-settings>

upvoted 1 times

Tonsku 1 year ago

Selected Answer: B

10 days

<https://answers.microsoft.com/en-us/windows/forum/all/rolling-back-feature-updates/9f77d4c3-21a7-430b-a935-675c29969964>

upvoted 2 times

madsa 1 year, 1 month ago

This one gives no confidence, there are a lot of sites stating 10 days, so I would go for 10 days.

upvoted 1 times

madsa 1 year, 1 month ago

Update in January 2022, the ability to roll back a feature update in Windows 10 is available for a limited time after the update is installed of 30 days.

upvoted 1 times

LiamAzure 1 year, 1 month ago

Selected Answer: B

You have 10 days to roll back a feature update

upvoted 1 times

VirtualJP 1 year, 2 months ago

Selected Answer: B

<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

BJ578 1 year, 3 months ago

<https://www.itechtics.com/rollback-windows-updates-after-10-days/>

upvoted 2 times

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. Join Azure AD.
- B. Configure Windows Defender Firewall.
- C. Create an event subscription
- D. Install the Azure Monitor Agent.

**Suggested Answer:** D

Community vote distribution

A (72%)

D (28%)

 **reastman66** Highly Voted 1 year ago

**Selected Answer: A**

No, the Azure Monitor Agent cannot be installed on a Windows 10 computer that isn't Azure AD joined. The Azure Monitor Agent uses Azure AD authentication to connect to the Log Analytics workspace, and Azure AD authentication requires the computer to be joined to Azure AD.

If you want to collect data from a Windows 10 computer that isn't Azure AD joined, you can use the Microsoft Monitoring Agent (MMA). The MMA is a legacy agent that does not require the computer to be joined to Azure AD. However, the MMA is not as feature-rich as the Azure Monitor Agent, and it is not supported as long.

In general, it is recommended to join all Windows 10 computers to Azure AD. This makes it easier to manage and secure the computers, and it enables you to use a variety of Azure services, such as Microsoft Intune and Azure Conditional Access.

upvoted 13 times

 **belyo** Highly Voted 1 year ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client#prerequisites>

The machine must be domain joined to a Microsoft Entra tenant (AADj or Hybrid AADj machines)

upvoted 5 times

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

I feel sorry for the noobs who are being fed wrong answers... That's why I always advise to STUDY first before coming here.

The correct answer is A!

Why?

"The machine must be domain joined to a Microsoft Entra tenant (AADj or Hybrid AADj machines), which enables the agent to fetch Microsoft Entra device tokens used to authenticate and fetch data collection rules from Azure."

Source: <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client#prerequisites>

upvoted 1 times

 **Frank9020** 4 months ago

**Selected Answer: D**

Even if the device is only connected to a workgroup, you can still use Azure Log Analytics to query events by installing the Azure Monitor Agent. Being in a workgroup does not prevent the device from sending logs to an Azure Log Analytics workspace.

upvoted 2 times

🗨️ 👤 **Prasis** 5 months, 3 weeks ago

To ensure that you can use Log Analytics to query events from Computer1, you should Install the Azure Monitor Agent (Option D) on Computer1.

D. Install the Azure Monitor Agent

upvoted 2 times

🗨️ 👤 **mark2525** 7 months, 3 weeks ago

**Selected Answer: D**

The question states , "You need to ensure that you can use Log Analytics to query events from Computer1." And not what needs to be done first.

What do you need to get the log analytics to work.

upvoted 2 times

🗨️ 👤 **Krayzr** 10 months ago

**Selected Answer: D**

D is must, A can be done later

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: A**

A is correct. with the old agent joning the domain/ aad is not needed.

upvoted 1 times

🗨️ 👤 **BigStan82** 10 months, 2 weeks ago

**Selected Answer: D**

To ensure that you can use Log Analytics to query events from a Windows 10 computer that is in a workgroup, you should:

D. Install the Azure Monitor Agent.

Installing the Azure Monitor Agent on Computer1 is necessary for it to communicate and send data to the Azure Log Analytics workspace. This agent collects monitoring data from the operating system and workloads of the computer, then sends it to the workspace where you can analyze and query the data. Joining Azure AD, configuring Windows Defender Firewall, or creating an event subscription are not directly related to enabling the collection and querying of events through Azure Log Analytics.

upvoted 1 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

**Selected Answer: A**

I think A as well

The machine must be domain joined to a Microsoft Entra tenant (AADj or Hybrid AADj machines), which enables the agent to fetch Microsoft Entra device tokens used to authenticate and fetch data collection rules from Azure.

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client#prerequisites>

upvoted 2 times

🗨️ 👤 **Krayzr** 10 months, 3 weeks ago

**Selected Answer: D**

The Azure Monitor Agent can be used to query events on a computer that is not joined to Azure AD. Joining Azure AD offers additional benefits like centralized management and conditional access, but it's not necessary for basic event collection.

Here's what you need to know for each method:

Using the Azure Monitor Agent:

Install the Azure Monitor Agent on the computer that is not joined to Azure AD.

Configure the agent to connect to your Log Analytics workspace using a Workspace Access Key instead of Azure AD authentication.

Define data collection rules to specify which events you want to collect.

The agent will collect and send the chosen events to your Log Analytics workspace where you can query them.

upvoted 3 times

🗨️ 👤 **Murad01** 11 months, 1 week ago

I would choose answer D, install Azure monitor Agent


upvoted 2 times

🗨️ 👤 **Merrybob** 11 months, 1 week ago

**Selected Answer: A**

Must be domain joined.

Ref: <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client#prerequisites>  
upvoted 1 times

  **frack** 11 months, 3 weeks ago

**Selected Answer: A**

is the right one. I initially thought I can just download the Azure Monitor Agent MSI. But then, I saw this

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client#:~:text=Not%20Microsoft%20Entra,try%20installation%20again>.

"join the device with a Microsoft Entra tenant"

upvoted 2 times

  **Tonsku** 1 year ago

**Selected Answer: D**

D. Install the Azure Monitor Agent

<https://learn.microsoft.com/en-us/azure/azure-monitor/logs/queries?tabs=groupby#permissions-required>

upvoted 1 times

  **abill** 1 year ago

think its D - <https://www.mdmandgpanswers.com/blogs/view-blog/windows-10-and-server-event-logs-to-azure-log-analytics-walkthru>

upvoted 1 times

  **NoursBear** 1 year ago

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client>

upvoted 2 times



You have a Microsoft 365 E5 subscription and 100 unmanaged iPad devices.

You need to deploy a specific iOS update to the devices. Users must be prevented from manually installing a more recent version of iOS.

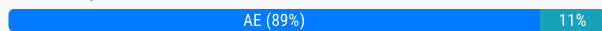
Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a device configuration profile.
- B. Enroll the devices in Microsoft Intune by using the Intune Company Portal.
- C. Create a compliance policy.
- D. Create an iOS app provisioning profile.
- E. Enroll the devices in Microsoft Intune by using Apple Business Manager.

**Suggested Answer: AE**

Community vote distribution



🗨️ 👤 **1655b71** 2 months ago

A en B

B. Enroll the devices in Microsoft Intune by using the Intune Company Portal:

In order to manage iPads and deploy iOS updates, the devices must first be enrolled in Microsoft Intune. The Intune Company Portal app allows users to register their devices for management, which is essential to control updates and enforce policies.

A. Create a device configuration profile:

After enrollment, a device configuration profile can be created to control OS updates. Within Intune, iOS update policies allow you to specify the iOS version to install on devices and prevent users from updating to newer versions than what is specified in the profile.

upvoted 1 times

🗨️ 👤 **Prasis** 5 months, 3 weeks ago

A and E

<https://learn.microsoft.com/en-us/mem/intune/protect/software-updates-ios>

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: AE**

The answer is correct. However it sucks for users since they need to reset their device.

upvoted 1 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

**Selected Answer: AE**

AE is correct

<https://learn.microsoft.com/en-us/mem/intune/protect/software-updates-ios>

upvoted 1 times

🗨️ 👤 **ckmay** 10 months, 2 weeks ago

**Selected Answer: AE**

Config profiles still allow you to prevent user from updating for up to 90 days but it will not deploy specific updates or versions.

to deploy specific updates or versions, you must create an iOS update policy but this is not one of the answer choices

however, the only way to achieve either of the other 2 steps, the device MUST be supervised and the ONLY way a device can be is if it is enrolled via ABM. Devices enrolled via company portal are NOT supervised.

upvoted 1 times

🗨️ 👤 **ckmay** 10 months, 2 weeks ago

<https://download.microsoft.com/download/e/6/2/e6233fdd-a956-4f77-93a5-1aa254ee2917/msft-intune-enrollment-options.pdf>  
<https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-ios-ipados>

Device enrollment with Company Portal: This option is a typical enrollment in the Company Portal app for personal devices. The device is managed, not just specific apps or features. With this option, consider the following information:

You can deploy certificates that apply to the whole device.

Users must install updates. Only devices enrolled using Automated Device Enrollment (ADE) can receive updates using MDM policies or profiles.

A user must be associated with the device. This user can be a device enrollment manager (DEM) account.

upvoted 1 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **Tonsku** 1 year ago

**Selected Answer: AE**

Create a device configuration profile, to configure settings on the devices, preventing users from manually installing a more recent version of iOS.

Enroll using Apple Business Manager to manage the devices and deploy the iOS update.

upvoted 1 times

🗨️ 👤 **yosry** 1 year ago

AE seems correct

upvoted 2 times

🗨️ 👤 **fco168** 1 year, 1 month ago

**Selected Answer: AE**

Correct.

You need to create a configuration profile to avoid users running the update.

Also, with the Apple Business Manager you can install a specific iOS Version manually to the device.

upvoted 4 times

🗨️ 👤 **RabbitB** 1 year, 2 months ago

**Selected Answer: AB**

Configure defer software update in Configuration profiles, but iOS need to be enrolled via Intune company portal.

upvoted 1 times

🗨️ 👤 **Contactfornitish** 1 year, 2 months ago

Compliance or app provisioning is irrelevant. To manage updates, you need device configuration profile so that's a given.

Enrollment is required though you need to via ABM to manage updates

ref: <https://learn.microsoft.com/en-us/mem/intune/protect/software-updates-ios>

upvoted 2 times

🗨️ 👤 **BJS78** 1 year, 3 months ago

Stupid question.

You can set iOS update policy ONLY on SUPERVISED devices, so yes, ABM is required.

iOS update policy is REQUIRED to define the exact update to have, but does not block you to update manually, for that you need a Device restriction policy in place.

That also blocks the user up to 90 days only, after that user can install update manually again.

upvoted 4 times

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have an update ring named UpdateRing1 that contains the following settings:

- Automatic update behavior: Auto install and restart at a scheduled time
- Automatic behavior frequency: First week of the month
- Scheduled install day: Tuesday
- Scheduled install time: 3 AM

From the Microsoft Intune admin center, you select Uninstall for the feature updates of UpdateRing1.


When will devices start to remove the feature updates?

- A. when a user approves the uninstall
- B. as soon as the policy is received
- C. next Tuesday
- D. the first Tuesday of the next month

**Suggested Answer:** B

Community vote distribution

B (100%)

 **ExamKiller020** Highly Voted 1 year, 3 months ago

**Selected Answer: B**

Given answer is correct.

Windows devices start removal of updates as soon as they receive the change in Intune policy. Update removal isn't limited to maintenance schedules, even when they're configured as part of the update ring.


REF: <https://learn.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings#uninstall>

upvoted 13 times

 **kay000001** 1 year, 1 month ago

Thanks for the Microsoft link and clarification!

upvoted 1 times

 **Darkfire** 10 months, 2 weeks ago

Very much correct :)

upvoted 1 times

 **oopspruu** Most Recent 5 months, 2 weeks ago

**Selected Answer: B**

Given answer is correct. The Uninstall command doesn't consider any schedules and will immediately start removing features. Also, it force restarts your device without giving you the ability to delay the restart.

upvoted 1 times

 **Merrybob** 11 months ago

**Selected Answer: B**

B. as soon as the policy is received

Ref: <https://learn.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings#uninstall-~:text=When%20you%20use%20the%20Uninstall%20option%2C%20Intune%20passes%20the%20uninstall%20request%20to%20devices%2C>

upvoted 1 times

You have a hybrid deployment of Azure AD that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Intune.

You discover that Group Policy settings override the settings configured in Microsoft Intune policies.

You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings.

What should you do?



- A. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy.
- B. From the Microsoft Intune admin center, create a custom device profile.
- C. From the Microsoft Intune admin center, create an Administrative Templates device profile.
- D. From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy.

**Suggested Answer: B**

Community vote distribution

B (69%)

C (31%)

 **ExamKiller020**  1 year, 3 months ago

**Selected Answer: B**

Given answer is correct.

REF: <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict#mdmwinsovergp>  
upvoted 11 times

 **yoha1558** 1 year, 2 months ago

tested in intune !

upvoted 1 times

 **smart008** 10 months, 3 weeks ago

Have you checked Administrative templates? If you are unable to find override group policy settings feature in administrative template, then you can choose custom.

upvoted 1 times

 **VirtualJP**  1 year, 2 months ago

**Selected Answer: C**

Here's why:

Administrative Templates device profiles in Microsoft Intune allow you to configure a wide range of settings, similar to Group Policy settings. When applied, these profiles can take precedence over Group Policy settings on enrolled devices.

upvoted 8 times

 **conartistique** 1 year, 2 months ago

That's it, you can look it up in Intune > Device Configuration Profiles > Administrative Templates > Turn off Local Group Policy Objects processing.

upvoted 2 times

 **MR\_Eliot** 10 months, 1 week ago

B is correct:

This policy setting prevents Local Group Policy Objects (Local GPOs) from being applied.

By default, the policy settings in Local GPOs are applied before any domain-based GPO policy settings. These policy settings can apply to both users and the local computer. You can disable the processing and application of all Local GPOs to ensure that only domain-based GPOs are applied.

If you enable this policy setting, the system does not process and apply any Local GPOs.

If you disable or do not configure this policy setting, Local GPOs continue to be applied.

Note: For computers joined to a domain, it is strongly recommended that you only configure this policy setting in domain-based GPOs. This policy setting will be ignored on computers that are joined to a workgroup.

Setting type: Device  
upvoted 2 times

🗨️ **Seek12** Most Recent 1 week, 3 days ago

**Selected Answer: A**

GPO: Computer Configuration > Administrative Templates > Windows Components > MDM  
> "MDM Policy Refresh" > "Enable MDM Wins Over GPO"  
upvoted 1 times

🗨️ **yhano** 1 month, 2 weeks ago

As of now there is available in settings catalogue already, but since not in the option then I would go on the custom. B.  
upvoted 2 times

🗨️ **59c6be3** 4 weeks, 1 day ago

Agreed, just checked. It's not in the Administrative Templates, but it is available in the settings catalogue.  
upvoted 1 times

🗨️ **1655b71** 2 months ago

C

Therefore, creating an Administrative Templates device profile in Intune is the best option to attempt to override conflicting Group Policy settings with Intune policies.

upvoted 2 times

🗨️ **Cezt** 5 months, 1 week ago

currently found in settings catalog  
upvoted 1 times

🗨️ **oopspruu** 5 months, 2 weeks ago

**Selected Answer: B**

The option where MDM wins over GP is not found in Settings Catalogue > Administrative Templates but instead in Settings Catalogue > Control Policy Conflict.

So in the given options, B is the correct answer.

upvoted 3 times

🗨️ **Prasis** 5 months, 3 weeks ago

To ensure that the settings configured in Microsoft Intune override the Group Policy settings, you should create a custom device profile from the Microsoft Intune admin center (Option B).

In this custom device profile, you need to define a custom policy named ControlPolicyConflict/MDMWinsOverGP

upvoted 1 times

🗨️ **CJL324** 7 months, 2 weeks ago

C. From the Microsoft Intune admin center, create an Administrative Templates device profile.

Functionality: Administrative Templates in Intune are similar to Group Policy settings and allow you to manage settings on Windows 10 devices through Intune.

Overrides Group Policy: By configuring these settings in Intune, you can ensure they take precedence over local Group Policy settings

The other options do not override GPOs

upvoted 1 times

🗨️ **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 2 times

🗨️ **MR\_Eliot** 10 months, 1 week ago

<https://www.anoopcnaair.com/mdm-wins-over-gpo-group-policy-intune-policy/>

upvoted 1 times

🗨️ **Darkfire** 10 months, 2 weeks ago

**Selected Answer: B**

B is correct

Sign in to the Microsoft Endpoint Manager admin center (Endpoint.Microsoft.com)

Select Devices -> Windows -> Configuration profiles > Create profile.

In Create Profile, You can select Platform: Windows 10 and later and Profile: Select Settings catalog (preview).

Click on Create button.

In Configuration Settings, select Add settings and use the following search keyword "MDM Wins Over GP." You need to choose the MDM Wins Over GP pol list.

[https://www.anoopcnaair.com/mdm-wins-over-gpo-group-policy-intune-](https://www.anoopcnaair.com/mdm-wins-over-gpo-group-policy-intune-policy/#:~:text=Option%20%231%20(New%20Method)%20%E2%80%93%20Intune%20Settings%20Catalog%20%7C%20Create%20MDM%20Wins%20Over%2)

[policy/#:~:text=Option%20%231%20\(New%20Method\)%20%E2%80%93%20Intune%20Settings%20Catalog%20%7C%20Create%20MDM%20Wins%20Over%2](https://www.anoopcnaair.com/mdm-wins-over-gpo-group-policy-intune-policy/#:~:text=Option%20%231%20(New%20Method)%20%E2%80%93%20Intune%20Settings%20Catalog%20%7C%20Create%20MDM%20Wins%20Over%2)

upvoted 2 times

🗨️ **smart008** 10 months, 3 weeks ago

**Selected Answer: C**

In my viewpoint, custom profile can do more than just over-ride GPO settings. However, our first priority will be using the built-in features which you can already find in Administrative templates and even you can then see the stats such as which GPOs were implemented, which were not or which made conflict. I would say custom profiles should be used if we can't find the settings we require all in one place or is not available in the built-in options.

upvoted 1 times

🗨️ **Merrybob** 11 months ago

**Selected Answer: B**

B. From the Microsoft Intune admin center, create a custom device profile.

Ref: [https://www.anoopcnaair.com/mdm-wins-over-gpo-group-policy-intune-](https://www.anoopcnaair.com/mdm-wins-over-gpo-group-policy-intune-policy/#:~:text=Option%20%231%20(New%20Method)%20%E2%80%93%20Intune%20Settings%20Catalog%20%7C%20Create%20MDM%20Wins%20Over%2)

[policy/#:~:text=Option%20%231%20\(New%20Method\)%20%E2%80%93%20Intune%20Settings%20Catalog%20%7C%20Create%20MDM%20Wins%20Over%2](https://www.anoopcnaair.com/mdm-wins-over-gpo-group-policy-intune-policy/#:~:text=Option%20%231%20(New%20Method)%20%E2%80%93%20Intune%20Settings%20Catalog%20%7C%20Create%20MDM%20Wins%20Over%2)

upvoted 1 times

🗨️ **BJ578** 1 year ago

The key is the wording here: "You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings." This means GPO setting MUST be applied but when it conflicts with Intune, Intune should prevail. Option "C" can "Turn off Local Group Policy Objects processing." which stops ALL GPO to be processed, so this NOT what the scenario describes here. (mdmwinsovergp can be set via Settings Catalog as well btw)

upvoted 4 times

🗨️ **CyberBuck\_92** 1 year ago

I'm not certain that the Admin Template answer is actually the correct because its really found in the Settings Catalog and doesn't outright credit itself as an Administrative Template

upvoted 1 times

🗨️ **yosry** 1 year ago

**Selected Answer: B**

B seems correct

upvoted 2 times

🗨️ **chandravamsi** 1 year, 1 month ago

**Selected Answer: B**

Although B can do the same , A standard template is available in C

upvoted 1 times

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to ensure that the startup performance of managed Windows 11 devices is captured and available for review in the Intune admin center.

What should you configure?

- A. the Azure Monitor agent
- B. a device compliance policy
- C. a Conditional Access policy
- D. an Intune data collection policy

**Suggested Answer: A**

*Community vote distribution*

D (100%)

🗨️ 👤 **027ea51** 4 months, 3 weeks ago

D. an Intune data collection policy

An Intune data collection policy allows you to collect performance and diagnostic data from managed devices. This includes data related to startup performance, which can then be reviewed in the Intune admin center.

Here's why the other options are not suitable for this task:

A. the Azure Monitor agent: While the Azure Monitor agent can capture various performance metrics and logs, it is not directly managed through Intune and is more commonly used in Azure environments for broader monitoring and diagnostics.

B. a device compliance policy: Compliance policies are used to ensure devices meet specific security and configuration requirements. They do not capture performance metrics.

C. a Conditional Access policy: Conditional Access policies control access to resources based on certain conditions but do not handle performance data collection.

upvoted 2 times

🗨️ 👤 **Cezt** 5 months, 1 week ago

currently is called windows health monitoring policy -> endpoint analytics

upvoted 1 times

🗨️ 👤 **OyYaGotta** 9 months, 3 weeks ago

**Selected Answer: D**

From Microsoft's own Copilot -

The Azure Monitor Agent (AMA) can collect a wide range of data from the guest operating system of Azure and hybrid virtual machines, including performance data<sup>1</sup>. However, it doesn't directly monitor or display the startup performance of a device<sup>2</sup>.

upvoted 3 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: D**

D is correct.

Keyword to look for: "for review in the Intune admin center".

upvoted 1 times

🗨️ 👤 **Krayzr** 10 months, 3 weeks ago

**Selected Answer: D**

D. an Intune data collection policy. Here's why:

Azure Monitor agent: While this agent collects performance data, it focuses on Azure resources, not individual devices managed by Intune.

Device compliance policy: These policies focus on ensuring devices meet security and configuration requirements, not collecting specific data like startup performance.

Conditional Access policy: These policies determine user access to resources, not data collection on devices.

Intune data collection policy: This is the specifically designed option for capturing various data points from managed devices, including startup performance metrics. You can configure this policy to collect boot and sign-in times, application launch times, and overall device health data.

Therefore, to capture and review startup performance of managed Windows 11 devices in the Intune admin center, you need to configure an Intune data collection policy.

upvoted 2 times

🗨️ **Merrybob** 11 months ago

**Selected Answer: D**

D. an Intune data collection policy.

Similar to how Log Analytics Workspaces work, you need a data collection rule/policy to forward data from the source (Windows 11 devices) to a datastore (aka database or workspace).

Ref: [https://learn.microsoft.com/en-us/mem/analytics/data-](https://learn.microsoft.com/en-us/mem/analytics/data-collection#:~:text=For%20Intune%2Dmanaged%20devices%2C%20this%20step%20configures%20the%20Intune%20data%20collection%20policy.)

[collection#:~:text=For%20Intune%2Dmanaged%20devices%2C%20this%20step%20configures%20the%20Intune%20data%20collection%20policy.](https://learn.microsoft.com/en-us/mem/analytics/data-collection#:~:text=For%20Intune%2Dmanaged%20devices%2C%20this%20step%20configures%20the%20Intune%20data%20collection%20policy.)

Ref: <https://learn.microsoft.com/en-us/mem/analytics/data-collection#:~:text=totalBootTimeInMilliseconds%3A%20Total%20boot%20time>

upvoted 2 times

🗨️ **Tonsku** 1 year ago

**Selected Answer: D**

D. an Intune data collection policy

<https://learn.microsoft.com/en-us/mem/intune/configuration/windows-health-monitoring#create-the-profile>

upvoted 1 times

🗨️ **kay000001** 1 year, 1 month ago

**Selected Answer: D**

Answer is D:

This is how you do it: <https://learn.microsoft.com/en-us/mem/intune/configuration/windows-health-monitoring>

upvoted 1 times

🗨️ **chandravamsi** 1 year, 1 month ago

Option : A

upvoted 1 times

🗨️ **ExamKiller020** 1 year, 3 months ago

**Selected Answer: D**

Given answer isn't correct. The azure monitoring agent can be used to collect Windows event logs for example.

Answer is D.

REF: <https://learn.microsoft.com/en-us/mem/analytics/data-collection>

upvoted 4 times

🗨️ **picho707** 1 year, 3 months ago

To ensure that the startup performance of managed Windows 11 devices is captured and available for review in the Intune admin center, you should configure an Intune data collection policy.

upvoted 3 times

🗨️ **Fortind1974** 1 year, 3 months ago

**Selected Answer: D**

D. an Intune data collection policy

[https://learn.microsoft.com/en-us/mem/analytics/enroll-intune#bkmk\\_onboard](https://learn.microsoft.com/en-us/mem/analytics/enroll-intune#bkmk_onboard)

upvoted 3 times



HOTSPOT

-

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

Devices are enrolled in Intune as shown in the following table.

Name	Platform	Enrolled by using
Device1	iOS	Apple Automated Device Enrollment (ADE)
Device2	iPadOS	Apple Automated Device Enrollment (ADE)
Device3	iPadOS	The Company Portal app

The devices are the members of groups as shown in the following table.

Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

You create an iOS/iPadOS update profile as shown in the following exhibit.

## Create profile ...

iOS/iPadOS

Basics
  Configuration settings
  Scope tags
  Assignments
  **5 Review + create**

### Summary

#### Basics

Name Profile1

Description ..

#### Update policy settings

Update to install	Install iOS/iPadOS Latest update			
Schedule type	Update outside of scheduled time			
Time zone	UTC ±00			
Time window	<b>Start day</b>	<b>Start time</b>	<b>End day</b>	<b>End time</b>
	Monday	1 AM	Wednesday	1 PM
	Friday	1 AM	Saturday	11 PM

#### Assignments

##### Included groups

**Group** **Group Members** ⓘ

Group1 3 devices, 0 users

##### Excluded groups

**Group** **Group Members** ⓘ

Group2 1 devices, 0 users

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


NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	<input type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input type="radio"/>	<input type="radio"/>

## Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	<input checked="" type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input type="radio"/>	<input checked="" type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input type="radio"/>	<input checked="" type="radio"/>

 **picho707** Highly Voted 9 months ago


The way I see the answers. Please correct me if I am wrong:

1: Yes, The update will be installed on Wednesday after 1 PM because the policy applies to the device.

2: No, If a device is excluded from a software update policy and an update is available for download, the device will not install the update automatically.

3: No, The device was not enrolled as a supervised device ( enrolled via the company portal) so the policy will not apply meaning the device will not update automatically.

upvoted 14 times

 **AdamRachel** 5 months, 3 weeks ago

and for device 3 can not be enrolled in Sunday as policy finish S.atursday

upvoted 3 times

 **MR\_Eliot** Most Recent 4 months, 1 week ago

I agree with the answer.

Second device, does not receive the policy because of exclusion group.

Third device, is not supervised, so you cannot control updates.

upvoted 3 times

 **Darkfire** 4 months, 2 weeks ago

Answer is right

Q1 > Yes Wednesday after 1PM (because of the OUTSIDE of scheduled time)

Q2 > No (because of the Group 2, exclude go over include, least rights)

Q3 > No (Because of the Company portal app, not added to ADE)

upvoted 4 times

 **onepunchkenshin** 5 months, 3 weeks ago

can anyone explain why the answer 1 is yes please? why not update immediately on Tuesday?

upvoted 1 times

 **ClaudiuR2023** 4 months, 4 weeks ago



Q1- yes, because:

- Device1 is part of Group1 (which is included )

-the update runs during the specified timeframe (Tuesday - which is between Monday and Friday)



Why not immediately? - it isn't relevant, could be multiple reasons (no Internet connectivity), important is to be in the specified time frame (Monday-Wednesday, Friday-Saturday, with the timestamp of course)

upvoted 1 times

  **Engr001** 4 months, 1 week ago



its because it can only install outside of the schedules time which is untill wednesday

upvoted 1 times

  **Grg433** 9 months, 3 weeks ago

can anyone please explain this : why second and third is No ?

upvoted 2 times

  **Fortind1974** 9 months, 3 weeks ago

2: Device 2 is in the included and excluded group, but excluded takes precedence. So there is no applicable update policy for it.

3: You can only manage software updates for iOS/iPad devices that are enrolled through Apple's Automated Device Enrollment (ADE).

upvoted 18 times

  **Casticod** 9 months ago

Agree +1

upvoted 3 times

You have a Microsoft Intune deployment that contains the resources shown in the following table.

Name	Type	Platform
Comply1	Device compliance policy	Windows 10 and later
Comply2	Device compliance policy	iOS/iPadOS
CA1	Conditional Access policy	<i>Not applicable</i>
Conf1	Device configuration profile	Windows 10 and later
Office1	Office app policy	<i>Not applicable</i>

You create a policy set named Set1 and add Comply1 to Set1.


Which additional resources can you add to Set1?

- A. Conf1 only
- B. Comply2 only
- C. Comply2 and Conf1 only
- D. CA1, Conf1, and Office1 only
- E. Comply2, CA1, Conf1, and Office1

**Suggested Answer: C**

Community vote distribution


C (100%)

 **Fortind1974** Highly Voted 1 year, 3 months ago


**Selected Answer: C**

C. Comply2 and Conf1 only


<https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets>  
upvoted 7 times

 **Crille** Most Recent 2 months ago

it say additional resources is not conf1 include in comply1?  
upvoted 1 times

 **matrixuser** 9 months, 2 weeks ago

please correct me - my answer is A-conf1 only  
reason comply 2 even though it is device compliance policy it is applied to ios/ipad the original set 1 includes win10 and later already added . is  
it possible to create set with compliance policys of two different OS ? please comment .. thankyou :)  
upvoted 1 times

 **oopspruu** 5 months, 2 weeks ago

When you create a policy set, you don't have to choose a particular OS. You just have to apply it to a group which can have devices with  
different OS.  
upvoted 1 times


 **Jaquelakzaque** 7 months, 1 week ago

From the Microsoft Learn Page: "Policy sets support Windows, Android, macOS, and iOS/iPadOS settings, and can be assigned cross-platform."

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets>

So given Answer C is correct.

upvoted 2 times

 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: C**

After my own research in my test tenant, C is the answer.  
upvoted 2 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

**Selected Answer: C**

C is correct

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets#:~:text=You%20can%20include,Settings%20catalog%20policies>  
upvoted 1 times

🗨️ 👤 **Merrybob** 11 months ago

C. Comply2 and Conf1 only

You can include the following management objects in a policy set:

Apps

App configuration policies

App protection policies

Device configuration profiles

Device compliance policies

Windows autopilot deployment profiles

Enrollment status page

Settings catalog policies

Ref: <https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets#:~:text=You%20can%20include,Settings%20catalog%20policies>  
upvoted 4 times

🗨️ 👤 **belyo** 1 year ago

**Selected Answer: C**

C - policy sets can be assigned cross-platform

it can include also app policy named office 1 but not listed in possible answers

cant contain CA policies

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets>

upvoted 4 times

🗨️ 👤 **Kevern** 1 year ago

**Selected Answer: C**

C - can't add CA1 or Office policies to sets according to MS Learn materials

upvoted 1 times

🗨️ 👤 **yosry** 1 year ago

**Selected Answer: C**

C seems correct

upvoted 1 times

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.

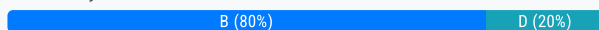
You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.

Which tool should you use?

- A. Microsoft Defender for Endpoint Power BI app
- B. Microsoft Secure Score
- C. Endpoint Analytics
- D. Microsoft 365 Defender portal

**Suggested Answer: D**

Community vote distribution



🗨️ 👤 **Pisces225** 1 month, 1 week ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/defender-vulnerability-management/tvm-security-baselines#get-started-with-security-baselines-assessment>  
upvoted 1 times

🗨️ 👤 **1655b71** 2 months ago

B:

So, Microsoft Secure Score is the best choice for assessing differences between your current configuration and Microsoft-recommended security baselines for Microsoft Defender for Endpoint.

upvoted 1 times

🗨️ 👤 **nsss** 2 weeks, 1 day ago

And the secure score can be found in the M365 Defender Portal... I don't get how you are supposed to choose, both answers can be correct imo

upvoted 1 times

🗨️ 👤 **RomanV** 3 months, 1 week ago

This one should not be difficult. I work in cyber sec. and it's the secure score I also use to check Microsoft recommendations regarding Defender4E.

Source --> <https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score?view=o365-worldwide>

upvoted 1 times

🗨️ 👤 **RFULL** 5 months, 2 weeks ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/defender-vulnerability-management/tvm-security-baselines#get-started-with-security-baselines-assessment>  
upvoted 3 times

🗨️ 👤 **CJL324** 7 months, 2 weeks ago

D. Microsoft 365 Defender portal

The Microsoft 365 Defender portal provides a centralized interface for managing security across your Microsoft 365 environment, including Microsoft Defender for Endpoint. It includes the "Threat & Vulnerability Management" (TVM) feature, which offers capabilities to compare your current security configuration against Microsoft's recommended baselines. This tool helps you identify gaps and deviations in your configuration, providing actionable insights to improve your security posture.

upvoted 1 times

🗨️ 👤 **CJL324** 7 months, 2 weeks ago

Why NOT B

While Secure Score provides an overall security posture assessment and recommendations for your Microsoft 365 environment, it is more focused on broad security measures rather than detailed configuration comparisons specifically for Microsoft Defender for Endpoint.

upvoted 1 times

🗨️ 👤 **OyYaGotta** 9 months, 3 weeks ago

Microsoft secure score does not compare settings of a security baseline with the available options in a custom security policy. You need to look at the baseline in 365 admin and assess the differences in creating a custom baseline. B isn't correct because secure score gives you a wide range of options to change to improve your score which do not necessarily only recommend the baseline. Correct answer is D.

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

**Selected Answer: B**

I think B should be the answer as well.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide>

upvoted 2 times

🗨️ 👤 **OyYaGotta** 9 months, 3 weeks ago

Where does that article mention Security Baselines? Answer is D where you look to assess the custom security policies over Security Policies.

upvoted 1 times

🗨️ 👤 **Tonsku** 1 year ago

**Selected Answer: B**

B. Microsoft Secure Score

upvoted 2 times

🗨️ 👤 **chandravamsi** 1 year, 1 month ago

**Selected Answer: B**

Option B: Microsoft Secure score

upvoted 1 times

🗨️ 👤 **cpaljhc4** 1 year, 1 month ago

Secure score is stated in MD101 exam topics

<https://www.examttopics.com/discussions/microsoft/view/65809-exam-md-101-topic-4-question-48-discussion/>

upvoted 2 times

🗨️ 👤 **iamforksu** 1 year, 2 months ago

**Selected Answer: B**

As other's stated.

upvoted 2 times

🗨️ 👤 **Fortind1974** 1 year, 3 months ago

**Selected Answer: B**

B. Microsoft Secure Score

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score>

upvoted 4 times

🗨️ 👤 **Crismo** 1 year, 3 months ago

I also tend to B. It's also chatGPTs choice:

B. Microsoft Secure Score

Microsoft Secure Score is a tool that helps organizations assess their security posture across various Microsoft products, including Microsoft Defender for Endpoint. It provides recommendations and best practices based on Microsoft's security baseline configurations. By using Microsoft Secure Score, you can evaluate the configuration of Microsoft Defender for Endpoint against the recommended configuration baseline and identify areas where improvements can be made to enhance your overall security posture.

upvoted 4 times

You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune.

You plan to integrate Intune with Microsoft Defender for Endpoint.

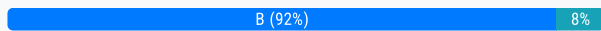
You need to establish a service-to-service connection between Intune and Defender for Endpoint.

Which settings should you configure in the Microsoft Intune admin center?

- A. Premium add-ons
- B. Connectors and tokens
- C. Tenant enrollment
- D. Microsoft Tunnel Gateway

**Suggested Answer: B**

Community vote distribution



**Moot2** 1 month, 2 weeks ago

**Selected Answer: B**

is correct

upvoted 1 times

**RomanV** 3 months, 1 week ago

There are 2 ways to do this.

1. Go to the Intune Management portal > Tenant administration > Connectors and tokens > Microsoft Defender for Endpoint (this is the option available here so the answer is B.

Or 2: Go to the Intune Management portal > Endpoint security > Microsoft Defender for Endpoint

upvoted 1 times

**CJL324** 7 months, 2 weeks ago

B. Connectors and tokens

Connectors and Tokens: This setting allows you to create and manage the connection between Intune and other services, including Microsoft Defender for Endpoint. By configuring connectors and tokens, you establish the integration between Intune and Defender for Endpoint, enabling them to communicate and share security information.

upvoted 3 times

**MR\_Eliot** 10 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

**Darkfire** 10 months, 2 weeks ago

**Selected Answer: B**

B is correct

<https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure>

upvoted 2 times

**Merrybob** 11 months ago

**Selected Answer: B**

B. Connectors and tokens

upvoted 2 times



🗨️ 👤 **Tonsku** 1 year ago

**Selected Answer: B**

B. Connectors and tokens  
upvoted 3 times

🗨️ 👤 **HawkieEyes** 1 year, 1 month ago

**Selected Answer: B**

Andrew is B  
upvoted 4 times

🗨️ 👤 **HawkieEyes** 1 year, 1 month ago

Sorry, Answer is B  
upvoted 3 times

🗨️ 👤 **cpaljchc4** 1 year, 1 month ago

MD101 has the same answer

<https://www.examttopics.com/discussions/microsoft/view/98243-exam-md-101-topic-5-question-40-discussion/>

upvoted 3 times

🗨️ 👤 **h38jhd38k** 1 year, 2 months ago

Answer correct and can see the confusion of Tenant since it is part of the steps.

<https://learn.microsoft.com/en-us/mem/configmgr/tenant-attach/device-sync-actions>

upvoted 3 times

🗨️ 👤 **Contactfornitish** 1 year, 2 months ago

**Selected Answer: C**

Tenant attach or Tenant enrollment it would be

Ref: <https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure>

You go to Defender portal and then just enable a switch, no connector menu etc

upvoted 1 times

🗨️ 👤 **VirtualJP** 1 year, 2 months ago

I go with B

upvoted 2 times

DRAG DROP

You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).

You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.

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

### Actions

From the Microsoft Intune admin center, configure enrollment restrictions.

From the Enterprise CA, configure certificate managers.

Obtain the root certificate.

From the Microsoft Intune admin center, create a trusted certificate configuration profile.

From the Microsoft Intune admin center, create a PKCS certificate configuration profile.

### Answer Area

1

2

3


### Answer Area

Obtain the root certificate.

### Suggested Answer:

From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.

From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile.

 **Casticod** Highly Voted 1 year, 3 months ago

Agreed

1) Obtain the root certificate

<https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure#export-the-root-certificate-from-the-enterprise-ca>

2) From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile

<https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure#create-a-trusted-certificate-profile>

3) From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile


<https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure#create-a-pkcs-certificate-profile>

upvoted 8 times

 **1125BravadoGuy** 11 months, 4 weeks ago

Why the heck does it say Intune though???

upvoted 1 times

 **oopspruu** 5 months, 2 weeks ago


If you don't know that Intune and Endpoint Manager are the same things, you really shouldn't attempt this exam at this time and need a lot of study.

upvoted 4 times

 **NoursBear** 11 months, 3 weeks ago

?? Intune = MS Endpoint Manager

upvoted 1 times

 **Moot2** Most Recent 1 month, 2 weeks ago

Answer correct - <https://learn.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure>

upvoted 1 times

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.

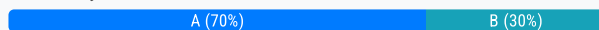
You need to ensure that the policies can target the devices based on their version of Android or iOS.

What should you configure first?

- A. groups that have dynamic membership rules in Azure AD
- B. Device categories in Intune
- C. Corporate device identifiers in Intune
- D. Device settings in Azure AD

**Suggested Answer:** A

Community vote distribution



**oopspruu** Highly Voted 4 months, 2 weeks ago

**Selected Answer: A**

There is no option at all in Device Category which would let you choose device platform or OS version. Stop choosing answers based on what ChatGPT tells you and actually open the Intune portal and see for yourselves. ChatGPT makes up a lot of nonsense and you are blindly believing it.

You can create a dynamic device type group based on deviceOSType or deviceOSVersion flags.

upvoted 5 times

**Cezt** Most Recent 5 months, 1 week ago

**Selected Answer: A**

A is correct

upvoted 2 times

**Prasis** 5 months, 3 weeks ago

To target devices based on their version of Android or iOS using Microsoft Intune, you should first configure groups that have dynamic membership rules in Azure AD (Option A).

upvoted 2 times

**CJL324** 7 months, 2 weeks ago

**Selected Answer: B**

B. Device categories in Intune

Device categories in Intune allow you to organize devices based on specific criteria such as device type, platform (Android or iOS), or version. By configuring device categories, you can group devices with similar characteristics together, making it easier to apply policies based on their version of Android or iOS.

A. Groups that have dynamic membership rules in Azure AD:

While Azure AD groups with dynamic membership rules can be useful for dynamically grouping users or devices based on attributes, they may not directly address the need to target policies based on the version of Android or iOS installed on the devices.

upvoted 2 times

**Darkfire** 10 months, 2 weeks ago

**Selected Answer: A**

A is correct

You can configure Android or iOS version to a Dynamic Group. Which then adds the device to the dynamic group based on the devices version.

With Device Categories you can't.

<https://learn.microsoft.com/en-us/archive/blogs/pauljones/dynamic-group-membership-in-azure-active-directory-part-2>  
upvoted 3 times

🗨️ **Merrybob** 11 months ago

**Selected Answer: A**

A. Groups that have dynamic membership rules in Azure AD

Ref 1: <https://learn.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping#:~:text=Device%20categories%20allow,Entra%20security%20groups>.

Ref 2: <https://techcommunity.microsoft.com/t5/microsoft-intune/targeting-different-intune-policies-to-different-devices-for-the/m-p/341172>

upvoted 2 times

🗨️ **Tonsku** 1 year ago

**Selected Answer: B**

B. Device categories in Intune

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-os-versions#operating-system-version-control-using-intune-mobile-device-management-enrollment-restrictions>

upvoted 1 times

🗨️ **NoursBear** 1 year ago

I think there is a misconception of Device Categories, from what I understand, categories are created, then the users themselves have to select what category their device belongs to. I don't think device categories are correct for the purpose of this question

upvoted 4 times

🗨️ **ckmay** 10 months, 2 weeks ago

Correct. Device categories is strictly a MANUAL category assignment to a device, either by the end user or an admin in the portal. Creating a categories literally only generates a list of all the created categories that can then be manually selected to apply to enrolled devices, but it does not query or determine device characteristics and then "tag" the device the category based on it's query.

A dynamic group does query device characteristics then add them to a group based on those characteristics. Example: you can create a device category called "iOS devices" and then create a dynamic group called "iOS devices" and configure the rules to include only devices who match the device category "iOS devices" but the problem is that Android users could have selected that category for their device so this would NOT ensure specific platforms or versions are selected correctly.

upvoted 1 times

🗨️ **ckmay** 10 months, 2 weeks ago

<https://learn.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>

"Regardless of platform, any device user can sign in to portal.manage.microsoft.com at anytime and go to My devices to select a category."

upvoted 1 times

🗨️ **HawkieEyes** 1 year, 1 month ago

**Selected Answer: A**

Answer is A

upvoted 3 times

🗨️ **Kiookr** 1 year, 1 month ago

**Selected Answer: A**

One thing I have learn in Azure Intune, "Groups" are very important to associate rules or any other things like polices .. Thus I will go with A

upvoted 1 times

🗨️ **Tigasmigas** 1 year, 1 month ago

**Selected Answer: A**

A - <https://www.examttopics.com/discussions/microsoft/view/5327-exam-md-101-topic-3-question-4-discussion/>

upvoted 3 times

🗨️ **cpaljchc4** 1 year, 1 month ago

Answer and discussion in MD101 goes with Dynamic groups

<https://www.examttopics.com/discussions/microsoft/view/5327-exam-md-101-topic-3-question-4-discussion/>

upvoted 3 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

I am with A, in a Dynamic Groups you use query expressions to group models etc...

upvoted 1 times

🗨️ 👤 **fco168** 1 year, 1 month ago

**Selected Answer: A**

In dynamic groups you can query the devices by OS versions.

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

**Selected Answer: B**

agree with virtualJP

upvoted 1 times

🗨️ 👤 **Mahi\_444** 1 year, 2 months ago

**Selected Answer: B**

Question is what should we configure first?!!

upvoted 1 times

🗨️ 👤 **cpaljchc4** 1 year, 1 month ago

Device categories didn't mention anything related to device version though.

Whereas under the dynamic device group, there is a function of that

upvoted 2 times

🗨️ 👤 **Contactfornitish** 1 year, 2 months ago

**Selected Answer: A**

Device category needs to use dynamic group based on device.osVersion

Confusing but answer would be A since B without dynamic group can not do that. It says what would you do FIRST

upvoted 2 times

DRAG DROP

-

You have 500 Windows 10 devices enrolled in Microsoft Intune.

You plan to use Exploit protection in Microsoft Intune to enable the following system settings on the devices:

- Data Execution Prevention (DEP)
- Force randomization for images (Mandatory ASLR)

You need to configure a Windows 10 device that will be used to create a template file.

Which protection areas on the device should you configure in the Windows Security app before you create the template file? To answer, drag the appropriate protection areas to the correct settings. Each protection area may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

### Protection areas

### Answer Area

- Account protection
- App & browser control
- Device security
- Virus & threat protection

DEP:


Mandatory ASLR:

### Answer Area

Suggested Answer:

DEP:

Mandatory ASLR:

 **TestTaker09876** Highly Voted 8 months, 3 weeks ago

Congrats if you made it this far. Keep on Going!

upvoted 43 times

 **665d390** 4 months ago

correcto

upvoted 2 times

 **1f85a58** 8 months, 2 weeks ago

Everytime I go through all the questions from scratch and I get here I want to upvote again haha

upvoted 6 times

 **oopspruu** Most Recent 5 months, 2 weeks ago

Exploit Protection is found under App & Browser control in Windows Security app. Given answer is correct. Both DEP and Force Randomization settings can be found there.

upvoted 1 times

 **Merrybob** 11 months ago

DEP: App & Browser Control

Ref: <https://support.microsoft.com/en-us/topic/what-is-data-execution-prevention-dep-60dabc2b-90db-45fc-9b18-512419135817#:~:text=Select%20App%20%26%20browser%20control>

Mandatory ASLR: App & Browser Control

Ref: [https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/customize-exploit-protection?view=o365-worldwide#:~:text=No-,Data%20Execution%20Prevention%20\(DEP\),No-,Randomize%20memory%20allocations](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/customize-exploit-protection?view=o365-worldwide#:~:text=No-,Data%20Execution%20Prevention%20(DEP),No-,Randomize%20memory%20allocations)  
upvoted 4 times

🗨️ 👤 **reastman66** 1 year, 1 month ago

App & Browser <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwideControl>  
upvoted 1 times

🗨️ 👤 **BJ578** 1 year, 3 months ago

Trick is that it is about "Windows Security" app. There DEP is the 2nd, randomization is the 3rd option in the Exploit Protection, which is under App & browser control. The answer is correct.  
upvoted 1 times

🗨️ 👤 **Grg433** 1 year, 3 months ago

Should be this no ?  
Virus & Threat Protection for DEP.  
App & Browser Control for Mandatory ASLR.  
upvoted 1 times

🗨️ 👤 **Grg433** 1 year, 3 months ago

sorry, I was wrong - answer is correct both can be found in - windows security > App & Browser Control  
upvoted 7 times



You have an Azure AD tenant named contoso.com.

You have a workgroup computer named Computer1 that runs Windows 11.

You need to add Computer1 to contoso.com.

What should you use?


- A. dsregcmd.exe
- B. Computer Management
- C. netdom.exe
- D. the Settings app

**Suggested Answer:** D

Community vote distribution

D (93%)

7%


 **ergacharsk** 5 months, 2 weeks ago

**Selected Answer: D**

To add a workgroup computer running Windows 11 to an Azure AD tenant, you should use:

D. the Settings app

upvoted 2 times

 **Darkfire** 10 months, 2 weeks ago

**Selected Answer: D**

D is correct

Settings > System > About > Domain or Workgroup > Change > Select Member of, Domain.

upvoted 3 times

 **Merrybob** 11 months ago

**Selected Answer: D**

D. the Settings app

upvoted 2 times

 **belyo** 1 year ago


**Selected Answer: D**

netdom is obsolete and used for oldest version, so doesnt apply here

dsregcmd is for status, i also got fooled in first place

you can join it from setting in this scenario

upvoted 1 times

 **F3RRY** 1 year, 1 month ago

**Selected Answer: D**

Question is in regard to Entra ID, so it is via Settings app


upvoted 1 times

 **Rocky83** 1 year, 2 months ago

**Selected Answer: D**

Should be D

upvoted 2 times

 **firefox15** 1 year, 2 months ago

**Selected Answer: D**

The question is in regard to Azure AD (not on-prem AD DS) which limits your options. Netdom isn't going to work. It needs to be the Settings app.

upvoted 2 times

🗨️ 👤 **Monades** 1 year, 2 months ago

**Selected Answer: D**

D

<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 3 times

🗨️ 👤 **majerzg** 1 year, 3 months ago

**Selected Answer: C**

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc788018\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc788018(v=ws.11))

upvoted 1 times

🗨️ 👤 **ckmay** 10 months, 2 weeks ago

Incorrect. This link pertains to windows server 2012, not windows 11 which is what the question is asking about.

upvoted 1 times

🗨️ 👤 **Kiookr** 1 year, 3 months ago

I think computer 1 can be added or joint to the domain contoso.com from the computer management of the computer itself. Also I think can be add from intune

upvoted 1 times

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage Windows 11 devices.

You need to implement passwordless authentication that requires users to use number matching.

Which authentication method should you use?

- A. Microsoft Authenticator
- B. voice calls
- C. FIDO2 security keys
- D. text messages

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗨️ **Merrybob** 5 months ago

**Selected Answer: A**

A. Microsoft Authenticator  
upvoted 2 times

🗨️ **fco168** 8 months ago

**Selected Answer: A**

Microsoft Authenticator. Passwordless auth typing the number on your phone.  
upvoted 1 times

🗨️ **picho707** 9 months, 2 weeks ago

The correct answer is A. Microsoft Authenticator.

Microsoft Authenticator is a mobile app that provides a variety of authentication methods, including passwordless authentication. To use passwordless authentication with Microsoft Authenticator, users must first register their device and add their Azure AD account to the app. Once registered, users can sign in to their Azure AD account by approving a notification on their device.

upvoted 3 times

🗨️ **Aji03** 6 months ago

but the authenticator popup comes usually only after user enters the password?

upvoted 1 times

You use a Microsoft Intune subscription to manage iOS devices.

You configure a device compliance policy that blocks jailbroken iOS devices.

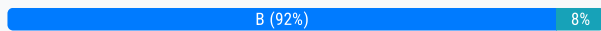
You need to enable Enhanced jailbreak detection.

What should you configure?

- A. the Compliance policy settings
- B. the device compliance policy
- C. a network location
- D. a configuration profile

**Suggested Answer: B**

Community vote distribution



**ExamKiller020** Highly Voted 9 months, 1 week ago

**Selected Answer: B**

'Enhanced jailbreak detection' isn't present in the current intune version anymore. It used to be in the Compliance policy settings blade.

ref: <https://www.petervanderwoude.nl/post/quick-tip-location-services-required-for-enhanced-jailbreak-detection/>

The only setting in intune that you can set is in the device compliance policy.

<https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios#device-health>

So my guess is B

upvoted 6 times

**mhmyz** Most Recent 4 months ago

**Selected Answer: B**

<https://learn.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-create-ios>

upvoted 1 times

**Darkfire** 4 months, 2 weeks ago

**Selected Answer: B**

B is correct

The Device Compliance Policy

<https://learn.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#:~:text=Define%20the%20rules%20and%20settings%20that%20users%20and%20managed,specified%20by%20threat%20management%20software>

upvoted 1 times

**NoursBear** 5 months, 2 weeks ago

It would be A before May

upvoted 1 times

**NoursBear** 5 months, 2 weeks ago

I checked an app protection policy for iOS and in the Conditional Launch blade, there is indeed a Jailbroken setting

upvoted 1 times

**NoursBear** 5 months, 2 weeks ago

huh I already replied two months ago lol

upvoted 1 times

**NoursBear** 8 months ago

Yes it's gone now but apparently if you want this feature there is a jailbreak detection in App protection policies, I have read, haven't checked. But if this question is still in the test, with these answers I guess we have to answer with the Compliance Policy Settings, which is where it was

upvoted 1 times

🗨️ 👤 **fco168** 8 months ago

**Selected Answer: B**

It's B. Not A - The Compliance Policy Settings is where you can 'Mark the device as compliant' and set the 'Compliance Status Validity Period'.

The 'Device Compliance Policy' means that you can create a CP for iOS/iPadOS devices and under compliance settings>Device Health>Jailbroken Devices: 'Block'

upvoted 4 times

🗨️ 👤 **BJ578** 7 months, 2 weeks ago

It is about Enhanced detection, which was in the device compliance settings until May and then it was removed.

upvoted 1 times

🗨️ 👤 **[Removed]** 8 months ago

**Selected Answer: A**

The Enhanced jailbreak detection option only applies to iOS and iPadOS devices, and it only works with devices that you target with a device compliance policy that blocks jailbroken devices. You can either Enable this setting or Disable it. This setting is Disabled by default, meaning it's turned off

for b - The device compliance policy is where you define the rules and settings that devices must meet to be considered compliant. While this policy does include a setting to block jailbroken devices, the specific setting for Enhanced jailbreak detection is found in the Compliance policy settings

upvoted 1 times

DRAG DROP

-

You have a Microsoft 365 subscription that contains two users named User1 and User2.

You need to ensure that the users can perform the following tasks:

- User1 must be able to create groups and manage users.
- User2 must be able to reset passwords for nonadministrative users.

The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

### Roles

### Answer Area

Global Administrator

Helpdesk Administrator

User1:

Security Administrator

User2:

User Administrator

### Answer Area


#### Suggested Answer:

User1:

User Administrator

User2:

Helpdesk Administrator

 **Darkfire** 4 months, 2 weeks ago

Answer is correct

User1: User Administrator

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#user-administrator?text=Helpdesk%20Administrator,and%20Helpdesk%20Administrators>.

User2: Helpdesk Administrator

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#user-administrator?text=User%20Administrator,for%20limited%20admins>.

upvoted 4 times

 **yosry** 6 months ago

Correct:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#user-administrator?text=Create%20users,manage%20all%20groups>

upvoted 1 times

 **fiskaba** 6 months, 3 weeks ago

User Administrator: Can manage all aspects of users and groups, including resetting passwords for limited admins.

Helpdesk Administrator: Can reset passwords for non-administrators and Helpdesk Administrators.

upvoted 1 times

 **LiamAzure** 8 months, 1 week ago

User Administrator  
Helpdesk Administrator  
upvoted 2 times

 **JBV85** 9 months, 2 weeks ago

Correct

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

upvoted 3 times

HOTSPOT

-

You have a Microsoft Intune subscription that has the following device compliance policy settings:

- Mark devices with no compliance policy assigned as: Compliant
- Compliance status validity period (days): 14

On January 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group1

On January 4, you create the following two device compliance policies:

- Name: Policy1
- Platform: Windows 10 and later
- Require BitLocker: Require
- Mark device noncompliant: 5 days after noncompliance
- Scope (Tags): Tag1
- Name: Policy2
- Platform: Windows 10 and later
- Firewall: Require
- Mark device noncompliant: Immediately
- Scope (Tags): Tag2

On January 5, you assign Policy1 and Policy2 to Group1.

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

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
On January 7, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
Suggested Answer: On January 7, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
On January 8, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
On January 8, Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>



N - no firewall, policy 2 marks it non compliant immediately

N - see above

Y - will be set to not compliant on the 10th

upvoted 18 times

🗨️ 👤 **AleFC1908** Most Recent 1 month, 3 weeks ago

N no firewall, policy2 marks it non compl immediately

N no firewall, policy2 marks it non compl immediately

Y will be not compliant on the Jan 10th

upvoted 1 times

🗨️ 👤 **Faceless\_Void** 5 months, 1 week ago

January 1, devices onboarded with 14 days. Modified to 5 days.

Device1 Tag1 Jan7 - NO - 5days validity from onboarding.

Device1 Tag1 Jan8 - NO - 5days validity from onboarding.

Device 2 TAG2 Jan8 - YES - Requirements MET - Firewall Enabled.

upvoted 2 times

🗨️ 👤 **ergacharsk** 5 months, 2 weeks ago

According to the Chat GPT correct answer is Y,Y,Y

upvoted 1 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

Scope Tags are just to throw you off and confuse you. They have no purpose when it comes to assignment. Given answers are correct.

upvoted 4 times

🗨️ 👤 **mhmyz** 10 months ago

I think YYY

Y - Device1=Tag1 Policy1 only apply

Y - Device1=Tag1 Policy1 only apply

Y - Device2=Tag2 Policy2 only apply

Scope Tag:

<https://learn.microsoft.com/en-us/mem/intune/protect/create-compliance-policy>

upvoted 4 times

🗨️ 👤 **2c57d1c** 6 months, 3 weeks ago

Assignment of Groups is how these are assigned...Scope tags mean nothing in this case.

upvoted 1 times

🗨️ 👤 **IrisM** 8 months ago

On January 5, you assign Policy1 and Policy2 to Group1

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

NNY for sure.

upvoted 4 times

🗨️ 👤 **Darkfire** 10 months, 2 weeks ago

I think NNN

Because both policies will mark devices as non-compliant. Eventhough some variables pass the criteria.

upvoted 1 times

🗨️ 👤 **Manojkl1206** 1 year ago

ITs NNN

Because: as both policy are applied

Policy2 says move the device immediately to Non compliant it will not wait for 5 days hence the 3rd answer should be N

upvoted 1 times

🗨️ 👤 **AdamRachel** 11 months, 3 weeks ago

Device is compliant for policy 2 but is not compliant for policy 1 where device will be mark non-compliant after 5 days which is 9 Jan.

upvoted 2 times

🗨️ 👤 **Krayzr** 10 months, 3 weeks ago

But it will not be marked "compliant", it will have "evaluating" or something like that till 10th.

upvoted 1 times

🗨️ 👤 **ZaFletch** 1 year, 2 months ago

Scope tags are irrelevant to policy deployment. So both policies apply to both machines on 4th.

Policy 2 marks non-compliance immediately so device 1 is marked non-compliant immediately as it fails the criteria.

Device 2 passes but it will fail on Policy 2. However it's not marked non-compliant until the 9th. So on the 8th it will remain compliant.

NNY

upvoted 4 times

🗨️ 👤 **Tr1v** 1 year, 1 month ago

Correct, but it says "On January 5, you assign Policy1 and Policy2 to Group1."

upvoted 1 times

🗨️ 👤 **RabbitB** 1 year, 2 months ago

Isn't the answer NNN??

Both devices are assigned a compliance policy, which means they don't mark them as "compliant".

Regardless of the day and devices, all are not marked as "compliant". Am I wrong?

upvoted 2 times

🗨️ 👤 **fiskaba** 1 year ago

Remember, the policies are assigned on Jan 5th. For this scenario, the device compliance policy settings are irrelevant because all devices have a policy assigned:

1 N) - Device 1 is NOT compliant on Jan 7th because the firewall is off and immediately becomes non-compliant.

2 N) - Device 1 is NOT compliant on Jan 8th because the firewall is still off.

3 Y) - Device 2 IS compliant on Jan 8th because the firewall is on, AND Policy1 does not go non-compliant until Jan 10th (5 days after non-compliance).

upvoted 3 times

🗨️ 👤 **RabbitB** 1 year, 2 months ago

Mistake, YYY

upvoted 1 times

🗨️ 👤 **ubiquituz** 1 year ago

Who you?

upvoted 1 times

🗨️ 👤 **iamforksu** 1 year, 2 months ago

NNY for the win

upvoted 1 times

🗨️ 👤 **reapernam** 1 year, 2 months ago

On Second thought, its N N Y.

Like ExamKiller020 says, the Scope Tags have no relevance in Policy or Group assignments. So both Policies are being applied.

upvoted 4 times

🗨️ 👤 **reapernam** 1 year, 3 months ago

The answer could be YYY.

Devices are already compliant before having the policies assigned to them. So when the newly added compliancy policies take effect, the devices are still compliant.

1. Yes- Device is still within its 14 day validity of initial compliance, and with 5-day rule, will only be labeled as non-compliant after 5 days, meaning its still compliant.

2. Same as above.

3. Yes, Look at cserra answer

upvoted 4 times

🗨️ 👤 **iTomi** 1 year ago

If policies are enforced and devicies report status of all reveived compliance policies to Intune, then this setting are meaningless. I think...

"Specify the time period in which devices must report the status for all received compliance policies. Devices that do not return status within this time period are treated as noncompliant. The default value is 30 days."

upvoted 1 times

🗨️ 👤 **ExamKiller020** 1 year, 3 months ago

Just remember: Scope (Tags) are used to determine which objects admins can see.

N,N,Y

upvoted 2 times

🗨️ 👤 **cserra** 1 year, 3 months ago

I think the answer is YYY

Initially, all devices are compliant.

1) On Jan 7, Policy1 don't mark yet as not compliant because need pass 5 days to apply the "noncompliant". Policy2 don't apply because Device1 is out of his scope (Tag2). Then, is it compliant? YES

2) On Jan 8, the case is the same than before. Then YES

3) To Device2, only the Policy2 is applicable (Tag2). The device has the firewall activated. Then, is it compliant? YES

upvoted 2 times

🗨️ 👤 **BJS78** 1 year, 3 months ago

Tag is for RBAC. No relevance in configuration implementation.

upvoted 3 times

🗨️ 👤 **Grg433** 1 year, 3 months ago

can someone please explain why N,N,Y ?

upvoted 2 times

🗨️ 👤 **Fortind1974** 1 year, 3 months ago

Policy1 & Policy2 are both assigned to Group1. Scope (Tags) are used to determine which objects admins can see.

1: Policy2 marks the device noncompliant immediately

2: Policy2 still marks the device noncompliant immediately

3: Policy1 marks device noncompliant after 5 days

upvoted 8 times

HOTSPOT

-

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have computers that run Windows 11 as shown in the following table.

Name	Azure AD status	Intune	BitLocker Drive Encryption (BitLocker)	Firewall
Computer1	Joined	Enrolled	Disabled	Enabled
Computer2	Registered	Enrolled	Enabled	Enabled
Computer3	Registered	Not enrolled	Enabled	Disabled

You have the groups shown in the following table.

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

You create and assign the compliance policies shown in the following table.

Name	Configuration	Action for noncompliance	Assignment
Policy1	Require BitLocker to be enabled on the device.	Mark device as noncompliant after 10 days.	Group1
Policy2	Require firewall to be on and monitoring.	Mark device as noncompliant immediately.	Group2

The next day, you review the compliance status of the computers.

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
The compliance status of Computer1 is in grace period.	<input type="radio"/>	<input type="radio"/>
The compliance status of Computer2 is Compliant.	<input type="radio"/>	<input type="radio"/>
The compliance status of Computer3 is Not compliant.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> The compliance status of Computer1 is in grace period.	<input checked="" type="radio"/>	<input type="radio"/>
The compliance status of Computer2 is Compliant.	<input checked="" type="radio"/>	<input type="radio"/>
The compliance status of Computer3 is Not compliant.	<input type="radio"/>	<input checked="" type="radio"/>

 **Stu5mmy** 5 months, 4 weeks ago

This is a tricky question when it comes to the evaluation of device 2. There are two types of compliance in devices in the Intune portal, one being the Intune compliance and the other one being the Entra ID compliance.


Device 2 will meet the compliance requirements for Intune compliance, but not the Entra ID compliance because it is registered and not in a Joined/Hybrid state.

upvoted 1 times

  **rcristiano** 8 months ago

resposta correta



upvoted 2 times

  **MR\_Eliot** 10 months, 1 week ago

I would say the answer is YYY.

Third one is not intune joined, so compliance policy does not apply. Anyway, I still say device is compliant. I have not found a single compliant device in my test tenant. They were either n/a or not compliant.

upvoted 4 times

  **MR\_Eliot** 10 months, 1 week ago

Computer 1 (intune)

- Bitlocker: Disabled

- Firewall : Enabled

- Policy: Policy 1

Result: not compliant (currently is grace period)

Computer 2 (intune)

- Bitlocker: Enabled

- Firewall : Enabled

- Policy: Policy 1

Result: compliant

Computer 3 (not enrolled)

- Bitlocker: Enabled

- Firewall : Disabled

- Policy: None (Because not intune joined)

- Result: Not compliant!

upvoted 12 times

  **Bukaj** 1 year ago

Answer from ChatGPT:

If a device is only registered with Azure AD but not enrolled in Intune, it does not have to comply with Intune compliance policies. Compliance policies in Intune are used to set rules for devices managed with Intune1.

However, there is a setting in Intune's compliance policy settings that determines how Intune treats devices that haven't been assigned a device compliance policy. This setting has two values1:

Compliant (default): Devices that aren't sent a device compliance policy are considered compliant.

Not compliant: Devices that haven't received a device compliance policy are considered noncompliant.

So, if you want to apply a compliance policy from Intune to a device, it needs to be enrolled in Intune. It does not matter if the device is Azure AD registered or joined as long as the device is enrolled in Intune2

upvoted 3 times

  **mks\_academy** 1 year ago

Y,Y,Y to me.

Computer 1 is in a grace period because policy 1 applies to it and it does not have bitlocker activated.

Computer 2 is compliant because policy 1 applies to it and bitlocker is activated.

Computer 3 is not compliance (SO THE ANSWER IS Y) because policy 2 applies to it and firewall is disabled.

upvoted 4 times

  **AdamRachel** 11 months, 3 weeks ago

yes but computer 3 is only register but not joined Azure AD so policy do not apply to this device and leave this device as compliant.

upvoted 1 times

🗨️ 👤 **AdamRachel** 11 months, 3 weeks ago

But device 3 is not enrolled to Intune so Policy not apply so will leave device as compliant.  
upvoted 1 times

🗨️ 👤 **riccardo1999** 1 year ago

computer 3 is not enrolled on Intune.  
upvoted 2 times

🗨️ 👤 **frack** 11 months, 3 weeks ago

it is registered.  
upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

amckinson\_Android\_10/16/2023\_4:38 PM

Intune

Personal

Noncompliant

Android (device administrator)

9.0

amckinson@sportinggroup.co.uk

29/11/2023, 04:29

Microsoft Entra registered

anutbrown\_Android\_3/15/2023\_1:34 PM

Intune

Personal

In grace period

Android (device administrator)

13.0

anutbrown@sportinggroup.co.uk

08/11/2023, 15:06

Microsoft Entra registered

The answer is Yes Yes Yes, if you can put a device in a group you can apply a compliance policy.

upvoted 1 times

🗨️ 👤 **NoursBear** 1 year, 1 month ago

I think the key is with Device 3 is "monitoring", Device 3 can't report back if not enrolled according to this:

<https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor>

If I understand right. It seems the device needs to be enrolled anyway, according to some other article too. Device 3 should be No I think

upvoted 3 times

🗨️ 👤 **benpatto** 1 year, 2 months ago

Computer 3 is not enrolled in Intune, therefore it can't receive the compliance policies. It may be registered in Azure AD but Intune ultimately is what plays the role here.

upvoted 3 times

🗨️ 👤 **Casticod** 1 year, 3 months ago

I have a question... IF computer 3 is not registered (or joined), how does it belong to group 3)

Beyond this joke, the answers seem to be correct

Computer 1 is in a grace period because policy 1 applies to it and it does not have bitlocker activated.

Team 2 is compliance because pass the policy1.

Team 3 is not compliance because it does not belong to the Azure Ad in question

upvoted 2 times

🗨️ 👤 **Contactfornitish** 1 year, 2 months ago

It clearly says its registered (computer3)

Compliance policy applies on all registered, hybrid, enrolled devices.

upvoted 2 times

🗨️ 👤 **Sonia33** 1 year ago

It can belong a group if it in AAD. But it cannot be compliant or not compliant if it is not in Intune.

upvoted 1 times

🗨️ 👤 **BJ578** 1 year, 3 months ago

Device must be joined to AAD and/or registered in Intune to receive compliance policy.  
Usually: AADJ: Corporate device, AADR: private device (does not apply with this question)  
upvoted 1 times

🗨️ 👤 **sh123df** 1 year, 3 months ago

No  
Yes  
Yes  
Looks like is wrong, correct me.  
upvoted 2 times

🗨️ 👤 **LiamAzure** 1 year, 2 months ago

Why No for the first one? This is after 1 day, it has 10 days  
upvoted 1 times

🗨️ 👤 **majerzg** 1 year, 2 months ago

I think that you are right.  
upvoted 1 times

🗨️ 👤 **sh123df** 1 year, 2 months ago

My answer is wrong. Look away from this  
upvoted 3 times

🗨️ 👤 **Grg433** 1 year, 3 months ago

should be Y,Y,Y ? no ?  
upvoted 4 times

🗨️ 👤 **SdovIA** 1 year, 3 months ago

The third device is just registered in AAD. The status is .  
upvoted 7 times

🗨️ 👤 **frack** 11 months, 3 weeks ago

table indicate Device3 as registered  
upvoted 1 times

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 AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you configure the Authentication methods.


Does this meet the goal?

- A. Yes
- B. No

**Suggested Answer:** B

Community vote distribution

B (100%)

 **ExamKiller020** Highly Voted 9 months, 1 week ago

**Selected Answer:** B

Devices > Enroll devices > Windows enrollment > Windows Hello for Business in Intune and configure a desired policy.  
upvoted 10 times


 **Darkfire** Most Recent 4 months, 2 weeks ago

**Selected Answer:** B

B is correct

<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/policy-settings?tabs=pin#:~:text=%E2%9C%85,-Maximum%20PIN%20length,-%E2%9C%85>

<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/configure#:~:text=Sign%20in%20to,might%20be%20configured>  
upvoted 1 times

 **Merrybob** 5 months ago

**Selected Answer:** B

B. No

Should be configured as a Windows Hello for Business policy.  
upvoted 1 times



You have a Microsoft 365 tenant that contains the objects shown in the following table.

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Main-enabled security group
Group4	Security group

You are creating a compliance policy named Compliance1.


Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

- A. Group3 and Group4 only
- B. Group3, Group4, and Admin1 only
- C. Group1, Group2, and Group3 only
- D. Group1, Group2, Group3, and Group4 only
- E. Group1, Group2, Group3, Group4, and Admin1

**Suggested Answer:** C

Community vote distribution


C (100%)

 **OyYaGotta** Highly Voted 9 months, 3 weeks ago

**Selected Answer: C**

Question has a typo -- says "main-enabled" which should be "mail-enabled". Groups with email address can be sent notifications which means C is correct.

upvoted 6 times

 **ergacharsk** 5 months, 2 weeks ago

thanks for clarification

upvoted 1 times

 **MR\_Eliot** Highly Voted 10 months, 1 week ago

**Selected Answer: C**

C is correct.

From my testings, I can only find/select Distribution Groups, Microsoft 365 Groups and Security mail-enabled groups.

Security groups and dynamic distribution groups is not supported.

upvoted 5 times

 **Tr619899** Most Recent 1 month ago

**Selected Answer: C**

C is Correct

upvoted 1 times

 **CeZt** 5 months, 1 week ago

it can not be sent to users, nor security groups

upvoted 1 times

 **Darkfire** 10 months, 2 weeks ago

**Selected Answer: C**

C is correct

<https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

<https://learn.microsoft.com/en-us/mem/intune/protect/quickstart-send-notification#:~:text=Add%20an%20action,your%20compliance%20policy.>

upvoted 1 times

🗨️ **NoursBear** 1 year, 1 month ago  
groups with email enabled  
<https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>  
upvoted 1 times

🗨️ **brunolopes01** 1 year, 2 months ago  
This question looks like question 158.  
upvoted 1 times

🗨️ **brunolopes01** 1 year, 2 months ago  
sry Question 156  
upvoted 1 times

🗨️ **Rocky83** 1 year, 2 months ago  
**Selected Answer: C**  
C is correct  
upvoted 1 times

🗨️ **ExamKiller020** 1 year, 3 months ago  
**Selected Answer: C**  
Given answer is correct. Tested in my own tenant. You can only select groups with email addresses  
upvoted 1 times

🗨️ **SdovIA** 1 year, 3 months ago  
**Selected Answer: C**  
The answer is correct. For action, Send email to end users. You can configure M365, distribution or mail-enabled security groups as additional recipients.  
upvoted 1 times

🗨️ **picho707** 1 year, 3 months ago  
The answer appears to be E based on the information below:  
In a compliance policy, you can specify the following objects as additional recipients of noncompliance notifications:

Users: You can add individual users as recipients of noncompliance notifications. This allows you to notify specific users when their devices are found to be noncompliant1.

Groups: You can add groups of users as recipients of noncompliance notifications. This allows you to notify multiple users at once when their devices are found to be noncompliant1.

Roles: You can add Azure AD roles as recipients of noncompliance notifications. This allows you to notify users with specific roles or responsibilities when their devices are found to be noncompliant1.

Email addresses: You can add email addresses as recipients of noncompliance notifications. This allows you to notify external stakeholders or distribution lists when devices are found to be noncompliant1.

upvoted 2 times

🗨️ **BJS78** 1 year, 3 months ago  
Nope, tested it. You can add only groups (groups with e-mail addresses)  
upvoted 2 times

🗨️ **Grg433** 1 year, 3 months ago  
Is this C option even correct ?  
upvoted 2 times

HOTSPOT

-

You have an Azure AD tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1@contoso.com.

You join a Windows 11 device named Client1 to contoso.com.

You need to add User1 to the local Administrators group of Client1.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Administrators /add " \user1@contoso.com"

net accounts	AzureAD
net localgroup	CONTOSO
net user	UPN

### Answer Area

Suggested Answer: Administrators /add " \user1@contoso.com"

net accounts	AzureAD
<b>net localgroup</b>	<b>CONTOSO</b>
net user	UPN

- Nozuka** Highly Voted 1 year, 3 months ago

Should be "AzureAD" since there is no mention of On-Premise AD.

<https://learn.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin#manually-elevate-a-user-on-a-device>

upvoted 26 times
- Sas2003** Highly Voted 1 year, 3 months ago

AzureAD is the correct answer

upvoted 14 times
- AleFCI1908** Most Recent 1 month, 3 weeks ago

net localgroup administrators /add "AzureAD\user1@contoso.com"

upvoted 3 times
- MR\_Eliot** 10 months, 1 week ago

Net localgroup

AzureAD

upvoted 4 times
- Darkfire** 10 months, 2 weeks ago

net localgroup administrators /add "AzureAD\user1@contoso.com"

Question contains no On-Premises.

<https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin#manually-elevate-a-user-on-a-device?~:text=Additionally%2C%20you%20can,add%20%22AzureAD%5CUserUpn%22>



upvoted 3 times

- iTomi** 1 year ago

NET LOCALGROUP and AZURE AD are correct answers.

<https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin#manually-elevate-a-user-on-a-device>

upvoted 3 times

  **madsa** 1 year, 1 month ago

You can also do like: `net localgroup administrators AzureAD\user1@contoso.com /add`

upvoted 1 times

  **Rocky83** 1 year, 2 months ago

AzureAD is the correct answer here

upvoted 4 times

  **Casticod** 1 year, 3 months ago

`net localgroup administrators /add "AzureAD\user1@contoso.com`

<https://superuser.com/questions/982336/how-do-i-add-azure-active-directory-user-to-local-administrators-group>

upvoted 2 times

You have a Microsoft 365 subscription.

You need to provide a user the ability Security defaults and create Conditional Access policies. The solution must use the principle of least privilege.

Which role should you assign to the user?

- A. Global Administrator
- B. Conditional Access Administrator
- C. Security Administrator
- D. Intune Administrator

**Suggested Answer: B**

Community vote distribution

B (65%)


C (35%)

 **Stuckbear** Highly Voted 1 year, 3 months ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-defaults>

To configure security defaults in your directory, you must be assigned at least the Security Administrator role.  
upvoted 10 times


 **Burkidur** 10 months, 1 week ago

^^^ This guy knows stuff.

"To enable security defaults (or confirm they're already enabled)  
Sign in to the Microsoft Entra admin center as least a Security Administrator."


<https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-turn-on-mfa?view=o365-worldwide&tabs=secdefaults>

Conditional Access Admin can change only CAPs, named locations and auth contexts. No security defaults.  
upvoted 1 times

 **picho707** Highly Voted 1 year, 3 months ago

B appears to be correct:

To set up security defaults and create Conditional Access policies, a user requires the Conditional Access Administrator or Security Administrator role1. However, the Security Reader or Global Reader role is sufficient if the purpose is solely to read policies1.  
upvoted 8 times

 **Seek12** Most Recent 1 week, 2 days ago

**Selected Answer: B**

security admin cannot create CA policy  
upvoted 2 times

 **Fiscini** 2 weeks, 2 days ago

**Selected Answer: B**

To configure security defaults in your directory, you must be assigned at least the Conditional Access Administrator role.  
upvoted 2 times

 **Tr619899** 1 month ago

**Selected Answer: B**

Conditional Access Administrator: This role allows the user to manage Conditional Access policies and other identity-related configurations. It adheres to the principle of least privilege because the user is given only the permissions required to manage Conditional Access settings.  
upvoted 2 times

 **Tr619899** 3 days, 20 hours ago

- To Support my answer:

[https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults?utm\\_source=chatgpt.com#enabling-security-defaults](https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults?utm_source=chatgpt.com#enabling-security-defaults)

upvoted 1 times

🗨️ 👤 **Nav90** 2 months ago

Selected Answer: C

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#enabling-security-defaults>

To configure security defaults in your directory, you must be assigned at least the Security Administrator role. By default the first account in any directory is assigned a higher privileged role known as Global Administrator.

upvoted 1 times

🗨️ 👤 **martinods** 2 months, 2 weeks ago

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#enabling-security-defaults> - To configure security defaults in your directory, you must be assigned at least the Security Administrator role. By default the first account in any directory is assigned a higher privileged role known as Global Administrator.

upvoted 1 times

🗨️ 👤 **RomanV** 3 months, 1 week ago

Correct answer is C: Security Administrator. Why? Because the Conditional Access Admin can only change or create or delete CA's and dos not have security defaults in it. Only the Security Admin or Global Admin have this. But the question says "LEAST privilege" so it's C. in this case.

Learn more about Azure build-in roles here:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#security-administrator>

upvoted 1 times

🗨️ 👤 **EUC\_PRO** 3 months, 3 weeks ago

Selected Answer: B

It is possible with B or C, however B has fewer privileges - <https://learn.microsoft.com/en-us/answers/questions/1462298/configure-security-defaults-which-role-can-do-this>

upvoted 1 times

🗨️ 👤 **Nav90** 2 months ago

as per your link its only possible with Security Administrator.

To configure security defaults in your directory, you must be assigned at least the Security Administrator role. By default the first account in any directory is assigned a higher privileged role known as Global Administrator.

upvoted 1 times

🗨️ 👤 **martinods** 2 months, 2 weeks ago

To configure security defaults in your directory, you must be assigned at least the Security Administrator role. By default the first account in any directory is assigned a higher privileged role known as Global Administrator. - from your link

upvoted 1 times

🗨️ 👤 **Pollosor** 4 months, 2 weeks ago

Selected Answer: B

With both it is possible, but the conditional access administrator has fewer privileges.

upvoted 2 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

Selected Answer: C

Conditional Access Admin CANNOT configure Security Defaults. C fulfils both requirements.

Source: <https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#enabling-security-defaults>

To configure security defaults in your directory, you must be assigned at least the Security Administrator role.

upvoted 2 times

🗨️ 👤 **Prasis** 5 months, 3 weeks ago

B

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>

upvoted 1 times

🗨️ 👤 **da\_terminator** 6 months, 3 weeks ago

Selected Answer: C

Answer is C:



<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>

To configure security defaults in your directory, you must be assigned at least the Security Administrator role.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#security-administrator>

Conditional Access Admin role can only edit Conditional Access related settings, they cannot edit Security Defaults

upvoted 2 times

  **CJL324** 7 months, 2 weeks ago

B. Conditional Access Administrator.

The Conditional Access Administrator role allows users to manage Azure Active Directory Conditional Access policies without giving them broader administrative permissions that come with roles like Global Administrator. This aligns with the principle of least privilege by granting only the necessary permissions for the task.

upvoted 1 times

  **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: B**

Given answer is correct.

upvoted 1 times

  **Darkfire** 10 months, 2 weeks ago

**Selected Answer: B**

B is correct

Conditional Access Administrator:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#conditional-access-administrator>:~:text=365%20admin%20center-,Conditional%20Access%20Administrator,-This%20is%20a

[https://learn.microsoft.com/en-us/entra/fundamentals/security-](https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#)

defaults#:~:text=If%20your%20organization%20has%20complex%20security%20requirements%2C%20you%20should%20consider%20Conditional%20Acce.

upvoted 2 times

  **belyo** 1 year ago

**Selected Answer: B**

B. tested in my tenant

CA admin can turn on/off security defaults

upvoted 2 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 8.1 and later	Require	<i>Not applicable</i>	5 days	Group1
Policy2	Windows 10 and later	Not configured	Require	7 days	Group2
Policy3	Windows 10 and later	Require	Require	10 days	Group2

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

Save Discard

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

Mark devices with no compliance policy assigned as  Compliant  Not Compliant

Enhanced jailbreak detection  Enabled  Disabled

Compliance status validity period (days)

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.

**Answer Area**

- | Statements                                 | Yes                   | No                    |
|--|-----------------------|-----------------------|
| On June 4, Device1 is marked as compliant. | <input type="radio"/> | <input type="radio"/> |
| On June 6, Device1 is marked as compliant. | <input type="radio"/> | <input type="radio"/> |
| On June 9, Device2 is marked as compliant. | <input type="radio"/> | <input type="radio"/> |

**Answer Area**

	Statements	Yes	No
Suggested Answer:	On June 4, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
	On June 6, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
	On June 9, Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>



iamforksu **Highly Voted** 1 year, 2 months ago

YNY - answer is correct

upvoted 29 times

AleFC11908 1 month, 3 weeks ago

Y - because of grace period = 5 days

N - because is out of the grace period = 5 days

Y - because of grace period , most restrictive policy grace period = 10 days

upvoted 3 times

665d390 4 months ago

correcto

upvoted 2 times

METAM 4 months, 1 week ago

explain please

upvoted 1 times

Casticod **Highly Voted** 1 year, 3 months ago

I think the answer is No, No, Yes.

Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO.

Then the third device has 2 policies, the first one is compliant and the second policy is not compliant but the device is not marked as non-compliant due to the fact that mark device as non-compliant is set to 10 days. This means that the machine will be compliant until june 10th.

Source:

Mark device non-compliant: By default, this action is set for each compliance policy and has a schedule of zero (0) days, marking devices as noncompliant immediately.

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

This action is supported on all platforms supported by Intune.

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

upvoted 16 times

firefox15 1 year, 2 months ago

Policy 1 is for Windows 8.1 \*and later\*. It should still apply unless I'm missing something. I feel it should be Y, N, Y.

upvoted 16 times

METAM **Most Recent** 4 months, 1 week ago

NNY. good

upvoted 1 times

Pollosor 4 months, 2 weeks ago

YES: It does not have BitLocker but will still be marked as compliant because it is within the grace period.

NO: It does not have BitLocker and exceeds the grace period.

YES: The most restrictive policy applies, in this case, the one with a 10-day grace period.

upvoted 3 times

WORKHOLIC 7 months ago

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>

upvoted 2 times

  **HvD** 2 months, 1 week ago

Box 1: Yes, because the device is indeed not compliant, but will be marked as such after 5 days, which is June 6.

upvoted 4 times

  **CJL324** 7 months, 2 weeks ago

Summary:

On June 4, Device1 is marked as compliant: No

On June 6, Device1 is marked as compliant: No

On June 9, Device2 is marked as compliant: No

upvoted 2 times

  **CJL324** 7 months, 2 weeks ago

Device1 Analysis:

Assigned Policy: Policy1

Requirements:

Encryption (Require)

Windows Defender Antimalware (Not applicable)

Compliance Marked: 5 days

Device1 on June 4:

Enrolled on June 1.

5 days from June 1 is June 6.

BitLocker (Encryption): No

Windows Defender: Enabled (Not applicable for Policy1)

On June 4, Device1 has not met the encryption requirement for 5 days yet, so it should not be marked as compliant.

Answer: No

Device1 on June 6:

upvoted 1 times

  **CJL324** 7 months, 2 weeks ago

By June 6, it has been 5 days since enrollment.

BitLocker (Encryption): No (still not compliant)

Windows Defender: Enabled (Not applicable for Policy1)

On June 6, Device1 should be marked as not compliant because it has not enabled BitLocker for 5 days.

Answer: No

Device2 Analysis:

Assigned Policy: Policy2 and Policy3

Requirements:

Policy2: Windows Defender Antimalware (Require), Mark device as not compliant in 7 days.

Policy3: Encryption (Require), Windows Defender Antimalware (Require), Mark device as not compliant in 10 days.

Device2 on June 9:

Enrolled on June 1.

7 days from June 1 is June 8.


10 days from June 1 is June 11.

BitLocker (Encryption): No

Windows Defender: Enabled (required by both Policy2 and Policy3)

By June 9, Device2 meets the Windows Defender requirement but fails the encryption requirement for both policies. Since Policy3 marks it non-compliant in 10 days and Policy2 in 7 days, by June 9, it should be marked as non-compliant according to Policy2.

upvoted 1 times

  **Dave808** 9 months, 2 weeks ago

Answer is D:

Manual Process:

Open Computer Management.

Click the Action menu.

Select Connect to Another Computer.

Type the Computer Name (e.g., "Computer1").

Click OK.

Expand Local Users and Groups.

Select Groups.

Double-click the Remote Desktop Users group.

Click Add.

Type the User Name as "User1".

Click OK.

Click OK again.

upvoted 1 times

  **MR\_Eliot** 10 months, 1 week ago

Y, N, Y

Device1:

Policies: Policy1

Verdict: Not compliant since bitlocker is disabled.

Device2:

Policies: Policy2, Policy3

Verdict: Not compliant since bitlocker is not enabled.

On June 4, device1 is marked as compliant

- Yes. Mark device as not compliant after 5 days. Within grace period.


On June 6, device 1 is marked as compliant

- No. Grace period is over. So device is not compliant.

On June 9, device2 is marked as compliant:

- Yes. Policy3 makes the device not compliant after 10 days. Device is within grace period.

upvoted 8 times

  **Krayzr** 10 months, 3 weeks ago

Confused :?

<https://www.examttopics.com/discussions/microsoft/view/51834-exam-md-101-topic-3-question-25-discussion/>

upvoted 1 times

  **NoursBear** 11 months, 3 weeks ago

I think I have just found out something, Windows 8.1 and later compliance policies do not affect Windows 10/11. It looks like the "later" part means what minimum and maximum sub version of Windows 8.1 it should affect. This is why I could not understand why Device 1 was not compliant in the grace period:

<https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows-8-1>

So this would mean Policy 1 is not applied and Device 1 has no policy.

upvoted 2 times

  **gavorgavin** 2 months, 1 week ago

BUT... (man this is confusing) in the minimum and maximum OS versions you can specify build versions greater than 8.1 for example in minimum OS: 6.3.9600, maximum: 10.0.22631

upvoted 1 times

🗨️ 👤 **Burkidur** 10 months, 1 week ago

Exactly. Otherwise the screenshot with devices with no compliance setting would make no sense in this question.  
upvoted 2 times

🗨️ 👤 **Greatone1** 1 year ago

NNY this question is on MS 101 exam  
upvoted 2 times

🗨️ 👤 **abill** 1 year ago

NNY for me  
upvoted 2 times

🗨️ 👤 **Kevern** 1 year ago

Should it not be Y,N,N?  
Device 1 is within the grace period on June 4  
Device 1 is out of grace period on June 6  
Device 2 is out of grace period (while having 2 policies assigned) on June 9  
upvoted 3 times

🗨️ 👤 **Sonia33** 1 year ago

For me it should be No, No, No. The third device should be In Grace period.  
upvoted 5 times

🗨️ 👤 **madsa** 1 year, 1 month ago

Yes No Yes  
upvoted 1 times

🗨️ 👤 **Bradadministrator** 1 year, 2 months ago

NNY  
Device 1 on June 4 isn't compliant as it's in grace period  
upvoted 3 times

🗨️ 👤 **Rubends** 1 year, 2 months ago

I think is NNY because question say put mark not complain without policy  
upvoted 3 times

You have a Microsoft 365 subscription that contains a user named User1 and uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices that run Windows 11.

User provides remote support for 75 devices in the marketing department.

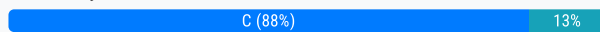
You need to add User1 to the Remote Desktop Users group on each marketing department device.

What should you configure?

- A. an app configuration policy
- B. a device compliance policy
- C. an account protection policy
- D. a device configuration profile

**Suggested Answer: B**

Community vote distribution



**Fortind1974** Highly Voted 1 year, 3 months ago

**Selected Answer: C**

C. an account protection policy

<https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy#manage-local-groups-on-windows-devices>  
upvoted 14 times

**Krayzr** 10 months, 3 weeks ago

You are correct Sir

Local user group membership (preview) – Use this profile to add, remove, or replace members of the built-in local groups on Windows devices. For example, the Administrators local group has broad rights. You can use this policy to edit the Admin group's membership to lock it down to a set of exclusively defined members.

upvoted 2 times

**Tr619899** Most Recent 1 month ago

**Selected Answer: D**

A Device Configuration Profile provides a way to manage device settings, including adding users or groups to local device groups like Remote Desktop Users.

upvoted 1 times

**EUC\_PRO** 3 months, 3 weeks ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy#manage-local-groups-on-windows-devices>  
upvoted 1 times

**METAM** 4 months, 1 week ago

**Selected Answer: C**

C good

upvoted 1 times

**Frank\_2022** 5 months, 1 week ago

**Selected Answer: D**

Device configuration profiles are used to configure settings on managed devices. In this case, you need to modify a specific setting (adding a user to a group) on multiple devices. This allows you to define this setting and push it out to the targeted devices (in this case, the marketing department's Windows 11 devices).

upvoted 1 times

🗨️ **ergacharsk** 5 months, 2 weeks ago

**Selected Answer: D**

A device configuration profile in Microsoft Intune allows you to manage various settings on Windows 11 devices, including user permissions. By creating a device configuration profile, you can specify settings to automatically add User1 to the Remote Desktop Users group on all targeted devices.

Steps to Configure a Device Configuration Profile:

\*Sign in to the Microsoft Intune admin center.

\*Select Devices > Configuration profiles > Create profile.

\*Platform: Choose Windows 10 and later.

\*Profile type: Select Custom.

\*Configuration settings: Use OMA-URI settings to configure the membership of the Remote Desktop Users group.

upvoted 1 times

🗨️ **oopspruu** 5 months, 2 weeks ago

**Selected Answer: C**

Account Protection section in Endpoint Security has the policy for exactly this purpose. We use this to create users in local Admin groups when making LAPS policies.

upvoted 1 times

🗨️ **Prasis** 5 months, 3 weeks ago

D

To add User1 to the Remote Desktop Users group on each marketing department device, you should configure a device configuration profile.

Device configuration profiles in Microsoft Intune allow you to define and push settings to managed devices. In this case, you can use a device configuration profile to manage the built-in group memberships on devices, including the Remote Desktop Users group. This will allow User1 to provide remote support for the devices in the marketing department.

upvoted 2 times

🗨️ **CJL324** 7 months, 3 weeks ago

D.

A device configuration profile in Intune allows you to manage settings and configurations on the devices, including adding users to specific local groups such as the Remote Desktop Users group. You can create a custom profile to automate this task across all the relevant devices.

upvoted 1 times

🗨️ **Dave808** 9 months, 2 weeks ago

**Selected Answer: D**

D is the answer

To add User1 to the Remote Desktop Users group on each marketing department device running Windows 11, you should configure a device configuration profile. This profile allows you to manage settings and configurations on devices enrolled in Microsoft Intune.

Here's how you can achieve this using PowerShell:

Manual Process:

Open Computer Management.

Click the Action menu.

Select Connect to Another Computer.

Type the Computer Name (e.g., "Computer1").

Click OK.

Expand Local Users and Groups

upvoted 1 times

🗨️ **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: C**

c is correct

upvoted 1 times

🗨️ **Darkfire** 10 months, 2 weeks ago

**Selected Answer: C**

Should be C idd.

[https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy#:~:text=Local%20user%20group%20membership%20\(preview\)%20%E2%80%93%20Use,Manage%20local%20groups%20on%20Windows%20devices.](https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy#:~:text=Local%20user%20group%20membership%20(preview)%20%E2%80%93%20Use,Manage%20local%20groups%20on%20Windows%20devices.)  
upvoted 1 times

🗨️ **Krayzr** 10 months, 3 weeks ago

**Selected Answer: C**

C is correct

Still in preview, but Tried in my tenant

<https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy#manage-local-groups-on-windows-devices>  
upvoted 2 times

🗨️ **Merrybob** 11 months ago

**Selected Answer: C**

C. an account protection policy

Ref: <https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin#manage-administrator-privileges-using-microsoft-entra-groups-preview#:~:text=Organizations%20can%20use%20Intune%20to%20manage%20these%20policies%20using%20Custom%20OMA%20DURI%20Settings%20or%2>  
upvoted 1 times

🗨️ **mp34** 11 months, 3 weeks ago

I thought if a topic was in preview then it would not be on the exam....the link provided by Fortind1974 says it is still in preview...

upvoted 1 times

🗨️ **Amir1909** 11 months, 4 weeks ago

C is correct

upvoted 1 times

🗨️ **Menovice** 1 year ago

C is correct.

Enabling Remote Desktop: Creating Configuration Profile

Adding Users to Remote Desktop: Account Protection

upvoted 1 times

HOTSPOT

-

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

Name	Member of	License
User1	Group1	Microsoft 365 E5
User2	Group2	Microsoft 365 E5

For contoso.com, the Mobility (MDM and MAM) settings have the following configurations:

- MDM user scope: Group1
- MAM user scope: Group2

You purchase the devices shown in the following table:

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android


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

### Answer Area

Statements	Yes	No
If User1 registers Device1 in contoso.com, Device1 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>
If User1 joins Device1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>
If User2 registers Device3 in contoso.com, Device3 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> If User1 registers Device1 in contoso.com, Device1 is enrolled automatically in Microsoft Intune.	<input checked="" type="radio"/>	<input type="radio"/>
If User1 joins Device1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 registers Device3 in contoso.com, Device3 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input checked="" type="radio"/>

 **benpatto** Highly Voted 1 year, 2 months ago

It really helps to read the question people!!!! Option 2 says user1 joins device1 to contoso.com - why would Device2 be affected by this?  
upvoted 18 times

 **riccardo1999** 1 year ago

the question is incorrect. For me, option two talks about device 2 and for me is "yes"  
upvoted 6 times

 **MR\_Eliot** Highly Voted 10 months, 1 week ago

NO: User registers the device. Device will be Entra ID registerd.

YES: Assuming the question has a typo. Joining Entra ID will also enroll the device in Intune.

NO: It's an android device. You will need to install company portal to enroll the device in Intune.



upvoted 9 times

🗨️ 👤 **Maclouis116** 6 months, 1 week ago

Automatic enrollment occurs when you join or register a device.

upvoted 4 times

🗨️ 👤 **Faceless\_Void** Most Recent 5 months, 1 week ago

Y - Group1 - MDM user scope

N - NO MDM

N - NO MDM

upvoted 1 times

🗨️ 👤 **ergacharsk** 5 months, 2 weeks ago

The given answer is correct Y, N, N

Y - because automatic enrollment occurs when you join or register a device.

N - because user is registering Device1, not Device2

N - automatic enrollment when you register device works only for Windows devices, for Android device user must enroll it via Corporate Portal app

upvoted 4 times

🗨️ 👤 **ergacharsk** 5 months, 2 weeks ago

The given answer is correct Y, N, N

Y - because automatic enrollment occurs when you join or register a device.

N - because user is registering Device1, not Device2

N - automatic enrollment when you register device works only for Windows devices, for Android device user must enroll it via Corporate Portal app

upvoted 2 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

Automatic Enrollment in Intune applies when device is either Registered or Joined to Entra ID. You just need to make sure the user is assigned the MDM scope correctly.

YYN - provided question 2 has typo

YNN - if Question 2 is intentionally misleading

upvoted 3 times

🗨️ 👤 **cuber** 6 months ago

It should be YYN, User1 is member of group 1 which is scoped for MDM, registering and joining a devices (Windows) both result in an Intune managed device.

User2 is in group 2 which has only a MAM scope therefore only apps will be managed and not the complete device by Intune.

upvoted 1 times

🗨️ 👤 **NoursBear** 11 months, 3 weeks ago

Attention !!! the second option is a trick, read it carefully

upvoted 3 times

🗨️ 👤 **Burkidur** 10 months, 1 week ago

It's likely a typo by ET. The key difference between Q1 and Q2 is "joined" vs "registered".

upvoted 3 times

🗨️ 👤 **Sonia33** 1 year ago

For me it should be Yes, Yes, No. User1 can enroll devices and registers Device 1 and 2 (both Windows). User2 is just a MAM scope, so it is just in AAD.

upvoted 3 times

🗨️ 👤 **Sonia33** 1 year ago

I read it wrong... Yes, No, No.

upvoted 1 times

🗨️ 👤 **riccardo1999** 1 year ago

why? For me, user 1 can enroll the device 2

upvoted 1 times

🗨️ 👤 **madsa** 1 year, 1 month ago

The given answer is correct: enrolling one device has nothing to do with enrolling another, and registering a device by MAM. For example outlook won't enroll the device in Intune.

upvoted 3 times

🗨️ 👤 **Contactfornitish** 1 year, 2 months ago

As far as I understand it should be YYN

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-windows#windows-automatic-enrollment>

Auto-enrollment not available for non-Windows devices but for windows 10 and onwards, whether its joined or registered, both kind of devices can be auto-enrolled.

upvoted 1 times

🗨️ 👤 **Mahi\_444** 1 year, 2 months ago

Second option talking about device 2 and thit is targeted to group 2 which is MAM user scope so ans is N

upvoted 1 times

🗨️ 👤 **riccardo1999** 1 year ago

device 2 is not targeted to group 2. The group are composed by user and not by device.

The second option talk about user 1 therefore group 1 =mdm. For me the second option is YES

upvoted 1 times

🗨️ 👤 **BJS78** 12 months ago

Sorry, but wrong. Maybe a typo but on the 2nd options it says: User1 enrolls Device2 and DEVICE1 got enrolled to Intune...

If it would be all about Device2, then you are right

upvoted 1 times

🗨️ 👤 **Monades** 1 year, 2 months ago

Seems correct:

<https://learn.microsoft.com/en-us/mem/intune/enrollment/quickstart-setup-auto-enrollment>

upvoted 2 times

🗨️ 👤 **VirtualJP** 1 year, 2 months ago

I'm thinking N,N,N

upvoted 5 times

🗨️ 👤 **VirtualJP** 1 year, 2 months ago

Not sure why I said N for all 3.

I retract my original answer in favour of: Y Y N.

upvoted 2 times

🗨️ 👤 **LiamAzure** 1 year, 2 months ago

Can you explain?

upvoted 2 times

🗨️ 👤 **BJS78** 1 year, 3 months ago

<https://call4cloud.nl/2021/08/the-battle-between-aadj-and-aadr/>

upvoted 1 times

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to deploy and manage Windows devices.

You have 100 devices from users that left your company.

You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.

What should you do?

- A. Deploy a new configuration profile to the devices.
- B. Perform a Windows Autopilot reset on the devices.
- C. Perform an in-place upgrade on the devices.
- D. Perform a clean installation of Windows 11 on the devices.

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗨️ **WORKHOLIC** 3 weeks, 2 days ago

**Selected Answer: B**

Windows Pilot Reset, removes user data but retains device enrollment  
upvoted 1 times

🗨️ **den5\_pepito83** 2 months, 1 week ago

Yes, but doesn't remove local admin on device.  
upvoted 1 times

🗨️ **MR\_Eliot** 4 months ago

**Selected Answer: B**

Answer is correct.  
upvoted 1 times

🗨️ **Darkfire** 4 months, 2 weeks ago

**Selected Answer: B**

B is correct

<https://learn.microsoft.com/en-us/autopilot/windows-autopilot-reset>  
upvoted 1 times

🗨️ **Amir1909** 5 months, 3 weeks ago

Correct  
upvoted 1 times

🗨️ **kay000001** 7 months, 1 week ago

**Selected Answer: B**

Answer is B:  
<https://learn.microsoft.com/en-us/education/windows/autopilot-reset>  
upvoted 1 times

🗨️ **LiamAzure** 8 months, 1 week ago

B Windows Pilot Reset, removes user data but retains device enrollment  
upvoted 1 times

🗨️ **iamforksu** 8 months, 2 weeks ago

**Selected Answer: B**

B seems solid  
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.

## Answer Area

### Create profile

Windows PC

✓ Basics   **2** Out-of-box experience (OOBE)   3 Assignments   4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode * ⓘ	User-Driven	▼
Join to Azure AD as * ⓘ	Azure AD joined	▼
Microsoft Software License Terms ⓘ	Show	Hide
ⓘ Important information about hiding license terms		
Privacy settings ⓘ	Show	Hide
ⓘ The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. <a href="#">Learn more</a>		
Hide change account options ⓘ	Show	Hide
User account type ⓘ	Administrator	Standard
Allow pre-provisioned deployment ⓘ	No	Yes
Language (Region) ⓘ	Operating system default	▼
Automatically configure keyboard ⓘ	No	Yes
Apply device name template ⓘ	No	Yes

## Answer Area

### Create profile

Windows PC

✓ Basics 2 **Out-of-box experience (OOBE)** 3 Assignments 4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode \*

Join to Azure AD as \*

Microsoft Software License Terms

#### Suggested Answer:

[Important information about hiding license terms](#)

Privacy settings

[The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. Learn more](#)

Hide change account options

User account type

Allow pre-provisioned deployment

Language (Region)

Automatically configure keyboard

Apply device name template

**[Removed]** [Highly Voted](#) 7 months, 3 weeks ago

To configure a Windows Autopilot deployment profile to meet the specified requirements, you need to set the following:

1. **Automatically enroll new devices and provision system apps without requiring end-user authentication:**  
- **Deployment mode:** Select "Self-Deploying mode" as it allows devices to be deployed with zero-touch, without requiring user authentication.
2. **Include the hardware serial number in the computer name:**  
- **Apply computer name template:** Use the template "%SERIAL%" which will include the hardware serial number in the computer name.

Therefore, the settings you need to configure are:

1. **Deployment mode:** Self-Deploying
2. **Apply computer name template:** %SERIAL%

Make sure to configure these settings in the Windows Autopilot deployment profile to meet the requirements.

upvoted 26 times

**ExamKiller020** [Highly Voted](#) 1 year, 3 months ago

Given answer is correct.

For deployment mode you can use self-deploying mode.

upvoted 7 times

**dnt91** [Most Recent](#) 3 months, 3 weeks ago

Answer is :

1. Allow pre-provisioned deployment
2. Apply Device name template

upvoted 1 times

**CJL324** 7 months, 3 weeks ago

Answer is correct.

Steps to configure these settings in the Autopilot deployment profile:

Create or edit an existing Windows Autopilot deployment profile in the Microsoft Endpoint Manager admin center.

Set the deployment mode:

Go to Windows Autopilot deployment profiles.

Select or create a profile and then go to Out-of-box experience (OOBE).

Choose Self-Deploying (preview) or Autopilot for pre-provisioned deployment under Deployment mode.

Configure the computer name template:

While still editing the profile, find the Apply device name template setting.

Enter the desired template, for example, PC-%SERIAL%

upvoted 1 times

  **kerimnl** 9 months ago

No i think the answer is wrong:

1- Allow pre-provisioned deployment:

Enable pressing Windows key 5 times to run OOBE without user authentication to enroll device and provision all system-context apps and settings. User-context apps and settings will be delivered when the user signs in.

Because Self deploying mode lets you deploy a Windows device as a kiosk, digital signage device, or a shared device. We see nothing in the question about: Kiosk mode etc.


2- Apply device name template

upvoted 4 times

  **fic** 8 months, 4 weeks ago

Surreeee!!

upvoted 1 times

  **MR\_Eliot** 10 months, 1 week ago

I would vouch for Pre-Provisioning. Self-deploying as told in other comments, is for shared devices without a user.

- Automatically enroll new devices and provision system apps without requiring end-user authentication

> You can enable pre-provisioning for this one.

- Include the hardware serial number in the computer name.

> Apply device name template.

upvoted 4 times

  **MR\_Eliot** 10 months, 1 week ago

<https://learn.microsoft.com/en-us/autopilot/self-deploying>



upvoted 1 times

  **chafe** 5 months, 3 weeks ago

From your link:

1. Create an Autopilot profile for self-deploying mode with the desired settings.

upvoted 1 times

  **Darkfire** 10 months, 2 weeks ago

Answer is correct

On the Out-of-box experience (OOBE) page, for Deployment mode, choose one of these two options:

User-driven: Devices with this profile are associated with the user enrolling the device. User credentials are required to enroll the device.

Self-deploying (preview): 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 self-deploying mode is used, only compliance policies targeting the device are applied.

<https://learn.microsoft.com/en-us/autopilot/profiles#:~:text=User%2Ddriven%3A%20Devices,device%20are%20applied.>

upvoted 2 times

  **Romke\_en\_Tomke** 1 year ago

Answer not correct. Question states provision system apps without user authentication.

That requires the option pre-provisioned deployment.

Device name template is correct. You can use %SERIAL% variable.

upvoted 4 times

  **NoursBear** 11 months, 3 weeks ago

I agree but then it would have needed 3 options to change

upvoted 1 times

  **abigailcarol** 7 months, 3 weeks ago

great!!!

upvoted 1 times

  **VirtualJP** 1 year, 2 months ago

Agree answer is correct

upvoted 6 times



You have a computer named Computer1 that runs Windows 11.

A user named User1 plans to use Remote Desktop to connect to Computer1.

You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.


What should you do on Computer1?

- A. Turn on Reputation-based protection
- B. Enable Network Level Authentication (NLA)
- C. Turn on Network Discovery
- D. Configure the Remote Desktop Configuration service

**Suggested Answer:** B

Community vote distribution

B (100%)

 **ergacharsk** 5 months, 2 weeks ago

**Selected Answer: B**

B is correct


Network Level Authentication (NLA) is a security feature for Remote Desktop Services that requires the user to authenticate themselves before a remote desktop session is established. This adds an extra layer of security by ensuring that the user is authenticated before the remote session is created, reducing the risk of unauthorized access.

upvoted 1 times

 **MR\_Eliot** 10 months, 1 week ago

B is correct.

upvoted 1 times

 **Darkfire** 10 months, 2 weeks ago

**Selected Answer: B**

B is correct.

<https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-access#:~:text=a%20strong%20password.,Why%20allow%20connections%20only%20with%20Network%20Level%20Authentication%3F,home%20network%20Feedback>

Feedback

upvoted 1 times

 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times


 **kay00001** 1 year, 1 month ago

**Selected Answer: B**

Answer is B:

Here is a good article: <https://zappedia.com/network-level-authentication/>

upvoted 1 times

 **fco168** 1 year, 1 month ago

**Selected Answer: B**

B it is!



upvoted 1 times

 **VirtualJP** 1 year, 2 months ago

**Selected Answer: B**

Given answer is correct.

upvoted 1 times

  **BJ578** 1 year, 3 months ago

<https://itcompanies.net/blog/network-level-authentication>

upvoted 1 times

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You have the devices shown in the following table.

Name	Operating system	Activation type
Device1	Windows 10 Pro for Workstation	Key
Device2	Windows 11 Pro	Key
Device3	Windows 11 Pro	Subscription

Which devices can be changed to Windows 11 Enterprise by using subscription activation?

- A. Device3 only
- B. Device2 and Device3 only
- C. Device1 and Device2 only
- D. Device1, Device2, and Device3

**Suggested Answer:** D

Community vote distribution

B (90%) 10%

 **Gillactus** Highly Voted 1 year, 3 months ago

**Selected Answer: B**

The correct answer is B. Read the note that states. Note

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>

upvoted 14 times

 **Omerozb** Most Recent 2 weeks, 3 days ago

**Selected Answer: B**

Subscription activation for Enterprise


Windows Enterprise E3 and E5 are available as online services via subscription. Windows Enterprise can be deployed in an organization without keys and reboots.

Devices with a current Windows Pro edition license can be seamlessly upgraded to Windows Enterprise.

Product key-based Windows Enterprise software licenses can be transitioned to Windows Enterprise subscription

<https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivot=windows-11>

upvoted 1 times

 **1655b71** 1 month, 3 weeks ago

Only device 3


upvoted 1 times

 **RomanV** 3 months, 1 week ago

If you came this far and still are unaware that Subscription does NOT upgrade your device from Windows 10 to 11, your failure on the exam is deserved. ;)

Answer is B.

upvoted 2 times

 **oopspruu** 5 months, 2 weeks ago

**Selected Answer: B**

The Windows Enterprise subscription will not magically upgrade Windows 10 to 11. It only upgrades Windows Pro to Enterprise. So correct answer is Device 2 and 3. Device 1 won't be changed to Windows 11 Enterprise, rather Windows 10 Enterprise.

upvoted 1 times

🗨️ **62b396d** 8 months, 3 weeks ago

Wouldn't this be A? since device3 is the only one with subscription?

upvoted 1 times

🗨️ **OyYaGotta** 9 months, 3 weeks ago

For all those saying you can't upgrade Win 10 Pro to 11 Pro with Windows Subscription Activation. You can. You'll only be prompted to upgrade if the Installation is not Windows 10 Pro.

upvoted 1 times

🗨️ **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: B**

B is correct. Device one, needst to be upgraded to Windows 11 first and activated using a Windows 11 key.

upvoted 1 times

🗨️ **Darkfire** 10 months, 2 weeks ago

**Selected Answer: B**

My first though was D aswell but:

For versions of Windows newer than Windows 10, an upgrade to Windows 10 would first be required, followed by upgrading to the version of Windows Enti

[https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation#subscription-activation-for-](https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation#subscription-activation-for-enterprise?text=For%20versions%20of%20Windows%20newer%20than%20Windows%2010%2C%20an%20upgrade%20to%20Windows%2010%20would%20)

[enterprise?text=For%20versions%20of%20Windows%20newer%20than%20Windows%2010%2C%20an%20upgrade%20to%20Windows%2010%20would%20](https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation#subscription-activation-for-enterprise?text=For%20versions%20of%20Windows%20newer%20than%20Windows%2010%2C%20an%20upgrade%20to%20Windows%2010%20would%20)

upvoted 1 times

🗨️ **Amir1909** 11 months, 4 weeks ago

B is correct

upvoted 1 times

🗨️ **yosry** 1 year, 1 month ago

**Selected Answer: B**

SEEMS CORRECT

upvoted 1 times

🗨️ **fco168** 1 year, 1 month ago

**Selected Answer: B**

B. Because the subscription cannot upgrade from Windows 10 to 11.

upvoted 1 times

🗨️ **LiamAzure** 1 year, 2 months ago

**Selected Answer: B**

2 and 3

upvoted 1 times

🗨️ **Grg433** 1 year, 3 months ago

**Selected Answer: A**

should be devie 3 only no ?

upvoted 2 times

🗨️ **Zelda78** 1 year, 3 months ago

Subscription activation for Enterprise

Windows Enterprise E3 and E5 are available as online services via subscription. You can deploy Windows Enterprise in your organization without keys and reboots.

Devices with a current Windows Pro edition license can be seamlessly upgraded to Windows Enterprise.

Product key-based Windows Enterprise software licenses can be transitioned to Windows Enterprise subscriptions.

<https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation>

upvoted 4 times

🗨️ **[Removed]** 1 year, 2 months ago

you have explained nothing

upvoted 2 times

🗨️ **Zelda78** 1 year, 1 month ago

subscription activation does not upgrade the OS magically from Windows 10 to Windows 11.

upvoted 1 times

  **AdamRachel** 11 months, 3 weeks ago

I think from Windows 10 Pro you can use to upgrade to Windows 11 Pro and from there to Windows 11 Enterprise

upvoted 4 times

## HOTSPOT

-

Your network contains an Active Directory domain named adatum.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10. Remote Desktop is enabled on Computer2.

The domain contains the user accounts shown in the following table.

Name	Member of
User1	Domain Admins
User2	Domain Users
User3	Domain Users

Computer2 contains the local groups shown in the following table.

Name	Members
Group1	ADATUM\User2 ADATUM\User3
Group2	ADATUM\User2
Group3	ADATUM\User3
Administrators	ADATUM\Domain Admins ADATUM\User3
Remote Desktop Users	Group1

The relevant user rights assignments for Computer2 are shown in the following table.

Policy	Security Setting
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Deny log on through Remote Desktop Services	Group2
Deny log on locally	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.

### Answer Area

Statements	Yes	No
User1 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>
User2 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>
User3 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> User1 can establish a Remote Desktop session to Computer2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can establish a Remote Desktop session to Computer2.	<input checked="" type="radio"/>	<input type="radio"/>

🗨️ 👤 **[Removed]** Highly Voted 👍 1 year, 3 months ago

it should be yes, no, no imo

User 3 is member of group 3 which is denied by the policy 'Deny log on locally'

upvoted 9 times

🗨️ 👤 **picho707** 1 year, 2 months ago

A user with "Deny logon locally" permissions can still connect via Remote Desktop Services, as these are two separate permissions.

On the other hand, the "Deny logon through Remote Desktop Services" policy determines which users are prevented from logging on to the device through a Remote Desktop connection. This means that the user cannot log in remotely via Remote Desktop Services.

upvoted 13 times

🗨️ 👤 **reapernam** 1 year, 3 months ago

Doesnt that mean deny local logins only.

But Allow Remote logins.

upvoted 6 times

🗨️ 👤 **AdamRachel** 11 months, 3 weeks ago

Yes, but he is also a member of the Administrator group which has access.

upvoted 1 times

🗨️ 👤 **Sprocket10** Highly Voted 👍 1 year, 2 months ago

Answers are correct YNY

upvoted 9 times

🗨️ 👤 **MR\_Eliot** Most Recent 🕒 10 months, 1 week ago

Answers are correct:

YES:

- User1 is domain administrator. Administrators group is enabled in Allow log on through Remote Desktop Services.

NO:

- User2 is member of Group1 and Group2.

- Group1 allows user2 to login, but group2 disallow the user from log on.

YES:

- User 3 is member of Group1 and Group3.

- Group1 is member of Remote Desktop Users.

upvoted 4 times

🗨️ 👤 **Burkidur** 10 months, 1 week ago

The answers are correct, but MS is full of BS -- how LOCAL group Group1 can be added to LOCAL group Remote Desktop Users? Just try. Open compmgmt.msc right now. I dare you.

upvoted 5 times

🗨️ 👤 **Maclouis116** 6 months, 2 weeks ago

Exactly you can't nest local groups ... it's just a test to see if you can be tricked rather than know what you're actually doing

upvoted 3 times

🗨️ 👤 **riccardo1999** 11 months, 2 weeks ago

but the user 1 why is enable?

upvoted 1 times

🗨️ 👤 **HvD** 2 months, 1 week ago

It is member of Domain Admins, and Domain Admins are local Administrators too.

upvoted 1 times

🗨️ 👤 **yosry** 1 year, 1 month ago

SEEMS CORRECT

upvoted 1 times

🗨️ 👤 **abill** 1 year, 1 month ago

Is it YNN or YNY?

upvoted 1 times

🗨️ 👤 **rcristiano** 9 months, 1 week ago



Correto: YNY

upvoted 1 times

  **LiamAzure** 1 year, 2 months ago

YNY, User 3 is an administrator

upvoted 3 times

  **NoursBear** 1 year, 1 month ago

yes he is an admin but domain users can connect as long as they are not in Group2

upvoted 1 times



You have two computers named Computer1 and Computer2 that run Windows 10. Computer2 has Remote Desktop enabled.

From Computer1, you connect to Computer2 by using Remote Desktop Connection.

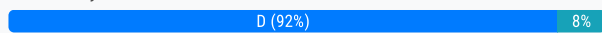
You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session.

What should you do?

- A. From Computer2, configure the Remote Desktop settings.
- B. From Windows Defender Firewall on Computer1, allow Remote Desktop.
- C. From Windows Defender Firewall on Computer2, allow File and Printer Sharing.
- D. From Computer1, configure the Remote Desktop Connection settings.

**Suggested Answer:** D

Community vote distribution



**Sprocket10** Highly Voted 1 year, 2 months ago

**Selected Answer: D**

D is correct as anyone using Windows 10 for 8 years would know. Setting from the originating device within the repair app upvoted 7 times

**RomanV** Most Recent 3 months, 1 week ago

It's D.

For more info, Google: Windows RDP Clients Drive Redirection

<https://docs.axissecurity.com/docs/verifying-that-the-rdp-client-allows-drive-redirection>

upvoted 1 times

**METAM** 4 months, 1 week ago

From Computer1, you connect to Computer2 by using Remote Desktop Connection.

You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session

I find this question illogical, from Computer1 he wants to access the local disk of the same computer1 !!! why does he need RDP ?? someone explain to me.

upvoted 1 times

**RomanV** 3 months, 1 week ago

Like oopspruu said:

Anyone that has actually used RD client on Windows should know this. The question states that the client needs to access their drives in the RDS. So they have to configure options in their own RD client before connecting.

upvoted 1 times

**oopspruu** 5 months, 2 weeks ago

**Selected Answer: D**

Anyone that has actually used RD client on Windows should know this. The question states that the client needs to access their drives in the RDS. So they have to configure options in their own RD client before connecting.

upvoted 2 times

**MR\_Eliot** 10 months, 1 week ago

**Selected Answer: D**

Provided answer is correct. You can change the settings before connecting to the remote computer.

upvoted 1 times

☒ **Merrybob** 11 months, 1 week ago

**Selected Answer: D**

D.

This is known as Client Drive Redirection and is part of the local computers RDP Properties/Settings. The setting has to be modified from Computer 1 so that it allows its local drives to be made visible with an RDP session.

upvoted 2 times

☒ **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

☒ **Cristy** 1 year, 1 month ago

Can someone tell me why is not B ?

upvoted 1 times

☒ **NoursBear** 1 year, 1 month ago

read the question again

upvoted 1 times

☒ **benpatto** 1 year, 2 months ago

I agree with Casticod, you can do it in local resources.

In remote desktop settings, you can enable remote desktop connections and setup NLA - you can also setup which accounts can be used to remote to your device but no option to allow for File sharing.

The repair app has nothing to do with the Remote Desktop Connection settings in this question, so irrelevant.

upvoted 1 times

☒ **Casticod** 1 year, 3 months ago

**Selected Answer: A**

A for Me, No it's in connections zone, its in Local resources: <https://www.ionos.com/help/server-cloud-infrastructure/dedicated-server-for-servers-purchased-before-102818/servers/transfer-files-using-remote-desktop/>

upvoted 1 times

☒ **RomanV** 3 months, 1 week ago

No one really cares what you think. It's D.

Google: Windows RDP Clients Drive Redirection

<https://docs.axissecurity.com/docs/verifying-that-the-rdp-client-allows-drive-redirection>

upvoted 1 times

☒ **Casticod** 1 year, 3 months ago

Local resources, sorry

upvoted 1 times

You have a Microsoft 365 subscription that uses Microsoft Intune.

You have five new Windows 11 Pro devices.

You need to prepare the devices for corporate use. The solution must meet the following requirements:

- Install Windows 11 Enterprise on each device.
- Install a Windows Installer (MSI) package named App1 on each device.
- Add a certificate named Certificate1 that is required by App1.
- Join each device to Azure AD.

Which three provisioning options can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.



- A. subscription activation
- B. a custom Windows image
- C. an in-place upgrade
- D. Windows Autopilot
- E. provisioning packages

**Suggested Answer:** BDE

Community vote distribution

BDE (61%)

ADE (39%)

  **someone1337** Highly Voted 1 year, 3 months ago

A, D, E.

Install Windows 11 Enterprise on each device:

Subscription activation

Install a Windows Installer (MSI) package named App1 on each device:

Provisioning packages

Add a certificate named Certificate1 that is required by App1:

Provisioning packages

Join each device to Azure AD:

Autopilot

upvoted 20 times

  **BJS78** 1 year, 1 month ago

"Each correct answer presents a complete solution", not "All 3 steps are required for a full solution".

upvoted 7 times

  **BJS78** Highly Voted 1 year, 3 months ago

Answer is correct. Pay attention to "Each correct answer presents a complete solution.". So ALL requirements must be filled by every single selection of solution.

a) subscription: upgrade only, nothing else

b) Custom image: yes, can do

c) In-place upgrade: upgrade only

d) Autopilot: yes

e) provisioning packages: yes



<https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages>

upvoted 13 times

  **Sprocket10** 1 year, 2 months ago

Should be ADE.

The purpose of Autopilot is to not require Custom Images so the answer would include both B and D together  
upvoted 1 times

  **BJS78** 1 year, 1 month ago

As I wrote: subscription activation does nothing with the app and certificate requirements. In custom image you can have the app and the certificate "built-in", also a task to join to AD. In Autopilot, if you do not have any device/app configs assigned to the devices, it just resets the OS, so the fully correct option there would be Autopilot + Intune/SCCM/GPO  
upvoted 3 times

  **HvD** 2 months, 1 week ago

Not true. When you have deployed the Windows 11 Pro with Autopilot, it will receive the subscription activation, which upgrades the device to Enterprise.  
upvoted 1 times

  **Tr619899** Most Recent 1 month ago

**Selected Answer: BDE**

D - Installs Windows 11 Ent., Deploy MSI package via Intune, Install Certificate through Configuration Profile, Join to Azure AD during provisioning process.

E - Created with Windows Configuration Designer, Upgrades the OS to Win 11 Ent., Installs MSI Package, Add Certificate, Join devices to Azure AD

B - Preinstall Win 11 Ent and App1 in custom image included with Certificate in the image, and we can configure devices to join Azure AD during deployment.



upvoted 1 times

  **AleFCI1908** 1 month, 3 weeks ago

**Selected Answer: BDE**

BDE because of "Each correct answer presents a complete solution"

upvoted 1 times

  **RomanV** 3 months, 1 week ago

**Selected Answer: BDE**

b) Custom image: yes

d) Autopilot: yes

e) provisioning packages: yes

Key sentence: "Each correct answer presents a complete solution"



upvoted 1 times

  **Cezt** 5 months, 1 week ago

**Selected Answer: ADE**

custom image wont join to AD



upvoted 1 times

  **ergacharsk** 5 months, 2 weeks ago

**Selected Answer: BDE**

BDE confirmed by ChatGPT :)

upvoted 1 times

  **oopspruu** 5 months, 2 weeks ago

**Selected Answer: BDE**

"Each correct answer presents a complete solution." THIS IS A REQUIREMENT

Subscription Activation cannot perform any other action apart from switching Pro to Enterprise.

So Autopilot, custom image, and provisioning packages.

upvoted 1 times

  **Prasis** 5 months, 3 weeks ago

B,D,E

Chatgpt:

D. Windows Autopilot

Windows Autopilot can be used to automatically join devices to Azure AD, upgrade Windows 11 Pro to Windows 11 Enterprise (through subscription activation), install required applications, and configure certificates.

E. provisioning packages

Provisioning packages can be used to configure devices for corporate use, including installing applications, configuring certificates, and joining devices to Azure AD.

B. a custom Windows image

A custom Windows image can include Windows 11 Enterprise, the MSI package (App1), and the certificate (Certificate1). After deployment, the devices can be joined to Azure AD.

upvoted 1 times



  **CJL324** 7 months, 3 weeks ago

B. a custom Windows image: You can create a custom Windows 11 Enterprise image that includes the required MSI package (App1) and the Certificate1, and then use this custom image to install Windows 11 Enterprise on each device.

D. Windows Autopilot: You can use Windows Autopilot to automate the deployment and configuration of new devices, including installing Windows 11 Enterprise, installing the MSI package (App1) as part of the Autopilot deployment profile, adding Certificate1, and joining the devices to Azure AD.


E. provisioning packages: You can create provisioning packages that include the installation of Windows 11 Enterprise, the installation of the MSI package (App1), adding Certificate1, and joining the devices to Azure AD. These provisioning packages can then be applied to each device during the initial setup process.

upvoted 1 times

  **BigTone** 2 months, 2 weeks ago

This doesn't make sense, your justification for B is that you use an image with the MSI installed and the certificate. In E you are going to use a provisioning package to install an MSI and a certificate that is already installed via the custom image. That has to be wrong



upvoted 1 times

  **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: BDE**

Provided answer is correct. Inplace upgrade and subscription activation doesn't magically join the device in Entra ID.

upvoted 1 times

  **kanuto** 10 months, 3 weeks ago

**Selected Answer: BDE**

Agreed

upvoted 1 times

  **Pasado** 11 months ago

ChatGPT: To prepare the Windows 11 Pro devices for corporate use with the provided requirements, you can use the following provisioning options:

B. A custom Windows image: This allows you to install Windows 11 Enterprise on each device.

D. Windows Autopilot: This allows you to join each device to Azure AD and customize the device setup, including the installation of applications and certificates.

E. Provisioning packages: You can create a provisioning package that includes the installation of the MSI package named App1 and the addition of the required certificate named Certificate1.

So, the correct selections are B, D, and E.

upvoted 1 times

  **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

  **nosmanav** 1 year ago

Just curious... How can you apply a custom image with Intune?

upvoted 1 times

🗨️ 👤 **nosmanav** 1 year ago

There is something wrong with this question. First it says "Each correct answer presents a complete solution". Then after "Each correct selection is worth one point". If we go for the first option I would say BDE.

upvoted 1 times

🗨️ 👤 **belyo** 1 year ago

**Selected Answer: ADE**

A D E

it says that you have machines with installed win 11 pro, so you dont need an installation

-subscription activation

-provisioning package

-autopilot

no need for custom images

upvoted 1 times

🗨️ 👤 **Cristyy** 1 year, 1 month ago

**Selected Answer: BDE**

BDE is correct

upvoted 2 times

DRAG DROP

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.

You import a Windows 11 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.

### Actions

### Answer Area

Modify a Windows 11 operating system setting.

Modify a selection profile.

Add App1 to DS1.

Identify the GUID of App1.

Modify CustomSettings.ini.

1

2

3



### Answer Area

Suggested Answer:

1

Add App1 to DS1.

2

Identify the GUID of App1.

3

Modify CustomSettings.ini.

**ergacharsk** 5 months, 2 weeks ago

ChatGPT says:

\*Add App1 to DS1.

First, you need to add the application to the deployment share.

\*Modify CustomSettings.ini.

After adding the application, you need to ensure that it is included in the task sequences by modifying the CustomSettings.ini file.

\*Modify a selection profile.

Finally, you modify a selection profile to include the application in the deployment.

upvoted 1 times

**MR\_Eliot** 10 months, 1 week ago

Seems correct to me.

upvoted 2 times

**Darkfire** 10 months, 2 weeks ago

Seems correct


<https://247-it.io/en/mdt-installation-of-applications-when-deploying-windows/>

upvoted 2 times

  **yosry** 1 year ago

SEEMS CORRECT

upvoted 2 times

  **kay000001** 1 year, 1 month ago

Answer is correct.

upvoted 2 times

  **cpaljhc4** 1 year, 1 month ago

<https://www.examttopics.com/discussions/microsoft/view/63336-exam-md-101-topic-2-question-83-discussion/>

upvoted 2 times



HOTSPOT

-

You have the devices shown in the following table.

Name	Operating system	Description
Device1	32-bit version of Windows 10	Retired device
Device2	64-bit version of Windows 11	New device
Server1	Windows Server 2019	File server

You need to migrate app data from Device1 to Device2. The data must be encrypted and stored on Server1 during the migration.

Which command should you run on each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Device1:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Device2:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

**Answer Area**

Suggested Answer:

Device1:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Device2:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

 **ergacharsk** 5 months, 2 weeks ago

given answer is correct  
upvoted 2 times

 **MR\_Eliot** 10 months, 1 week ago

Provided answer is correct.  
upvoted 3 times


 **Darkfire** 10 months, 2 weeks ago

Correct

<https://learn.microsoft.com/en-us/windows/deployment/usmt/understanding-migration-xml-files#overview-of-the-migappxml->



file:~:text=ScanState.exe%20/i%3Amigapps.xml%20/i%3AMigDocs.xml%20/genconfig%3Ac%3A%5CmyFolder%5CConfig.xml

upvoted 2 times

  **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times



  **yosry** 1 year, 1 month ago

Device 1: 6th option

Device 2: 3rd option

<https://learn.microsoft.com/en-us/windows/deployment/usmt/understanding-migration-xml-files#overview-of-the-migappxml-file>

upvoted 2 times

  **yosry** 1 year, 1 month ago

Sorry i'm wrong, shown answer is correct!



the question in talking about APP Data so app settings and cache files at first I thought it was talking about files.

upvoted 1 times

  **Rocky83** 1 year, 2 months ago

Correct answer

upvoted 2 times

  **BJS78** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax>

<https://learn.microsoft.com/en-us/windows/deployment/usmt/usmt-loadstate-syntax>

upvoted 4 times

You have a Microsoft 365 subscription.

You plan to use Windows Autopilot to provision 25 Windows 11 devices.

You need to configure the Out-of-box experience (OOBE) settings.

What should you create in the Microsoft Intune admin center?

- A. an enrollment status page (ESP)
- B. a deployment profile
- C. a compliance policy
- D. a PowerShell script
- E. a configuration profile

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗨️ **CJL324** 1 month, 2 weeks ago

Correct B. a deployment profile.

In the Microsoft Intune admin center, a deployment profile allows you to configure various settings for the Autopilot deployment, including the Out-of-box experience (OOBE) settings. Within the deployment profile, you can define options such as language and region settings, privacy settings, Wi-Fi configuration, and more to customize the initial setup experience for the provisioned devices.

upvoted 1 times

🗨️ **MR\_Eliot** 4 months ago

**Selected Answer: B**

ESP does nothing by itself. You need to create a deployment profile.

upvoted 4 times

🗨️ **Darkfire** 4 months, 2 weeks ago

**Selected Answer: B**

B is correct

[https://learn.microsoft.com/en-](https://learn.microsoft.com/en-us/autopilot/profiles#:~:text=On%20the%20Out%2Dof%2Dbox%20experience%20(OOBE)%20page%2C%20for%20Deployment%20mode%2C%20choose%20)

[us/autopilot/profiles#:~:text=On%20the%20Out%2Dof%2Dbox%20experience%20\(OOBE\)%20page%2C%20for%20Deployment%20mode%2C%20choose%20](https://learn.microsoft.com/en-us/autopilot/profiles#:~:text=On%20the%20Out%2Dof%2Dbox%20experience%20(OOBE)%20page%2C%20for%20Deployment%20mode%2C%20choose%20)

upvoted 2 times

🗨️ **Amir1909** 5 months, 3 weeks ago

Correct

upvoted 1 times

🗨️ **kay000001** 7 months, 1 week ago

**Selected Answer: B**

Answer is B:

<https://learn.microsoft.com/en-us/autopilot/profiles>

upvoted 1 times

🗨️ **yosry** 7 months, 1 week ago

**Selected Answer: B**

Seems correct


upvoted 1 times

🗨️ **LiamAzure** 8 months, 1 week ago

**Selected Answer: B**


Deployment Profile which you would assign to a group, as part of Windows Autopilot

upvoted 1 times

 **h38jhd38k** 8 months, 2 weeks ago

<https://learn.microsoft.com/en-us/partner-center/autopilot>

upvoted 1 times

 **ExamKiller020** 9 months, 1 week ago

**Selected Answer: B**

Given answer is correct. Checked in own tenant

upvoted 2 times

You have an Azure AD tenant that contains the devices shown in the following table.

Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered

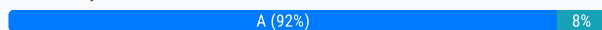
You purchase Windows 11 Enterprise E5 licenses.

Which devices can use Subscription Activation to upgrade to Windows 11 Enterprise?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device2, Device3, and Device4

**Suggested Answer:** C

Community vote distribution



**Darkfire** Highly Voted 10 months, 2 weeks ago

**Selected Answer: A**

Should be A

Devices must be Microsoft Entra joined or Microsoft Entra hybrid joined. Workgroup-joined or Microsoft Entra registered devices aren't supported.

<https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation#:~:text=for%20identity%20management.-,Devices%20must%20be%20Microsoft%20Entra%20joined%20or%20Microsoft%20Entra%20hybrid%20j,For%20Microsoft%20customers>

The Subscription does NOT upgrade Windows 10 pro to windows 11 Enterprise

upvoted 7 times

**CJL324** Highly Voted 7 months, 3 weeks ago

A

Subscription Activation allows devices to upgrade to Windows 11 Enterprise if they have the appropriate license assigned to them in the Azure AD tenant. Since Windows 11 Enterprise E5 licenses have been purchased, only Azure AD Joined devices are eligible for Subscription Activation. Therefore, only Device1 can use Subscription Activation to upgrade to Windows 11 Enterprise.

upvoted 7 times

**subbuhotmail** Most Recent 3 months, 3 weeks ago

**Selected Answer: A**

AD Registered device cannot be activated.

<https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation? pivots=windows-11# windows-enterprise-requirements>

upvoted 1 times

**Daniel\_G** 3 months, 4 weeks ago

**Selected Answer: C**

C is correct. Answer A is Device 1 only and Device 1 is the same as Device 3; therefore, both Device 1 and 3 are correct.

upvoted 1 times

**Daniel\_G** 3 months, 4 weeks ago

Cancel this comment.

upvoted 3 times

🗨️ 👤 **Ce2t** 5 months, 1 week ago

**Selected Answer: A**

Devices must be Microsoft Entra joined or Microsoft Entra hybrid joined. Workgroup-joined or Microsoft Entra registered devices aren't supported.  
<https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivot=windows-10#subscription-activation-for-enterprise-~:text=for%20identity%20management.,Devices%20must%20be%20Microsoft%20Entra%20joined%20or%20Microsoft%20Entra%20hybrid%20jo>  
For%20Microsoft%20customers

upvoted 1 times

🗨️ 👤 **Irism** 7 months, 3 weeks ago

**Selected Answer: C**

"Devices with a current Windows Pro edition license can be seamlessly upgraded to Windows Enterprise."

<https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivot=windows-10#subscription-activation-for-enterprise>

upvoted 1 times

🗨️ 👤 **Pablodijkman** 6 months ago

Codeword is "current"

From 11 to 11 is current. Windows 10 is NOT current.

upvoted 1 times

🗨️ 👤 **matrixuser** 9 months, 2 weeks ago

correct answer is D Device1, Device2, Device3, and Device4

upvoted 1 times

🗨️ 👤 **pxdPhil2** 9 months ago

No. You can only use subscription activation for Entra Joined devices running the same OS version

upvoted 1 times

🗨️ 👤 **sergioandreslq** 10 months ago

Question 68 ask about which device can be activated with subscription activation: in that case was Dev1 Win11 PRO and Dev3 Win10 PRO.

However, for this question is which device can be upgrade to Win11 Enterprise using Subscription activation, in that case, Only Win11 Pro can be upgraded.

Subscription activation doesn't support Upgrade WIN10 PRO to Win11 Enterprise.

upvoted 4 times

🗨️ 👤 **MR\_Eliot** 10 months, 1 week ago

**Selected Answer: A**

Agree with Darkfire.

Device must be Entra ID joined.

upvoted 1 times

🗨️ 👤 **Mattia8** 11 months, 1 week ago

**Selected Answer: A**

Subscription Activation cannot upgrade to 11

upvoted 1 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **magnopds** 11 months, 4 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#the-evolution-of-deployment>

upvoted 1 times

🗨️ 👤 **belyo** 1 year ago

**Selected Answer: A**

Devices must be Microsoft Entra joined or Microsoft Entra hybrid joined.

Workgroup-joined or Microsoft Entra registered devices aren't supported.

Subscription activation doesn't update a device from Windows 10 to Windows 11

upvoted 4 times

🗨️ 👤 **madsa** 1 year, 1 month ago

It is not the fact that it does not upgrade is the fact that it will take the version to enterprise and allow an upgrade, the question does not say immediately upgrade.

upvoted 2 times

🗨️ 👤 **madsa** 1 year, 1 month ago

There are several questions like this one and took me time to properly investigate "Subscription Activation is a method for upgrading Windows 10 Pro to Windows 11 Enterprise using the Azure AD join type." Giving answer is correct.

upvoted 2 times

🗨️ 👤 **yosry** 1 year, 1 month ago

**Selected Answer: A**

THE CORRECT ANSWER IS A:

Subscription activation does not UPGRADE windows.

upvoted 2 times

🗨️ 👤 **h38jhd38k** 1 year, 2 months ago

Device 1 only. Subscription activation doesn't upgrade versions.

<https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#the-evolution-of-deployment>

upvoted 1 times

You have a Microsoft 365 Subscription that uses Microsoft Intune.

You add apps to Intune as shown in the following table.

Name	App type
App1	Android store app
App2	Android line-of-business app
App3	Managed Google Play app

You need to create an app configuration policy named Policy1 for the Android Enterprise platform.

Which apps can you manage by using Policy1?

- A. App2 only
- B. App3 only
- C. App1 and App3 only
- D. App2 and App3 only
- E. App1, App2, and App3

**Suggested Answer:** B

Community vote distribution


B (63%) D (38%)

 **Tr619899** 1 month ago

**Selected Answer: B**

These apps are specifically built and deployed for Android Enterprise and fully support app configuration policies.

upvoted 1 times

 **Alex\_UC** 1 month, 3 weeks ago

**Selected Answer: B**

In theory answer B is correct, but only because is not explained that the LOB apps is wrapped with intune SDK. So without making assumptions the B is correct, but in real word the D is the correct answer


upvoted 4 times

 **AleFCI1908** 1 month, 3 weeks ago

**Selected Answer: D**


D; app1 and app3 , you can apply a policy to both lob and managed g play store

upvoted 1 times

 **93831b0** 4 months, 2 weeks ago

D. Standard Android Store Apps are not typically managed by Android Enterprise policies unless they are added as Managed Google Play apps. Therefore, only the Managed Google Play App (and potentially an Android LOB app deployed via Managed Google Play) can be managed by Policy1.

upvoted 1 times


 **SSK500** 4 months, 4 weeks ago

Not sure what will Microsoft accept as correct answer.

B: Managed Google Play app supports App config policy

D: Android LOB app supports App config policy when wrapped using Intune App Wrapping tool.

upvoted 1 times

 **ergacharsk** 5 months, 2 weeks ago

**Selected Answer: B**

B is correct



\*App1: Android store app - These are general apps available in the Google Play Store.



\*App2: Android line-of-business app - These are internally developed apps not listed in the public Google Play Store.

\*App3: Managed Google Play app - These are apps managed and distributed through Managed Google Play, which is part of Android Enterprise.

upvoted 3 times

  **oopspruu** 5 months, 2 weeks ago

**Selected Answer: B**

When deploying app config policy to a managed device, which uses the MDM channel, the app must be pinned to the management profile on iOS/iPadOS or deployed through Managed Google Play on Android devices.


Correct answer is B.

upvoted 1 times

  **Maclouis116** 6 months, 1 week ago

B is right for managing lob you have to use wrapping or sdk



upvoted 1 times

  **Frank9020** 7 months, 2 weeks ago

**Selected Answer: D**

D. App2 and App3 only

upvoted 2 times

  **CJL324** 7 months, 3 weeks ago

B.

For the Android Enterprise platform, app configuration policies can only be applied to Android line-of-business apps or Managed Google Play apps. Therefore, you can only manage App3 using the app configuration policy named Policy1.



upvoted 1 times

  **Thorgal\_Aegirsson** 9 months, 4 weeks ago

**Selected Answer: B**

I tested, for a policy for the platform supports only Managed Google Play

upvoted 3 times

  **ckmay** 10 months, 2 weeks ago

**Selected Answer: D**

LOB Apps CAN be configured if meets the following conditions:



"To support app configuration through the MAM channel, the app must be integrated with Intune App SDK. Line-of-business apps can either integrate the

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

I tested this in my own environment. I was able to upload a private .apk to the managed google play store then create both an MAM and MDM app config I was also able to create a MAM config policy for the same LOB app but not by uploading it to the managed google play store as a private app, but by up app wrapping tool

regular android store apps could NOT be added to app config profiles

upvoted 4 times

  **Darkfire** 10 months, 2 weeks ago

I agree

D is correct

Managed Google Play

[https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-](https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-android#:~:text=App%20configuration%20policies%20in%20Microsoft%20Intune%20supply%20settings%20to%20Managed%20Google%20Play%20apps)

[android#:~:text=App%20configuration%20policies%20in%20Microsoft%20Intune%20supply%20settings%20to%20Managed%20Google%20Play%20apps](https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-android#:~:text=App%20configuration%20policies%20in%20Microsoft%20Intune%20supply%20settings%20to%20Managed%20Google%20Play%20apps)

Line Of Business

[https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview#:~:text=To%20support%20app%20configuration%20through;](https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview#:~:text=To%20support%20app%20configuration%20through;upvoted%201%20times)

upvoted 1 times

  **[Removed]** 11 months, 1 week ago

"managed" is the key word here.

upvoted 1 times

  **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗉 👤 **yosry** 1 year, 1 month ago

**Selected Answer: B**

Seems correct

upvoted 1 times

🗉 👤 **Vlad99** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

You will only see apps from Managed Google Play store, not the Google Play store, when using Managed Devices as the Enrollment Type for Android devices.

Correct answer.

upvoted 3 times

🗉 👤 **Casticod** 1 year, 3 months ago

**Selected Answer: B**

Correct : <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-android>

upvoted 2 times

You have a Microsoft 365 subscription that uses Microsoft Intune.

You need to ensure that you can deploy apps to Android Enterprise devices.


What should you do first?

- A. Create a configuration profile.
- B. Add a certificate connector.
- C. Configure the Partner device management settings.
- D. Link your managed Google Play account to Intune.

**Suggested Answer:** D

Community vote distribution

D (100%)

 **Darkfire** 3 months, 3 weeks ago

**Selected Answer:** D

D is correct

<https://learn.microsoft.com/en-us/mem/intune/enrollment/connect-intune-android-enterprise#:~:text=To%20support%20the%20following%20Android%20enrollment%20types%2C%20you%20must%20connect%20your%20Intune%20tenant>

upvoted 1 times

 **Merrybob** 5 months ago

**Selected Answer:** D

D. Link your managed Google Play account to Intune.


upvoted 1 times

 **yosry** 7 months, 1 week ago

**Selected Answer:** D

Seems correct


upvoted 1 times

 **LiamAzure** 8 months, 1 week ago

**Selected Answer:** D

D Link your Managed Goolge

upvoted 2 times

 **VirtualJP** 8 months, 3 weeks ago

**Selected Answer:** D

Agreed

upvoted 3 times

You have a Microsoft 365 tenant that uses Microsoft Intune.

You use the Company Portal app to access and install published apps to enrolled devices.

From the Microsoft Intune admin center, you add a Microsoft Store app.

Which two App information types are visible in the Company Portal?

NOTE: Each correct selection is worth one point.

- A. Privacy URL
- B. Information URL
- C. Developer
- D. Owner

**Suggested Answer:** AC

Community vote distribution



**Fortind1974** Highly Voted 1 year, 3 months ago

**Selected Answer:** AB

- A. Privacy URL
- B. Information URL

<https://learn.microsoft.com/en-us/mem/intune/apps/store-apps-microsoft>  
upvoted 17 times

**yoha1558** 1 year, 2 months ago

Answer is corrected

<https://www.examttopics.com/discussions/microsoft/view/64554-exam-md-101-topic-5-question-7-discussion>  
upvoted 2 times

**h38jhd38k** 1 year, 2 months ago

<https://learn.microsoft.com/en-us/mem/intune/apps/store-apps-microsoft#step-2-search-the-microsoft-store>  
Exact link of the page for the correct answer  
upvoted 2 times

**Azure20** Most Recent 1 month ago

**Selected Answer:** D

It seems I might be overlooking something. The question specifically refers to apps "visible in the Company Portal," not in the "Microsoft Store."

According to <https://learn.microsoft.com/en-us/mem/intune/user-help/manage-apps-cpweb#view-all-apps>, the information visible includes the Name, Publisher, Date Published, Status, and Category.

Additionally, the app details page shows: Name, Publisher, "App Version", "Date Published", Categories, and "Device Management Required", as described in:

<https://learn.microsoft.com/en-us/mem/intune/user-help/manage-apps-cpweb#view-app-details>

So, it's possible that some of the previous answers are outdated.

upvoted 1 times

**ergacharsk** 5 months, 2 weeks ago

**Selected Answer:** AB

AB is correct

upvoted 1 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

**Selected Answer: AB**

In the New MS App Store type apps, I am seeing the Privacy URL pre-filled but info URL being empty, same as Developer and Owner. In this, I'd go with Info URL option as Developer + Owner is something you'll always have to manually fill while Publisher comes pre-filled.

upvoted 2 times

🗨️ 👤 **CJL324** 7 months, 3 weeks ago

B and C

These details help users understand more about the app they are installing and who developed it. Privacy URL and Owner are not typically displayed in the Company Portal for Microsoft Store apps added to Intune.

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months ago

**Selected Answer: AB**

Correct answer is AB.

Developer and Owner information is only visible in admin center.

upvoted 2 times

🗨️ 👤 **bigreg** 4 months ago

Just confirmed it as well.

upvoted 1 times

🗨️ 👤 **kanuto** 10 months, 3 weeks ago

**Selected Answer: AC**

Checking in prod and lab, all I see is

A. Information URL

C. Developer

upvoted 1 times

🗨️ 👤 **kanuto** 10 months, 3 weeks ago

A. Privacy URL, I meant

upvoted 1 times

🗨️ 👤 **Pasado** 11 months ago

ChatGPT: In the Company Portal app, when you add a Microsoft Store app from the Microsoft Intune admin center, the two App information types that are visible are:

B. Information URL

C. Developer

So the correct selections are B and C.

upvoted 2 times

🗨️ 👤 **VirtualJP** 1 year, 2 months ago

**Selected Answer: AB**

These App information types are provided by the app developer. The Privacy URL links to the developer's privacy policy, and the Information URL links to the developer's website.

upvoted 1 times

🗨️ 👤 **SHIT159** 1 year, 2 months ago

**Selected Answer: AB**

a and b

upvoted 1 times

🗨️ 👤 **flim322** 1 year, 3 months ago

Answer is corrected

<https://www.examttopics.com/discussions/microsoft/view/64554-exam-md-101-topic-5-question-7-discussion/>

upvoted 2 times

🗨️ 👤 **Zelda78** 1 year, 3 months ago

indeed Privacy url and information.

upvoted 1 times

HOTSPOT

-

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune.

You need to set a custom image as the wallpaper and sign-in screen.

Which two settings should you configure in the Device restrictions configuration profile? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

## Device restrictions

Windows 10 and later

✓ Basics **2 Configuration settings** ③ Assignments ④ Applicability Rules ⑤ Review + create

∨ App Store

∨ Cellular and connectivity

∨ Cloud and Storage

∨ Cloud Printer

∨ Control Panel and Settings

∨ Display

∨ General

∨ Locked Screen Experience

∨ Messaging

∨ Microsoft Edge Browser

∨ Network proxy

∨ Password

∨ Per-app privacy exceptions

∨ Personalization

∨ Printer

∨ Privacy

∨ Projection

Previous

Next

## Device restrictions

Windows 10 and later

✓ Basics 2 Configuration settings 3 Assignments 4 Applicability Rules 5 Review + create

- ▽ App Store
- ▽ Cellular and connectivity
- ▽ Cloud and Storage
- ▽ Cloud Printer
- ▽ Control Panel and Settings
- ▽ Display
- ▽ General
- ▽ Locked Screen Experience
- ▽ Messaging
- ▽ Microsoft Edge Browser
- ▽ Network proxy
- ▽ Password
- ▽ Per-app privacy exceptions
- ▽ Personalization
- ▽ Printer
- ▽ Privacy
- ▽ Projection

Previous Next

Suggested Answer:

- 🗨️ **Casticod** Highly Voted 9 months ago  
lock screen Experience > "locked screen picture url" option.  
Personnalization > "Desktop background picture url" option.  
so answers are correct.  
upvoted 10 times
- 🗨️ **Darkfire** Most Recent 3 months, 3 weeks ago  
Answers are correct  
upvoted 4 times
- 🗨️ **MR\_Eliot** 4 months ago  
answers are correct  
upvoted 4 times
- 🗨️ **Pasado** 4 months, 3 weeks ago  
Correct  
upvoted 3 times
- 🗨️ **Merrybob** 5 months ago  
Straight forward enough. Answers are correct.  
upvoted 3 times



You have computers that run Windows 11 Pro. The computers are joined to Azure AD and enrolled in Microsoft Intune.

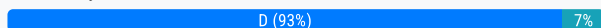
You need to upgrade the computers to Windows 11 Enterprise.

What should you configure in Intune?

- A. a device compliance policy
- B. a device cleanup rule
- C. a device enrollment policy
- D. a device configuration profile

**Suggested Answer:** D

Community vote distribution



**oopspruu** Highly Voted 5 months, 2 weeks ago

**Selected Answer: D**

As a gentle reminder, DO NOT TRUST Chat GPT. I see a lot of people here just providing ChatGPT answers instead of using their own brain and logic.

Learn WHY the answer is correct.

For this one, the setting is found in Devices > Windows > Configuration > Templates > Edition Upgrade and Mode Switch > Edition to upgrade to > choose Windows 10/11 Enterprise.

This is why D is correct answer.

upvoted 12 times

**ergacharsk** Most Recent 5 months, 2 weeks ago

**Selected Answer: D**

D is correct

upvoted 1 times

**CJL324** 7 months, 3 weeks ago

D

With a device configuration profile in Intune, you can specify the Windows 11 Enterprise edition and initiate the upgrade process on the enrolled devices. This profile allows you to manage settings and configurations on devices, including initiating OS upgrades, ensuring a seamless transition to Windows 11 Enterprise.

upvoted 2 times

**Pasado** 11 months ago

ChatGPT: To upgrade computers from Windows 11 Pro to Windows 11 Enterprise managed by Microsoft Intune, you should configure a device configuration profile (option D). This profile will allow you to specify the settings and configurations needed for the upgrade process.

upvoted 1 times

**mp34** 11 months, 3 weeks ago

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

configuration profile/Template/Edition upgrade and mode switch

upvoted 1 times

**Tigasmigas** 1 year, 1 month ago

**Selected Answer: D**

Create Windows 11 Enterprise Upgrade Profile:

In Microsoft Intune, create a Windows 11 Enterprise upgrade profile. This profile includes the details and settings for the upgrade. Here's a general outline of the steps:

In the Microsoft Endpoint Manager admin center, go to Devices > Windows > Configuration profiles.

upvoted 2 times

  **DiFortes** 1 year, 1 month ago

**Selected Answer: C**

device enrollment policy ?

Device Enrollment Policy (Option C):

A device enrollment policy in Microsoft Intune is used to control the enrollment of devices into Intune. It specifies the settings that are applied to a device during the enrollment process.

When you want to upgrade Windows editions or make other specific configurations during enrollment, you can use a device enrollment policy to target and configure those settings.

upvoted 1 times

  **NoursBear** 11 months, 3 weeks ago

This is the key here: The computers are joined to Azure AD and enrolled in Microsoft Intune.

upvoted 2 times

  **Sprocket10** 1 year, 2 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

You have computers that run Windows 10 and are managed by using Microsoft Intune.

Users store their files in a folder named D:\Folder1.

You need to ensure that only a trusted list of applications is granted write access to D:\Folder1.

What should you configure in the device configuration profile?

- A. Microsoft Defender Exploit Guard
- B. Microsoft Defender Application Guard
- C. Microsoft Defender SmartScreen
- D. Microsoft Defender Application Control

**Suggested Answer: A**

*Community vote distribution*

A (76%)


D (24%)

 **Tr619899** 1 month ago

**Selected Answer: A**

We should configure Controlled Folder Access under Microsoft Defender Exploit Guard. Controlled Folder Access is a feature of Microsoft Defender for Endpoint that protects sensitive folders from unauthorized changes by malicious or untrusted applications.

upvoted 1 times

 **93831b0** 4 months, 2 weeks ago

**Selected Answer: A**

Configure Controlled Folder Access:

In the Endpoint protection profile, go to Microsoft Defender Exploit Guard.

Under Controlled folder access, enable the setting.

Specify D:\Folder1 as the folder that you want to protect.

Define the list of trusted applications that are allowed to write to the folder by specifying the file paths of these apps under the Allow apps to access protected folders section.


upvoted 3 times

 **Cezt** 5 months, 1 week ago

**Selected Answer: A**

you need to add the folder to be protected


upvoted 1 times

 **ergacharsk** 5 months, 2 weeks ago

**Selected Answer: A**

A is correct, trust me

upvoted 1 times

 **oopsruu** 5 months, 2 weeks ago

**Selected Answer: A**

Windows > Configuration > Administrative Templates > Windows Components > MS Defender AV > MS Defender Exploit Guard > Controlled Folder Access.

This is why A is correct.

upvoted 1 times

 **CJL324** 7 months, 3 weeks ago

D

Microsoft Defender Application Control (formerly known as Windows Defender Application Control) allows you to control which applications are allowed to run on your devices based on defined policies. By configuring Application Control policies in the device configuration profile, you can restrict write access to the D:\Folder1 directory to only trusted applications, thereby ensuring the security of the folder's contents.

upvoted 1 times

🗉 **mail2bala3011** 9 months, 1 week ago

**Selected Answer: A**

Tested. option A

upvoted 2 times

🗉 **OyYaGotta** 9 months, 2 weeks ago

Devil is in the detail. "Managed using Intune". Microsoft Defender Application Control is set up through The defender Portal, therefore answer is A because it need sto be set up "managing" via Intune.

upvoted 1 times

🗉 **MR\_Eliot** 10 months ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/create-deploy-exploit-guard-policy>

upvoted 2 times

🗉 **Pasado** 11 months ago

ChatGPT: To ensure that only a trusted list of applications is granted write access to the folder D:\Folder1 on Windows 10 computers managed by Microsoft Intune, you should configure **Microsoft Defender Application Control** (option D) in the device configuration profile. Microsoft Defender Application Control allows you to control which applications are allowed to run on the device, thereby ensuring that only trusted applications have access to the specified folder.

upvoted 2 times

🗉 **Merrybob** 11 months ago

**Selected Answer: A**

A. Microsoft Defender Exploit Guard

This is an ASR rule which is part of Exploit Guard

Ref: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-controlled-folders?view=o365-worldwide#microsoft-intune>

Ref: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-deployment-implementation?view=o365-worldwide>

upvoted 3 times

🗉 **NoursBear** 11 months, 1 week ago

Some of you are mixing up what WDAC is all about:

<https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/deployment/deploy-wdac-policies-using-intune>

Given answer A is correct

upvoted 2 times

🗉 **yosry** 1 year ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/create-deploy-exploit-guard-policy#create-an-exploit-guard-policy?~:text=Controlled%20folder%20access%3A%20Configure%20blocking%20or%20auditing%2C%20and%20then%20add%20Apps%20that%20can%20by>

upvoted 2 times

🗉 **7ab89e0** 1 year ago

**Selected Answer: A**

Answer is A.

upvoted 2 times

🗉 **7ab89e0** 1 year ago

**Selected Answer: A**

Answer is A.

upvoted 2 times

🗉 **kay000001** 1 year, 1 month ago

**Selected Answer: A**

Answer is A:

<https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/create-deploy-exploit-guard-policy>

You can configure and deploy Configuration Manager policies that manage all four components of Windows Defender Exploit Guard. These components include:

Attack Surface Reduction

Controlled folder access

Exploit protection

Network protection

upvoted 3 times

🗨️ 👤 **St\_Ives** 11 months ago

Microsoft Configuration Manager ??? The question states that the devices are Intune managed...

upvoted 1 times

🗨️ 👤 **Tigasmigas** 1 year, 1 month ago

**Selected Answer: A**

Windows Defender Exploit Guard is designed to lock down the device against a wide variety of attack vectors and block behaviors commonly used in malware attacks. The components are:

\* Attack Surface Reduction (ASR)

\* Network protection

\* Controlled folder access -> protects sensitive data from ransomware by blocking untrusted processes from accessing your protected folders.

(...)

<https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2019>

upvoted 3 times

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune.

You need to create Endpoint security policies to meet the following requirements:









- Hide the Firewall & network protection area in the Windows Security app.
- Disable the provisioning of Windows Hello for Business on the devices.

Which two policy types should you use? To answer, select the policies in the answer area.

NOTE: Each correct selection is worth one point.









### Answer Area

#### Manage

-  Antivirus
-  Disk encryption
-  Firewall
-  Endpoint detection and response
-  Attack surface reduction
-  Account protection
-  Device compliance
-  Conditional access

### Answer Area

#### Manage

-  Antivirus
-  Disk encryption
-  Firewall
-  Endpoint detection and response
-  Attack surface reduction
-  Account protection
-  Device compliance
-  Conditional access

Suggested Answer:

🗨️ 👤 **CeZt** 5 months, 1 week ago

this question

apply only to the device configuration profile template for Identity protection, which was deprecated in July 2024.

upvoted 2 times

🗨️ 👤 **Darkfire** 9 months, 3 weeks ago

Answer is correct

<https://learn.microsoft.com/en-us/mem/intune/protect/antivirus-security-experience-windows-settings>

<https://learn.microsoft.com/en-us/mem/intune/protect/identity-protection-windows-settings>

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 10 months ago

correct

upvoted 2 times

🗨️ 👤 **Merrybob** 11 months ago

Firewall and Network properties: Antivirus

Ref: [https://learn.microsoft.com/en-us/mem/intune/protect/antivirus-security-experience-windows-](https://learn.microsoft.com/en-us/mem/intune/protect/antivirus-security-experience-windows-settings#:~:text=to%20have%20effect.,Hide%20the%20Virus%20and%20threat%20protection%20area%20in%20the%20Windows%20Security%20app,-CSP%3A%20DisableVirusUI)

[settings#:~:text=to%20have%20effect.,Hide%20the%20Virus%20and%20threat%20protection%20area%20in%20the%20Windows%20Security%20app,-CSP%3A%20DisableVirusUI](https://learn.microsoft.com/en-us/mem/intune/protect/antivirus-security-experience-windows-settings#:~:text=to%20have%20effect.,Hide%20the%20Virus%20and%20threat%20protection%20area%20in%20the%20Windows%20Security%20app,-CSP%3A%20DisableVirusUI)

Windows Hello for Business: Account Protection (Identity Protection)

Ref: [https://msendpointmgr.com/2022/09/04/manage-windows-hello-for-business-whfb-with-](https://msendpointmgr.com/2022/09/04/manage-windows-hello-for-business-whfb-with-intune/#:~:text=Endpoint%20Security%20%3E%20Account%20protection%20(Preview))

[intune/#:~:text=Endpoint%20Security%20%3E%20Account%20protection%20\(Preview\)](https://msendpointmgr.com/2022/09/04/manage-windows-hello-for-business-whfb-with-intune/#:~:text=Endpoint%20Security%20%3E%20Account%20protection%20(Preview))

upvoted 2 times

🗨️ 👤 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **yosry** 1 year ago

CORRECT

upvoted 1 times

🗨️ 👤 **Casticod** 1 year, 3 months ago

Correct:

<https://www.examttopics.com/discussions/microsoft/view/74677-exam-md-101-topic-4-question-58-discussion/>

upvoted 3 times

🗨️ 👤 **LMaina** 1 year, 3 months ago

How can Antivirus be correct to "Hide the Firewall & network protection area in the Windows Security app".

upvoted 1 times

🗨️ 👤 **BJS78** 1 year, 3 months ago

As with Antivirus settings, you can control aspects of Windows Defender Security Center.

Here the relevant part is "Disable Network UI".

upvoted 1 times

🗨️ 👤 **picho707** 1 year, 3 months ago

Answer is correct based in the link below:

<https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-profile-settings>

upvoted 3 times

You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune.

You need to review the startup processes and how often each device restarts.

What should you use?

- A. Endpoint analytics
- B. Device Management
- C. Azure Monitor
- D. Intune Data Warehouse

**Suggested Answer:** D

Community vote distribution

A (100%)

🗳️ 👤 **Fortind1974** Highly Voted 10 months ago

Selected Answer: A

A. Endpoint analytics

<https://learn.microsoft.com/en-us/mem/analytics/restart-frequency>  
upvoted 11 times

🗳️ 👤 **CJL324** Most Recent 1 month, 2 weeks ago

A. Endpoint analytics.

Endpoint analytics provides insights into device performance, including startup processes and restart frequency. By analyzing the data collected by Endpoint analytics, you can gain visibility into the startup behavior of each device enrolled in Intune, helping you identify any issues and optimize device performance.

upvoted 1 times

🗳️ 👤 **OyYaGotta** 3 months, 2 weeks ago

Selected Answer: A

From Microsoft's own Copilot -

No, the Intune Data Warehouse does not directly provide the ability to monitor the startup processes of your fleet<sup>1</sup>. The Intune Data Warehouse is primarily used for generating reports and providing insights into your enterprise mobile environment, such as enrollment trends, app and OS versions breakdown, and device compliance trends<sup>1</sup>.

However, Microsoft provides a separate feature called Endpoint Analytics within Intune, which includes Startup Performance<sup>2</sup>. Startup Performance helps IT get users from power-on to productivity quickly, without lengthy boot and sign-in delays<sup>2</sup>. It provides a startup score based on boot time and sign-in time, and also provides insights into the processes that are causing delays during startup<sup>2</sup>. But this feature is not part of the Intune Data Warehouse<sup>2</sup>.

upvoted 1 times

🗳️ 👤 **sergioandreslq** 3 months, 4 weeks ago

Same question 16., the answer is endpoint analytics.

Endpoint analytics is a feature within Microsoft Endpoint Manager that provides insights into device performance and user experience. It can help you analyze startup times, shutdown times, and restart frequencies of devices. This tool allows you to identify issues affecting device performance and take actions to improve the user experience.

upvoted 1 times

🗳️ 👤 **MR\_Eliot** 4 months ago

Selected Answer: A

A is correct.

upvoted 1 times



🗨️ 👤 **Krayzr** 4 months, 3 weeks ago

Selected Answer: A

A. Endpoint analytics

Endpoint analytics within Microsoft Intune specifically provides insights into device performance and health, including information about startup processes and restart frequency. It offers features like:

Startup performance: Analyzes boot and sign-in times, identifying slow devices and their specific bottlenecks.

Restart frequency: Tracks how often devices restart overall and per model, helping identify unusual occurrences.

Model performance: Compares boot and sign-in performance across different device models.

upvoted 1 times

🗨️ 👤 **Pasado** 4 months, 4 weeks ago

ChatGPT: To review the startup processes and how often each device restarts in Microsoft Intune, you should use **Endpoint analytics** (option A). Endpoint analytics provides insights into device performance, startup processes, and restart frequency, allowing you to monitor and optimize device performance effectively.

upvoted 1 times

🗨️ 👤 **yosry** 6 months ago

Selected Answer: A

A IS CORRECT

upvoted 1 times

🗨️ 👤 **belyo** 6 months, 3 weeks ago

Selected Answer: A

A. Endpoint analytics

warehouse cannot provide this type of info

upvoted 1 times

🗨️ 👤 **chandravamsi** 7 months, 3 weeks ago

Selected Answer: A

Option : A

upvoted 1 times

🗨️ 👤 **fco168** 8 months ago

Selected Answer: A

Endpoint Analytics collects and analyzes data related to device boot time, application reliability, and system responsiveness.

upvoted 2 times

🗨️ 👤 **h38jhd38k** 8 months, 2 weeks ago

<https://learn.microsoft.com/en-us/mem/analytics/startup-performance>

Endpoint analytics

upvoted 1 times

🗨️ 👤 **Sprocket10** 9 months ago

Answer should be A. Tested and confirmed

upvoted 1 times

🗨️ 👤 **BJS78** 9 months, 1 week ago

<https://learn.microsoft.com/en-us/mem/analytics/restart-frequency>

<https://learn.microsoft.com/en-us/mem/analytics/startup-performance>

upvoted 1 times

🗨️ 👤 **Grg433** 9 months, 2 weeks ago

Selected Answer: A

To review the startup processes and how often each device restarts in Microsoft Intune, we should use Endpoint analytics. Endpoint analytics provides insights into the performance and health of your devices, including startup and restart data.

So, the correct option is:

A. Endpoint analytics

we can use this feature to gain valuable insights into device performance, user experience, and more, helping we make informed decisions about device management and optimization.

upvoted 3 times

DRAG DROP

You have a Microsoft 365 subscription that contains devices enrolled in Microsoft Intune.

You need to create Endpoint security policies to enforce the following requirements:

- Computers that run macOS must have FileVault enabled.
- Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled.
- Computers that run Windows 10 must have Microsoft Defender Application Control enabled.

Which Endpoint security feature should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

**Features**

**Answer Area**

- Account protection
- Attack surface reduction (ASR)
- Disk encryption
- Endpoint detection and response (EDR)

- Computers that run macOS must have FileVault enabled:
- Computers that run Windows 10 must have Microsoft Defender Application Control enabled:
- Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled:

**Suggested Answer:**

Computers that run macOS must have FileVault enabled:

Computers that run Windows 10 must have Microsoft Defender Application Control enabled:

Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled:

**oopspruu** Highly Voted 5 months, 2 weeks ago  
 Provided answers are correct as of 2024/07.  
 upvoted 5 times

**Merrybob** Most Recent 11 months ago  
 Disk Encryption

ASR - Ref <https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy#:~:text=Application%20control%2D%20Application,Constrained%20Language%20Mode>.

Account Protection - Ref <https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/configure?tabs=intune#:~:text=You%20can%20also%20configure%20Credential%20Guard%20by%20using%20an%20account%20protection%20profile%20in%20endpc>  
 upvoted 4 times

**yosry** 1 year ago  
<https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/configure?tabs=intune#:~:text=You%20can%20also%20configure%20Credential%20Guard%20by%20using%20an%20account%20protection%20profile%20in%20endpc>  
 upvoted 1 times

**Contactfornitish** 1 year, 2 months ago  
 ASR is correct  
<https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>  
 upvoted 1 times

**[Removed]** 1 year, 2 months ago  
 ASR??  
 Anyone also Unsure about the second Point???  
 upvoted 2 times

🗨️ 👤 **NoursBear** 11 months, 3 weeks ago

Yes I have a doubt, from my research WDAC is configured through OMA-URI, I see no policy under Endpoint Security blade and under ASR Policy I don't see anything for WDAC

upvoted 1 times

🗨️ 👤 **NoursBear** 11 months, 3 weeks ago

OK so when creating a new ASR profile, you can chose an Application Control template. This is new since 2022. So all good

upvoted 1 times

🗨️ 👤 **VirtualJP** 1 year, 2 months ago

Agree answer is correct

upvoted 2 times

Your company has 200 computers that run Windows 10. The computers are managed by using Microsoft Intune.

Currently, Windows updates are downloaded without using Delivery Optimization.

You need to configure the computers to use Delivery Optimization.

What should you create in Intune?

- A. a device compliance policy
- B. a Windows 10 update ring
- C. a device configuration profile
- D. an app protection policy


**Suggested Answer: C**

Community vote distribution

C (100%)

 **BJS78** Highly Voted 1 year, 3 months ago

<https://learn.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-windows>  
upvoted 6 times

 **CJL324** Most Recent 7 months, 2 weeks ago


C. a device configuration profile  
upvoted 1 times

 **TC1Labs** 10 months, 3 weeks ago

Correct, lab tested  
upvoted 2 times

 **Amir1909** 11 months, 4 weeks ago

- A device configuration policy  
upvoted 2 times

 **RomanV** 3 months, 1 week ago

It's really C :)

With Intune, you can use Delivery Optimization settings for your Windows devices to reduce bandwidth consumption when those devices download applications and updates. This article describes how to configure Delivery Optimization settings as part of an Intune device configuration profile. After you create a profile, you then assign or deploy that profile to your Windows devices.

<https://learn.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-windows>


upvoted 1 times

 **yosry** 1 year ago

Selected Answer: C

CORRECT


upvoted 2 times

 **fco168** 1 year, 1 month ago

Selected Answer: C

C is correct.

upvoted 2 times

 **LiamAzure** 1 year, 2 months ago

Selected Answer: C

BJS78 is correct, configuration profile

upvoted 2 times

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

Auto-enrollment in Intune is configured.

You have 100 Windows 11 devices in a workgroup.

You need to connect the devices to the corporate wireless network and enroll 100 new Windows 11 devices in Intune.

What should you use?

- A. a provisioning package
- B. a Group Policy Object (GPO)
- C. mobile device management (MDM) automatic enrollment
- D. a device configuration policy

**Suggested Answer:** C

Community vote distribution

A (100%)

🗨️ 👤 **93831b0** 4 months, 2 weeks ago

Selected Answer: A

As MDM Automatic Enrollment is already configured the Provisioning Package can be used to configure the Wi-Fi connection on workgroup devices before the enrollment.

upvoted 2 times

🗨️ 👤 **oopspruu** 5 months, 2 weeks ago

Selected Answer: A

Provisioning Package fulfils both requirements. You can automatically connect devices to corp WIFI and join to Entra which will enroll devices into Intune.

upvoted 1 times

🗨️ 👤 **CJL324** 7 months, 3 weeks ago

A. a provisioning package.

Provisioning packages allow you to apply settings and configurations to Windows devices, including connecting to wireless networks and enrolling in Intune, without the need for Active Directory or Azure AD. This is particularly useful for devices in a workgroup environment.

upvoted 1 times

🗨️ 👤 **56c78aa** 9 months, 1 week ago

question, you have 100 existing devices enrolled that need to a connection to wifi, AND enroll 100 new devices.

Why would you not use the configured auto enrollment with a device configuration profile?

i dont know if the provisioning package can be used on existing devices.

And it would mean if i understand it correctly that you need to manuel click the provisioning package either on online folder or usb to install for 200 devices.

While the device configuration policy is applied automatically after assigned?

upvoted 1 times

🗨️ 👤 **Darkfire** 9 months, 3 weeks ago

Selected Answer: A

A is correct

<https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-bulk-enroll>

C is already active

upvoted 1 times

  **MR\_Eliot** 10 months ago

**Selected Answer: A**

A is correct.

upvoted 1 times

  **Krayzr** 10 months, 3 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-bulk-enroll>

"" Join new Windows devices to Microsoft Entra ID and Intune. To bulk enroll devices for your Microsoft Entra tenant, you create a provisioning package with the Windows Configuration Designer (WCD) app. Applying the provisioning package to corporate-owned devices joins the devices to your Microsoft Entra tenant and enrolls them for Intune management. Once the package is applied, it's ready for your Microsoft Entra users to sign in. ""


upvoted 3 times

  **IcE** 11 months, 2 weeks ago

**Selected Answer: A**

A the way

upvoted 2 times

  **IcE** 12 months ago

**Selected Answer: A**

Should be A

upvoted 1 times

  **Amir1909** 1 year ago

A is correct

upvoted 1 times

  **belyo** 1 year ago

**Selected Answer: A**



voting for A - provisioning package, as this will deliver VPN or whatever configuration is needed

no GPO here as devices are in workplace

auto enrollment is said its already enabled



device config profile is after enrollment

upvoted 3 times

  **madsa** 1 year, 1 month ago

A agreed.

upvoted 1 times

  **Rocky83** 1 year, 2 months ago

**Selected Answer: A**



Should be A

upvoted 1 times

  **picho707** 1 year, 3 months ago

The answer appears to be A due to the fact that the MDM autoenrollment is already configured.

upvoted 4 times

  **Crismo** 1 year, 3 months ago


Agree on A: <https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-bulk-enroll>

B: Not an option since the machines are not domain joined

C: Already configured but won't have an impact without manual steps

D: Can only be applied after the Intune enrollment



upvoted 2 times

  **Krayzr** 10 months, 3 weeks ago

thanks for this link

<https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-bulk-enroll>

upvoted 1 times

  **BJ578** 1 year, 3 months ago

Agree. To start the enrollment you have to connect automatically to WiFi which can be provided by the package (and by USB)

upvoted 1 times



## HOTSPOT

You have a Microsoft 365 tenant that uses Microsoft Intune to manage personal and corporate devices. The tenant contains Windows 10 devices as shown in the following exhibit.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
LON-CL2	✔ Yes	Windows	10.0.17763.615	Azure AD registered	User2	Microsoft Intune	✔ Yes
LON-CL4	✔ Yes	Windows	10.0.17763.107	Azure AD joined	User1	Microsoft Intune	✔ Yes

How will Intune classify each device after the devices are enrolled in Intune automatically? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Identified by Intune as a personal device:

▼

LON-CL2 only

LON-CL4 only

Both LON-CL2 and LON-CL4

Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

▼

LON-CL2 only

LON-CL4 only

Both LON-CL2 and LON-CL4

Neither LON-CL2 or LON-CL4

### Answer Area

Suggested Answer:

Identified by Intune as a personal device:

▼

LON-CL2 only

LON-CL4 only

Both LON-CL2 and LON-CL4

Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

▼

LON-CL2 only

LON-CL4 only

Both LON-CL2 and LON-CL4

Neither LON-CL2 or LON-CL4

**BJS78** Highly Voted 1 year, 3 months ago

In general --> Joined: Corporate, Registered: Private  
upvoted 20 times

**oopspuu** Most Recent 5 months, 2 weeks ago

IF a device is not Entra Joined or uploaded its hash to Autopilot, the ownership always stays Personal. Registered devices are considered as Personal ownership.  
upvoted 1 times

**rcristiano** 7 months, 4 weeks ago



Dispositivo de uso pessoal => Registered (privado) e Dispositivo de uso corporativo => Joined (empresa)  
upvoted 2 times

**Darkfire** 9 months, 3 weeks ago

Answer is correct

See comment of BJS78

upvoted 3 times

  **yosry** 1 year, 1 month ago

Seems correct

upvoted 2 times

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices. All devices are in the same time zone.

You create an update rings policy and assign the policy to all Windows devices.

On the November 1, you pause the update rings policy.

All devices remain online.

Without further modification to the policy, on which date will the devices next attempt to update?

- A. December 1
- B. December 6
- C. November 15
- D. November 22

**Suggested Answer: B**

Community vote distribution

B (100%)

 **LiamAzure** Highly Voted 1 year, 2 months ago

**Selected Answer: B**

Pause

Select Pause to prevent assigned devices from receiving feature or quality updates for up to 35 days from the time you pause the ring. After the maximum days have passed, pause functionality automatically expires and the device scans Windows Updates for applicable updates. Following this scan, you can pause the updates again. If you resume a paused update ring, and then pause that ring again, the pause period resets to 35 days.

upvoted 7 times

 **oopspruu** Highly Voted 5 months, 2 weeks ago

**Selected Answer: B**

Correct.

Pause feature pauses the updates for 35 days. The question itself seems ridiculous. Why would an admin need to remember exactly how many days it applies to? Thank God for MS learn during exams.

upvoted 5 times

 **Daniel\_G** 3 months, 4 weeks ago

Certification exams seem to be about memorizing content and questions versus the material itself. Need to work in the field and gain experience...that is where the skill comes from in my opinion.

upvoted 2 times

 **Darkfire** Most Recent 9 months, 3 weeks ago

**Selected Answer: B**

B is correct

<https://learn.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings#pause:~:text=Select%20Pause%20to,to%2035%20days>.

upvoted 3 times

 **MR\_Eliot** 10 months ago

**Selected Answer: B**

Ref: <https://learn.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings#pause>

upvoted 1 times

 **Amir1909** 1 year ago

B is correct

upvoted 1 times

🗨️ 👤 **benpatto** 1 year, 2 months ago

What a crazy world we'd live in if Microsoft just standardised things!! Why is this 35 days yet another policy will have a default of 30. There's no need!!!!

upvoted 2 times

🗨️ 👤 **picho707** 1 year, 2 months ago

**Selected Answer: B**

Answer is B

November 1st + 35 days = December 6.

upvoted 3 times

🗨️ 👤 **ExamKiller020** 1 year, 3 months ago

Select Pause to prevent assigned devices from receiving feature or quality updates for up to 35 days from the time you pause the ring. After the maximum days have passed, pause functionality automatically expires and the device scans Windows Updates for applicable updates. Following this scan, you can pause the updates again. If you resume a paused update ring, and then pause that ring again, the pause period resets to 35 days.

Ref: <https://learn.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings#pause>

upvoted 3 times

🗨️ 👤 **Kiookr** 1 year, 3 months ago

Sorry !! are you telling the correct answer or what ?? what is the explanation has to do with the answer .. SO is the answer is B as show or you have deferent opinion ?

upvoted 1 times

🗨️ 👤 **Fortind1974** 1 year, 3 months ago

**Selected Answer: B**

B. December 6

<https://learn.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings#pause>

upvoted 4 times

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

Name	Operating system	Enrolled in Microsoft Intune
Device1	Windows 11	Yes
Device2	Windows 10	Yes
Device3	Android	Yes
Device4	iOS	Yes

All devices have Microsoft Edge installed.

From the Microsoft Intune admin center, you create a Microsoft Edge Baseline profile named Edge1.

You need to apply Edge1 to all the supported devices.

To which devices should you apply Edge1?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1, Device2, and Device3 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

**Suggested Answer: B**

Community vote distribution

B (100%)

 **oopspruu** Highly Voted 5 months, 2 weeks ago

**Selected Answer: B**

Security Baselines:

Edge = Windows Only

Endpoint Security = Windows Only

M365 Apps For Enterprise = Windows Only

upvoted 7 times

 **CJL324** Most Recent 7 months, 2 weeks ago

B. Device1 and Device2 only

Microsoft Edge Baseline profiles are typically designed to enforce security and compliance settings for Microsoft Edge on Windows devices.

Since Device3 is an Android device and Device4 is an iOS device, they wouldn't typically be managed using Microsoft Edge Baseline profiles from the Microsoft Intune admin center.

upvoted 3 times

 **Darkfire** 9 months, 3 weeks ago

**Selected Answer: B**

B is correct

<https://learn.microsoft.com/en-us/mem/intune/protect/security-baselines-configure>

upvoted 1 times

 **MR\_Eliot** 10 months ago

**Selected Answer: B**

Correct. Baseline policies are for Windows devices.

upvoted 2 times

 **Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **yosry** 1 year ago

**Selected Answer: B**

CORRECT

upvoted 1 times

🗨️ 👤 **Tigasmigas** 1 year, 1 month ago

**Selected Answer: B**

This feature applies to:

\* Windows 10 version 1809 and later

\* Windows 11

<https://learn.microsoft.com/en-us/mem/intune/protect/security-baselines-configure>

upvoted 3 times

🗨️ 👤 **fco168** 1 year, 1 month ago

**Selected Answer: B**

Windows 10 and later.

upvoted 1 times

🗨️ 👤 **h38jhd38k** 1 year, 2 months ago

<https://learn.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-edge?pivots=edge-sept-2020#microsoft-edge>

Answer is correct

upvoted 2 times

🗨️ 👤 **BJ578** 1 year, 3 months ago

Edge baseline is for W10+ only

upvoted 3 times

## HOTSPOT

-

You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to manage Windows updates by using Intune.

You create an update ring for Windows 10 and later and configure the User experience settings for the ring as shown in the following exhibit.

**User experience settings**

Automatic update behavior ⓘ	<input type="text" value="Auto install at maintenance time"/>
Active hours start * ⓘ	<input type="text" value="8 AM"/>
Active hours end * ⓘ	<input type="text" value="5 PM"/>
Restart checks ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Skip
Option to pause Windows updates ⓘ	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Option to check for Windows updates ⓘ	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Change notification update level ⓘ	<input type="text" value="Use the default Windows Update notifications"/>
Use deadline settings ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Not configured
Deadline for feature updates ⓘ	<input type="text" value="5"/> ✓
Deadline for quality updates ⓘ	<input type="text" value="2"/> ✓
Grace period ⓘ	<input type="text" value="1"/> ✓
Auto reboot before deadline ⓘ	<input type="radio"/> Yes <input checked="" type="radio"/> No

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.

**Answer Area**

Automatic restarts are blocked  
[answer choice].

- before 8 AM
- between 8 AM and 5 PM
- after 5 PM

A restart will be forced on a device  
[answer choice] after the deadline.

- 1 day
- 2 days
- 5 days

## Answer Area

Suggested Answer:

Automatic restarts are blocked  
[answer choice].

before 8 AM  
between 8 AM and 5 PM  
after 5 PM

A restart will be forced on a device  
[answer choice] after the deadline.

1 day  
2 days  
5 days


 **Fortind1974** Highly Voted 1 year, 3 months ago

Automatic restarts are blocked between 8 AM - 5 PM.  
A restart will be forced on a device 1 day after the deadline.

<https://learn.microsoft.com/en-us/mem/intune/protect/windows-update-settings>  
upvoted 31 times

 **LiamAzure** 1 year, 2 months ago


So a restart will be forced on, when? None of the available answers seem right by that  
upvoted 1 times

 **BJS78** 1 year, 3 months ago


Correct  
upvoted 3 times

 **Moot2** Most Recent 1 month, 2 weeks ago

Grace period should be 1 day  
upvoted 1 times

 **yhano** 1 month, 2 weeks ago

Automatic restarts are blocked between 8 AM - 5 PM.  
A restart will be forced on a device 1 day after the deadline.  
upvoted 3 times

 **TMpics** 9 months, 2 weeks ago

Correct  
upvoted 1 times

 **yosry** 1 year ago

- between 8 AM - 5 PM.  
-1 day after the deadline.  
upvoted 1 times

 **yosry** 1 year ago

Box1: Between 8AM and 5PM  
Box2: 1 Day  
upvoted 1 times

 **b0gdan433** 1 year, 1 month ago

Deadline - Is how long patch will stay available in Windows Update section until force installed  
Grace period - Is how long until a reboot is forced.  
So the correct response is 1 day until will force a reboot  
upvoted 3 times

 **benpatto** 1 year, 2 months ago

The answer is wrong for no.2 - It needs to be 1 day.  
The deadline is 5 days HOWEVER, there is a grace period of 1 day so 1 day is the right answer. The grace period only takes place after the deadline has ended, and as there's a grace period of 1 day, it allows for 1 day before a device is forced into shutdown.  
upvoted 3 times



You have a Microsoft 365 tenant.

You have devices enrolled in Microsoft Intune.

You assign a conditional access policy named Policy1 to a group named Group1. Policy1 restricts devices marked as noncompliant from accessing Microsoft OneDrive for Business.

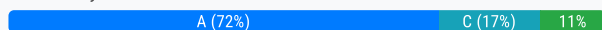
You need to identify which noncompliant devices attempt to access OneDrive for Business.

What should you do?

- A. From the Microsoft Entra admin center, review the Conditional Access Insights and Reporting workbook.
- B. From the Microsoft Intune admin center, review Device compliance report.
- C. From the Microsoft Intune admin center, review the Noncompliant devices report.
- D. From the Microsoft Intune admin center, review the Setting compliance report.

**Suggested Answer:** C

Community vote distribution



🗨️ **Fortind1974** Highly Voted 1 year, 3 months ago

**Selected Answer: A**

A. From the Microsoft Entra admin center, review the Conditional Access Insights and Reporting workbook.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting>  
upvoted 9 times

🗨️ **SilverFox22** 1 year, 1 month ago

I don't understand why this is the answer. That report does not even mention device compliance, it provides information on user sign-ins. The question asks to review device compliance, not Conditional Access. The device compliance report would show you that information, answer B.

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/reports>

upvoted 1 times

🗨️ **SilverFox22** 1 year, 1 month ago

I stand corrected, I misunderstood the question.

upvoted 2 times

🗨️ **Tr619899** Most Recent 1 month ago

**Selected Answer: A**

This workbook provides detailed reporting on Conditional Access policy results, including which devices are blocked and the reasons for those blocks, such as noncompliance.

upvoted 1 times

🗨️ **665d390** 2 months, 1 week ago

Correct Answer is: C I've already done the exam and the correct is C.

upvoted 1 times

🗨️ **RomanV** 3 months, 1 week ago

**Selected Answer: A**

"The summary shows how many users or sign-ins during the time range resulted in Success, Failure, User action required or Not applied when the selected policies were evaluated."

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-insights-reporting>

I'm really sorry for the people who pay for this and are getting GPT answers from noobs who do not study at all, misleading the people with incorrect GPT answers.....

upvoted 1 times

🗨️ 👤 **METAM** 3 months, 3 weeks ago

Selected Answer: B

B

logical

upvoted 1 times

🗨️ 👤 **oopsruu** 5 months, 2 weeks ago

Selected Answer: A

If the question have ended at "You need to identify noncompliant devices", then B would have been correct. But you need to know which non-compliant device "Accessed OneDrive for Business". That can only be done by A.

Also there is no such thing as "noncompliant device report" in MS Intune > Reports. Stop copying answers from ChatGPT and use your research and test tenants.

upvoted 2 times

🗨️ 👤 **Frank9020** 7 months, 2 weeks ago

Selected Answer: C

C. From the Microsoft Intune admin center, review the Noncompliant devices report.

By reviewing the Noncompliant devices report in the Intune admin center, you can identify devices that are marked as noncompliant and attempting to access Microsoft OneDrive for Business. This report provides details about device names, users, and specific compliance issues.

upvoted 3 times

🗨️ 👤 **CJL324** 7 months, 3 weeks ago

A. From the Microsoft Endpoint Manager admin center, review the Conditional Access Insights and Reporting workbook.

The Conditional Access Insights and Reporting workbook provides comprehensive insights into the usage and effectiveness of conditional access policies. You can use it to review detailed information about device compliance status and access attempts, including any instances where noncompliant devices attempted to access OneDrive for Business. This will help you identify which devices are noncompliant and attempted access to OneDrive for Business, allowing you to take appropriate actions to remediate the compliance issues.

upvoted 1 times

🗨️ 👤 **TMpics** 9 months, 2 weeks ago

A totally agree

upvoted 2 times

🗨️ 👤 **MR\_Eliot** 10 months ago

Selected Answer: A

A is correct.

upvoted 1 times

🗨️ 👤 **Pasado** 11 months ago

ChatGPT: To identify which noncompliant devices attempt to access OneDrive for Business after assigning a conditional access policy, you should **\*\*review the Noncompliant devices report\*\*** (option C) in the Microsoft Intune admin center. This report will provide you with details on devices that are marked as noncompliant, allowing you to see which devices are attempting to access OneDrive for Business and are being restricted by Policy1.

upvoted 1 times

🗨️ 👤 **NoursBear** 11 months, 3 weeks ago

Under Intune Admin, under Devices\Reports there are many reports available, e.g.:

Noncompliant devices and settings

See each device that is not compliant with policy alongside the compliance policy settings these devices are not compliant with.

upvoted 1 times

🗨️ 👤 **yosry** 1 year ago

Selected Answer: A

A IS CORRECT

upvoted 1 times

🗨️ 👤 **Tigasmigas** 1 year, 1 month ago

Selected Answer: A

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-insights-reporting>

upvoted 1 times

🗨️ 👤 **BJS78** 1 year, 3 months ago

I think the question is very badly formed. (on purpose, of course)

If you have OD enabled and configured, than yes, any device (including the non-compliant) will try to access it.

If it is not, the non-compliant report will give you only info about which device cannot access, not about did that device try it at all...so no audit info available. So I would vote on "A".

upvoted 3 times

🗨️ 👤 **Grg433** 1 year, 3 months ago

**Selected Answer: B**

To identify noncompliant devices that attempt to access OneDrive for Business, you should review the Device compliance report in the Microsoft Intune admin center.

Option B is the correct choice. This report will provide information about the compliance status of devices and can help you identify which devices are noncompliant and attempting to access OneDrive for Business.

and I think 'Conditional access insights and reporting workbook' is only possible in 'Azure' not in Microsoft Entra admin center'

upvoted 1 times

🗨️ 👤 **BJS78** 1 year, 3 months ago

<https://entra.microsoft.com/> from here you can go to Conditional Access via the "Protection" menu element.

upvoted 1 times

HOTSPOT

-

You use Microsoft Intune 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 enrollment
- 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.

### Answer Area

Data source:  ▼

- Audit logs in Azure AD
- Audit logs in Microsoft Intune
- Azure Synapse Analytics
- The Microsoft Intune Data Warehouse

Data visualization tool:  ▼

- Azure Data Studio
- Microsoft Power BI
- Microsoft Intune admin center

### Answer Area


Suggested Answer:

Data source:  ▼

- Audit logs in Azure AD
- Audit logs in Microsoft Intune
- Azure Synapse Analytics
- The Microsoft Intune Data Warehouse**

Data visualization tool:  ▼


- Azure Data Studio
- Microsoft Power BI**
- Microsoft Intune admin center

 **TMpics** 3 months, 1 week ago

Correct answers  
upvoted 1 times

 **MR\_Eliot** 4 months ago



Correct answers.  
upvoted 1 times

 **Amir1909** 5 months, 3 weeks ago

Correct  
upvoted 1 times

 **yosry** 6 months ago



CORRECT  
upvoted 1 times

  **h38jhd38k** 8 months, 2 weeks ago

<https://learn.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports>

<https://learn.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi>

upvoted 4 times

  **VirtualJP** 8 months, 3 weeks ago

Answer appears to be correct

upvoted 3 times