EXAMTOPICS

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



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

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.

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.

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.

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.

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.

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.

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.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

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

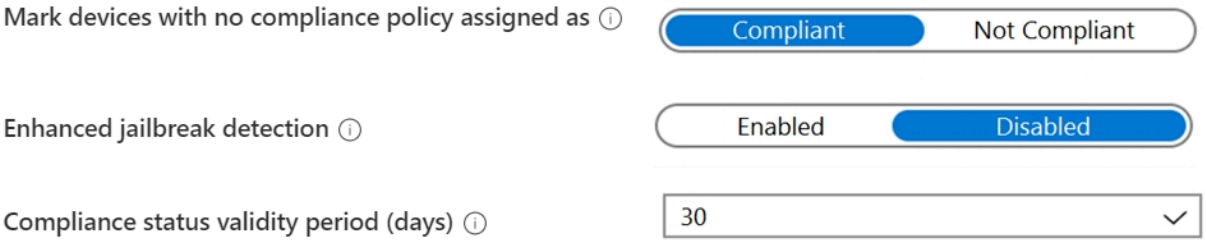
Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

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*

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.



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

Answer Area

Statements	Yes	No
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	○	○
User2 can remove D:\Folder1 from the list of protected folders on Device2.	○	○
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	○	◉
User2 can remove D:\Folder1 from the list of protected folders on Device2.	◉	○
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	○	◉

volto Highly Voted 3 years, 3 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.Why does the MAM policy apply here?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.No, user 3 cannot create a file on the destop. 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 32 times

volto Highly Voted 3 years, 3 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 31 times

Arahnofob Most Recent 3 months, 1 week ago

NNN

1 User1 creates file via Notepad on Device4 Notepad isn't in the CFA allow-list

2 User2 removes D:\Folder1 from protected list on Device2 MDM-enforced policy overrides local admin changes

3 User3 creates file via PowerShell on Device2 Desktop is a default (unremovable) protected folder; PowerShell isn't allow-listed

upvoted 2 times

Ginessp 1 year, 1 month ago

1 NO. Protected folder, only App1.exe allowed.

2 NO. Intune policy blocks local changes.

3 NO. Protected desktop, PowerShell not allowed.

upvoted 3 times

Futfuyfyjfj 3 years, 2 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.No, user 3 cannot create a file on the destop. 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 8 times

Futfuyfyjfj 3 years, 2 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

HvD 2 years, 1 month ago

Question 2: User2 can remove D:\Folder1 from the list of protected folders on Device2. The qeustion 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 3 times

deit 3 years, 3 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.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.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..Default Execution Policy is remote signed, which allows the script to be executed if the script is signed, or created locally, or scripts that are downloaded from the internet and not signed, if the scripts are unblocked, such as by using the Unblock-File cmdlet. Ref: cripts that are downloaded from the internet and not signed, if the scripts are unblocked, such as by using the Unblock-File cmdlet.

upvoted 17 times

deit 3 years, 3 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 17 times

Tonsku 2 years, 11 months ago

MAM user scope: GroupB

upvoted 2 times

NoursBear 2 years, 9 months 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..Default Execution Policy is remote signed, which allows the script to be executed if the script is signed, or created locally, or scripts that are downloaded from the internet and not signed, if the scripts are unblocked, such as by using the Unblock-File cmdlet. Ref: cripts that are downloaded from the internet and not signed, if the scripts are unblocked, such as by using the Unblock-File cmdlet.

upvoted 3 times

NoursBear 2 years, 9 months 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 3 times

OyYaGotta 2 years, 5 months 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 2 times

OyYaGotta 2 years, 5 months 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 2 years, 8 months ago

Second one should be NO.

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

upvoted 1 times

Tonsku 2 years, 1 month 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 2 times

LionelDerBoven 2 years, 2 months 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 2 times

Tonsku 2 years, 1 month 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, GroupBMAM user scope: GroupB

upvoted 2 times

spillb 2 years, 2 months ago

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

upvoted 1 times

Merrybob 2 years, 1 month 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 7 times

LionelDerBoven 2 years, 2 months 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 2 times

Merrybob 2 years, 1 month 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.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 7 times

MR_Eliot 2 years, 1 month 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 3 times

Blessing_ 2 years, 3 months ago

1. Device 4 is for personally owned

upvoted 3 times

MR_Eliot 2 years, 1 month 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.)Second one should be NO. Third one should be NO as well. Because exection policy is enabled by default.- 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 3 times

kiik32 2 years, 4 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

cruzi 2 years, 1 month 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 4 times

AlSuds 2 years, 11 months 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 6 times

cruzi 2 years, 1 month 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. YesAlmost. 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 4 times

NoursBear 1 year, 10 months ago

User 2 is local admin due to his Azure role

upvoted 1 times

majerzg 3 years, 1 month 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

kiik32 2 years, 4 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

kiik32 2 years, 4 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 well1. Device 4 is for personally owned

upvoted 2 times

lucianosesantos 2 years, 12 months 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 4 times

Dinkan 1 year, 3 months ago

Default Execution Policy is remote signed, which allows the script to be executed if the script is signed, or created locally, or scripts that are downloaded from the internet and not signed, if the scripts are unblocked, such as by using the Unblock-File cmdlet.

Ref: cripts that are downloaded from the internet and not signed, if the scripts are unblocked, such as by using the Unblock-File cmdlet.

upvoted 1 times

Futfuyfyjfj 3 years, 2 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

lucianosesantos 2 years, 12 months 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.User 2 is local admin due to his Azure role

upvoted 4 times

prBo 3 years, 1 month ago

Why does the MAM policy apply here?

upvoted 2 times

FAlien 2 years, 12 months ago

No, user 3 cannot create a file on the destop. 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 6 times

Question #2 *Topic 1*

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.

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.

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.

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.

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.

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.

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?

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

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

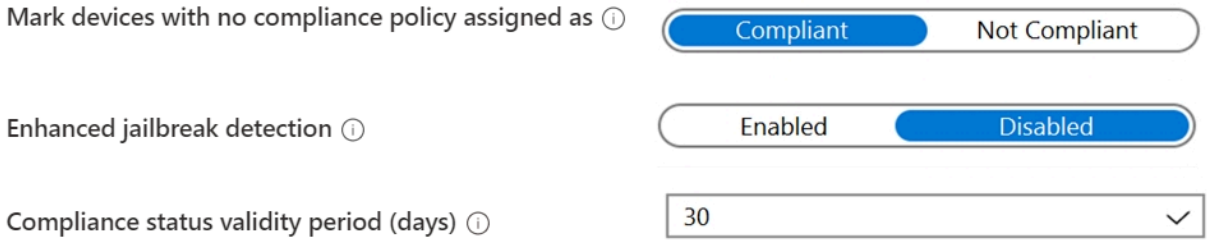
Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

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*

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.



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

A. Device1 only

B. Device3 only

C. Device1 and Device3 only

D. Device1, Device2, and Device3

Suggested Answer: *A*

Community vote distribution

A (80%) C (19%) 1

volto Highly Voted 2 years, 2 months 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 26 times

volto Highly Voted 2 years, 2 months ago

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 AEsta correto, o Windows Autopilot é uma ferramenta projetada exclusivamente para cenários de propriedade corporativa (Corporate-owned devices), sendo assim apenas a letra A esta correta.Sorry If, but I could not found 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 then 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 OOBE).The setting will register the devices that are not, but will also apply the configuration to the once that are already.

upvoted 28 times

AloisioCarvalho 5 months, 3 weeks ago

Esta correto, o Windows Autopilot é uma ferramenta projetada exclusivamente para cenários de propriedade corporativa (Corporate-owned devices), sendo assim apenas a letra A esta correta.

upvoted 1 times

Tati_Oliveira 3 years ago

Sorry If, but I could not found 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 then 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 OOBE).

upvoted 2 times

fco168 3 years ago

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

upvoted 2 times

krzysztofbr 3 years, 2 months ago

its pretty simple. device 3 is personally owned, can't be IN autopilot. so is only one possible answer A

upvoted 7 times

martin451 Most Recent 5 months, 2 weeks ago

The reasoning is: The Autopilot profile has Convert all targeted devices to Autopilot = Yes. The profile is targeted to Group 1 and excludes Group 2. Device1 is in Group1 and not excluded → gets registered with Autopilot. Device2 is in both Group1 and Group2 → excluded. Device3 is personally owned. The automatic conversion feature only registers corporate-owned Intune-managed devices, not personal/BYOD devices. Therefore, only Device1 is registered by using the Windows Autopilot deployment service. Answer: A. Device1 only This is one of those questions where the distinction between already registered in Autopilot and automatically registered through the "Convert all targeted devices to Autopilot" setting makes all the difference.

upvoted 1 times

martin451 5 months, 2 weeks ago

the answer is not A. The correct answer is: C. Device1 and Device3 only Reason: the question asks which devices are registered by using the Windows Autopilot deployment service, not which devices are currently deployed by Autopilot. In the Autopilot exhibit, Device1 and Device3 are registered Autopilot devices. Device2 is not. So: Device1: Yes Device2: No Device3: Yes Answer: C

upvoted 1 times

e70d081 5 months, 3 weeks ago

Because the question is so long, I was able to get it right, but it took me like 10 minutes smh. That is not ideal when taking the actual test.

upvoted 2 times

jazzmirza 6 months, 2 weeks ago

Convert to Autopilot = YES Include = Group1 Exclude = Group2 (exclude wins) Device1 → G1 → YES Device2 → G1 + G2 → EXCLUDED → NO Device3 → G1 → YES Answer: Device1 and Device3 only (C)

upvoted 1 times

Jhojan 1 year, 3 months ago

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

upvoted 1 times

Jacobddu 1 year, 5 months ago

Device2 is excluded as it's in Group2. Device3 is personal owned device. So only Device1.

upvoted 2 times

Moiseskoper 1 year, 6 months ago

Key fact: All the devices are enrolled in Intune, all of them can be Autopilot as long as you have the hardware hash. That said, Device 2 is part of group 1 and 2, however, group 2 is excluded from the profile and exclusion always takes precedence. So, we only have Device 1 and Device 3 left. Again, they both can be registered as Autopilot as long as you have the hardware hash.

upvoted 1 times

NoursBear 1 year, 10 months ago

Back here preparing for my certification update assessment ohhh boy

upvoted 1 times

subbuhotmail 2 years, 2 months 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 3 times

FemiA55 1 year, 11 months ago

Only Device 1 because it is corporate owned and member of Group 1 qualifies for OOBE 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 1 year, 11 months ago

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

upvoted 1 times

neothwin 2 years ago

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

upvoted 1 times

kiik32 2 years, 4 months 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

lucianosesantos 2 years, 1 month ago

In my opinion the correct answer is A beacuse in link bellow 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

SajjH 2 years, 4 months 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

Darkfire 2 years, 1 month ago

I think A. Based on Device2 which is excluded from the Deployment Profile because its in Group2. Device3 is a personally owned device which cannot be registred 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 Device1 ticks al boxes being registered. But the main question is. Which answer will be right @ the exam?! =O Anyone recently passed and had this quest? =P

upvoted 1 times

091095f 2 years, 4 months 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

subbuhotmail 2 years, 2 months ago

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.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 3 times

kiik32 2 years, 4 months ago

Selected Answer: D

inclusion wins over exclusion

upvoted 1 times

Ayind3 1 year, 11 months 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

Clauster 2 years, 4 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 necesarlly 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

oopspruu 2 years, 2 months ago

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

upvoted 1 times

Question #3 *Topic 1*

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.

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.

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.

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.

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.

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.

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.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

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

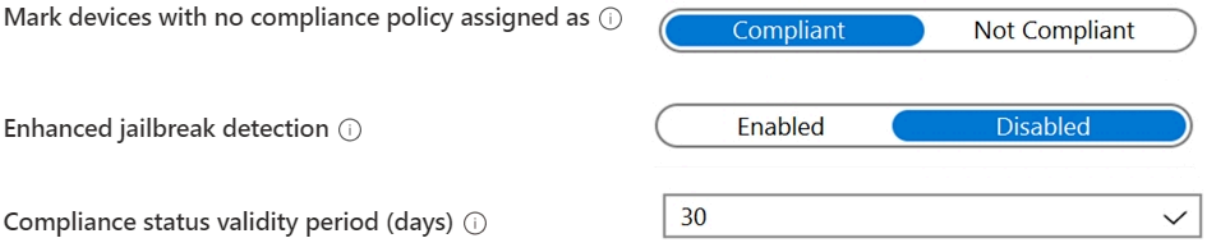
Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

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*

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.



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

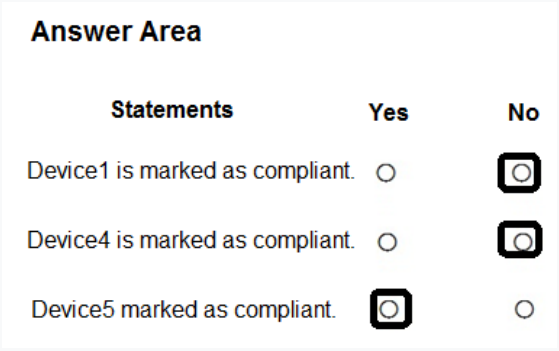
Assignments

Included groups	Group1
Excluded groups	Group2

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	○	○
Device4 is marked as compliant.	○	○
Device5 marked as compliant.	○	○

Suggested Answer:



Meowpidz 5 months ago

What would be the point of a device being in Group 1 if it's assigned to policy 1 and 2 when Group 2 essentially does the same thing, requires bitlocker and secure boot with Policy 3? They make Group 1 seem like it could have either Policy 1 OR Policy 2...

upvoted 1 times

Trice01 1 year, 5 months ago

N,N,Y

Device1 is not compliant because it is a member of Group1. Group1 has 2 compliance Policies, Policy1 & Policy2. Policy1 requires bitlocker only and Device1 has bitlocker turned on. Policy2 requires Secure Boot only which Device1 does not have turned on.

Device4 is a member of Group2 which requires both BitLocker and Secure Boot but Device4 does not have BitLocker turned on.

Device5 is a member of Group3 which is not assigned to a compliance policy and i nthe Compliance Policy settings picture any device without a policy is automatically marked compliant.

upvoted 6 times

emolnes85 1 year, 6 months ago

YNY. Are we looking at the same question? Device 1 i only member og group1, so policy1. Not group2 or policy 2.

upvoted 1 times

Victor3 Most Recent 1 month, 2 weeks ago

Device 1 is in Group 1 which has both Policy 1 and 2 applied. It's not compliant since Secure Boot is not on.

upvoted 1 times

MR_Eliot 2 years, 1 month 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, becuase of configuration.

upvoted 6 times

Tonsku Highly Voted 2 years, 1 month 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 complience 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 complience 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 complience as Complient

Device5 : compliance

upvoted 17 times

7798da3 2 years, 4 months ago

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

upvoted 1 times

7798da3 2 years, 4 months ago

where is policy2 I see one only

upvoted 1 times

Clauster 2 years, 4 months ago

Provided answer is Correct 100%

upvoted 1 times

b0gdan433 2 years, 12 months ago

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

upvoted 1 times

madsa 2 years, 11 months ago

No, No, Yes is correct.

upvoted 1 times

b0gdan433 2 years, 12 months ago

The answer is No, No, Yes, i just took the exam today.So...? MS doesnt reveal right answers.No way you could've confirmed this.

upvoted 1 times

Merrybob 2 years, 9 months ago

No way you could've confirmed this.

upvoted 1 times

iTomi 2 years, 11 months ago

So...? MS doesnt reveal right answers.

upvoted 2 times

picho707 3 years, 1 month ago

Can someone explain why Device4 is 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

Contactfornitish 3 years, 1 month 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 3 years, 1 month ago

Can someone explain why Device4 is 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

Jacob75 2 years, 9 months 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 3 years, 2 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 Ive 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

NoursBear 2 years, 9 months 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

FrenchDuck 3 years, 2 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 Ive 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-policyIn stead of what you are writing you mean it's a No?

upvoted 2 times

Futfuyfyjfj 3 years, 2 months ago

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

upvoted 1 times

NoursBear 3 years, 2 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

picho707 3 years, 2 months ago

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

upvoted 8 times

NoursBear 3 years, 2 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 meBut device1 is assigned to 2 policies, which makes a No for device 1….dunno why I came up with this, clearly NNY is correct, I see more clearly now lol

upvoted 4 times

NoursBear 2 years, 9 months ago

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

upvoted 1 times

Futfuyfyjfj 3 years, 2 months ago

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

upvoted 2 times

ShiftDeL 3 years, 2 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 3 years, 2 months ago

I'm going with:

No

No

Yes

upvoted 3 times

krzysztofbr 3 years, 2 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

Futfuyfyjfj 3 years, 2 months ago

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

upvoted 3 times

BossAceVentura 3 years, 3 months ago

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 4 times

Futfuyfyjfj 3 years, 2 months ago

Wrong: Mark devices with no compliance policy assigned as: Compliant" has been configured.

upvoted 1 times

krzysztofbr 3 years, 2 months ago

hmm I checked answer again

about device 1 there is a conflict of two different compliance policies, group1 has two different compliance polices

"If a compliance policy evaluates against the same setting in another compliance policy, then the most restrictive compliance policy setting applies."

the answers

NO

NO

NO

upvoted 1 times

Futfuyfyjfj 3 years, 3 months ago

Wrong group 1 is assigned to Policy 1 AND policy 2. So members of group 1 are required to have bitlocker enabled and secure boot.

Furthermore device 5 isn't assigned to Andy compliance policy. The image of the default compliance policy shows these kind of Devices are considered Compliant.

upvoted 1 times

sh123df Highly Voted 3 years, 3 months ago

No

No

Yes

Answer is correct

upvoted 23 times

Joe9011 3 years, 3 months ago

Should Device 1 not be "yes"? Its a member of group1 which require BitLocker only, which it has?

upvoted 2 times

Joe9011 3 years, 3 months ago

Nvm, on 2nd read-through seen that Policy 2 is applied to Group1 which requires Secure boot.

No

No

Yes

upvoted 4 times

krzysztofbr 3 years, 2 months ago

device 5 this impossible. there is no Group 3 policy. Im thinking about device 1

upvoted 1 times

Futfuyfyjfj 3 years, 2 months ago

Device with no policies are marked as compliant based in the setting in the image. Furthermore policy 1 & 2 are assigned both to group 1, so device 1 can't be compliant

upvoted 4 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.

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.

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.

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.

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.

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.

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?

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

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

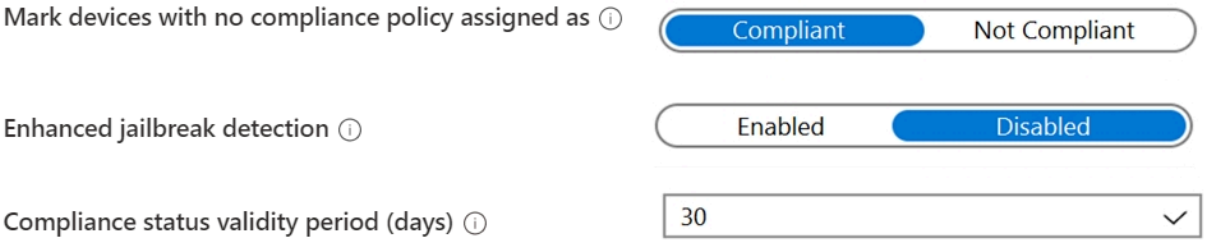
Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

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*

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.



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

A. Device2 only

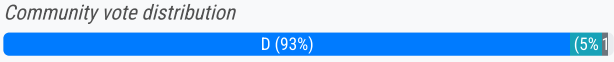
B. Device3 only

C. Device1, Device2, and Device5 only

D. Device1, Device2, Device3, and Device4 only

Suggested Answer: *D*

Community vote distribution



letters1234 Highly Voted 3 years, 2 months ago

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

upvoted 44 times

letters1234 Highly Voted 3 years, 2 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 doesnt receive the policy.

upvoted 42 times

iTomi 2 years, 11 months ago

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

upvoted 6 times

deinth 3 years, 3 months ago

I think it should be D. As the boundary group is asigned to Group 1 and 2I read it the sameNot 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 BScope 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.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 7 times

deinth 3 years, 3 months ago

Selected Answer: D

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

upvoted 7 times

Joe9011 3 years, 3 months ago

I read it the same

upvoted 1 times

volto 3 years, 3 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 BScope 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.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 9 times

volto 3 years, 3 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 3 years, 2 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.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 12 times

letters1234 3 years, 2 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 2 years, 11 months 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

AloisioCarvalho Most Recent 5 months, 3 weeks ago

O perfil Boundary1 foi criado com a etiqueta de escopo Tag1. No Microsoft Intune, as Scope Tags são utilizadas para determinar quais administradores podem ver/gerenciar determinados objetos, ou para filtrar políticas se houver restrições específicas de RBAC. No entanto, o fator determinante para a aplicação de perfis de configuração de endpoint diretamente no sistema do dispositivo final são as atribuições de grupos de segurança do Entra ID/Intune. Como os dispositivos 1, 2, 3 e 4 fazem parte do escopo de inclusão (Group1 ou Group2), a política é direcionada e aplicada a eles. O Device5 fica totalmente de fora por pertencer estritamente ao Group3. Portanto, a política se aplica a Device1, Device2, Device3 e Device4.

upvoted 1 times

7a9c653 7 months, 3 weeks ago

Letter D. Scope makes no diff.

upvoted 1 times

Lourdes_RD 8 months, 2 weeks ago

Boundary1 included in Group 1 & 2 so Devices 1,2,3,4 (D) is the answer

upvoted 1 times

reyrey 8 months, 4 weeks ago

correct answer

upvoted 1 times

Jhojan 1 year, 3 months ago

Group 1 and 2 contains only devices Device 1, Device 2, Device 3 and Device4, to which the network limit of 192.168.1.0/24 applies.

upvoted 1 times

NoursBear 1 year, 10 months ago

Many answers here referring to the scope tag. I suggest you read the documentation on how and when scope tags would be used. Scope tags have no use in any of the scenarios of this series

upvoted 1 times

JayHall 1 year, 12 months 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 years ago

B: because tag scope and assignment: only device 3

upvoted 2 times

Zachypoo 2 years, 4 months 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

AnoG 2 years, 7 months ago

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

upvoted 1 times

c813ce5 2 years, 5 months ago

Device 3 because of the scope tag

upvoted 3 times

AnoG 2 years, 7 months ago

Answer is B because of the scope tag,, Device 3 onlyNo, you are wrong.

upvoted 1 times

2c57d1c 2 years, 5 months ago

No, you are wrong.

upvoted 1 times

AnoG 2 years, 7 months ago

Answer is A because of the scope tag..

upvoted 1 times

MR_Eliot 2 years, 9 months 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

BigStan82 2 years, 9 months 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 2 years, 9 months ago

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.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 2 times

MR_Eliot 2 years, 8 months 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

Tonsku 2 years, 11 months ago

Selected Answer: D

D Boundary1 has the following assignments: Included groups: Group1, Group2

Device1 (Group1) Device2 (Group1, Group2) Device3 (Group2) Device4 (Group2)

upvoted 4 times

onepunchkenshin 2 years, 10 months ago

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

upvoted 5 times

Question #5 *Topic 1*

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.

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.

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

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

Suggested Answer:

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

krzysztofbr Highly Voted 3 years, 2 months ago

pin and account credentials reset app pin NOT device pin

upvoted 66 times

krzysztofbr Highly Voted 3 years, 2 months ago

pin and account credentials reset app pin NOT device pinyes , it should be 'rest app pin' no ?Why pin and account credentials for the first one? Isn't only pin will be required?Because "Work or school account credentials for access" is set to true.

upvoted 67 times

ThomasE Most Recent 1 month, 1 week ago

I would say PIN and account credentials. According to https://learn.microsoft.com/en-us/intune/app-management/protection/ref-settings-android#access-requirements Work or school account credentials for access: Choose Require to require the user to sign in with their work or school account instead of entering a PIN for app access. When set 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

Victor3 1 month, 2 weeks ago

Answer is "PIN only" and "reset the app PIN". Why? Because the "App PIN when device PIN is set" setting is set to "Require". App PIN is seperate from device PIN if this option is on.

upvoted 1 times

redline13 2 years, 9 months ago

Why pin and account credentials for the first one? Isn't only pin will be required?Because "Work or school account credentials for access" is set to true.

upvoted 2 times

redline13 2 years, 9 months ago

Why pin and account credentials for the first one? Isn't only pin will be required?

upvoted 2 times

Arahnofob 4 months, 1 week ago

PIN ONLY, because PIN because it says "override biometric with PIN after timeout"

reset the app PIN because this whole exhibit is an iOS app protection policy

upvoted 2 times

solitudewriter 4 months, 4 weeks ago

This exact question was in my exam today -- I marked APP and Account Credentials and Reset App PIN only. Hope that helps.

upvoted 1 times

Temptset 2 years, 1 month 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.The question is asking about the App protection policy. So this is correct. Thank you.

upvoted 20 times

Temptset 2 years, 1 month 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 19 times

jazzmirza 6 months, 2 weeks ago

1. PIN and account credentials

2. Reset the app PIN

upvoted 2 times

35429bb 11 months, 1 week ago

I asked copilot "IF i have a IOS app protection policy in intune with the parameter work or school account credential for access activated i have to provide my credentials when my device is blocked because inactivity"

and the answer was "Yes — if you configure an iOS App Protection Policy in Intune with “Require work or school account credential for access” enabled, then when the app is blocked due to inactivity, the user must provide their work or school account credentials (not just the App PIN) to regain access."

upvoted 2 times

Dinkan 1 year, 2 months ago

1. PIN and account credentials

2. Reset the app PIN

upvoted 3 times

Digo 1 year, 9 months ago

1. PIN Only

2. Reset the app PIN

My understanding is that the requirement for account credentials is for initial access, not for rechecking after inactivity. but did not test it.

upvoted 1 times

xXDaveOnFireXx 1 year, 10 months 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 2 times

Futfuyfyjfj 3 years, 2 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

letters1234 2 years, 1 month 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

NoursBear 3 years, 2 months ago

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

upvoted 7 times

NoursBear 2 years, 1 month 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

letters1234 2 years, 1 month 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.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 4 times

Rndadhdman 1 year, 11 months ago

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

upvoted 1 times

MR_Eliot 2 years, 9 months ago

Answer:

1> Pin and login using account

2> App pin.

upvoted 5 times

NoursBear 2 years, 1 month 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 appsorry my bad, App PIN... I misread something

upvoted 2 times

Mattia8 2 years, 10 months ago

Pin and account Credentials is correct

upvoted 1 times

Amir1909 2 years, 10 months ago

PIN and account credentials

reset the app PIN

upvoted 3 times

Tonsku 2 years, 11 months ago

PIN and account credentials

reset the app PIN

PIN for access: Require

Work or scholl account credential for access: Require

Max PIN attempts value 5 - action: Reset PIN

upvoted 1 times

Zelda78 3 years 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 3 years, 1 month ago

Pin and account credentials

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

upvoted 4 times

VirtualJP 3 years, 2 months ago

I'm going with krzysztofbr's answer

upvoted 2 times

MR_Eliot 2 years, 9 months ago

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

upvoted 4 times

Grg433 3 years, 2 months ago

yes , it should be 'rest app pin' no ?

upvoted 3 times

ansilva 3 years, 3 months ago

this would reset the app pin not the device pin

upvoted 3 times

Rewound 3 years, 3 months ago

How would iOS APP protection policy reset DEVICE PIN?

upvoted 7 times

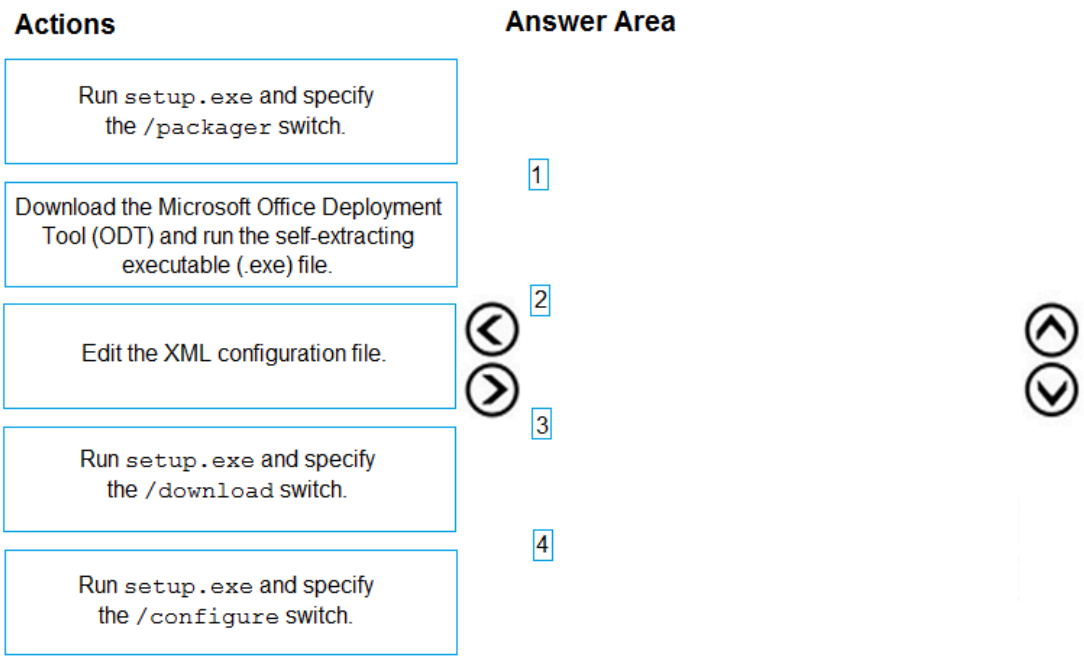
Question #6 *Topic 1*

DRAG DROP -

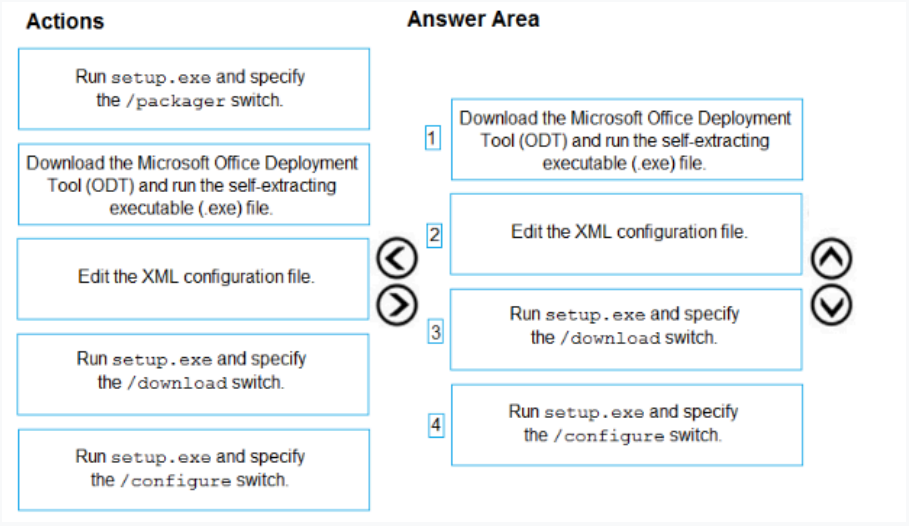
You have a Microsoft 365 E5 subscription and a computer that runs Windows 11.

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.



Suggested Answer:



casti Highly Voted 3 years, 3 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-appssorry, 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.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?I think the /configure is require as we don't want to distribute the package with /download optionThere 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 88 times

casti Highly Voted 3 years, 3 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 87 times

ollyijeh Most Recent 2 months, 2 weeks ago

1. Download the ODT Application

2. Edit the XML

3. use setup.exe /download to download the installation files

4. use setup.exe /configure to deploy the app

upvoted 3 times

MR_Eliot 2 years, 9 months 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

MR_Eliot 2 years, 9 months 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.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?I think the /configure is require as we don't want to distribute the package with /download optionThere 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 3 times

jazzmirza 6 months, 2 weeks ago

ODT → XML → Download → Configure

upvoted 1 times

laurentiu13 1 year, 11 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 2 times

AleFCI1908 2 years 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 2 times

tempelier1975 3 years, 2 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 installsorry, 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.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 15 times

tempelier1975 3 years, 2 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 15 times

OliTakesTests 2 years, 8 months ago

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

upvoted 4 times

MR_Eliot 2 years, 9 months 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.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

ENGELHENDY 2 years, 3 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

upvoted 3 times

solitudewriter 4 months, 3 weeks ago

This exact question was in my exam on 6/22/2026. Passed with 959/1000. I answered: Download the ODT tool, setup /download and setup /configure

upvoted 1 times

MR_Eliot 2 years, 1 month ago

First: Download ODT Tool Second: Extrat the files using the exe file. Third: Edit XML configuration file if needed. Fourth: Run Setup and specifiy /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

ushahid 2 years, 10 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 4 times

Tonsku 2 years, 11 months 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

MR_Eliot 2 years, 1 month ago

First: Download ODT Tool Second: Extrat the files using the exe file. Third: Edit XML configuration file if needed. Fourth: Run Setup and specifiy /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.Your 1st and 2nd are a single option in the answers. Might want to rethink this.

upvoted 2 times

mohdAj 2 years, 11 months 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

ThePrutser 2 years, 11 months ago

yes the download step is required.

upvoted 1 times

ZaFletch 3 years, 1 month ago

The packager 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

HawkieEyes 3 years 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

HawkieEyes 3 years 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?yes the download step is required.

upvoted 1 times

cvos 1 year, 10 months 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 2 times

NoursBear 3 years, 2 months ago

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

upvoted 2 times

GaloCO 3 years, 3 months ago

The order of those steps re wrong

upvoted 1 times

letters1234 3 years, 2 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 3 years, 3 months ago

The order of those steps re wrong1. 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

SajjH 2 years, 3 months 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 2 years, 5 months ago

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

upvoted 1 times

OyYaGotta 2 years, 8 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

GaloCO 3 years, 3 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

Question #7 *Topic 1*

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

On which devices can you apply app configuration policies?

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

A. Device2 only

B. Device1 and Device2 only

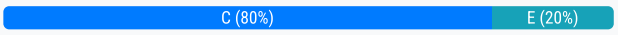
C. Device3 and Device4 only

D. Device2, Device3, and Device4 only

E. Device1, Device2, Device3, and Device4

Suggested Answer: *C*

Community vote distribution



volto Highly Voted 3 years, 3 months ago

Selected Answer: C

iOS and Android only

upvoted 27 times

volto Highly Voted 3 years, 3 months ago

iOS and Android onlyapp configuration exist also for Windows but in preview. I hope exam measure features not in preview. so i Agree wit YouNo you are referring to app PROTECTION policies. Question is about app CONFIGURATION policies

upvoted 29 times

krzysztofbr 3 years, 2 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

krzysztofbr 3 years, 2 months ago

app configuration exist also for Windows but in preview. I hope exam measure features not in preview. so i Agree wit YouNo you are referring to app PROTECTION policies. Question is about app CONFIGURATION policies

upvoted 1 times

Futfuyfyjfj 3 years, 2 months ago

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

upvoted 2 times

krzysztofbr 3 years, 3 months ago

was for Android and IOS only not for Windows:)

upvoted 9 times

teckinfor Most Recent 5 months ago

I know many people think the answer is D, given the recent addition of MAM on Windows, but the correct answer is still C. Microsoft's documentation states that Intune MAM on Windows supports unmanaged devices. However, the question refers to managed devices.

upvoted 1 times

spikek22 6 months, 1 week ago

Currently I can configure apps intune, maybe before you could not but now you can

upvoted 1 times

2938b52 10 months, 3 weeks ago

How it works for Windows: Managed Devices vs. Managed Apps: For Windows, you typically use the "Managed Devices" channel in App Configuration Policies to push settings directly to the device via Mobile Device Management (MDM). Configuration Designer: You use the Configuration Designer within Intune to define specific key-value pairs and data types for apps that support AppConfig standards. App Types: This works for Universal Windows Platform (UWP) apps and Win32 apps deployed through Intune. Consistency: These policies are great for setting up bookmarks, default browsers, or forcing specific account usage within apps like Outlook or Teams, ensuring a standardized user environment.

upvoted 1 times

Naebun 11 months, 3 weeks ago

So when this question was released i believe just mobile was available, but you can now also secure windows apps with MAM

upvoted 4 times

GryffindorOG 1 year, 7 months ago

The answer is correct, you can create device config PROFILES for Windows devices, not "policies"

upvoted 1 times

BestSumy 1 year, 8 months ago

For mercy microsoft open the door for Windows

upvoted 1 times

Besxp 2 years 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 4 times

mikekrt 1 year, 8 months ago

Nowadays you can also create them for Windows.

upvoted 1 times

BPN14 1 year, 8 months ago

App configuration policies now can be applied to Windows devices as well

upvoted 2 times

Besxp 2 years 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.Sir you are absolutely wrong. Stop depending on AI for answers! Intune > apps > configuration > create > managed devices > platform There's only two options listed there. iOS/ipadOS and Android Enterprise. This is all under Create app configuration policy. The correct answer is C

upvoted 4 times

cd2cfde 1 year, 4 months ago

Sir you are absolutely wrong. Stop depending on AI for answers! Intune > apps > configuration > create > managed devices > platform There's only two options listed there. iOS/ipadOS and Android Enterprise. This is all under Create app configuration policy. The correct answer is C

upvoted 3 times

JGMG 2 years, 1 month 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 5 times

OigresMG 2 years, 1 month ago

Correct option is E: https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-managed-app

upvoted 8 times

Futfuyfyjfj 3 years, 2 months ago

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

upvoted 3 times

OigresMG 2 years, 1 month 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 4 times

JGMG 2 years, 1 month 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.Wrong, take a look yourself Intune-Apps-app configuration policies and try to create one , you will see you are wrongThat'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 5 times

Futfuyfyjfj 3 years, 2 months ago

Wrong, take a look yourself Intune-Apps-app configuration policies and try to create one , you will see you are wrongThat'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 3 times

Jimix 2 years, 1 month 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 3 times

Haider_Raza 2 years, 1 month 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

Shawn_Chen 2 years, 8 months ago

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

upvoted 4 times

veliyath 2 years, 1 month ago

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 2 years, 4 months 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

Friscini 2 years 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 2 years, 9 months ago

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

upvoted 2 times

HOTSPOT -

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

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.

Name	Operating system
Device1	Windows 10
Device2	Android 8.0
Device3	Android 9
Device4	iOS 11.0
Device5	iOS 11.4.1

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

Suggested Answer:

Answer Area

Policy type: App protection policy

Minimum number of policies: 3

ihan Most Recent 7 months, 2 weeks ago

It should be

App protection policy

number of policies 2

"App protection policy" only supports mobile apps - Android and iOS. You cannot use App Protection Policies (APP) to control copy/paste on Windows 10/11.

upvoted 4 times

MR_Eliot Highly Voted 2 years, 9 months ago

Answer is correct. I research all my answers before commenting.Comment was written in English. I research my response before replying

upvoted 14 times

MR_Eliot 2 years, 9 months ago

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

upvoted 14 times

iTomi 2 years, 12 months ago

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

upvoted 3 times

PranilR 2 years, 1 month 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 devices1. 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 apps2. You only need one policy to apply this setting to all devices that have App1 installed1. 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

veliyath 2 years, 1 month 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 6 times

PranilR 2 years, 1 month 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 devices1. 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 apps2. You only need one policy to apply this setting to all devices that have App1 installed1. 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-pasteYou are wrong. Minimun number of policies is 3. Each win, android and ios need own policies.

upvoted 2 times

mohdAj Highly Voted 2 years, 1 month 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 27 times

Zachypoo 2 years, 4 months 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 o explicitly state this in the documentation but is visible in the provided screenshot.

upvoted 3 times

wakka9876 1 year, 10 months ago

Comment was written in English. I research my response before replying

upvoted 3 times

Murad01 2 years, 9 months ago

Given answer is correct

upvoted 2 times

Tonsku 2 years, 11 months 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 3 years 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

NoursBear 3 years, 2 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 2 times

FrenchDuck 3 years, 2 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 3 years, 2 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.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 2 times

NoursBear 3 years, 2 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

F3RRY 3 years, 2 months ago

But why is the minimum 3?

upvoted 1 times

letters1234 3 years, 2 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 3 years, 2 months ago

But why is the minimum 3?should be two. for Android and IOS only. protection for Windows is something pretty new. still in previewShould 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.one for each platform

upvoted 1 times

krzysztofbr 3 years, 2 months ago

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

upvoted 1 times

krzysztofbr 3 years, 2 months ago

should be two. for Android and IOS only. protection for Windows is something pretty new. still in previewShould 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 1 times

Futfuyfyjfj 3 years, 2 months ago

one for each platform

upvoted 4 times

krzysztofbr 3 years, 3 months ago

answer seems be correct. just beacuse 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

krzysztofbr 3 years, 3 months ago

answer seems be correct. just beacuse We also have protection for Windows but this is in PREVIEW https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-windowsThey 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 politiek

upvoted 1 times

Futfuyfyjfj 3 years, 2 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

Futfuyfyjfj 3 years, 2 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 politiek

upvoted 1 times

Question #9 *Topic 1*

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

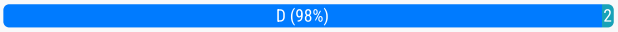
B. a dynamic device group

C. a detection rule

D. the App2 deployment configurations

Suggested Answer: *D*

Community vote distribution



WTH Highly Voted 3 years, 3 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 31 times

WTH Highly Voted 3 years, 3 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?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 app1Think so as well. Detection rule is only so that Intune know that the application is correctly installed. With SCCM for example, even when the deteciton 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.Agreed.

upvoted 31 times

ollyijeh Most Recent 2 months, 2 weeks ago

Selected Answer: D

To ensure that App 1 is installed before App 2, the correct answer is D. App2 deployment can be configured so it requires app 1 to be installed.

upvoted 2 times

henil_154762 1 year, 3 months ago

Selected Answer: D

The correct answer is: D. the App2 deployment configurations

In Intune, when you need one Win32 app to be installed after another, you configure install dependencies on the app that should be installed later.

Here, App1 must be installed before App2.

That means App2 should have App1 set as a dependency in its deployment configuration.

This ensures Intune will automatically install App1 first, then App2.

upvoted 1 times

examprepboy 1 year, 5 months ago

Selected Answer: D

Requirement or dependencies are the answer here. These must be configured on the 2nd app.

upvoted 1 times

PranilR 2 years, 1 month 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 2 years, 2 months ago

Selected Answer: D

Wrong. You configure dependency's on APP2.

upvoted 1 times

GSBXL 2 years, 4 months 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 2 years, 4 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 3 times

veliyath 2 years, 4 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 2 years, 4 months 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 2 years, 5 months ago

Answer D is the correct answer

upvoted 1 times

kerimnl 2 years, 7 months ago

Selected Answer: D

D. the App2 deployment configurations

upvoted 1 times

Darkfire 2 years, 9 months 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 2 years, 10 months ago

D is correct

upvoted 1 times

Tonsku 2 years, 11 months 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 2 years, 11 months 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 2 years, 11 months 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 2 years, 11 months ago

Selected Answer: D

App1 as a dependency of App2.

upvoted 1 times

Dieter_0026 3 years ago

Selected Answer: D

list app1 as a dependency?

upvoted 2 times

chandravamsi 3 years ago

Selected Answer: D

d is Correct

upvoted 1 times

abhi_151 3 years, 1 month ago

Answer D is correct

upvoted 1 times

neki99 3 years, 1 month ago

To ensure that App 1 is installed before App 2: you need to configure the deployment sequence.

1. create a separate deployment profile for App 1 and App 2 in Intune

2. configure dependencies > in the deployment profile for APP 2, set APP 1 as a dependency (this ensures that app 1 is installed before app 2).

upvoted 2 times

Praveenm2712 3 years, 1 month ago

D is correct as you need to add dependency.

upvoted 1 times

norelissme 3 years, 1 month ago

Selected Answer: D

D is correct

upvoted 1 times

ExamKiller020 3 years, 2 months ago

Answer is D. But don't use the detection rule methode as some other mentioned. Use the dependency option in intune. Detection rule is to check if the application installed succesfully. You would have no idea if the seconde app installed succesfully.

upvoted 1 times

WTH 3 years, 2 months ago

Selected Answer: D

correct answer is D

upvoted 1 times

AryViegas 3 years, 2 months ago

A é a correta.

upvoted 1 times

Mavrix 3 years, 2 months ago

Selected Answer: D

Detection rules in Win32 apps are telling Intune how to tell if the application has been installed or not. Configure a dependency in the win32 app deployment screen even has this wording:

"Software dependencies are applications that must be installed before this application can be installed"

Configure App1 first so that it'll be selectable in the dependencies section

upvoted 1 times

letters1234 3 years, 2 months ago

Selected Answer: D

D correct

upvoted 2 times

blacky14 3 years, 3 months ago

Selected Answer: D

D is correct

upvoted 3 times

ZaFletch 3 years, 3 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 12 times

Sprocket10 3 years, 3 months ago

Selected Answer: D

correct answer is D

upvoted 5 times

casti 3 years, 3 months ago

Checked in my test environment. It is possible to configure the detection rule, to install (or not) checking that a registry key exists (or not)

Therefore, in the application that is installed second, the detection rule can be set so that it is not installed until there is a registry key that creates the installation of the first App.

upvoted 2 times

Futfuyfyjfj 3 years, 2 months ago

I think you are mistaking, detection rules in the Win32 app config solely serve the application installation detection. It is not meant to create depedencies or aan app install order:

https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-add#step-4-detection-rules

D is correct

upvoted 3 times

casti 3 years, 3 months ago

C it,s Correct

upvoted 2 times

Ksobier 2 years, 9 months 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

MR_Eliot 2 years, 9 months ago

Agreed.

upvoted 1 times

GarySappig 3 years, 3 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 deteciton 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 3 times

Question #10 *Topic 1*

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

An app named App1 is installed on each device.
What is the minimum number of app configuration policies required to manage App1?

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

A. 1

B. 2

C. 3

D. 4

E. 5

Suggested Answer: *B*

Community vote distribution



krzysztofbr Highly Voted 3 years, 2 months ago

Selected Answer: B

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

upvoted 18 times

krzysztofbr Highly Voted 3 years, 2 months ago

answer B is correct You need app protection for both platforms, separatelyCorrect, although the answer remains the same, the question is about app configuration policies, not app protection policies :-)

upvoted 18 times

Futfuyfyjfj 3 years, 2 months ago

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

upvoted 6 times

lmpcanada Most Recent 8 months, 2 weeks ago

the minimum number of app con guration policies required to manage App1 is 2. Answer is B

upvoted 1 times

Robert69 1 year, 1 month ago

When you configure an Azure Log Analytics workspace to collect all available events from the Windows event logs, it will collect events from all the standard Windows event log categories, including: Event 1 - Application/Success ✓ Event 2 - System/Information ✓ Event 3 - Security/Audit Success ✓ Event 4 - System/Error ✓

upvoted 1 times

theptr 1 year, 7 months ago

B is correct

upvoted 1 times

Perycles 1 year, 10 months ago

assuming that it's possible to add IOS and Android Apps in the same configuration under "selecting public apps " or "selectied custom apps"

upvoted 2 times

Carlio2024 1 year, 11 months ago

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

upvoted 1 times

PranilR 2 years, 1 month 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 2 years, 1 month ago

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.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.We were wrong, right answer is 2.

upvoted 4 times

ThePrutser 2 years, 1 month 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 2 years, 11 months 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.We were wrong, right answer is 2.

upvoted 2 times

iTomi 2 years, 11 months 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 2 years, 11 months ago

We were wrong, right answer is 2.

upvoted 5 times

iTomi 2 years, 1 month ago

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

RazielLycas 2 years, 1 month 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

RazielLycas 2 years, 1 month 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"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 2 times

Zoom2020 2 years, 2 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

veliyath 2 years, 1 month ago

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 2 years, 2 months ago

It's B

upvoted 1 times

MR_Eliot 2 years, 9 months ago

You need seperate policies for each OS.

upvoted 2 times

NoursBear 2 years, 9 months ago

Again this is debatable, devices are enrolled so one can presume you will select "managed devices", there you have to chose 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 2 years, 11 months ago

B. one app configuration policy for each platforms

upvoted 1 times

mohdAj 2 years, 11 months ago

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 2 years, 12 months ago

Correct ans is B For iOS and for Android.

upvoted 1 times

Question #11 *Topic 1*

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%)

kmyazwin Most Recent 4 months, 4 weeks ago

Selected Answer: B

B. .ipa: This is the correct file format for iOS and iPadOS app packages.

C. .apk: This extension is used for Android app packages.

D. .appx: This is a package format for Windows apps.

A. .intunemac: This is not a standard file extension used for deploying LOB apps in Intune. A related format, .pkg, is used for macOS LOB apps

upvoted 4 times

budekzkie 1 year, 2 months ago

Selected Answer: B

As indicated in Intune when creating LOB app, To add a custom or in-house app, upload the app's installation file. Make sure the file extension matches the app's intended platform. Intune supports the following line-of-business app platforms and extensions:

Android (APK)

iOS (IPA)

macOS (.pkg)

Windows (.msi, .appx, .appxbundle, .msix, and .msixbundle)

upvoted 4 times

yaktownboii 1 year, 3 months ago

Selected Answer: B

B is correct.

upvoted 1 times

veliyath 2 years, 4 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 2 times

MR_Eliot 2 years, 9 months ago

Selected Answer: B

Correct answer is given.

upvoted 1 times

Darkfire 2 years, 9 months 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 2 years, 11 months ago

Selected Answer: B

IPA (iOS)

upvoted 1 times

mohdAj 2 years, 11 months 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

krzysztofbr Highly Voted 3 years, 2 months ago

Selected Answer: B

B correct IPA (like beer:))

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

upvoted 30 times

Gr8Greet 3 years, 3 months ago

Selected Answer: B

correct

upvoted 2 times

casti 3 years, 3 months ago

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

upvoted 3 times

Question #12 *Topic 1*

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%)

Pisces225 Most Recent 1 year, 12 months 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 2 times

veliyath 2 years, 4 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 3 times

MR_Eliot 2 years, 8 months ago

Selected Answer: E

E is correct.

upvoted 2 times

Darkfire 2 years, 9 months 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 2 years, 10 months ago

E

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

upvoted 1 times

Amir1909 2 years, 10 months ago

Correct

upvoted 1 times

Tonsku 2 years, 11 months ago

Selected Answer: E

Grant: Block access -

client Apps block only legacy authentication

upvoted 1 times

mohdAj Highly Voted 2 years, 11 months 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 13 times

Praveenm2712 2 years, 12 months 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 3 years, 1 month 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 3 years, 1 month ago

Correct

upvoted 1 times

Rocky83 3 years, 1 month ago

Selected Answer: E

Correct

upvoted 1 times

pinda 3 years, 1 month ago

Selected Answer: E

Correct

upvoted 1 times

Gr8Greet Highly Voted 3 years, 3 months ago

Selected Answer: E

Seems to be correct.

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

upvoted 13 times

HOTSPOT -

All users have Microsoft 365 apps deployed.

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

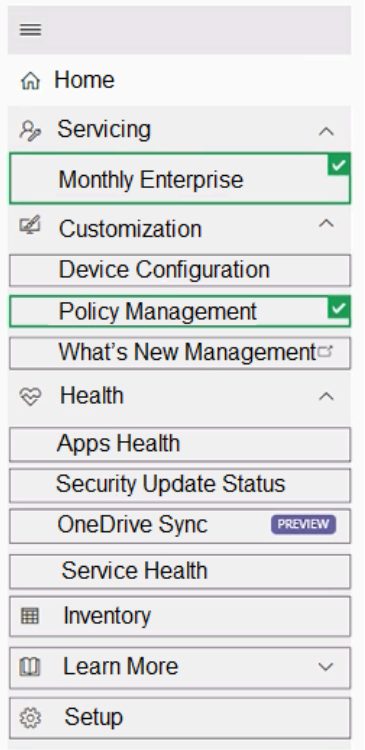
Enable the automatic installation of WebView2 Runtime.

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.

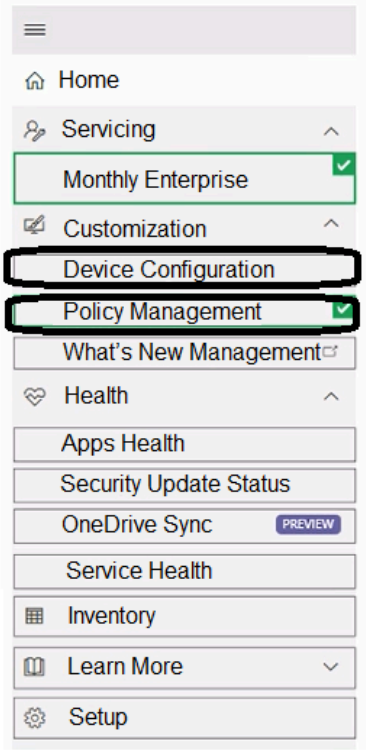
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



ollyijeh Most Recent 2 months, 2 weeks ago

This can be configured in Device Configuration to enable automatic installation of webview2 runtime and Policy management to prevent users from submitting feedback

upvoted 3 times

NoursBear Highly Voted 3 years, 2 months ago

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

upvoted 8 times

NoursBear 3 years, 2 months ago

I don't understand Microsoft 365 apps is not covered anywhere in the MD102 courseYes it is, exam ref MD-102 Microsoft Endpoint Administrator book chapter 4, skill 4.1iTomi, where did you purchase the MD-102 book? Thank you!Microsoft Press Store

upvoted 8 times

Dinkan 1 year, 2 months ago

□ Device Configuration

□ Policy Management

upvoted 2 times

iTomi 2 years, 11 months ago

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

upvoted 4 times

iTomi 2 years, 11 months ago

Yes it is, exam ref MD-102 Microsoft Endpoint Administrator book chapter 4, skill 4.1iTomi, where did you purchase the MD-102 book? Thank you!Microsoft Press Store

upvoted 4 times

kiik32 2 years, 4 months ago

both are under device configuration now a days.

modern app settings tab for webview

My configurations tab > app preferences to block feedback

upvoted 3 times

Gbreezy162 2 years, 5 months ago

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

upvoted 2 times

Gbreezy162 2 years, 5 months ago

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

upvoted 2 times

ten1ton 2 years, 3 months ago

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

upvoted 1 times

MR_Eliot 2 years, 9 months ago

Given answers are correct.

upvoted 3 times

Darkfire 2 years, 9 months ago

Anwser 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

kiik32 2 years, 4 months ago

both are under device configuration now a days. modern app settings tab for webview My configurations tab > app preferences to block feedback

upvoted 3 times

Amir1909 2 years, 10 months ago

Correct

upvoted 1 times

yosry 2 years, 10 months ago

correct

upvoted 1 times

Tonsku 2 years, 11 months ago

configure in the Microsoft 365 Apps admin:

Device Configuration & Policy Management

upvoted 2 times

ExamKiller020 Highly Voted 3 years, 2 months ago

Given answer is correct:

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

Prevent users from submitting feedback > Policy management

upvoted 11 times

ronct 3 years, 2 months ago

i verified this in the admin center at config.office.com and it is correct

upvoted 3 times

Roska 2 years ago

Microsoft Press Store

upvoted 1 times

Question #14 *Topic 1*

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.

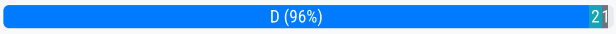
B. From Azure AD, add an app registration.

C. From Azure AD, add an enterprise application.

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

Suggested Answer: *D*

Community vote distribution



Dinkan Most Recent 1 year, 2 months ago

Selected Answer: D

Intune > Apps > All Apps > Create > App type: Microsoft 365 Apps > Windows 10 and later

upvoted 3 times

theptr 1 year, 4 months ago

Selected Answer: D

It should be D

upvoted 1 times

yhano 2 years 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 2 years, 4 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:

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 8 times

veliyath 2 years, 4 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 2 years, 4 months 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 2 years, 6 months 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 2 years, 6 months ago

Selected Answer: D

Answer is D

upvoted 1 times

Titi150 2 years, 6 months ago

Answer D

upvoted 1 times

mestorrent86 2 years, 8 months 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

MR_Eliot 2 years, 9 months 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 5 times

Darkfire 2 years, 9 months ago

Selected Answer: D

I think D is correct as well.

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

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

upvoted 1 times

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

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.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 1 times

vijay0715 2 years, 9 months 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

MR_Eliot 2 years, 9 months 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 2 years, 10 months ago

Selected Answer: D

correct

upvoted 1 times

AdamRachel 2 years, 10 months 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

AdamRachel 2 years, 10 months ago

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.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

Tonsku 2 years, 11 months ago

Selected Answer: D

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

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

upvoted 1 times

mohdAj 2 years, 11 months ago

Selected Answer: D

Option D, "From the Microsoft Intune admin center, add an app," aligns with the process of deploying Win32 apps, such as Microsoft 365 Apps, to devices managed by Microsoft Intune.

upvoted 1 times

kiro_e 3 years ago

Selected Answer: D

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

upvoted 1 times

HawkieEyes 3 years ago

Selected Answer: D

Answer is D

upvoted 1 times

chandravamsi 3 years ago

Selected Answer: A

While add an APP in intune is OK, it is more Proficient to create Windows and create an APP.

upvoted 1 times

ThePrutser 2 years, 11 months ago

Windows has already been deployed, you want to redeploy Windows with office 365? For future deployments you might be right, but as Windows has already been deployed in this case, adding an app is more proficient.

upvoted 2 times

Ksobier 2 years, 9 months ago

Agree. It's hard enough to get one user back to the office, yet redeploy all users is impossible.

upvoted 1 times

ZaFletch 3 years, 1 month ago

Selected Answer: D

It's pretty clearly D

upvoted 2 times

ExamDumpEnjoyer 3 years, 1 month ago

Selected Answer: D

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

upvoted 1 times

Rocky83 3 years, 1 month ago

Selected Answer: D

Admin please change the answer.

upvoted 1 times

zeos_ucok 3 years, 1 month ago

Selected Answer: D

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

upvoted 1 times

Rocky83 3 years, 1 month ago

Selected Answer: D

I would like a very good explanation why A

upvoted 4 times

HN99 3 years, 2 months ago

Selected Answer: D

D is correct

upvoted 1 times

minniesj 3 years, 2 months ago

Selected Answer: D

Answer is D

upvoted 1 times

usmansyed23 3 years, 2 months ago

Selected Answer: D

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

upvoted 1 times

RAJKPB 3 years, 2 months ago

Selected Answer: D

D is the correct answer

upvoted 2 times

ZaFletch Highly Voted 3 years, 3 months ago

Selected Answer: D

Who in the world put A here?

upvoted 14 times

krzysztofbr 3 years, 3 months ago

answer D

upvoted 2 times

Gr8Greet Highly Voted 3 years, 3 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 32 times

Question #15 *Topic 1*

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

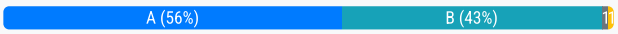
B. a Retire action

C. a Fresh Start action

D. an Autopilot Reset action

Suggested Answer: *A*

Community vote distribution



ExamKiller020 Highly Voted 3 years, 2 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 37 times

ExamKiller020 Highly Voted 3 years, 2 months ago

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-centerThis action immediately deletes the device from Intune, and it cannot be undone. However, it does not trigger a wipe of the device.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 AI agree it's a bad question that contradicts it's 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.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.From: https://learn.microsoft.com/en-us/intune/intune-service/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

upvoted 41 times

Aido Most Recent 19 hours ago

Selected Answer: B

Removes the device from Intune management.

Removes managed apps, profiles, policies, certificates, and corporate data.

Leaves personal files and user-installed apps intact.

upvoted 1 times

iTomi 2 years, 11 months 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 4 times

iTomi 2 years, 11 months ago

This action immediately deletes the device from Intune, and it cannot be undone. However, it does not trigger a wipe of the device.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 5 times

mil2026 2 days ago

Selected Answer: B

The Answer should be B. Check this line "The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed."

If you delete it, the device is no longer in Intune, and when it comes back online, intune cannot remove any apps provisioned. The Retire action will remove apps once the device receives the command. Delete action is good if the device is online currently.

upvoted 1 times

s.i.r.24 1 month, 2 weeks ago

Selected Answer: B

Removes company data/apps, keeps personal : CHATGPT checked

upvoted 1 times

noa808a 4 months, 3 weeks ago

Selected Answer: A

Delete action both wipes org data and removes device from Intune. Retire action wipes org data but keeps device in intune. Correct answer is A.

upvoted 2 times

kseannng 5 months ago

Selected Answer: B

It's B, geniuses, smh, we need to retire it so it will retain OEM apps. Deleting remove the machine completely.

upvoted 1 times

Djonzi 8 months, 1 week ago

Selected Answer: A

If you click on 'delete' it says: If you delete this device, you will no longer be able to view or manage the device from the Intune portal. The device will no longer be allowed to access your company's corporate resources. Company data may be wiped from the device if the device tries to check-in after it is deleted.

upvoted 1 times

HueCumber 7 months ago

What Delete actually does in Intune

Delete = server-side only

When you use Delete on a device in Intune:

 Removes the device record from Intune

 Removes the device from the Intune admin console

 Does NOT send any command to the device

 Does NOT remove company apps, profiles, or data from the device

 Has no effect if the device later comes back online

Think of Delete as “forget this device exists,” not “clean it up.”

upvoted 1 times

moluccanvibe 9 months, 2 weeks ago

Selected Answer: B

A Retire action:

- Removes the device from Intune immediately, even if it's offline

- Flags the device so that if it ever checks in again, Intune will:

- Remove managed apps

- Remove managed data

- Remove configuration profiles

- Leaves personal data, user-installed apps, and OEM apps untouched

This is precisely what the scenario requires.

upvoted 1 times

solitudewriter 4 months, 3 weeks ago

This exact question was in my exam on 6/22/2026. Passed with 959/1000. I answered Delete.

upvoted 2 times

MadhuAz 11 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/intune/intune-service/remote-actions/?tabs=windows

upvoted 1 times

O3Support 11 months ago

Selected Answer: A

The definitive answer is A although I was inclined to choose B.

Reason: https://learn.microsoft.com/en-us/intune/intune-service/remote-actions/device-delete?pivots=windows

For iOS/iPadOS, macOS, and Windows devices, the Delete action always triggers a Retire command.

So this one covers the first requirement - remove immediately, AND the others.

Then why not Retire?

Well - https://learn.microsoft.com/en-us/intune/intune-service/remote-actions/device-retire?pivots=windows

Retire keeps user content intact. The action is triggered the next time the device checks in with Intune. Until then, the device might still appear in the admin center. If you need to remove a device immediately, consider using the Delete action instead.

End discussion.

upvoted 1 times

Djonzi 8 months, 1 week ago

If you click on 'delete' it says: If you delete this device, you will no longer be able to view or manage the device from the Intune portal. The device will no longer be allowed to access your company's corporate resources. Company data may be wiped from the device if the device tries to check-in after it is deleted.What Delete actually does in Intune Delete = server-side only When you use Delete on a device in Intune: Removes the device record from Intune Removes the device from the Intune admin console Does NOT send any command to the device Does NOT remove company apps, profiles, or data from the device Has no effect if the device later comes back online Think of Delete as “forget this device exists,” not “clean it up.”

upvoted 1 times

35429bb 11 months, 2 weeks ago

Selected Answer: A

Well acording the MS documentation delete is the only option that mention delete from Intune as option, then must be A

upvoted 1 times

Gayoub 1 year ago

Selected Answer: A

you need to remove the device Device1 from Intune immediately its in the question. delete remove Device1 from Intune immediately retire its in the next check in

upvoted 1 times

Alaeddine100 1 year ago

Selected Answer: A

A

Quand tu supprimes un appareil, il est immédiatement retiré d'Intune.

Si l'appareil se reconnecte, toutes les données et paramètres d'entreprise sont supprimés.

upvoted 1 times

Robert69 1 year, 1 month ago

Selected Answer: B

Retire Action

The Retire action is specifically designed to:

Remove Intune-managed apps and data

Remove company data provisioned by Intune

Retain user-installed apps, personal data, and OEM-installed apps

Work even when the device checks in later (the retire command is queued)

Remove the device from Intune management

upvoted 1 times

Mohamed555 1 year, 1 month ago

Selected Answer: B

The Retire action:

Unenrolls the device from Intune.

Removes corporate data, policies, and managed apps.

Retains user's personal data and personal apps.

Works even if the device is currently offline — the command is queued and runs at next check-in

upvoted 1 times

fayawax 1 year, 1 month ago

Selected Answer: A

Clicking on the delete option pop explains that it will delete the data during next check-in The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed.

upvoted 1 times

khalid2ti 1 year, 1 month ago

Selected Answer: B

Delete action

This removes the device from Intune immediately, but does not send any command to the device. If the device comes back online, it will not receive any wipe or retire commands.

upvoted 1 times

khalid2ti 1 year, 1 month ago

after reviewing this response I would say answer A is correct since you have to remove Device1 from Intune immediately, everyone using ChatGPT will get B, try to argue ChatGPT and explain to him that i need to remove Device1 from Intune immediately and once it checks in again device has to be wiped. please read the differences between all of them again instead of just relaying on ChatGPT

upvoted 1 times

Asif1982 1 year, 2 months ago

Selected Answer: A

Correct: A

Retire:

Removes corporate data and management, waits for device check-in to complete the process.

Delete:

Removes corporate data and management and immediately removes the device record from the Intune portal.

upvoted 1 times

budekzkie 1 year, 2 months ago

Selected Answer: B

I'll go for B.

What Happens When You Retire a Device in Intune:

- Company apps and data are removed (e.g., Outlook, Teams, OneDrive for Business).

- Device is unenrolled from Intune.

- Configuration profiles, compliance policies, and certificates are removed.

- Company portal app remains, but the device is no longer managed.

- Personal apps, photos, and files are not deleted.

upvoted 1 times

Dinkan 1 year, 2 months ago

Selected Answer: A

Delete Action will remove from intune immediately and perform retire or wipe if the device checkin again depending on the platform

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

upvoted 1 times

khalid2ti 1 year, 1 month ago

Delete action This removes the device from Intune immediately, but does not send any command to the device. If the device comes back online, it will not receive any wipe or retire commands.after reviewing this response I would say answer A is correct since you have to remove Device1 from Intune immediately, everyone using ChatGPT will get B, try to argue ChatGPT and explain to him that i need to remove Device1 from Intune immediately and once it checks in again device has to be wiped. please read the differences between all of them again instead of just relaying on ChatGPT

upvoted 1 times

sxcap 1 year, 2 months ago

Selected Answer: B

The correct answer is: B. a Retire action

 Why Retire is the right choice:

- Removes corporate data and apps: The Retire action removes all Intune-managed apps, profiles, policies, and certificates.

- Preserves personal data: It does not wipe user-installed apps, personal files, or OEM-installed software.

- Deferred execution: Even though Device1 is offline, the retire command will be queued and executed as soon as the device checks in again.

- Meets the requirement: Ensures that Intune-provisioned content is removed while retaining everything else.

upvoted 1 times

henil_154762 1 year, 2 months ago

Selected Answer: B

B. Retire action

Removes Intune-managed apps, settings, and corporate data.

Keeps user apps, personal data, OEM apps.

If the device is offline, the retire action waits and applies when the device checks in again.

➡ Correct — matches exactly what's asked.

upvoted 1 times

a405051 1 year, 3 months ago

Selected Answer: A

I'm not an expert as I am still learning, but I strongly believe the correct answer is A. This is a tricky question due to Retire and Delete have similar functionalities, but Delete Action meets both requirements. What I understand is the following... By performing a Delete Action, the user will remove the device from intune, which the device itself and the corporate data will be removed immediately, but personal data will be retained by default. I hope it helps to understand.

upvoted 1 times

henil_154762 1 year, 3 months ago

Selected Answer: B

Ans: B Retire action

Removes Intune-managed apps, settings, and company data.

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

If the device is offline, the retire command is queued and runs on the next check-in.

Why not the others?

A. Delete → Removes the record from Intune immediately but does not send wipe/retire commands, so company data remains if the device later checks in.

C. Fresh Start → Reinstalls Windows while removing all apps (including personal apps), so it doesn't meet the requirement to retain user-installed apps.

D. Autopilot Reset → Resets Windows and reapplies provisioning; removes personal data, so it's not suitable here.

upvoted 1 times

theptr 1 year, 5 months ago

Selected Answer: B

B retire

upvoted 1 times

Besxp 1 year, 5 months ago

Selected Answer: B

B. Retire action

What it does:

Removes Intune-provisioned apps, configuration profiles, and company data.

Keeps user data, user-installed apps, and OEM apps.

If the device is offline, the retire command will execute when it next checks in.

 Correct choice — exactly meets your requirements.

upvoted 1 times

KrisDeb 1 year, 5 months ago

Selected Answer: A

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 2 times

Pallieter 1 year, 5 months ago

Selected Answer: B

If you remove the device from intune the data is still there when the device comes back online again. Doesn't seem secure at all

upvoted 1 times

iamchoy 1 year, 5 months ago

Selected Answer: B

B. Retire action: The "Retire" (also known as "Remove company data") action removes company apps and data from a device. It leaves personal data and user-installed apps intact. This perfectly matches the requirement of eliminating Intune-provisioned apps/data while retaining personal/OEM data. If the device checks in after the Retire action, it will receive the command to remove company data.

upvoted 1 times

mehdyzaki 1 year, 6 months ago

Selected Answer: B

What each action does:

Action Description

A. Delete Removes the device from Intune immediately, but does not remove anything from the device. If the device checks in again, it might re-enroll unless blocked. Not sufficient.

 B. Retire Removes Intune-managed apps, policies, and company data, but leaves personal data, user-installed apps, and OEM apps intact. This is exactly what is required. Correct.

C. Fresh Start Reinstalls Windows and removes most apps—including OEM and user apps—but keeps user data. Too aggressive for the requirement.

D. Autopilot Reset Resets the device to a business-ready state and removes user data and settings. Not suitable here.

upvoted 2 times

NasX 1 year, 7 months ago

Selected Answer: A

I think the keyword here is delete "immediately". While retire does the what the questions asks for it does not remove the device from Intune until the device checks in to intune. But delete immediately removes the device from Intune.

This was confusing at first, but I have gone through both the documentations for Retire, Delete as well as Wipe.

Check this as it clearly says what I've mentioned:

https://learn.microsoft.com/en-us/intune/intune-service/remote-actions/devices-wipe#delete-devices-from-the-intune-admin-center:~:text=device%20still%20shows%20up%20in%20Intune%20until%20the%20device%20checks%20in.%20If%20you%20want%20to%20remove%20stale%20devices%20immediately%2C%20use%20the%20Delete%20action

upvoted 1 times

justITtopics 1 year, 8 months ago

Selected Answer: B

In order to accomplish with the maintaining of personal data, which is more important, I will vote for B. Retire.

Retire

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.

Effect of the Retire action on data that remains on the device

When you use the Retire device action, the user's personal data is not removed from the device.

upvoted 1 times

justITtopics 1 year, 8 months ago

Delete

Delete Will remove the device immediately, but you must to retain User-installed apps, personal data, and OEM-installed apps.

Review the effect of Delete action depending on the OS/Enrollment type:

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

Windows All RETIRE - All Profiles are deleted, work and school account is signed out

upvoted 1 times

Grimmgore 1 year, 8 months ago

Selected Answer: A

If you want to remove stale devices immediately, use the Delete action instead.

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

upvoted 1 times

Knight_Of_Peace 1 year, 8 months ago

Selected Answer: A

Retire action is included in Delete action but with immediate effect.

"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."

Ref:

https://learn.microsoft.com/en-us/mem/intune-service/remote-actions/devices-wipe#delete-devices-from-the-intune-admin-center:~:text=If%20you%20want%20to%20remove%20stale%20devices%20immediately%2C%20use%20the%20Delete%20action%20instead.

Please, check the following comment.

upvoted 2 times

Knight_Of_Peace 1 year, 8 months ago

"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."

"Windows All RETIRE - All Profiles are deleted, work and school account is signed out"

Ref:

https://learn.microsoft.com/en-us/mem/intune-service/remote-actions/devices-wipe#delete-devices-from-the-intune-admin-center:~:text=is%20signed%20out-,Windows,All%20Profiles%20are%20deleted%2C%20work%20and%20school%20account%20is%20signed%20out,-macOS

upvoted 1 times

br99mlpt 1 year, 8 months ago

Selected Answer: B

Simply the question required the device to check-in again. So it's retire instead of delete. https://learn.microsoft.com/en-us/answers/questions/1791950/remote-actions-in-intune

upvoted 1 times

HiddenQuest 1 year, 8 months ago

Selected Answer: A

To satisfy both requirements - 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. Select Delete. Why you may ask? Read carefully

Delete

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.

Retire

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.

Both requirements are met with delete action

upvoted 2 times

e6d6bf4 1 year, 7 months ago

This is an exact explanation from an MDM expert!

upvoted 1 times

RJTW070 1 year, 9 months ago

Selected Answer: B

The Retire action in Microsoft Intune removes company-managed apps and data while keeping user-installed apps, personal data, and OEM-installed apps intact. This aligns with the requirement to remove provisioned apps and data but retain personal and OEM-installed content.

If the device checks in again, Intune will still ensure company data is removed.

upvoted 2 times

Jz23 1 year, 9 months ago

Selected Answer: B

B. a Retire action

Explanation:

The Retire action in Intune removes company apps and data but retains user-installed apps, personal data, and OEM-installed apps.

If the device comes online again, Intune will still remove corporate data but won't fully wipe the device.

This fits your requirement of ensuring corporate apps and data are removed while keeping personal content intact.

Why not the other options?

A. Delete action: This removes the device from Intune immediately, but it does not trigger the removal of company apps and data if the device comes online again.

C. Fresh Start action: This reinstalls Windows while removing all apps except OEM-installed ones, which does not meet the requirement of keeping user-installed apps and data.

D. Autopilot Reset action: This resets the device to a business-ready state, removing all apps and settings, including personal data, which does not meet the requirement.

upvoted 2 times

7793 1 year, 9 months ago

Selected Answer: B

Retiring a device removes corporate data, apps, and configurations that were deployed via Intune, but user data and OEM-installed apps are not removed.

upvoted 12 times

StudyBM 1 year, 10 months ago

Selected Answer: B

Using the Delete option in Intune will remove the device from the Intune portal, but it does not automatically trigger the Retire action. The device will no longer appear in the Intune console, but it won't be unenrolled from Intune, and the management profile will remain on the device. This means that any apps and data provisioned by Intune will not be removed.

To ensure that the device is unenrolled from Intune and all Intune-provisioned apps and data are removed, you should use the Retire option2. This action will:

Remove the Intune management profile and policies from the device.

Remove any company apps and data installed by Intune.

Retain user-installed apps, personal data, and OEM apps.

upvoted 2 times

Grimmgore 1 year, 10 months 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 2 times

MacWilson 1 year, 11 months 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 1 year, 11 months 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 2 times

Omerozb 1 year, 11 months 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 3 times

Alboo007_rs007 1 year, 11 months ago

Selected Answer: A

A Delete Action * remove Device 1 immediately

upvoted 1 times

edo1803 1 year, 11 months ago

Selected Answer: B

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

upvoted 3 times

Sonia33 1 year, 11 months ago

Selected Answer: A

It is delete action the one that removes inmediatly 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 2 years 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 4 times

neothwin 2 years 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 2 years, 1 month 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 2 years, 2 months 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 2 years, 2 months ago

Selected Answer: B

B for retire

upvoted 2 times

daviis 2 years, 2 months 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 2 years, 2 months 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 2 years, 2 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 2 years, 2 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

ENGELHENDY 2 years, 3 months ago

Answer: B.

a Retire action: This is the correct choice as it removes Intune-managed data and settings while keeping user-installed apps and personal data intact.

upvoted 1 times

Leoweb 2 years, 3 months ago

Correct Answer is B, To remove Device1 from Intune while retaining user-installed apps, personal data, and OEM-installed apps, you should use the Retire action. This action allows you to remove devices from Intune that are no longer needed or are missing, while preserving the specified data and applications

upvoted 2 times

Bu5ter 2 years, 3 months ago

So I had a chat with ChatGPT on this and it clarified something for me. When you delete a device in Intune, it immediately removes any trace that the device was in Intune. In this scenario, we want to ensure the company data is removed if the device comes back online. If we were to delete the device, we would not be able to ensure that the data gets removed since it is no longer in Intune. This is what makes retiring the correct answer in my opinion.

upvoted 2 times

METAM 2 years, 2 months ago

ChatGPT:

The correct answer is C. Fresh Start.

Explanation:

The Fresh Start action in Microsoft Intune removes corporate apps and settings while keeping user-installed apps, personal data, and original equipment manufacturer (OEM) apps. This fits your requirement to remove apps and data provisioned by Intune while preserving user data and personal apps.

Other options, like deletion or retirement, do not ensure that corporate apps and data are removed if the device reconnects.

upvoted 2 times

AVN1711 2 years, 3 months ago

and now attention to the details come ahead , thy mentioned action Delete not a Wipe, and regarding MS it will only do next:..." You can use the Delete action to remove device records from the Azure portal for devices that you know are unreachable and unlikely to communicate with Azure again. The Delete action doesn't remove a device from management." I vote for B

upvoted 1 times

kiik32 2 years, 4 months ago

Selected Answer: A

when retiring removing company data from devices enrolled to entra is not supported.

upvoted 1 times

veliyath 2 years, 4 months ago

Selected Answer: A

The correct answer to remove Device1 from Intune immediately and ensure that any apps and data provisioned by Intune are removed (while retaining user-installed apps, personal data, and OEM-installed apps) is:

A. a Delete action

This action will immediately remove the device from Intune, and any company data will be removed the next time the device checks in.

upvoted 1 times

Maclouis116 2 years, 5 months ago

Selected Answer: B

Answer is B

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

Retiring the device wipes company data and apps leaving only the personal data and apps

upvoted 2 times

Maclouis116 2 years, 5 months ago

My apologies A is the correct answer we need to remove the device immediately therefore A is correct

upvoted 1 times

CJL324 2 years, 6 months ago

A

A. Delete action: This removes the device from Intune but does not remove any provisioned apps or data if the device checks in again.

B. Retire action: This removes managed apps, settings, and data provisioned by Intune while keeping user-installed apps, personal data, and OEM-installed apps.

upvoted 1 times

ten1ton 2 years, 7 months ago

I selected 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.

upvoted 1 times

RazielLycas 2 years, 7 months ago

Selected Answer: A

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

upvoted 1 times

slimmerik7 2 years, 8 months ago

Selected Answer: A

Only correct option is 'A - Delete'.

This will immediately remove the device from Intune (as requested) AND yes this will also remove all company data the next time the device checks in.

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

upvoted 2 times

zeos_ucok 2 years, 8 months ago

Selected Answer: A

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

Retire

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.

upvoted 1 times

Pollosor 2 years, 8 months ago

The "Delete" option practically formats the computer...

upvoted 1 times

Haider_Raza 2 years, 8 months ago

Selected Answer: B

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 Most Voted

B. a Retire action

C. a Fresh Start action

D. an Autopilot Reset action

upvoted 1 times

Krayzr 2 years, 8 months ago

Selected Answer: B

B, I belive it is B

upvoted 1 times

ckmay 2 years, 8 months ago

Selected Answer: A

In order to remove a stale device from the subscription, you need to use the delete action.

Retiring a device means it will remove the data, but it will still be visible in Intune.

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

upvoted 1 times

Darkfire 2 years, 9 months ago

Selected Answer: A

i'd go for A

Keyword: immediately

https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe#delete-devices-from-the-intune-admin-center:~:text=remove%20stale%20devices-,immediately,-%2C%20use%20the%20Delete

upvoted 1 times

MR_Eliot 2 years, 9 months ago

Selected Answer: A

Correct Answer Shoud Be A.

Deleting the device from intune, immediatly remove it from Intune, and next time device comes online, company data will be wiped.

upvoted 2 times

MR_Eliot 2 years, 9 months ago

I have tested this on a device. A is correct!

upvoted 2 times

Hekagros 2 years, 9 months ago

The correct answer is: "A" - delete

because the keyword in the question is "remove immediately"

The below article says: " 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

Blessing_ 2 years, 9 months ago

A 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.

upvoted 1 times

Merrybob 2 years, 9 months ago

Selected Answer: A

A. Delete

"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."

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

upvoted 2 times

mertak 2 years, 9 months ago

Selected Answer: B

Explanation

A retire action removes a device from Intune management and removes any apps and data provisioned by Intune. User-installed apps, personal data, and OEM-installed apps are retained. A retire action can be performed on devices that are offline for more than 30 days. References:

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

upvoted 2 times

Ksobier 2 years, 9 months ago

Removal happens the next time the device checks in and receives the remote Retire action. - It is not 'removed immediately' as states in the question.

It makes sense to use it in real live so you can see it for some.

upvoted 2 times

vijay0715 2 years, 9 months ago

Selected Answer: A

The delete action removes a device from the Intune portal immediately. It also sends a retire command to the device and 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

upvoted 2 times

frack 2 years, 10 months ago

Selected Answer: B

A retire action removes a device from Intune management and removes any apps and data provisioned by Intune. User-installed apps, personal data, and OEM-installed apps are retained. A retire action can be performed on devices that are offline for more than 30 days.

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

upvoted 4 times

Amir1909 2 years, 10 months ago

A is correct

upvoted 1 times

ushahid 2 years, 10 months ago

https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipeYou can configure Intune to automatically remove devices that appear to be inactive, stale, or unresponsive. These cleanup rules continuously monitor your device inventory so that your device records stay current. Devices deleted in this way are removed from Intune management. This setting affects all devices managed by Intune, not just specific ones.

When a device clean-up rule runs, it deletes the device from Intune. At that point, the device must go through a re-enrollment process in order for it to show up in the console.

Sign in to the Microsoft Intune admin center.

Choose Devices > Device cleanup rules > Yes.

In the Delete devices that haven't checked in for this many days box, enter a number between 30 and 270.

Choose Save.

upvoted 1 times

03038b8 2 years, 11 months ago

Selected Answer: B

Copilot answers

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

upvoted 1 times

Tonsku 2 years, 11 months ago

Selected Answer: B

User-installed apps, personal data, and OEM-installed apps must be retained.

What should you use? B. a Retire action

upvoted 1 times

arsh807 2 years, 11 months ago

It is A - Delete. Please visit the website - https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe. It clearly states : "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."

upvoted 1 times

Kevern 2 years, 11 months ago

Selected Answer: A

This should be A - retiring a device seems to need the device to check in before it starts with the retiring process, deleting a device will remove the device from Intune immediately and then retire it once it checks in

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

upvoted 2 times

belyo 2 years, 11 months ago

Selected Answer: A

deleted does the same as wipe upon device check-in, mostly depends on the enrollment type

i have 4 years experience with Intune on corporate environment 100k + devices, when you wipe, it will stay in MEM in pending state untill the device check-in, i have cases where wiped device stays there for weeks/months

i would go for A Although B does the same

upvoted 1 times

ThePrutser 2 years, 11 months ago

Selected Answer: A

Intune also retires a device when deleting it from the admin center. Key is that the question states to immediately remove it.

upvoted 1 times

mohdAj 2 years, 11 months ago

Selected Answer: A

A. Delete action

upvoted 1 times

iTomi 2 years, 11 months ago

Selected Answer: B

Retire action: This action marks the device as retired in Intune, and it initiates an unenrollment process on the device. When the device comes online, it will receive the retire command and perform an unenrollment, removing Intune management. This action helps retain user-installed apps, personal data, and OEM-installed apps while removing Intune-specific apps and settings.

upvoted 3 times

ThePrutser 2 years, 11 months ago

Last sentence is critical; a delete also retires a device:

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. 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.

upvoted 1 times

madsa 2 years, 11 months ago

It is B correct, remove the device immediately from management, and keeps OEM and user data.

upvoted 3 times

ThePrutser 2 years, 11 months ago

That is actually A you are explaining there.

upvoted 1 times

b0gdan433 2 years, 12 months ago

It's B, just took the exam today.

upvoted 2 times

chandravamsi 3 years ago

Selected Answer: C

Fresh Start Action - takes care of the device's previous data and user apps and If user returns they are retained

upvoted 1 times

iTomi 2 years, 11 months ago

This option is more applicable to Windows Autopilot and Windows 10 scenarios, and it reinstalls a clean, updated version of Windows while keeping user data intact. It's not designed for immediate removal from Intune.

upvoted 1 times

pinda 3 years ago

How does a fresh start delete the device?

upvoted 1 times

cpaljchc4 3 years ago

"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.)"

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

upvoted 3 times

Krayzr 3 years ago

Selected Answer: B

I think it is B "retire". I am no pro, but it says the user data/apps must be retained. A "delete' might remove all data, including user's stuff.

upvoted 2 times

NoursBear 3 years ago

https://karstenkleinschmidt.de/2020/09/09/intune-what-is-retire-wipe-delete-fresh-start-autopilot-reset/

upvoted 1 times

Soest009 3 years ago

The "Retire action" in Intune is designed to remove device management without wiping the device entirely. This action will unenroll the device from Intune and remove Intune-specific policies and settings but will not factory reset or wipe the device. User-installed apps, personal data, and OEM-installed apps will be retained. If the device checks in again after being retired, it will no longer receive Intune management.

upvoted 1 times

k24 3 years ago

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. This 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.

upvoted 1 times

kj2021 3 years, 1 month ago

Selected Answer: D

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.

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

upvoted 1 times

iamforksu 3 years, 1 month ago

Selected Answer: A

Delete removes it immediately and also performs the 'retire' functions.

upvoted 2 times

mhmyz 3 years, 1 month ago

Selected Answer: B

Retire action can remove Company apps and associated data installed by Intune.

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

upvoted 1 times

Contactfornitish 3 years, 1 month ago

Selected Answer: A

Only two actions remove the device from Intune/Azure AD - Retire or Delete. Retire removes the device object 180 days after retire action so Delete remains only option. Delete is only action which acts once the device checks in and remove corp data specifically and doesn't touch personal

upvoted 1 times

ansilva 3 years, 1 month ago

Theres contradictory statements in this questions. "Remove immediately" makes me think its also A but if the question also says "personal data must be retained" the only option that provides that is retire. Wiping the device removes both personal and company data which is not what the question stated as a requirement.

upvoted 1 times

Rocky83 3 years, 1 month ago

Selected Answer: A

Delete

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.

upvoted 2 times

zeos_ucok 3 years, 1 month ago

Selected Answer: B

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

When you use the Retire device action, the user's personal data is not removed from the device.

upvoted 1 times

pinda 3 years, 1 month ago

Selected Answer: B

The Retire action in Intune is designed to gracefully remove a device from management. When a device is retired, it will remove the company data and settings while preserving user data, personal apps, and OEM-installed apps. If the device checks in again, it won't trigger a wipe of user data and personal apps.

upvoted 2 times

pinda 3 years, 1 month ago

Selected Answer: B

"retire" removes the corperate date

upvoted 1 times

Thesa7 3 years, 1 month ago

For me it should be B "Retire". Intune Profile will be remove immediate at the same time, personal apps is retained.

upvoted 1 times

CheMetto 1 year, 6 months ago

From: https://learn.microsoft.com/en-us/intune/intune-service/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 2 times

LionelDerBoven 2 years, 2 months 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 3 times

OyYaGotta 2 years, 9 months ago

I agree it's a bad question that contradicts it's 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

ThePrutser 2 years, 11 months 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 17 times

ronct 3 years, 2 months ago

Retire:

The Retire action removes app data, settings, and Intune managed email profiles from the device12.

The device will still show up in Intune until the device checks in12.

Retire leaves users' personal data on the device2.

If your device has an Autopilot hash assigned (Zero Touch ID, ZTDID) it will NOT be deleted from Azure AD2.

Delete:

Delete performs the same tasks that Retire does3.

However, it removes the device from the Intune "All devices" list immediately3.

If you want to remove stale devices immediately, use the Delete action instead12.

answer is A Delete

upvoted 2 times

Grg433 3 years, 2 months ago

Selected Answer: B

I think as question mentioned - User-installed apps, personal data, and OEM-installed apps must be retained. - for this we can choose 'retire'

: The Retire action is specifically designed to retire the device from Intune management. When you retire a device, it unenrolls from Intune, and Intune removes the company data and apps that were deployed to the device while preserving user-installed apps, personal data, and OEM-installed apps.

upvoted 2 times

picho707 3 years, 2 months ago

Delete will remove corporate and personal data. A is not the right answer.

upvoted 1 times

Futfuyfyjfj 3 years, 1 month ago

Source?

As the question states "You need to remove Device1 from Intune immediately" I'd be inclined to go with option A as a delete yields: The next time the device checks in, any company data on it will be removed as Intune also retires a device when deleting it. https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe#delete-devices-from-the-intune-admin-center

upvoted 1 times

NoursBear 3 years, 2 months ago

A for me too

upvoted 1 times

VirtualJP 3 years, 2 months ago

Selected Answer: A

As the question states "You need to remove Device1 from Intune immediately" I'd be inclined to go with option A as a delete yields: The next time the device checks in, any company data on it will be removed as Intune also retires a device when deleting it.

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

upvoted 3 times

VirtualJP 3 years, 1 month ago

I am incorrect as I did not read the question properly.

It states "User-installed apps, personal data, and OEM-installed apps must be retained."

For this outcome, the answer would have to be "B"

upvoted 2 times

letters1234 3 years, 2 months ago

Selected Answer: A

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

"If you want to remove stale devices immediately, use the Delete action instead."

Otherwise, the device will stay in Intune console till your configured cleanup rule.

upvoted 2 times

krzysztofbr 3 years, 2 months ago

please read carefully question " The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed"

answer B

upvoted 7 times

Futfuyfyjfj 3 years, 2 months ago

Reply carefully please:

From https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe " If you want to remove stale devices immediately, use the Delete action instead" "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."

upvoted 2 times

RAJKPB 3 years, 2 months ago

Selected Answer: A

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.

If you want to remove stale devices immediately, use the Delete action instead.

Delete will also issue the retire command but it will remove the device from the All devices list immediately

upvoted 2 times

moshkoshbgosh 3 years, 3 months ago

Selected Answer: A

The requirement is immediate removal, so I would choose A instead.

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

" If you want to remove stale devices immediately, use the Delete action instead"

"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."

upvoted 2 times

krzysztofbr 3 years, 2 months ago

NO, retire will be exactly the same fast as Wipe. and You will not erase personal data.

upvoted 2 times

Futfuyfyjfj 3 years, 2 months ago

Retire won't delete the device immediatly as required

upvoted 1 times

krzysztofbr 3 years, 3 months ago

answer B correct

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

upvoted 1 times

Futfuyfyjfj 3 years, 2 months ago

From https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe " If you want to remove stale devices immediately, use the Delete action instead" "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."

upvoted 1 times

Question #16 *Topic 1*

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 (96%) (4

krzysztofbr Highly Voted 3 years, 3 months ago

D seems correcthttps://learn.microsoft.com/en-us/mem/analytics/startup-performance

upvoted 10 times

krzysztofbr 3 years, 3 months ago

D seems correct

upvoted 9 times

Futfuyfyjfj Highly Voted 3 years, 2 months ago

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

upvoted 10 times

jaba2050 7 months, 1 week ago

B is correct B. Intune Data Warehouse Used for raw data extraction and reporting Designed for: Power BI Historical reporting Not used directly to review startup or restart performance

upvoted 1 times

HueCumber Most Recent 7 months ago

 B. Intune Data Warehouse Used for raw data extraction and reporting Designed for: Power BI Historical reporting Not used directly to review startup or restart performance

upvoted 1 times

budekzkie 1 year, 2 months ago

D is correct. Key Insights Available in Endpoint Analytics 1 Startup Performance 2 Application Reliability 3 Work from Anywhere 4 Battery Health 5 Endpoint Scores 6 User Experience Metrics

upvoted 2 times

veliyath 2 years, 4 months ago

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 2 years, 6 months ago

Answer D

upvoted 1 times

Haider_Raza 2 years, 8 months ago

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 2 years, 9 months ago

Answer is correct

upvoted 2 times

Darkfire 2 years, 9 months ago

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 2 years, 11 months ago

review the startup times and restart frequencies of the devices. D. Endpoint analytics

upvoted 2 times

mohdAj 2 years, 11 months ago

D. Endpoint analytics

upvoted 1 times

iTomi 2 years, 11 months ago

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 2 years, 12 months ago

D is correct.

upvoted 2 times

zeos_ucok 3 years ago

D is correct https://learn.microsoft.com/en-us/mem/analytics/restart-frequency?source=recommendations

upvoted 2 times

Gentlemanners 3 years ago

D is the correct answer, you can view the start-up preformance in Endpoint Analytics. https://learn.microsoft.com/en-us/mem/analytics/startup-performance

upvoted 2 times

pinda 3 years, 1 month ago

Correct

upvoted 3 times

Question #17 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription.

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

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

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
User experience settings	
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

Answer Area

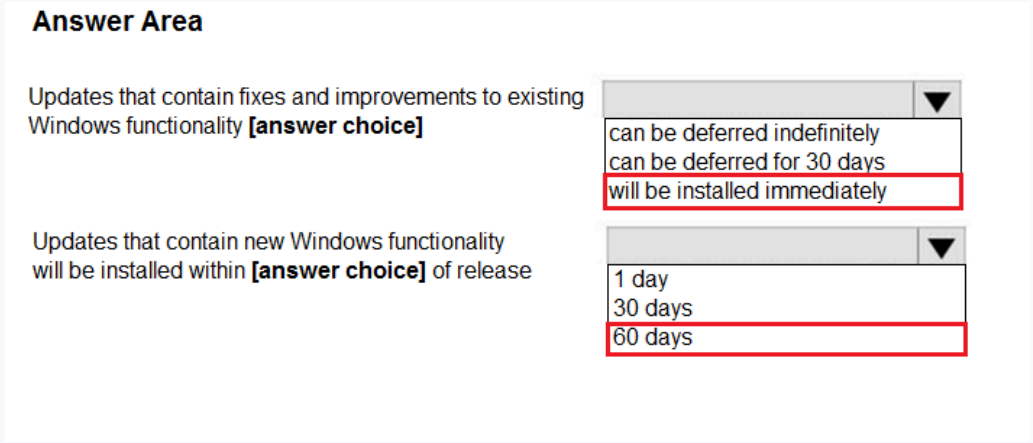
Updates that contain fixes and improvements to existing Windows functionality **[answer choice]**

- 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

Suggested Answer:



Contactfornitish Highly Voted 3 years, 1 month 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-policiesquality updates, deadline 0 days, 0 deferral day = immediately deadline 30 days plus 30 deferral days = 60daysI guess that the Feature Updates will only be available on the machine 30 days after releaseing 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 24 times

Contactfornitish Highly Voted 3 years, 1 month 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 22 times

ollyijeh Most Recent 2 months, 2 weeks ago

This is a trick question, the first answer is definitely 'immediately' but the feature updates can be deferred for 30 days AND have a deadline of another 30 days.

upvoted 2 times

muzufx 11 months ago

I also thought about the fact that the hard deadline for the FU is only 30 days and that the answer shall be 30 days.

However, going back to read the question and the requirements, it tells you --->>

Updates that contain new Windows functionality will be installed within __ of "release".

so most definitely the "release" word relates to when Microsoft released the update and not when said update is available for the workstation.

i suppose MS wants us NOT to make assumptions and go directly to the most acceptable answer.

upvoted 1 times

greatsparta 1 year, 2 months ago

I don't think it's 60 days but rather 30. My reasoning being that the question asks “Updates that contain new Windows functionality will be installed within”. That’s referring to the deadline, not the deferral. So while the full lifecycle can be 60 days, the installation window, once the update is available is 30 days.

upvoted 1 times

henil_154762 1 year, 3 months ago

immediately and 60 days That wording is specifically about when the update is offered and installed automatically if no action is taken, based on deferral, not the full forced install deadline.

upvoted 1 times

henil_154762 1 year, 3 months ago

immediately and 60 days That wording is specifically about when the update is offered and installed automatically if no action is taken, based on deferral, not the full forced install deadline.Ans is immediately and 30 daysMy bad Ans is 60 Days correct

upvoted 1 times

henil_154762 1 year, 2 months ago

My bad Ans is 60 Days correct

upvoted 2 times

henil_154762 1 year, 3 months ago

Ans is immediately and 30 days

upvoted 1 times

henil_154762 1 year, 3 months ago

Ans is immediately and 30 daysMy bad Ans is 60 Days correct

upvoted 1 times

SandipChauhan 1 year, 3 months ago

Thanks

upvoted 1 times

Parvezg 1 year, 6 months ago

It should be immediately and 60 days. If the option is given 31 days would be correct if given in the option as the question says (within and not after) so 30 days can't be true. Only option is left beyond 30 days is 60 days.

upvoted 1 times

CliffyNitsef 1 year, 5 months ago

I am sharing this clip that would help implementing this policy. https://www.youtube.com/watch?v=ChPSbXA3XpMThanks

upvoted 1 times

CliffyNitsef 1 year, 5 months ago

I am sharing this clip that would help implementing this policy.

https://www.youtube.com/watch?v=ChPSbXA3XpM

upvoted 1 times

hieunm2411 1 year, 10 months ago

Answer is incorrect.

Configuration:

Feature update deferral period: 30 days

Deadline for feature updates: 30 days

Workflow:

April 1: Microsoft releases a new feature update.

May 1: The feature update becomes visible to devices (due to the 30-day deferral period).

May 30: Devices must install the update by this date (30 days after it becomes visible).

After May 30: If the update hasn't been installed, it is enforced, and the device restarts as needed.

Important Notes:

The deferral period acts as a buffer before devices even know about the update.

The deadline ensures timely installation after the update becomes visible.

upvoted 2 times

veliyath 2 years, 4 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 6 times

Victor3 3 months ago

This is correct. https://learn.microsoft.com/en-us/windows/deployment/update/wufb-compliancedeadlines?tabs=w11-22h2-policy%2Cw11-23h2-notifications

"The deadline calculation for both quality and feature updates is based off the time when the client initially discovered the update through scan."

Microsoft releases new features update 0 day, deferred for 30 days, must install after 30 days. Not 30 deferred days + 30 deadline days. Correct answer is 30 days.

upvoted 1 times

slimmerik7 2 years, 8 months 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 2 times

Burkidur 2 years, 8 months 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 2 years, 9 months ago

Answer is correct.Not correct. After further evaluation, the answer should be 60 days. Update is deffered 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 2 times

MR_Eliot 2 years, 9 months ago

Answer is correct.

upvoted 2 times

MR_Eliot 2 years, 8 months ago

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

Update is deffered 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 2 years, 9 months 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 2 years, 9 months ago

Answer is correct

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

upvoted 4 times

Merrybob 2 years, 9 months 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 2 years, 11 months 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 2 years, 11 months ago

immediately and 60 days quality update deferral periode 0 day feature update deferral periode 30 days + deadline for feature update 30 daysi am wrong, it should be immediately and 30 days deferral periode

upvoted 4 times

Tonsku 2 years, 11 months ago

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

upvoted 4 times

iTomi 2 years, 11 months 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 2 years, 12 months ago

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

upvoted 2 times

b0gdan433 2 years, 12 months ago

It's 30 days, i just took the exam today and got the 2 points.B...S..., MS / Pearson doesn't reveal how many points you get each question.MS Pearson exam does not release the answer at all. U will only able to see your total score.

upvoted 2 times

Murad01 2 years, 9 months ago

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

upvoted 2 times

iTomi 2 years, 11 months ago

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

upvoted 10 times

Anonymous 3 years 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

HvD 2 years, 2 months ago

I guess that the Feature Updates will only be available on the machine 30 days after releaseing 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 2 years, 9 months ago

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

deadline 30 days plus 30 deferral days = 60days

upvoted 13 times

Rocky83 3 years, 1 month 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 3 years, 2 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 2 years, 11 months 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 3 years, 2 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 3 years, 2 months ago

answer is correct

upvoted 2 times

Sprocket10 3 years, 3 months ago

Immediately and 30 days seems correct to me.

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

upvoted 3 times

Buzl 3 years, 3 months ago

I think second box should be 60 days: deferral of 30 days for feature updates and then needs to be installed within the next 30 days

upvoted 3 times

volto 3 years, 3 months ago

Deadline for updates means "Specifies the number of days a user has before (...) updates are installed on their devices automatically."

upvoted 1 times

Question #18 *Topic 1*

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.

Which events are collected in the Log Analytics workspace?

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

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: *E*

Community vote distribution



mhmyz Highly Voted 3 years, 1 month 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 18 times

mhmyz Highly Voted 3 years, 1 month ago

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=portalyes 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.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%20and%20other%20Azure%20services%2C%20such%20as%20Microsoft%20Sentinel%20and%20Microsoft%20Defender%20for%20Cloud.Should be the key be the statement in the question, " The workspace is configured to collect all available events from the Windows event logs". The E is the correct answer.My bad, there is no Audit log in Windows Events, so D is correct.I mean Azure agent doesn't collect that

upvoted 18 times

NoursBear 2 years, 11 months 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.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%20and%20other%20Azure%20services%2C%20such%20as%20Microsoft%20Sentinel%20and%20Microsoft%20Defender%20for%20Cloud.Should be the key be the statement in the question, " The workspace is configured to collect all available events from the Windows event logs". The E is the correct answer.My bad, there is no Audit log in Windows Events, so D is correct.I mean Azure agent doesn't collect that

upvoted 1 times

NoursBear 2 years, 11 months 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 2 years, 8 months 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%20and%20other%20Azure%20services%2C%20such%20as%20Microsoft%20Sentinel%20and%20Microsoft%20Defender%20for%20Cloud.Should be the key be the statement in the question, " The workspace is configured to collect all available events from the Windows event logs". The E is the correct answer.My bad, there is no Audit log in Windows Events, so D is correct.I mean Azure agent doesn't collect that

upvoted 1 times

NSA_Poker 2 years, 8 months 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%20and%20other%20Azure%20services%2C%20such%20as%20Microsoft%20Sentinel%20and%20Microsoft%20Defender%20for%20Cloud.

upvoted 1 times

SajjH 2 years, 3 months 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". The E is the correct answer.

upvoted 1 times

SajjH 2 years, 3 months 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". The E is the correct answer.My bad, there is no Audit log in Windows Events, so D is correct.I mean Azure agent doesn't collect that

upvoted 1 times

SajjH 2 years, 3 months ago

My bad, there is no Audit log in Windows Events, so D is correct.I mean Azure agent doesn't collect that

upvoted 1 times

SajjH 2 years, 3 months ago

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

upvoted 1 times

SajjH 2 years, 3 months ago

I mean Azure agent doesn't collect that

upvoted 1 times

letters1234 3 years, 2 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 17 times

letters1234 3 years, 2 months ago

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.Why D (1, 2, and 4 only) is incorrect Answer D excludes Event 3, which is: Log: Security Type: Audit Success Computer: Computer2 Why that exclusion is invalid On MD-102: Security logs ARE Windows event logs Audit Success IS a valid Security log level Azure Log Analytics does not auto-exclude Security/Audit events when “all available events” is enabled Therefore, Event 3 must be collected. Any answer that omits Event 3 is automatically wrong.

upvoted 17 times

HueCumber 7 months ago

Why D (1, 2, and 4 only) is incorrect Answer D excludes Event 3, which is: Log: Security Type: Audit Success Computer: Computer2 Why that exclusion is invalid On MD-102: Security logs ARE Windows event logs Audit Success IS a valid Security log level Azure Log Analytics does not auto-exclude Security/Audit events when “all available events” is enabled Therefore, Event 3 must be collected. Any answer that omits Event 3 is automatically wrong.

upvoted 1 times

9e82800 6 months, 2 weeks ago

When Log Analytics is configured to collect all events, it ingests every event from: Application log System log Security log Any other enabled Windows event log

upvoted 1 times

xdb 7 months, 2 weeks ago

the correct answer should be 2,3 and 4 only. but that option isn't there application Success doesn't exist. https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-windows-events

upvoted 2 times

Le_Patriarche2025 9 months ago

I think it's E

upvoted 2 times

moluccanvibe 9 months, 2 weeks ago

When a Windows 10 device sends events to an Azure Log Analytics workspace, Security events are not collected by default, even if the workspace is set to “collect all available events.” Security events require additional configuration (Azure Security Center / Defender for Cloud, or the legacy MMA Security baseline).

upvoted 1 times

MichinelliM 11 months, 1 week ago

Audit Success is not an event collectible

upvoted 1 times

henil_154762 1 year, 2 months ago

Selected Answer: D

D. 1, 2, and only 4

upvoted 1 times

Alaeddine100 1 year ago

Étant donné que la question précise que «the workspace is configured to collect all available events from the Windows event logs», je penche pour E. car cela suggère que la configuration couvre aussi le journal de sécurité (événement 3)

upvoted 1 times

Robert69 1 year, 1 month ago

When you configure an Azure Log Analytics workspace to collect all available events from the Windows event logs, it will collect events from all the standard Windows event log categories, including: Event 1 - Application/Success ✓ Event 2 - System/Information ✓ Event 3 - Security/Audit Success ✓ Event 4 - System/Error ✓

upvoted 2 times

henil_154762 1 year, 2 months ago

D. 1, 2, and only 4Security log events are not collected by this data source with the legacy Log Analytics agent; Security events require Defender for Cloud / Sentinel or collection via the Azure Monitor Agent (AMA) with a DCR. So Event 3 (Security – Audit Success) is excluded

upvoted 1 times

theptr 1 year, 5 months ago

Selected Answer: D

Event 3 (Security - Audit Success) → Not collected unless explicitly enabled

upvoted 2 times

henil_154762 1 year, 2 months ago

Security log events are not collected by this data source with the legacy Log Analytics agent; Security events require Defender for Cloud / Sentinel or collection via the Azure Monitor Agent (AMA) with a DCR. So Event 3 (Security – Audit Success) is excluded

upvoted 1 times

hvastija 1 year, 3 months ago

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

upvoted 2 times

theptr 1 year, 5 months ago

Event 3 (Security - Audit Success) → Not collected unless explicitly enabledThe question states "The workspace is configured to collect all available events from the Windows event logs." So it is enabled

upvoted 2 times

MSBITSM Most Recent 4 months, 2 weeks ago

The question states "The workspace is configured to collect all available events from the Windows event logs." So it is enabled

upvoted 1 times

8choxo 1 year, 5 months ago

"Success" is not an event log type

upvoted 1 times

fabioperosa 1 year, 5 months ago

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

upvoted 2 times

Alboo007_rs007 1 year, 11 months ago

Selected Answer: D

1. 2 .4 Only

upvoted 1 times

dc0223a 1 year, 6 months ago

Answer: E Explanation All events from Windows event logs are collected in the Log Analytics workspace, regardless of the event level or source. Therefore, events 1, 2, 3, and 4 are all collected in the workspace. References: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events

upvoted 2 times

HiddenQuest 1 year, 8 months ago

The question is 'Which events are collected in the Log Analytics workspace?' Answer - Application + System + Security Events Therefore 1,2,3 and 4 is correct If you're thinking hmmm there is no Application Success event log type. Notice there is no option to select 2,3 and 4

upvoted 3 times

TedEx2 1 year, 11 months ago

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 2 times

Question #19 *Topic 1*

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 (98%) 2

letters1234 Highly Voted 3 years, 2 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 37 times

ModernoDecor 8 months, 3 weeks ago

Selected Answer: D

Outdated question. It's now under Device Configuration profile > Win10 or later > Templates > Kiosk > Configuration Settings

upvoted 2 times

MSBITSM Most Recent 4 months, 2 weeks ago

What has Windows to do with this question? It clearly states Android Enterprise devices

upvoted 1 times

fayawax 1 year, 1 month ago

Selected Answer: A

D. Device experience

upvoted 1 times

manoj2020 1 year, 1 month ago

Selected Answer: D

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

upvoted 2 times

ModernoDecor 8 months, 3 weeks ago

Selected Answer: D

Outdated question. It's now under Device Configuration profile > Win10 or later > Templates > Kiosk > Configuration Settings

upvoted 2 times

Dinkan 1 year, 2 months ago

Selected Answer: D

https://cloudclients.co.uk/2022/05/android-enterprise-single-app-kiosk-with-intune/

upvoted 1 times

iamchoy 1 year, 11 months 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 2 years, 4 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 2 years, 4 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

MR_Eliot 2 years, 9 months ago

Selected Answer: D

D is correct. I do MDM for a living

upvoted 8 times

Darkfire 2 years, 9 months 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 2 years, 10 months ago

Correct

upvoted 1 times

mohdAj 2 years, 11 months ago

Selected Answer: D

D. Device experience

upvoted 2 times

NoursBear 3 years, 2 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

NoursBear 3 years, 2 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

Futfuyfyjfj 3 years, 2 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 3 years, 2 months ago

D is correct. This is located unter "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 3 years, 2 months ago

Selected Answer: D

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

upvoted 1 times

letters1234 Highly Voted 3 years, 2 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 37 times

krzysztofbr 3 years, 2 months ago

thanks for this comment i agree

upvoted 6 times

krzysztofbr 3 years, 2 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

Question #20 *Topic 1*

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.

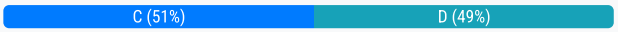
B. From the Microsoft Intune admin center, create a security baseline.

C. Install Defender for Endpoint on the macOS devices.

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

Suggested Answer: *D*

Community vote distribution



ronct Highly Voted 3 years, 2 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.I agree. The answer is C.

upvoted 40 times

ronct Highly Voted 3 years, 2 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 39 times

ollyijeh Most Recent 2 months, 2 weeks ago

Selected Answer: D

Mac's don't have Defender for Endpoint installed at base, so it can't be anything else other than C. Once @Defender for endpoint is installed only then CAN it receive any policies you create

upvoted 2 times

HueCumber 7 months ago

Selected Answer: C

 Why C. Install Defender for Endpoint on the macOS devices is correct

-Microsoft Defender for Endpoint is not built into macOS

-Intune security policies do not install Defender automatically

-Once installed:

-----The macOS devices automatically onboard to Defender for Endpoint

-----Intune can apply Defender AV / endpoint security policies

-At scale (500 devices), this can be done via:

-----Intune app deployment (PKG)

-----Existing MDM workflows

➡ Installing Defender is the minimum required action to make policies work at all.

upvoted 4 times

BossAceVentura 3 years, 3 months ago

C wont minimize admin effort Answer is D

upvoted 13 times

BossAceVentura 3 years, 3 months ago

C wont minimize admin effort Answer is DMacs 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).You can install Defender for Endpoint by using configuration profile.

upvoted 13 times

a5f91f0 7 months, 1 week ago

Selected Answer: C

The correct answer is C. Install Defender for Endpoint on the macOS devices.

upvoted 2 times

Burkidur 2 years, 8 months 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

a5f91f0 7 months, 1 week ago

Selected Answer: C

The Breakdown

While it might seem counterintuitive to "minimize effort" by installing software, this is a hard technical prerequisite. Antivirus policies in Microsoft Intune (located under Endpoint Security) function by sending configurations to the Microsoft Defender for Endpoint agent on the device.

upvoted 2 times

jaba2050 7 months, 1 week ago

Selected Answer: D

For macOS management in Intune, the Settings Catalog is often the easiest way to find and configure all available Microsoft Defender settings in one place, significantly reducing administrative effort compared to manual .plist file uploads.

upvoted 1 times

xdb 7 months, 2 weeks ago

Selected Answer: D

D is correct see

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

step 12 is to install defender otherwise defender will not be setup correctly

upvoted 1 times

epyonkills 8 months, 1 week ago

Selected Answer: C

but doesn't deploy Defender itself.

Correct choice: C. Install Defender for Endpoint on the macOS devices.

upvoted 1 times

Djonzi 8 months, 1 week ago

Selected Answer: C

First you need to install Defender.

upvoted 1 times

ModernoDecor 8 months, 3 weeks ago

Selected Answer: C

Microsoft Defender for Endpoint must be installed on MacOS device.

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

upvoted 1 times

Le_Patriarche2025 9 months ago

Selected Answer: C

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

upvoted 1 times

moluccanvibe 9 months, 2 weeks ago

Selected Answer: C

You can use configuration profiles to onboard Defender, but that alone doesn’t install Defender. The Defender app must be installed first.

upvoted 1 times

Quink 10 months, 3 weeks ago

Selected Answer: D

This is a very typical Microsoft set of answers to choose from.

The correct answer is D. You can use a custom configuration profile to onboard MacOS devices in Defender, this will also install Defender. You can then use a settings catalog to configure Defender.

Answer C is an answer they put in to set you on the wrong foot and people who look at every question in a very semantic way will fall for that trap. By looks of the discussion here, it works very well... 'Install Defender on all MacOS devices' is a way too vague answer for Microsoft to be used as a correct answer, they usually want it a bit more specific than that. It's also not catering to the requirement to minimize effort as it does not state how to install Defender.

Usually, in any MS exam, when the question states 'with minimal effort', the answer is using a feature from within the tool you are examed about.

upvoted 5 times

Alaeddine100 1 year ago

Selected Answer: D

D

Parce que la question insiste sur la réduction de l’effort administratif, les profils de configuration dans Microsoft Intune permettent de déployer Defender et d’appliquer les stratégies à grande échelle sans installation manuelle.

upvoted 3 times

Robert69 1 year, 1 month ago

Selected Answer: C

To apply Microsoft Defender for Endpoint antivirus policies to macOS devices through Intune, you must first have Defender for Endpoint installed on those devices. Once installed, you can then manage and deploy antivirus policies directly from the Microsoft Intune admin center.

upvoted 1 times

Mohamed555 1 year, 1 month ago

Selected Answer: C

Answer: C. Install Defender for Endpoint on the macOS devices

upvoted 1 times

fayawax 1 year, 1 month ago

Selected Answer: C

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

Before creating the system configuration profiles, the Overview step include "Deploy the Microsoft Defender for Endpoint on macOS application"

upvoted 1 times

Dinkan 1 year, 2 months ago

Selected Answer: C

You can create and assign Microsoft Defender for Endpoint antivirus policies to the macOS device, but to get them applied, you need to install MDE.

upvoted 1 times

henil_154762 1 year, 3 months ago

Selected Answer: C

Ans is C

Microsoft Defender for Endpoint (MDE) is not preinstalled on macOS like it is on Windows 10/11.

Before Intune can push antivirus policies (or EDR, attack surface reduction, etc.) to a macOS device, the MDE agent must be installed and onboarded.

The "configuration profile" in Intune (D) is used to configure MDE after the product is installed — it does not install Defender by itself.

upvoted 1 times

theptr 1 year, 4 months ago

Selected Answer: C

C is the correct answer

upvoted 1 times

theptr 1 year, 5 months ago

Selected Answer: C

Install Defender for Endpoint on the macOS devices first

upvoted 1 times

HiddenQuest 1 year, 8 months ago

Selected Answer: C

Answer is C. To pass these test you have to be able to read through the noise. What is the objective? 'You need to ensure that you can APPLY Microsoft Defender for Endpoint antivirus POLICIES to the macOS devices'. You can't APPLY the policy until MDE is installed.

upvoted 3 times

ExamBud 1 year, 8 months ago

Selected Answer: C

I think it is C, but using Intune (it doesn't say you need to manually install the app). Installing the app is needed for onboarding the devices to Defender for Endpoint.

upvoted 1 times

sorinaccio 1 year, 8 months ago

Selected Answer: C

C. Install Defender for Endpoint on the macOS devices.

upvoted 1 times

JunetGoyal 1 year, 9 months ago

Selected Answer: C

To apply Microsoft Defender for Endpoint (MDE) antivirus policies to macOS devices, Defender for Endpoint must first be installed on the devices. Without the installation, the policies cannot be enforced. Once MDE is installed, you can then manage security settings through Microsoft Intune or security baselines.

upvoted 1 times

GoombaLMAO 1 year, 9 months ago

Selected Answer: D

D

First section of deploying Defender for endpoint on a macOS is to "Create System configuration Profiles"

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

upvoted 3 times

HiddenQuest 1 year, 8 months ago

While that may be true, the question is not about deploying Defender for endpoint on a macOS, it's ENSURING that you can APPLY Microsoft Defender for Endpoint antivirus POLICIES to the macOS devices. Which solution minimizes that administrative effort (C)

upvoted 1 times

StudyBM 1 year, 10 months ago

Selected Answer: D

I think I understand the confusion here. It is true Defender for Endpoint needs to be installed first, but, in order to do so, a configuration profile would be created/used to install Defender for Endpoint on all 500 devices, as doing it manually would not minimise efforts. This is a trick question

upvoted 6 times

ITExperts 1 year, 10 months ago

Selected Answer: C

need to first install the app

upvoted 1 times

vfnj 1 year, 10 months ago

Selected Answer: D

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

upvoted 1 times

OHMSS 1 year, 11 months 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 1 year, 11 months ago

Selected Answer: C

Microsoft portals and tests says its C

upvoted 2 times

Tr619899 2 years 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 3 times

AleFCI1908 2 years 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 2 years, 1 month 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 2 years, 2 months 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 2 years, 2 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 2 years, 2 months 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 2 years, 4 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 2 years, 5 months ago

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

upvoted 3 times

CJL324 2 years, 6 months 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 2 years, 7 months 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 2 years, 7 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 2 years, 7 months ago

Selected Answer: C

Answer is C

upvoted 1 times

Shawn_Chen 2 years, 8 months ago

C. To apply configured Microsoft Defender for Endpoint antivirus policies to macOS devices, you must install Microsoft Defender for Endpoint on macOS.

upvoted 1 times

Sssssg 2 years, 8 months ago

Who writes these questions. The wording is really bad. Questions should be easy and clear. Anyways, my answer is C.

upvoted 2 times

MR_Eliot 2 years, 9 months ago

Selected Answer: C

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

Keyword apply. So the policies are already there. You only need to install Defender for endpoint on the computer to recieve and onboard the macbook devices.

So, my answer is C.

upvoted 4 times

Vukosir 2 years, 6 months ago

thank you very much for your comment, I search for your comment each time i o not understand the answer

upvoted 2 times

Krayzr 2 years, 9 months ago

Selected Answer: C

Bing AI says C is first and most important

upvoted 2 times

Merrybob 2 years, 9 months ago

Selected Answer: D

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

The very first step to install Defender for macOS is to create a Configuration Profile. Ref: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-install-with-intune?view=o365-worldwide#create-system-configuration-profiles

upvoted 4 times

sbermejor 2 years, 11 months ago

D

Before deploying the App we need to deploy the onboarding package by using a configuration profile.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-install-with-intune?view=o365-worldwide

https://www.youtube.com/watch?v=VHKyYeRkArI&list=PLZ8cmQe-R7Hb_kuV24zW1G-6vDtmOgaoQ&index=12

upvoted 3 times

yosry 2 years, 11 months ago

Selected Answer: C

the question is to ensure that you can apply Microsoft Defender for Endpoint antivirus policies.

so we need to ensure that Microsoft defender for endpoint is installed before applying said policies.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac?view=o365-worldwide

upvoted 3 times

mohdAj 2 years, 11 months ago

Selected Answer: C

C Installing Defender for Endpoint on macOS Devices:

Microsoft Defender for Endpoint for macOS is a separate installation that needs to be deployed on each macOS device. Once installed, it integrates with Microsoft Defender Security Center and can be managed through Microsoft Intune.

https://www.google.com/search?q=Installing+Defender+for+Endpoint+on+macOS+Devices&oq=Installing+Defender+for+Endpoint+on+macOS+Devices&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIKCAEQIRgWGB0YHtIBBzQ3N2owajeoAgCwAgA&sourceid=chrome&ie=UTF-8#fpstate=ive&vld=cid:5185ac1e,vid:M2mSCTrYgCY,st:0

upvoted 2 times

iTomi 2 years, 11 months ago

Selected Answer: C

Installing Defender for Endpoint on the mac, you ensure that you can apply antivirus policies. Without installation policies are useless.

upvoted 3 times

Temptset 3 years, 1 month ago

Selected Answer: D

The answer has to be "D":

- Installing the client app (MDE) manually results in administrative overhead

- MDE can be deployed through the Intune portal by adding the app: MDE (macOS)

- Configuration policy does NOT equal to the configuration of MDE antivirus policies

Theoretically, this means you should NOT install the app (manually) due to administrative overhead it would cause, hence you should use Microsoft Intune to deploy the app like any other app through the portal (add app).

Secondly, the most important key takeaway, even if you would install the MDE client app and have MDE antivirus policies configured, the policy still wouldn't apply, because a configuration profile is required (for licensing purposes). The following documentation proves this:

upvoted 6 times

Temptset 3 years, 1 month ago

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-install-with-intune?view=o365-worldwide

To add the cherry on top for your own visualization, go to "Dean Ellerby MVP"'s YT account and watch both videos on MDE posted on the 18th and 21th of August 23.

upvoted 3 times

nayf87 1 year, 5 months ago

I agree. The answer is C.

upvoted 7 times

Burkidur 2 years, 8 months 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 2 years, 3 months ago

You can install Defender for Endpoint by using configuration profile.

upvoted 5 times

ZaFletch 3 years, 3 months ago

Selected Answer: D

The question asks to make sure you can apply policies to Defender.

In theory that will require C and D, if defender is not installed it can't apply policies.

If only one option is allowed then D, C on it's own won't allow policy, just installs the app.

D can apply policies, they'll have no effect if the app is not present but they will apply. Wording of the question implies that defender may already be installed.

It's a poorly phrased question but D seems the best answer.

upvoted 7 times

Gr8Greet 3 years, 3 months ago

Selected Answer: D

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac

On macOS 11 (Big Sur) and above, Microsoft Defender for Endpoint requires additional configuration profiles. If you are an existing customer upgrading from earlier versions of macOS, make sure to deploy the additional configuration profiles listed on New configuration profiles for macOS Big Sur and newer versions of macOS.

upvoted 3 times

Futfuyfyjfj 3 years, 2 months ago

But the question states:

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

So it’s not a matter of HOW to apply them (which config type i.e.) but how you can ENSURE that you CAN apply them. In this case I would say C, without the client you can’t apply anything. Need to admit it’s a vague question

upvoted 4 times

Question #21 *Topic 1*

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: *D, E*

Community vote distribution



deinth Highly Voted 3 years, 2 months ago

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 antiviurs D: https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#microsoft-defender-antivirusDE is the Answer D:Microsoft Defender Antivirus: Device config-Device Restrictions- It has 28-34 settings for Antivrus. E: Microsoft Defender Firewall- Device config- Endpoint Protection (Global settings, netwok settings, Firewall rules) I have cross checked the lab. THe Endpoint Protection does not have the option for MS Defender Antivirus.Checked this in Intune and DE is the only correct aswer!

upvoted 38 times

deinth Highly Voted 3 years, 2 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 antiviurs D: https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#microsoft-defender-antivirus

upvoted 38 times

pnxrq69 Most Recent 2 weeks ago

Selected Answer: DE

It's D and E. The Microsoft Defender Antivirus is configured through Device restrictions. Firewall = Enpoiint protection

upvoted 1 times

SalonaSahni 3 years, 2 months ago

DE is the Answer D:Microsoft Defender Antivirus: Device config-Device Restrictions- It has 28-34 settings for Antivrus. E: Microsoft Defender Firewall- Device config- Endpoint Protection (Global settings, netwok settings, Firewall rules)

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

upvoted 11 times

SalonaSahni 3 years, 2 months ago

DE is the Answer D:Microsoft Defender Antivirus: Device config-Device Restrictions- It has 28-34 settings for Antivrus. E: Microsoft Defender Firewall- Device config- Endpoint Protection (Global settings, netwok settings, Firewall rules) I have cross checked the lab. THe Endpoint Protection does not have the option for MS Defender Antivirus.Checked this in Intune and DE is the only correct aswer!

upvoted 11 times

ThomasE 1 month, 1 week ago

Selected Answer: DE

Firewall is DEFINITELY configured thru Endpoint Protection. However, I only see options to configure the firewall, think enabling on or off for the different profiles, in Device Restrictions. The Endpoint Protection template only seems to have settings to allow users to have access to the Virus and threat protection areas.

upvoted 1 times

MaryndenOuden 3 months, 3 weeks ago

Selected Answer: CE

The correct answers are C and E, because both Microsoft Defender Antivirus and Microsoft Defender Firewall are configured through Intune Endpoint Protection profiles, which provides the required settings while keeping administrative effort to a minimum.

upvoted 3 times

minasamy 3 years, 3 months ago

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.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 7 times

minasamy 3 years, 3 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

bel88 4 months, 2 weeks ago

Selected Answer: CE

Whenever you see Defender Antivirus, Firewall, or BitLocker, your first thought should be:

Endpoint protection

not

Device restrictions

upvoted 1 times

noa808a 4 months, 3 weeks ago

Selected Answer: CE

Answer is outdated. As of June 2026 (and a little previously), both should be configured via Endpoint Protection.

upvoted 3 times

HueCumber 7 months ago

Selected Answer: CE

On MD-102, Defender Antivirus and Defender Firewall are configured using a device configuration profile with the Endpoint protection template.

upvoted 2 times

a5f91f0 7 months, 1 week ago

Selected Answer: CE

The answer is outdated, as the antivirus settings can now be configured in the endpoint secuity section

upvoted 3 times

JoonL 7 months, 2 weeks ago

Selected Answer: CE

Because the devices are managed by Intune, the most efficient and modern approach is to use Intune device configuration profiles, not Group Policy.Intune provides a built-in Endpoint protection profile specifically for Microsoft Defender Antivirus. The same Endpoint protection profile includes Defender Firewall settings

upvoted 2 times

epyonkills 8 months, 1 week ago

Selected Answer: CE

C and E

upvoted 3 times

Impcanada 8 months, 2 weeks ago

Selected Answer: DE

D et E sont correcte

upvoted 1 times

Le_Patriarche2025 9 months, 2 weeks ago

Selected Answer: CE

C – Pour configurer Microsoft Defender Antivirus

Créer un profil de configuration d'appareil et configurer les paramètres de protection du point de terminaison

→ C'est bien dans Endpoint Security → Antivirus dans Intune.

C'est correct.

✔ E – Pour configurer le pare-feu Microsoft Defender

Créer un profil de configuration d'appareil et configurer les paramètres de protection des terminaux

→ C'est bien dans Endpoint Security → Firewall dans Intune.

C'est correct.

upvoted 2 times

nkcodiac 11 months ago

Selected Answer: DE

Hello All

According to this question

Write answer is D and E

but now Intune is updated

so we can do both things from Endpoint Security

upvoted 3 times

Naebun 11 months, 3 weeks ago

Selected Answer: CE

The answer is outdated, as the antivirus settings can now be configured in the endpoint secuity section

upvoted 6 times

jonker 11 months, 4 weeks ago

Selected Answer: CE

both should be configure from Endpoint security node

upvoted 4 times

Robert69 1 year, 1 month ago

Selected Answer: CE

Since the devices are Azure AD joined and managed by Intune (not hybrid or on-premises AD joined), you should use Intune device configuration profiles to manage both Microsoft Defender Firewall and Antivirus settings. This minimizes administrative effort by managing everything centrally through Intune.

Why these are correct:

Option C - Defender Antivirus via Endpoint Protection

Endpoint protection settings in Intune device configuration profiles include comprehensive Microsoft Defender Antivirus configuration options

This is the native Intune method for configuring antivirus settings

Minimizes administrative effort for cloud-managed devices

Option E - Defender Firewall via Endpoint Protection

Endpoint protection settings also include Microsoft Defender Firewall configuration options

Allows you to configure firewall rules, notifications, and security settings

Centrally managed through Intune for Azure AD joined devices

upvoted 5 times

Mohamed555 1 year, 1 month ago

Selected Answer: CE

Feature Intune profile category Correct answer?

Microsoft Defender Antivirus Device configuration profile → Endpoint protection settings C

Microsoft Defender Firewall Device configuration profile → Endpoint protection settings E

upvoted 4 times

Dinkan 1 year, 2 months ago

Selected Answer: DE

Tested in LAB

upvoted 1 times

hvastija 1 year, 3 months ago

Selected Answer: DE

Check on Intune device configuration profiles. The Answer is correct

upvoted 1 times

henil_154762 1 year, 3 months ago

Selected Answer: CE

Ans - C, E

upvoted 1 times

theptr 1 year, 5 months ago

Selected Answer: CE

C and E

upvoted 1 times

CheMetto 1 year, 6 months ago

Selected Answer: CE

From: https://learn.microsoft.com/en-us/intune/intune-service/protect/endpoint-protection-configure

With Intune, you can use device configuration profiles to manage common Endpoint protection security features on devices, including:

Firewall

BitLocker

Allowing and blocking apps

Microsoft Defender and encryption

upvoted 3 times

Nko01 1 year, 6 months ago

Selected Answer: CE

Firewall and antivirus are both under endpoint security menu in intune

upvoted 3 times

cd2cfde 1 year, 5 months ago

This is absolutely wrong. Antivirus is not under endpoint security. It is under device restrictions.

upvoted 1 times

PXAbstraction 1 year, 4 months ago

I am looking at the Intune portal right now and this is wrong. Firewall and Antivirus are absolutely under Endpoint Security.

upvoted 3 times

Viddah 1 year, 6 months ago

Selected Answer: CE

C and E are the correct answers

MS recommandations are to managed into Endpoint protection section for advance security.

it's the same situation like Bitlocker configuration.

upvoted 4 times

cd2cfde 1 year, 5 months ago

What in the world are you talking about? Have you ever even used intune? Antivirus is not under endpoint security. It's under device restrictions. Just log in and see if it is listed there. Smh

upvoted 1 times

PXAbstraction 1 year, 4 months ago

You are wrong. I'm looking at the portal right now and both are under Endpoint Protection.

upvoted 2 times

Knight_Of_Peace 1 year, 8 months ago

Selected Answer: DE

Given answer is correct.

Microsoft Defender Antivirus setup:

Intune --> Devices --> Configuration --> Create new policy --> Windows 10 and later --> Template --> Device Restrictions --> Microsoft Defender Antivirus.

Windows Firewall setup:

Intune --> Devices --> Configuration --> Create new policy --> Windows 10 and later --> Template --> Endpoint protection --> Windows Firewall.

upvoted 5 times

sorinaccio 1 year, 9 months ago

Selected Answer: CE

C and E are the correct answers and this is why:

Endpoint Protection Settings: These are specifically used for configuring security features like Microsoft Defender Antivirus, Microsoft Defender Firewall, and other advanced security settings.

Why the other options are not correct?

Device Restrictions Settings: While they do include some basic security options, they are more focused on restricting device features and user behavior. They do not provide the detailed configuration for antivirus or firewall settings that Endpoint protection does.

upvoted 4 times

RJTW070 1 year, 9 months ago

Selected Answer: CE

Since the Windows 10 devices are Azure AD joined and managed by Microsoft Intune, the best approach to configure Microsoft Defender Antivirus and Microsoft Defender Firewall while minimizing administrative effort is using Intune Device Configuration Profiles.

Microsoft Defender Antivirus Configuration:

In Intune, Endpoint protection settings under Device configuration profiles allow you to manage Defender Antivirus policies.

This setting enables real-time protection, cloud-delivered protection, automatic sample submission, exclusions, and Defender updates.

This matches option C.

Microsoft Defender Firewall Configuration:

The Microsoft Defender Firewall settings are also configured within Endpoint protection settings in an Intune Device configuration profile.

This allows for enforcing firewall rules, inbound/outbound protection, and controlling network traffic centrally via Intune.

This matches option E.

upvoted 3 times

br99mlpt 1 year, 9 months ago

Selected Answer: DE

checked on the portal. DE is true

upvoted 2 times

Jz23 1 year, 9 months ago

Selected Answer: CE

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.

Explanation:

Since the Windows 10 devices are Azure AD joined and managed by Microsoft Intune, the correct way to configure Microsoft Defender Antivirus and Microsoft Defender Firewall is through Intune policies, not Group Policy Objects (GPOs).

C. Microsoft Defender Antivirus:

In Microsoft Intune, you need to create a Device Configuration Profile using the Endpoint protection template to configure Microsoft Defender Antivirus settings.

E. Microsoft Defender Firewall:

Similarly, to configure Defender Firewall, you must use an Endpoint protection profile in Intune.

upvoted 1 times

MSRock123 1 year, 10 months ago

Selected Answer: CE

Answer is CE.

Go into Intune. Devices>Windows>Configuration>Create>Windows 10 and later>Templates>Endpoint Protection

The information button for Endpoint protection says: "With Intune, you can use device configuration profiles to manage common endpoint protection security features on Windows devices, including Firewall, BitLocker, Microsoft Defender and encryption."

Also doublechecked with Copilot, answer is CE.

upvoted 1 times

hieunm2411 1 year, 10 months ago

Selected Answer: DE

D and E are the correct answers.

upvoted 1 times

OHMSS 1 year, 11 months ago

Selected Answer: CD

Both in Endpoint security

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

upvoted 2 times

RJTW070 1 year, 11 months 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 year, 12 months ago

CE is the Answer

upvoted 2 times

SSL2 2 years, 1 month 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 2 years, 2 months ago

Selected Answer: DE

Yes, FOR AV - Device Restriction and AV

For FW - Endpoint Protection - FW

upvoted 2 times

clucks 2 years, 3 months 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 2 years, 3 months ago

That's correct, I had forgotten.

upvoted 2 times

veliyath 2 years, 3 months 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 2 years, 4 months ago

Selected Answer: DE

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

upvoted 3 times

kiik32 2 years, 4 months ago

Selected Answer: CE

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

upvoted 1 times

kiik32 2 years, 4 months ago

actually from enpoint protection you enable the antivirus rather than configuring, so for that you will need a device restrictions template.

upvoted 1 times

nicholaswildern 2 years, 4 months 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 2 times

keshav80 2 years, 6 months ago

DE is 100% right. I have verified. Be relaxed.

upvoted 1 times

Bhuru 2 years, 6 months 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

Sssssg 2 years, 8 months ago

Answer is DE

upvoted 1 times

MR_Eliot 2 years, 9 months 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

Anonymouse1312 2 years, 9 months ago

Selected Answer: CE

Dumb question. C is also correct it seems:

"Antivirus policies include the same settings as found endpoint protection or device restriction templates for device configuration policy. However, those policy types include additional categories of settings that are unrelated to Antivirus. ----->>>>> The additional settings can complicate the task of configuring Antivirus workload"

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

correct me if im wrong, but fail to see how

upvoted 1 times

Krayzr 2 years, 9 months ago

Selected Answer: DE

AGREE WITH DE

upvoted 1 times

proservices 2 years, 10 months ago

Selected Answer: DE

D & E - Just checked in the Lab

upvoted 1 times

ThePrutser 2 years, 11 months ago

Selected Answer: DE

Went through the intune admin center:

- Firewall config is done via Endpoint Protection

- Antivirus config is done via Device restrictions

upvoted 1 times

Tati_Oliveira 2 years, 11 months ago

O Antivirus é configurado dentro de Device Restrictions e não dentro de Endpoint Protection. Dentro de Endpoint Protection é possível configurar:

Application Guard

Firewall

Defender Smart Screen

Windows Encryption

Defender Exploit Guard

Defender Application Control

Defender Credential Guard

Defender Security Center

Local device security Options

XBox Services

upvoted 1 times

b0gdan433 2 years, 12 months ago

Correct answer is DE, took the exam today and the 2 points for this.

upvoted 1 times

iTomi 2 years, 11 months ago

Good for you, but MS/Pearson does'n reveal right answers after test. Or did you get 900 points? Doubting that...

upvoted 1 times

NoursBear 2 years, 11 months ago

that's what I thought about this, you can only know which topics you did well on but no way can you tell based on a question

upvoted 1 times

Tr1v 3 years ago

Selected Answer: DE

Deinth is right:

D: MS Defender AV = Device Restriction

E: Firewall = Endoint Protection

upvoted 1 times

chandravamsi 3 years ago

Selected Answer: BE

Option B, E

upvoted 1 times

Rocky83 3 years, 1 month ago

Selected Answer: CE

If you think about admin effort ... CE makes sense

upvoted 3 times

pinda 3 years, 1 month ago

Selected Answer: BC

B. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings. This will allow you to configure firewall settings via Intune, ensuring consistency across your devices.

C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings. This will allow you to configure antivirus settings and policies via Intune, making it easy to manage across your devices.

upvoted 2 times

BJS78 3 years, 1 month ago

Weird question.

Antivirus can be configured inside: Device configuration / Admin templates/Endpoint protection, Device configuration /Admin templates/ Custom (OMA-URI) / Endpoint Security / Antivirus as well.

Firewall can be configured via Device configuration /Admin templates/ Custom (OMA-URI) and Endpoint Security / Firewall.

So for "minimize administrative effort" could be the key. For me, it would be configure both on Endpoint Security. (Worth to mention is that the best way for Antivirus would be Settings Catalog as there you can have LOT others, like Security Center settings under one config)

upvoted 1 times

BJS78 3 years, 1 month ago

Admin templates --> Templates

upvoted 1 times

NoursBear 3 years, 2 months ago

For me it's B and E. When I go to my Intune and create a Policy, go to Device Restrictions I have all the settings for Defender AV. To configure the Firewall (Firewall and rules) I go to Intune select Endpoint Security, Firewall and there create a profile. The problem things keep moving so god knows how old this question is

upvoted 1 times

NoursBear 3 years, 2 months ago

arghhh sorry D and E

upvoted 3 times

Futfuyfyjfj 3 years, 2 months ago

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

upvoted 3 times

JP1900 3 years, 2 months ago

Selected Answer: DE

D - MS Defender Antivirus is under Device Restriction settings

E - Defender Firewall is under Endpoint Protection settings

Both are under Devices, then Configuration profiles, then select Templates from the dropdown.

upvoted 3 times

letters1234 3 years, 2 months ago

Selected Answer: CE

Antivirus and Firewall can be configured on Endpoint Protection, Firewall can't be configured on Device Restrictions. Configuring the two requirements on the one Endpoint Protection profile reduces administrative overhead. Having the extended options of Antivirus on a Device Restriction profile also increases overhead, more to configure/understand before implementation.

upvoted 4 times

letters1234 3 years, 2 months ago

Didn't look at the lab close enough, the AV configuration in Endpoint Protection is just blocking end user access to AV section in Defender Security Centre on the device. Minasamy is right.

upvoted 1 times

Futfuyfyjfj 3 years, 2 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 5 times

Question #22 *Topic 1*

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

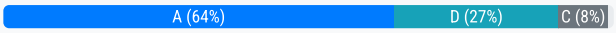
B. Settings

C. Scope (Tags)

D. Applicability Rules

Suggested Answer: *A*

Community vote distribution



krzysztofbr Highly Voted 3 years, 2 months ago

there is no option, You have to modify assignmentsI'll go with A too. I tried, with applicability rules you can choose OS Edition or OS Version. So it means nothing. What i'll do is create a filter named "Bob" with the property "DeviceName Equals Device1". Then in the assignment, put include "group 1" and in the assignment filter choose: Include filtered device in assignments -> Bob

upvoted 21 times

krzysztofbr Highly Voted 3 years, 2 months ago

Selected Answer: A

there is no option, You have to modify assignments

upvoted 21 times

HueCumber Most Recent 7 months ago

Selected Answer: D

Applicability rules decide whether a device applies a profile after it has already been assigned.

Assignment happens → Applicability Rule decides if the settings actually apply

upvoted 1 times

Impcanada 8 months, 2 weeks ago

Selected Answer: A

Inclure le groupe1 et exclure simplement le Device2

upvoted 1 times

PattyBear 9 months, 1 week ago

Selected Answer: D

Applicability rules allow you to:

Filter devices by attributes (name, OS version, model, etc.)

Target only specific devices within a group

Exclude Device2 while including Device1

Example:

You could create a rule like:

Device name equals "Device1"

So only Device1 receives Profile1.

upvoted 1 times

yihjie 1 year ago

Selected Answer: A

Assignment , apply a filter which uses the property "(device.deviceName -eq "Device1")"

https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/filters-device-properties

upvoted 1 times

Robert69 1 year, 1 month ago

Selected Answer: D

A. Assignments: Modifying assignments would mean removing Group1 and assigning the profile only to a new group containing just Device1. While this works, the question implies modifying the profile to handle the existing group assignment, and Applicability Rules is the feature designed for this granular filtering after the initial group assignment.

upvoted 2 times

Mohamed555 1 year, 1 month ago

Selected Answer: D

Applicability rules allow you to:

Include or exclude devices by OS version, edition, or model.

For example, apply only if:

OS edition = Windows 10 Enterprise

Model = “Surface Pro 8”

So, if Device1 meets the defined rule (e.g., model or OS version), and Device2 doesn’t, then Profile1 will apply only to Device1 — even though both are in the same assigned group.

This matches the exact requirement in the question.

 Final Answer

Setting Choice

Answer D. Applicability Rules

upvoted 3 times

budekzkie 1 year, 2 months ago

Selected Answer: A

A. Either you create a new group (call it group2) specifically for device2 to exclude it from the assignment or remove device2 from group1.

upvoted 2 times

Dinkan 1 year, 2 months ago

Selected Answer: A

Under assignment use assignment filter

upvoted 1 times

henil_154762 1 year, 3 months ago

Selected Answer: D

Ans - D

You leave Profile1 assigned to Group1 (both Device1 & Device2), but you add an applicability rule so only Device1 meets the condition (e.g., by device model or OS version).

upvoted 2 times

Dinkan 1 year, 2 months ago

Applicability Rule has only two properties to choose from, OS Edition & OS Version. Question doesn't mention anything about the devices being a different OS Edition or Version. So this answer is wrong

upvoted 2 times

theptr 1 year, 5 months ago

Selected Answer: D

Correct answer is D

upvoted 2 times

henil_154762 1 year, 3 months ago

Selected Answer: D

Ans - D You leave Profile1 assigned to Group1 (both Device1 & Device2), but you add an applicability rule so only Device1 meets the condition (e.g., by device model or OS version).

upvoted 2 times

CoffeeGr0und 1 year, 6 months ago

Selected Answer: D

A. Assignments: You already assigned the profile to Group1. Changing this would affect both devices unless you remove Group1 and assign Device1 directly, which increases administrative effort.

B. Settings: These define what the profile does, not who it applies to.

C. Scope (Tags): Used for RBAC (role-based access control), not for targeting devices.

upvoted 2 times

RJTW070 1 year, 9 months ago

Selected Answer: D

Since Profile1 is assigned to Group1 (which includes both Device1 and Device2), modifying the applicability rules is the best way to ensure that the profile applies only to Device1 without changing the group membership.

How Applicability Rules Work in Intune

Applicability rules allow you to filter which devices receive a configuration profile based on OS edition, OS version, or device model.

This means that even though Profile1 is assigned to Group1, it will only apply to Device1 if it matches the criteria set in the applicability rules.

upvoted 5 times

GoombaLMAO 1 year, 9 months ago

Selected Answer: A

LAB Experience:

on Assignments tab, you can assign device 2 to another group and add that group to excluded groups.

upvoted 1 times

hieunm2411 1 year, 10 months ago

Selected Answer: A

Use a filter in Assignments.

upvoted 2 times

hieunm2411 1 year, 10 months ago

In the question, both devices have the same Windows 10 Enterprise edition. There is no way to satisfy the requirement with the Applicability Rules if both devices have the same OS version. Instead, we can use a filter.

upvoted 3 times

SoLZeRa 1 year, 11 months ago

Selected Answer: A

The answer is A.

upvoted 1 times

iamchoy 1 year, 11 months 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 3 times

LionelDerBoven 2 years, 2 months ago

Selected Answer: A

Scopes is for administrative restriction for configuration NOT for assigment to a device of user (group).

upvoted 1 times

iamchoy 1 year, 11 months ago

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.In the question, both devices have the same Windows 10 Enterprise edition. There is no way to satisfy the requirement with the Applicability Rules if both devices have the same OS version. Instead, we can use a filter.

upvoted 3 times

subbuhotmail 2 years, 2 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 2 years, 2 months ago

Selected Answer: A

in Assignments we can use filter to exclude some members from groups

upvoted 2 times

Frank9020 2 years, 2 months 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 2 years, 2 months ago

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

Assignments

upvoted 1 times

oopspruu 2 years, 3 months ago

Selected Answer: A

The "Filter" option in Assignment section can be used to accomplish what the question is asking.

upvoted 1 times

kiik32 2 years, 4 months ago

applicability rules would not make it.

upvoted 1 times

7798da3 2 years, 4 months 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 2 years, 4 months 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 2 years, 6 months 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 2 years, 7 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 2 years, 8 months 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 2 years, 8 months 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

Haider_Raza 2 years, 8 months ago

Selected Answer: C

To ensure that Profile1 applies to Device1 only, even though it's originally assigned to Group1 which contains both Device1 and Device2, you should use:

C. Scope (Tags)

upvoted 3 times

MR_Eliot 2 years, 9 months ago

Selected Answer: A

Answer is A. You need add the device in the exclusions.

Also scope does nothing. It's only a thing to make it easier to know what de policy does. It's only information, nothing else!

upvoted 3 times

AVN1711 2 years, 4 months ago

Scope tags in Microsoft Intune allow administrators to divide devices in their organization into logical groups. These groups, also known as tags, can be used to make certain settings, applications, and policies available only to specific users or devices. By using Intune scope tags, you can streamline your IT infrastructure, improve security and make your life easier.

upvoted 1 times

Judith1969 2 years, 9 months ago

Answer A. Assignments in combination with a filter.

upvoted 2 times

Darkfire 2 years, 9 months ago

Selected Answer: C

I think C is correct.

Because Group1 contains both Device1 and Device2. You configure Profile1 and assign it to Group1. But Profile1 should apply on Device1. So you do that witch ScopeTag.

Otherwise you should configure two Profiles and two Groups which is not the question.

upvoted 3 times

Krayzr 2 years, 9 months ago

Selected Answer: A

The correct answer is **A. Assignments**.

In Azure AD, the Assignments section of a device configuration profile determines which users, devices, or groups the profile applies to. If you want Profile1 to apply to Device1 only, you should modify the Assignments of Profile1 to include only Device1. The other options (Settings, Scope (Tags), and Applicability Rules) do not directly control which devices a profile applies to.

Please note that this will only work if Device1 and Device2 are not in the same Azure AD group that Profile1 is assigned to. If they are, you might need to create a new group for Device1 and assign the profile to that group.

upvoted 2 times

Tonsku 2 years, 11 months ago

Selected Answer: A

using include/exclude

upvoted 2 times

neken123 2 years, 11 months ago

You can add filters under scope

Answer is C

upvoted 2 times

ThePrutser 2 years, 11 months ago

Selected Answer: D

If you update the assignments, you remove both devices. If you configure applicability rules in the same configuration policy you can filter the other device out.

upvoted 1 times

iTomi 2 years, 11 months ago

Selected Answer: A

Create conf profile and after choosing included groups you can edit filter on same blade. There is excluded devices

upvoted 3 times

chandravamsi 3 years ago

Selected Answer: C

Scope tags

upvoted 3 times

SajjH 2 years, 3 months ago

Scope tag doesn't control assignment of profile, it only deals with which IT Admin groups are allowed to manage the devices.

upvoted 1 times

iTomi 2 years, 11 months ago

conf prof doesnt have scope tags

upvoted 2 times

TC1Labs 2 years, 11 months ago

it has.

upvoted 1 times

mhmyz 3 years ago

Selected Answer: A

Assignments>Group>Filter

> Include filtered devices in assignment

https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters

upvoted 3 times

benpatto 3 years ago

In assignments, surely you can put group1 as the assigned group but then in the excluded options, remove the device that isn't needed? Just because a device is in the group, doesn't mean you can't use that group as the main assigning point. Take an 'all users' group for example, you can add that but then exclude a service account etc...

upvoted 1 times

ZaFletch 3 years, 1 month ago

Selected Answer: A

D is not possible in this case because it only allows OS version or edition as variables. To specify a device you have to use A.

A is the only way to specify the device.

upvoted 2 times

fiskaba 2 years, 11 months ago

I agree, the wording is : "Group1 contains two Windows 10 Enterprise devices named Device1 and Device2."

Both machines are the same OS edition, and we can assume they are also the same OS version as there is no wording to suggest otherwise. So the ONLY other option to pick is A.

upvoted 2 times

Rocky83 3 years, 1 month ago

Selected Answer: A

Assignments >> Filter ... Add device2 in the excluded devices

upvoted 5 times

WalexyJimi 3 years, 1 month ago

Selected Answer: D

I believe the correct and is D. You can use the Applicability Rule to specify which device receives the profile1.

Read more here: https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-create.

upvoted 1 times

BJS78 3 years, 1 month ago

Scope (Tags) is for RBAC.

upvoted 5 times

ronct 3 years, 2 months ago

Selected Answer: D

Assignments in Microsoft Intune are used to determine which users or devices should receive a particular policy, app, or other item. In this case, the policy (Profile1) is already assigned to Group1, which contains both Device1 and Device2.

If you were to modify the assignments, you would be changing which users or devices the policy applies to. However, since both devices are in the same group (Group1), modifying the assignments wouldn't allow you to target only Device1.

On the other hand, Applicability Rules allow you to further filter within an assigned group based on certain criteria. This means you can set rules that make the policy applicable only to Device1, even though it's assigned to a group that also contains Device2. That's why modifying the Applicability Rules is the correct choice in this scenario.

upvoted 2 times

Futfuyfyjfj 3 years, 1 month ago

Do you know applicability rules solely give you the option to specify an OS version and an OS edition? In this case the edition is the same, so you can't use this variable. The exact Windows version/build is unknown, so you can't use this either. So D is wrong

upvoted 5 times

Grg433 3 years, 2 months ago

Selected Answer: D

I am sure it is not A as by doing that the Device 2 will also be added (as question mentioned the profile1 applies to device1 only)

My reasoning for D is = In the Applicability Rules section of the device configuration profile, you can specify conditions or rules that determine which devices the profile should apply to. By creating an applicability rule that targets Device1 specifically, you can ensure that Profile1 only applies to that device, even though it's assigned to Group1. This allows you to target specific devices within a group.

https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-create

upvoted 2 times

NoursBear 2 years, 11 months ago

No. Applicability Rules can only be used to differentiate devices based on OS versions or Edition. In this case both devices have the same edition and probably same version

upvoted 2 times

Futfuyfyjfj 3 years, 2 months ago

Good point, however I don't agree with you. Although the question and the answers lack some required details, applicability rules solely give you the option to specify an OS version and an OS edition. OS edition is no option since the question states both are Enterprises editions. We don't know which version the devices are running, so we can't rely on this.

Therefore my shot is B, modify Assignments and add a filter or an exclude group, but question does not specify whether this is possible and the order of performing these action is for both answers a little weird.

upvoted 4 times

Futfuyfyjfj 3 years, 2 months ago

I meant A off course

upvoted 2 times

picho707 3 years, 2 months ago

I agree with you. It is D. Neither C or A makes any sense regarding what is being requested as the final outcome.

upvoted 1 times

NoursBear 3 years, 2 months ago

A probably. Applicability Rules does exist I have it in my Intune but that can only be applied if in a group some computers have another edition or OS 1version that can be differentiated, so no good for this scenario. There will have to be an exclusion assignment too I guess.

upvoted 3 times

Crismo 3 years, 2 months ago

I would take A as well. Scope tags seems incorrect to me since its purpose is to restrict access of an admin group to a collection of machines.

upvoted 3 times

letters1234 3 years, 2 months ago

You could use filters but that isn't an option. Applicability Rules doesn't exist in Intune anymore for deployment of a Configuration Profile. Settings would be the actual configuration profile. Scope Tags are administrative instead of targeting. Assignments would require another group to be available for targeting such as Exclude group.

upvoted 4 times

CheMetto 1 year, 6 months ago

I'll go with A too.

I tried, with applicability rules you can choose OS Edition or OS Version. So it means nothing. What i'll do is create a filter named "Bob" with the property "DeviceName Equals Device1". Then in the assignment, put include "group 1" and in the assignment filter choose: Include filtered device in assignments -> Bob

upvoted 3 times

minasamy 3 years, 3 months ago

Selected Answer: A

I will go for A

upvoted 10 times

Question #23 *Topic 1*

DRAG DROP -

You have a Microsoft 365 subscription that includes Microsoft Intune.

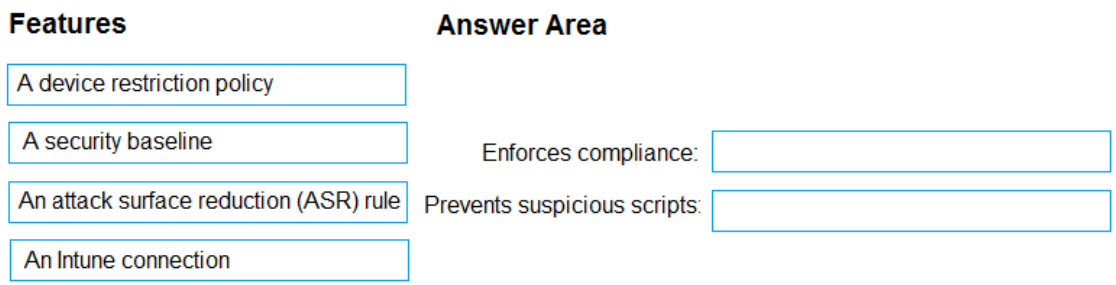
You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:

Enforces compliance for Defender for Endpoint by using Conditional Access

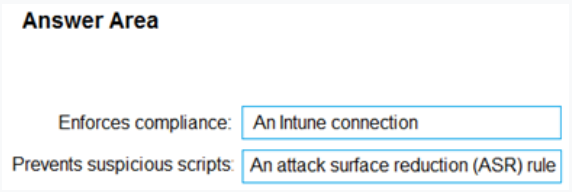
Prevents suspicious scripts from running on devices

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.



Suggested Answer:



JP1900 Highly Voted 3 years, 2 months ago

Without an Intune connection, how can the policies apply? The original answer is correct.

upvoted 12 times

JP1900 Highly Voted 3 years, 2 months ago

Without an Intune connection, how can the policies apply? The original answer is correct.Enforces compliance: An Intune connection Prevents suspicious scripts: An attack surface reduction (ASR) rule Here's why: -Device restriction policies are useful for configuring device settings. -But to enforce compliance based on Defender for Endpoint signals, you must have an Intune connection configured. -That's what makes "An Intune connection" the correct answer for enforcing Conditional Access based on Defender for Endpoint.

upvoted 13 times

ollyijeh Most Recent 2 months, 2 weeks ago

to block scripts an ASR rule has to be configured. But for enforcing conditional access on defender for endpoint, an intune connection has to be present

upvoted 2 times

HueCumber 7 months ago

MD-102 memory rules

Defender + Conditional Access = Intune connection

Blocking scripts = ASR rules

Baselines = broad hardening, not precise script control

upvoted 3 times

MR_Eliot 2 years, 9 months ago

Enforces compliance for Defender for Endpoint by using Conditional Access - A Device Restriction policy. After which you can configure conpliance 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!Btw, intune connection is required for Microsoft Defender integaration and Intune. So that answer is totally not correct!Experience does not imply competence, please provide evidence and stop saying this every time you comment, it makes you less trustworthy every time you say itI believe your logic but the Microsoft practice tests do the same thing connection before policy these exams are so convoluted. LOLI'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 6 times

MR_Eliot 2 years, 9 months ago

Enforces compliance for Defender for Endpoint by using Conditional Access - A Device Restriction policy. After which you can configure conpliance 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 5 times

Robert69 1 year, 1 month ago

Enforces compliance using Conditional Access → An Intune connection:

For Conditional Access to leverage device compliance data from Microsoft Defender for Endpoint, the device needs to be managed and marked as compliant (or non-compliant) by Microsoft Intune. The integration between Defender for Endpoint and Intune is what enables the compliance status to be reported and subsequently enforced by Conditional Access policies.

Prevents suspicious scripts → An attack surface reduction (ASR) rule:

Attack Surface Reduction (ASR) rules are a primary feature of Microsoft Defender for Endpoint designed to prevent software from performing risky actions. Specifically, ASR rules can block malicious scripts, stop obfuscated scripts, and prevent scripts from performing dangerous file or registry operations.

upvoted 2 times

mikekrt 1 year, 8 months ago

First one is a device restriction policy, It asks you specifically to enforce it. an intune connection is not enforcing anything.

upvoted 1 times

SaiK1234 2 years, 8 months ago

The original answer is correct. Establish a connection and then you can enforce.

second is ASR

upvoted 2 times

CheMetto 1 year, 6 months ago

compliance policy are not related to device restriction policy. I can create a compliance policy without having a device restriction. Also we are not talking about both policies! We are talking abount Compliance for defender for endpoint, which is managed by security.microsoft.com, so all it need is to turn on the connector.

upvoted 1 times

wakka9876 1 year, 10 months ago

Experience does not imply competence, please provide evidence and stop saying this every time you comment, it makes you less trustworthy every time you say it

upvoted 4 times

Rylz 2 years, 3 months 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 2 years, 4 months 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 2 years, 9 months ago

Btw, intune connection is required for Microsoft Defender integaration and Intune. So that answer is totally not correct!

upvoted 2 times

NoursBear 2 years, 11 months 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

Amir1909 2 years, 10 months ago

Correct

upvoted 1 times

NoursBear 2 years, 11 months 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

iTomi 2 years, 11 months 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

OyYaGotta 2 years, 8 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 2 years, 11 months 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 2 years, 11 months 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 2 times

mail2bala3011 3 years, 3 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

VirtualJP 3 years, 1 month ago

I believe this answer to be correct

upvoted 3 times

mail2bala3011 3 years, 3 months ago

Seems like the answer is correct: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-conditional-access?view=o365-worldwideYou are wrong Intune connection doesn't enforce antyhingQuestion 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-configureNo 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 3 times

krzysztofbr 3 years, 2 months ago

You are wrong Intune connection doesn't enforce antyhing

upvoted 1 times

krzysztofbr 3 years, 2 months ago

You are wrong Intune connection doesn't enforce antyhingQuestion 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-configureNo 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

Besxp 1 year, 5 months ago

Enforces compliance: An Intune connection

Prevents suspicious scripts: An attack surface reduction (ASR) rule

Here's why:

-Device restriction policies are useful for configuring device settings.

-But to enforce compliance based on Defender for Endpoint signals, you must have an Intune connection configured.

-That’s what makes "An Intune connection" the correct answer for enforcing Conditional Access based on Defender for Endpoint.

upvoted 2 times

krzysztofbr 3 years, 3 months ago

the second part about ASR seems correct but enforces comliance "intune connection" it should be security baseline i guess. this is set off seetings relevant for compliance requirements

upvoted 3 times

iTomi 2 years, 11 months 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

Futfuyfyjfj 3 years, 2 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 3 years, 3 months ago

the second part about ASR seems correct but

enforces comliance "intune connection"

it should be security baseline i guess. this is set off seetings relevant for compliance requirements

upvoted 3 times

Futfuyfyjfj 3 years, 2 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

Question #24 *Topic 1*

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.

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?

Name	GPO value
LockoutBadCount	0
MaximumPasswordAge	42
MinimumPasswordAge	1
MinimumPasswordLength	7
PasswordComplexity	True
PasswordHistorySize	24

A. Administrative Templates

B. Endpoint protection

C. Device restrictions

D. Custom

Suggested Answer: *C*

Community vote distribution

C (48%) A (40%) D (9%) 2

volto Highly Voted 3 years, 3 months ago

Answer C is correct https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#passwordYou are correct! so many wrong answers again! inside device restrictions, You have password settings. your link shows everything regarding passwordThe 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.Password setting usually reflect on accounts know?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!Actually you're wrong. Administrative template has been retired. The answer is c. Funny thing is you spoke so confidently as if you're the sole authority on this. 😂😂His answer was valid when he submitted it almost 9 months ago broskiActually you're wrong. The answer was right then as it

upvoted 32 times

volto Highly Voted 3 years, 3 months ago

Selected Answer: C

Answer C is correct https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#password

upvoted 32 times

krzysztofbr 3 years, 2 months ago

You are correct! so many wrong answers again! inside device restrictions, You have password settings. your link shows everything regarding passwordThe 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.Password setting usually reflect on accounts know?

upvoted 5 times

krzysztofbr 3 years, 2 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 2 years, 2 months 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 7 times

vijay0715 2 years, 9 months ago

Password setting usually reflect on accounts know?

upvoted 1 times

RomanV 2 years, 2 months 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 7 times

RomanV 2 years, 2 months 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!Actually you're wrong. Administrative template has been retired. The answer is c. Funny thing is you spoke so confidently as if you're the sole authority on this. 😂😂His answer was valid when he submitted it almost 9 months ago broskiActually you're wrong. The answer was right then as it is now. It didn't just magically became the right answer after all of this time.Correct: The Endpoint protection profile in Intune includes password policies, account lockout settings, and local device security options. It is designed to replicate security baselines and common GPO security settings like those found in the Default Domain Policy. □ Why not the others? A. Administrative Templates -Used for importing GPO settings that exist in ADMX-backed format (e.g., Office or Windows registry-based policies), not password or lockout settings. C. Device restrictions -Used for UI settings (camera, Bluetooth, copy/paste, etc.), not password or account lockout policies. D. Custom -Used for OMA-URI or CSP-based settings not exposed directly in the UI. Not necessary here since built-in options cover the required settings.Go to EndPoint Security > Account Protection > Create Policy > Profile is Account Protection > This is only for WHFB!! No legacy passwords.

upvoted 8 times

bigdaddyzaddy 1 year, 8 months ago

Actually you're wrong. Administrative template has been retired. The answer is c. Funny thing is you spoke so confidently as if you're the sole authority on this. 😂😂

upvoted 6 times

bigdaddyzaddy 1 year, 8 months ago

Actually you're wrong. Administrative template has been retired. The answer is c. Funny thing is you spoke so confidently as if you're the sole authority on this. 😂😂His answer was valid when he submitted it almost 9 months ago broskiActually you're wrong. The answer was right then as it is now. It didn't just magically became the right answer after all of this time.Correct: The Endpoint protection profile in Intune includes password policies, account lockout settings, and local device security options. It is designed to replicate security baselines and common GPO security settings like those found in the Default Domain Policy. Why not the others? A. Administrative Templates -Used for importing GPO settings that exist in ADMX-backed format (e.g., Office or Windows registry-based policies), not password or lockout settings. C. Device restrictions -Used for UI settings (camera, Bluetooth, copy/paste, etc.), not password or account lockout policies. D. Custom -Used for OMA-URI or CSP-based settings not exposed directly in the UI. Not necessary here since built-in options cover the required settings.Go to EndPoint Security > Account Protection > Create Policy > Profile is Account Protection > This is only for WHFB!! No legacy passwords.

upvoted 6 times

8choxo 1 year, 5 months ago

His answer was valid when he submitted it almost 9 months ago broskiActually you're wrong. The answer was right then as it is now. It didn't just magically became the right answer after all of this time.

upvoted 1 times

8choxo 1 year, 5 months ago

His answer was valid when he submitted it almost 9 months ago broski

upvoted 1 times

cd2cfde 1 year, 4 months ago

Actually you're wrong. The answer was right then as it is now. It didn't just magically became the right answer after all of this time.

upvoted 1 times

Besxp 1 year, 5 months ago

Correct: The Endpoint protection profile in Intune includes password policies, account lockout settings, and local device security options. It is designed to replicate security baselines and common GPO security settings like those found in the Default Domain Policy. Why not the others? A. Administrative Templates -Used for importing GPO settings that exist in ADMX-backed format (e.g., Office or Windows registry-based policies), not password or lockout settings. C. Device restrictions -Used for UI settings (camera, Bluetooth, copy/paste, etc.), not password or account lockout policies. D. Custom -Used for OMA-URI or CSP-based settings not exposed directly in the UI. Not necessary here since built-in options cover the required settings.Go to EndPoint Security > Account Protection > Create Policy > Profile is Account Protection > This is only for WHFB!! No legacy passwords.

upvoted 1 times

Besxp 1 year, 5 months ago

Correct:

The Endpoint protection profile in Intune includes password policies, account lockout settings, and local device security options.

It is designed to replicate security baselines and common GPO security settings like those found in the Default Domain Policy.

 Why not the others? A. Administrative Templates -Used for importing GPO settings that exist in ADMX-backed format (e.g., Office or Windows registry-based policies), not password or lockout settings.

C. Device restrictions -Used for UI settings (camera, Bluetooth, copy/paste, etc.), not password or account lockout policies.

D. Custom -Used for OMA-URI or CSP-based settings not exposed directly in the UI. Not necessary here since built-in options cover the required settings.

upvoted 1 times

7a9c653 7 months, 3 weeks ago

Go to EndPoint Security > Account Protection > Create Policy > Profile is Account Protection > This is only for WHFB!! No legacy passwords.

upvoted 1 times

iTomi 2 years, 11 months ago

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 13 times

Pablosanchez Most Recent 4 months, 4 weeks ago

It's natural to assume that this should be an administrative template because of GPO, but it involves passwords, and this is implemented through device restrictions.

upvoted 1 times

HueCumber 7 months ago

 MD-102 memory rule If the goal is to migrate existing Group Policy settings to Intune, use Administrative Templates first.

upvoted 2 times

a5f91f0 7 months, 1 week ago

C. Device restrictions The Rationale In Microsoft Intune, password policy settings (such as length, complexity, age, and history) for Windows devices are natively managed within the Device restrictions profile template.

upvoted 1 times

jonker 11 months, 4 weeks ago

Selected Answer: B

should be Endpoint protection using Security baseline

upvoted 1 times

7a9c653 7 months, 3 weeks ago

A is the one to migrate a GPO policy.

upvoted 2 times

ModernoDecor 8 months, 3 weeks ago

Today it is Settings Catalog (Administrative Templates is retired) https://learn.microsoft.com/en-us/intune/intune-service/configuration/group-policy-analytics-migrate

upvoted 1 times

ModernoDecor 8 months, 4 weeks ago

Today is a Group Policy analytics used, but might be able to do it with Custom

upvoted 1 times

jonker 11 months, 4 weeks ago

should be Endpoint protection using Security baselineGo to EndPoint Security > Account Protection > Create Policy > Profile is Account Protection > This is only for WHFB

upvoted 1 times

7a9c653 7 months, 3 weeks ago

Go to EndPoint Security > Account Protection > Create Policy > Profile is Account Protection > This is only for WHFB

upvoted 1 times

Alaeddine100 1 year ago

A Lorsque le terme migration est utilisé, cela implique que vous prenez les paramètres existants d'Active Directory (GPO) et que vous les transférez dans Intune. Pour cela, la méthode appropriée est Administrative Templates (ou aujourd'hui Settings Catalog, car Administrative Templates est retiré pour la création de nouveaux profils).

upvoted 1 times

Robert69 1 year, 1 month ago

Administrative Templates: Used for configuring settings based on traditional ADMX/ADML templates, which often cover general operating system, application, or user interface settings, but not the core domain password policies themselves. Endpoint protection: This option is typically used to manage settings related to antivirus, firewall, encryption (e.g., BitLocker), or Windows Defender features, not the password rules themselves. Device restrictions: This type of configuration profile in Intune (and other device management tools) is specifically designed for setting password policies, access limitations, enforcing device-level encryption, and other fundamental limitations on device security and functionality. Settings like minimum password length and password history are typically found under the password policy section within Device restrictions.

upvoted 1 times

greatsparta 1 year, 2 months ago

device restrictions covers UI and user experience settings like camera, Bluetooth, app store access etc. Not account lockout or password rules.

upvoted 1 times

RJTW070 1 year, 9 months ago

Selected Answer: A

Since the Default Domain Policy GPO typically contains Group Policy settings related to security, user experience, and system configurations, the best way to migrate these settings to Microsoft Intune is by using the Administrative Templates profile type.

Why Use Administrative Templates? Administrative Templates in Intune mimic Group Policy Objects (GPOs) in Active Directory. They allow you to apply the same settings as traditional GPOs without requiring on-premises Active Directory. Many common GPO settings are already available in Intune Administrative Templates, making migration easier.

upvoted 3 times

hvastija 1 year, 3 months ago

Answer C is Correct

upvoted 1 times

hieunm2411 1 year, 10 months ago

Selected Answer: C

Starting with the December 2412 release, you can't create new Administrative Templates policies from the Templates > Administrative Templates profile type in the Intune admin center. https://learn.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows?tabs=template

upvoted 2 times

theptr 1 year, 4 months ago

Use the Windows 10/11 “Device restrictions” template. That template’s Password section lets you set all of the items that appear in the Default Domain Policy—minimum length, maximum and minimum age, history, complexity, and lock-out values—without having to fall back to custom OMA-URI settings.

upvoted 1 times

wakka9876 1 year, 10 months ago

Selected Answer: C

Answer is C - Device Restrictions

Administrative templates has been deprecated by Microsoft and now shows as retired when you create a configuration profile

upvoted 2 times

Besxp 1 year, 5 months ago

The Endpoint protection profile in Intune includes password policies, account lockout settings, and local device security options. It is designed to replicate security baselines and common GPO security settings like those found in the Default Domain Policy. Why not the others? A. Administrative Templates -Used for importing GPO settings that exist in ADMX-backed format (e.g., Office or Windows registry-based policies), not password or lockout settings. C. Device restrictions -Used for UI settings (camera, Bluetooth, copy/paste, etc.), not password or account lockout policies. D. Custom -Used for OMA-URI or CSP-based settings not exposed directly in the UI. Not necessary here since built-in options cover the required settings. -Comments saying "Device restrictions" are either outdated or confusing it with mobile device PIN policies. -For your GPO migration with password and lockout policies, the correct and current profile type is: Endpoint protection.

upvoted 1 times

Grimmgore 1 year, 10 months 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

AnindaR 1 year, 8 months ago

It should be custome as you get all mentioned options under settings catalog by choosing device lock optioins.

upvoted 1 times

Question #25 *Topic 1*

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: *C, D, E*

Community vote distribution



HvD Highly Voted 3 years, 1 month 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 30 times

kdub1234565 Most Recent 18 hours ago

Selected Answer: ACDE

I looked into it and currently Analytics can check all but B. I'm Guessing it was added as an update recently

upvoted 1 times

ollyijeh 2 months, 2 weeks ago

Selected Answer: ADE

The correct answer to this question is ADE

Failure events can be collected from AMA

Average processor utilization can be collect via performance counts

Error events can be collected from the Event log collection

upvoted 1 times

HueCumber 7 months ago

Selected Answer: ACD

A. failure events from the Security log

C. the average processor utilization

D. error events from the System log

upvoted 1 times

Besxp 1 year, 5 months ago

Selected Answer: ACD

Most Accurate and Updated Answers (2025): A. Failure events from the Security log → □ (now supported via AMA) C. Average processor utilization → □ (always supported via performance counters) D. Error events from the System log → □ (supported via event log collection)

□ Why Are Answers Online So Varied? Outdated agent models: Most confusion is due to the transition from MMA (Log Analytics agent) to AMA (Azure Monitor Agent), which has far more granular control over data collection.

Custom logs (E) require manual configuration, so some people incorrectly rule them out entirely.

Process info (B) is misleading — while some performance counters are available per process, actual execution time logging is not a default feature of Log Analytics.

upvoted 11 times

Besxp 1 year, 5 months ago

Most Accurate and Updated Answers (2025): A. Failure events from the Security log → □ (now supported via AMA) C. Average processor utilization → □ (always supported via performance counters) D. Error events from the System log → □ (supported via event log collection) □ Why Are Answers Online So Varied? Outdated agent models: Most confusion is due to the transition from MMA (Log Analytics agent) to AMA (Azure Monitor Agent), which has far more granular control over data collection. Custom logs (E) require manual configuration, so some people incorrectly rule them out entirely. Process info (B) is misleading — while some performance counters are available per process, actual execution time logging is not a default feature of Log Analytics.You are absolutely correct. AME can collect this info by itself. Log analytics is now deprecated.Typo I meant AMA (azure monitoring agent)

upvoted 14 times

a5f91f0 7 months, 1 week ago

Selected Answer: CDE

The Correct Selections

C. The average processor utilization: Log Analytics can collect Performance Counters from Windows machines. This includes CPU utilization, memory usage, disk I/O, and network statistics. You can configure the collection interval (e.g., every 10 seconds) to calculate averages over time.

D. Error events from the System log: You can collect standard Windows Event Logs (System, Application, and Security). You can specifically filter to collect only "Error" or "Warning" levels to minimize data costs while still capturing critical failures.

E. Third-party application logs stored as text files: Log Analytics supports Custom Logs. This allows you to define the path to a text file on the local drive (e.g., C:\Logs\App1.log) and ingest that data into the workspace as a searchable table.

upvoted 1 times

cd2cfde 1 year, 5 months ago

You are absolutely correct. AME can collect this info by itself. Log analytics is now deprecated.

upvoted 1 times

cd2cfde 1 year, 5 months ago

You are absolutely correct. AME can collect this info by itself. Log analytics is now deprecated.Typo I meant AMA (azure monitoring agent)

upvoted 1 times

JoonL 7 months, 2 weeks ago

Selected Answer: ACD

E: Log Analytics can ingest custom logs, but: They must be explicitly configured as custom log sources. They are not collected by default

A : Log Analytics can collect Windows Security event logs.Includes failed logon events, audit failures, etc. Commonly used for security monitoring and SIEM scenarios

upvoted 1 times

Le_Patriarche2025 8 months, 2 weeks ago

Selected Answer: RCD

c est la bonne reponse

upvoted 1 times

ModernoDecor 8 months, 4 weeks ago

Selected Answer: BCD

This question is obsolete. It is Endpoint Analytics today.

https://learn.microsoft.com/en-us/intune/endpoint-analytics/data-collection

upvoted 1 times

Aymanproof1 11 months, 2 weeks ago

Selected Answer: ACD

Correct

upvoted 1 times

Robert69 1 year, 1 month ago

Selected Answer: ACD

Azure Log Analytics, a component of Azure Monitor, uses agents on Windows computers to collect operational data.

Windows Event Logs (A and D): The agent is configured to collect events from standard Windows Event Logs, such as the Security log (where authentication failures, account lockouts, and system access attempts are logged) and the System log (where core operating system errors and service failures are logged).

Performance Data (C): The agent routinely collects performance counters, such as processor utilization, memory usage, and disk I/O rates, which are then stored as performance data in the Log Analytics workspace.

upvoted 1 times

henil_154762 1 year, 2 months ago

Selected Answer: CDE

C. Average processor utilization — Azure Monitor/Log Analytics collects performance counters (e.g., Processor\% Processor Time) and you can query/average them.

Microsoft Learn

+1

D. Error events from the System log — You can collect Windows Event Logs (e.g., System) with selected severities (Error, Warning, etc.).

Azure Docs

E. Third-party app logs stored as text files — Custom Logs let you ingest text-file logs into a workspace.

Microsoft Learn

+1

upvoted 3 times

hvastija 1 year, 3 months ago

Selected Answer: ACD

ACD is righ

upvoted 1 times

henil_154762 1 year, 3 months ago

Selected Answer: ACD

Ans- A,C,D

upvoted 1 times

yoyoyo99 1 year, 4 months ago

Selected Answer: ACD

Azure Log Analytics can collect events from Windows event logs (e.g., security logs and system logs).

Additionally, performance counters (e.g. CPU usage) can also be collected.

However, B. lists of processes and their execution times and E. third-party logs stored as text files are not collected by default in Log Analytics or require additional configuration or custom scripts.

upvoted 1 times

theptr 1 year, 4 months ago

Selected Answer: ACD

A. failure events from the Security log

C. the average processor utilization

D. error events from the System log

upvoted 2 times

cd2cfde 1 year, 5 months ago

Selected Answer: ACD

Azure monitoring agent has now replaced log analytics agent. With AMA the correct answers are A,C,and D

upvoted 1 times

bigdaddyzaddy 1 year, 8 months ago

Selected Answer: C

The answer is C guys. Administrative template (A) has been retired

upvoted 2 times

cd2cfde 1 year, 5 months ago

Typo I meant AMA (azure monitoring agent)

upvoted 1 times

bigdaddyzaddy 1 year, 8 months ago

The answer is C guys. Administrative template (A) has been retiredI posted this answer on the wrong question. Sorry

upvoted 2 times

bigdaddyzaddy 1 year, 8 months ago

I posted this answer on the wrong question. Sorry

upvoted 3 times

ExamBud 1 year, 8 months ago

Selected Answer: ACD

As today you can collect security logs using the Azure Log Analytics, I think it can be ACDE.

upvoted 3 times

hieunm2411 1 year, 10 months ago

Selected Answer: CDE

C: Perf | where ObjectName == "Processor" and CounterName == "% Processor Time" and InstanceName == "_Total" | summarize AVGCPU = avg(CounterValue) by Computer Average CPU utilization across all computers

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-performance-counters

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 6 times

TedEx2 1 year, 11 months 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 4 times

c4e009c 1 year, 12 months 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 5 times

KBMS 2 years, 2 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 3 times

CJL324 2 years, 6 months 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 2 years, 7 months 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 2 years, 8 months 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).

upvoted 4 times

MR_Eliot 2 years, 9 months ago

Selected Answer: BCD

See comment from HvD.

upvoted 2 times

Merrybob 2 years, 9 months 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 2 years, 9 months ago

BCD - I've set this up in a Log Analytics Workspace and tried it myself.

upvoted 1 times

ubiquituz 2 years, 10 months 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 2 years, 10 months ago

Selected Answer: BCD

seems correct

upvoted 1 times

belyo 2 years, 11 months 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 2 years, 9 months ago

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-custom-logs

upvoted 1 times

cpaljchc4 3 years ago

1. Performance Data: This includes infomration 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-arty 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 3 years, 1 month ago

Why B is not?

upvoted 1 times

VirtualJP 3 years, 1 month ago

Selected Answer: BDE

Personally I think I'd have to go with BDE

upvoted 1 times

VirtualJP 3 years, 1 month ago

Correction, I go with BCD

upvoted 4 times

HvD Highly Voted 3 years, 1 month 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 32 times

MR_Eliot 2 years, 9 months ago

Totally agree with you. BCD is the answer.

upvoted 5 times

Rubends 3 years, 1 month ago

I think it's correct, E: you must configure it.

upvoted 1 times

yingo20 3 years, 2 months ago

CDE it's a correct answers

upvoted 1 times

letters1234 3 years, 2 months ago

Selected Answer: CDE

JP1900's answer has A however that is security log, which cant be collected as it requires Defender for Cloud - https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events#configure-windows-event-logs

Current processes and times are also not natively supported, which means that local log files, standard event log and cpu utilization can be collected.

upvoted 5 times

Futfuyfyjfj 3 years, 2 months ago

https://github.com/uglide/azure-content/blob/master/articles/log-analytics/log-analytics-data-sources-performance-counters.md

upvoted 2 times

krzysztofbr 3 years, 2 months ago

Selected Answer: CDE

We have to exclude security, and list of process.

possible is CDE

upvoted 2 times

JP1900 3 years, 3 months ago

Selected Answer: ACE

You cannot collect failure events from the Security log or the list of processes and their execution times by using Log Analytics.

upvoted 2 times

Futfuyfyjfj 3 years, 1 month ago

So you are actually saying CDE?

upvoted 1 times

krzysztofbr 3 years, 2 months ago

A is about security, You are wrong

upvoted 1 times

Question #26 *Topic 1*

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

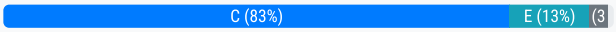
C. an endpoint detection and response (EDR) policy

D. an account protection policy

E. an antivirus policy

Suggested Answer: *C*

Community vote distribution



krzysztofbr Highly Voted 3 years, 2 months ago

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-configure?view=o365-worldwideDirect link: https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure#onboard-windows-devices

upvoted 12 times

krzysztofbr Highly Voted 3 years, 2 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-configure?view=o365-worldwide

upvoted 11 times

7a9c653 Most Recent 7 months, 3 weeks ago

Selected Answer: C

C shows and applies onboard devices.

upvoted 2 times

ModernoDecor 8 months, 4 weeks ago

Selected Answer: E

The Defender for Endpoint agent depends on Microsoft Defender Antivirus to scan files and provide information about them.https://learn.microsoft.com/en-us/defender-endpoint/onboarding

upvoted 1 times

kkoddi3624 1 year, 2 months ago

Selected Answer: B

Microsoft provides security baselines that include pre-configured settings aligned with best practices.

The Microsoft Defender for Endpoint baseline includes onboarding settings that automatically connect devices to the Defender for Endpoint service.

It simplifies deployment—no need to manually configure every setting.

upvoted 1 times

NasX 1 year, 7 months ago

Selected Answer: C

Screenshot: https://learn.microsoft.com/en-us/intune/intune-service/protect/media/advanced-threat-protection-configure/select-preconfigured-policy.jpg

upvoted 3 times

weslenfranks 1 year, 8 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/mem/intune-service/protect/advanced-threat-protection-configure#enable-microsoft-defender-for-endpoint-in-intune

upvoted 1 times

veliyath 2 years, 4 months 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 2 years, 4 months ago

Selected Answer: E

It should be E

upvoted 1 times

Haider_Raza 2 years, 8 months 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 2 years, 9 months 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 Endpoit.

This currently only works for Windows. For MacOS it's a different story.

upvoted 2 times

Darkfire 2 years, 9 months 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 2 years, 9 months 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 2 years, 9 months ago

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.C - Would also work because it is required to create an EDR. Creating an Antrivirus 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-worldwideChecked 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

Merrybob 2 years, 9 months ago

C - Would also work because it is required to create an EDR. Creating an Antrivirus 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 2 years, 9 months ago

C - Would also work because it is required to create an EDR. Creating an Antrivirus 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-worldwideChecked 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

Merrybob 2 years, 9 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 2 years, 10 months 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 2 years, 10 months ago

ChatGPT tells E is the correct answerGPT 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

onepunchkenshin 2 years, 10 months ago

ChatGPT tells E is the correct answer

upvoted 1 times

RomanV 2 years, 2 months 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 2 years, 10 months ago

Correct

upvoted 2 times

chandravamsi 3 years ago

Selected Answer: E

Option: E

upvoted 1 times

Daveazure 3 years 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 3 years, 1 month ago

Selected Answer: C

Correct

upvoted 1 times

Futfuyfyjfj 3 years, 2 months ago

Direct link:

https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure#onboard-windows-devices

upvoted 4 times

Question #27 *Topic 1*

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.

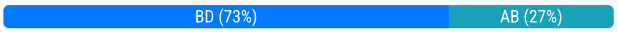
B. From Platform Settings, set Android Enterprise (work profile) to Allow.

C. From Platform Settings, set Android device administrator Personally Owned to Allow.

D. From Platform Settings, set Android device administrator to Block.

Suggested Answer: *B, D*

Community vote distribution



ollyijeh Most Recent 2 months, 2 weeks ago

Selected Answer: BD

selecting D ensures that they're unable to enroll as they aren't an admin

B is correct as it just allows work profiles

upvoted 1 times

hvastija 1 year, 3 months ago

Selected Answer: BD

BD Is right, are the options on Intune

upvoted 1 times

Besxp Highly Voted 1 year, 5 months ago

Selected Answer: AB

A + B

Pros: Fine-tuned, supports corp-owned admin temporarily, recommended by MS for BYOD

Cons: Might allow device admin for corp-owned unless blocked separately

B + D

Pros: Strong block against all device admin

Cons: Overkill for BYOD-only goal; breaks corp admin if still needed

A + B is the best-balanced, Intune-recommended approach.

People choose B + D when they want a broad, uncompromising block, or if they aren't differentiating between personal vs corporate ownership

"BD" answers were valid once, but A + B is the better answer now.

upvoted 7 times

RJTW070 1 year, 11 months ago

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.You want to block the entire Android Device Administrator platform.... not just the personally owned portion of the device Android Device Administrator platform.

upvoted 3 times

RJTW070 1 year, 11 months 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 1 year, 11 months 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 Highly Voted 2 years, 4 months 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 7 times

Cheban 2 years, 7 months 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 2 years, 8 months ago

Selected Answer: BD

Ther's is no "androind Personally owned" option, only Work profile and Admin

upvoted 2 times

MR_Eliot 2 years, 9 months ago

Selected Answer: BD

BD agreed. Also device administrator will be out of support by Microsof very soon.

upvoted 2 times

Merrybob 2 years, 9 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 2 times

mirak123 3 years, 2 months ago

why is it D?Because Android Device Admin may not enroll at all so when blocking Android Device Admin unter the platform setting, the personally owned device is greyed out automatically so you don't set the "block" there

upvoted 3 times

Rocky83 3 years, 1 month 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 4 times

mirak123 3 years, 2 months ago

why is it D?

upvoted 3 times

NoursBear 2 years, 9 months ago

Because Android Device Admin may not enroll at all so when blocking Android Device Admin unter the platform setting, the personally owned device is greyed out automatically so you don't set the "block" there

upvoted 2 times

Futfuyfyjfj 3 years, 2 months ago

Answers are 100% correct

upvoted 2 times

krzysztofbr 3 years, 2 months ago

Selected Answer: BD

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

upvoted 6 times

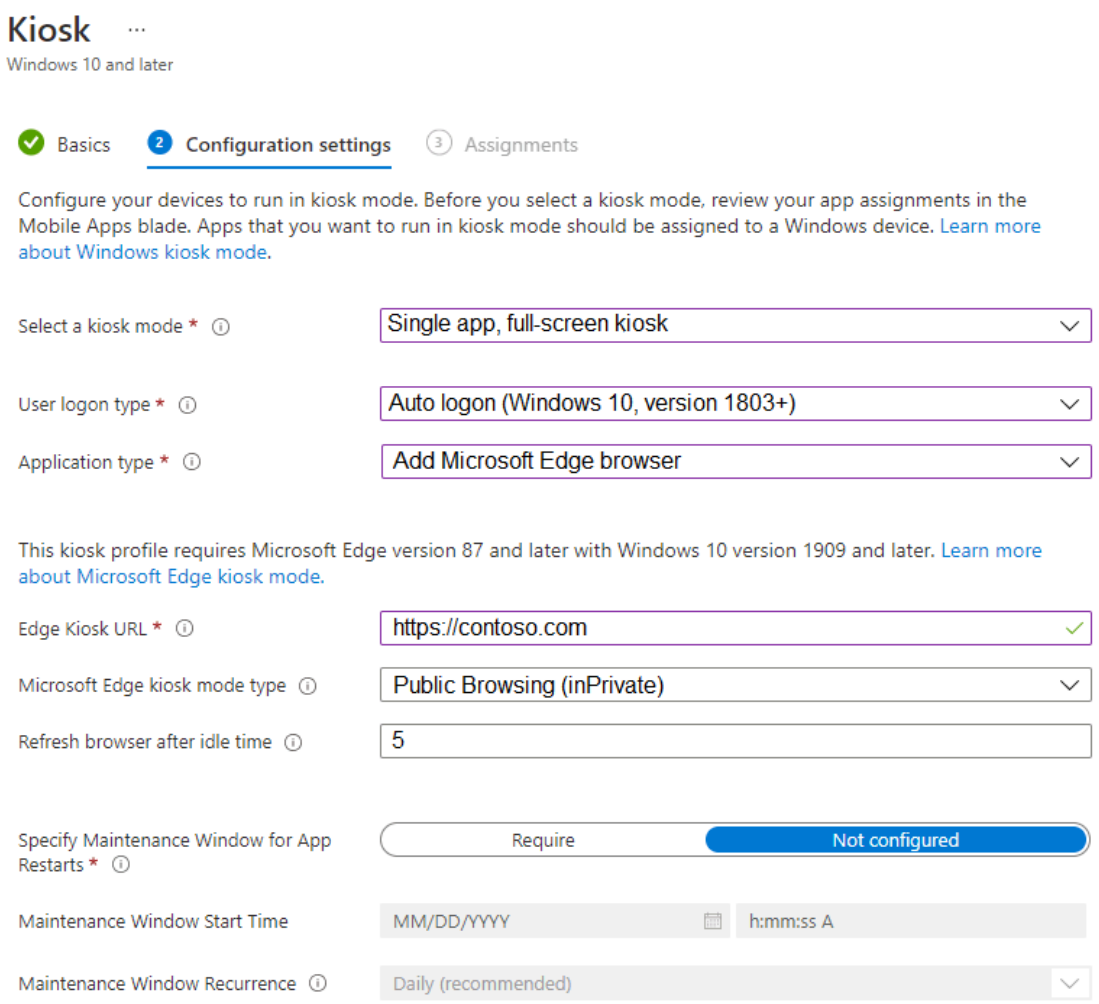
Question #28 *Topic 1*

HOTSPOT -

You have the device configuration profile shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer Area

Users **[answer choice]**.

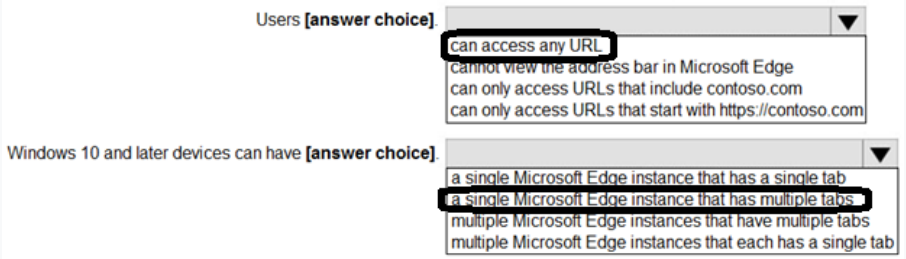
- can access any URL
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com

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

Suggested Answer:

Answer Area



NasX Most Recent 1 year, 7 months ago

Answers are correct.

From MS:

Public Browsing (InPrivate): Runs a limited multi-tab version of Microsoft Edge. Users can browse publicly, or end their browsing session.

upvoted 2 times

7798da3 2 years, 4 months ago

I have seen it show multiple browser single tab

upvoted 1 times

MR_Eliot 2 years, 9 months ago

https://learn.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode#overview

upvoted 2 times

yosry 2 years, 11 months ago

Seems Correct

upvoted 2 times

MR_Eliot 2 years, 9 months ago

Answers are correct!https://learn.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode#overview

upvoted 4 times

MR_Eliot 2 years, 9 months ago

Answers are correct!

upvoted 4 times

Rocky83 3 years, 1 month ago

Correct

upvoted 3 times

letters1234 Highly Voted 3 years, 2 months ago

https://learn.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode#overview

Would require Digital/Interactive Signage experience instea dof Public-Browsing to be limited to one site.

Multiple tabs are also part of PBE

upvoted 5 times

krzysztofbr Highly Voted 3 years, 2 months ago

answers are correct

https://learn.microsoft.com/en-us/mem/intune/configuration/kiosk-settings-windows

upvoted 16 times

Question #29 *Topic 1*

HOTSPOT -

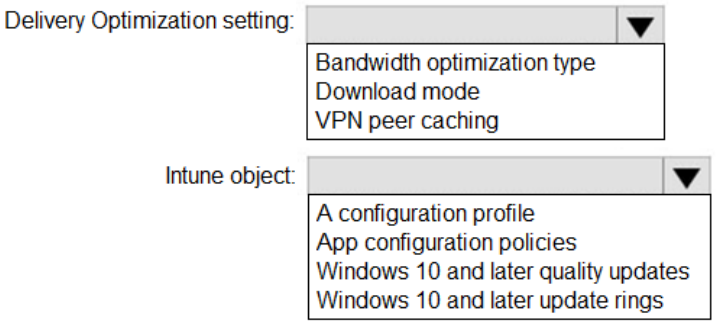
You have 100 Windows 10 devices enrolled in Microsoft Intune.

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.

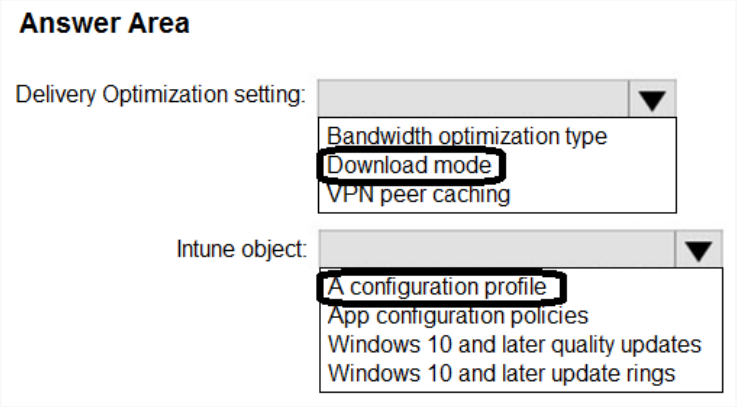
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



HueCumber Most Recent 7 months ago

MD-102 Memory Rule

Where updates come from = Delivery Optimization (Download mode)

How updates are delivered via Intune = Configuration profile

upvoted 3 times

kkoddi3624 1 year, 2 months ago

1. Download Mode

2. Windows 10 and later update rings - This allows you to manage update behaviour

upvoted 1 times

oopspruu 2 years, 4 months ago

Provided answers are correct. Update Rings doesn't have delivery optimization settings.

upvoted 1 times

MR_Eliot 2 years, 9 months ago

Answer is correct.

upvoted 3 times

Darkfire 2 years, 9 months ago

Answer is correct

upvoted 1 times

yosry 2 years, 11 months ago

seems correct

upvoted 1 times

madsa 2 years, 11 months ago

Correct, Download mode, Configuration Profile>Templates>Delivery optimization.

upvoted 1 times

ExamKiller020 3 years, 2 months ago

Answer is correct, just checked in my own tenant

upvoted 4 times

NoursBear 3 years, 2 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

NoursBear 3 years, 2 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....You cant config that in Update rings...

upvoted 1 times

ExamKiller020 3 years, 2 months ago

You cant config that in Update rings...

upvoted 4 times

letters1234 Highly Voted 3 years, 2 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 12 times

krzysztofbr 3 years, 2 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

Question #30 *Topic 1*

HOTSPOT -

You have an Azure AD tenant that contains the users shown in the following table.

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

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.

Name	Member of
User1	Group1
User2	Group2

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

Answer Area

Statements	Yes	No
User1 receives Notification1 on Device1.	○	○
User2 receives Notification1 on Device2.	○	○
User1 receives Notification1 on Device3.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 receives Notification1 on Device1.	○	◉
User2 receives Notification1 on Device2.	○	◉
User1 receives Notification1 on Device3.	◉	○

Futfuyfyjfj Highly Voted 3 years, 1 month 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 35 times

ollyijeh Most Recent 2 months, 2 weeks ago

Notifications can only be sent to Android and iOS devices, not windows so this rules out option 1.

The only 'Yes' here is the 3rd option. user 1 is in group 1 inherently even though they're on a group2 device. They're also on a mobile device so they can receive it

upvoted 2 times

HueCumber 7 months ago

Big rule here only the users receive notifications and only mobile devices can receive notifications.

User 1 is in the right group but on windows, so NO

User 2 is not in the right group, NO notification

User 1 is in the right group and device 3 is android, so Yes

upvoted 2 times

Casticod 3 years, 1 month 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 10 times

jaba2050 7 months, 1 week ago

Statement 1 (No): Although User1 and Device1 are both in Group1 (the target group), Device1 runs Windows 10. Since Windows does not support Intune custom notifications, the message will not be received on that device.

Statement 2 (Yes): User1 is in Group1, and Device2 is also in Group1. Device2 is an Android device, which is a supported platform. Therefore, the notification will be successfully delivered to Device2.

Statement 3 (No): Notification1 was sent specifically to Group1. Both User2 and Device3 are members of Group2. Since neither the user nor the device is in the target group, they will not receive the notification.

upvoted 1 times

onepunchkenshin 2 years, 10 months ago

user takes precedence, so Futfuyfyjfj is rightBut what I don't undrstand 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 2 times

onepunchkenshin 2 years, 10 months ago

user takes precedence, so Futfuyfyjfj is right

upvoted 2 times

SyafiqBakri 7 months, 1 week ago

1. User1 receives Notification1 on Device1 (Windows 10)?

 No

Windows 10 cannot receive Intune custom notifications.

2. User2 receives Notification1 on Device2 (Android)?

 No

User2 is not in Group1, so receives nothing.

3. User1 receives Notification1 on Device3 (iOS)?

 No

Device3 belongs to Group2, not Group1.

Even though the device is iOS (supported), it does not belong to Group1 and is not assigned to User1.

upvoted 2 times

IamMilu 8 months, 3 weeks ago

lol. it should be Yes, No, NO

upvoted 2 times

krzysztofbr 3 years, 2 months ago

so many wrong answers again:)! custom doesnt work for Windows and MacOS DEVICE 1 (Windows) NO Device 2 (Android) YES Device 3 (IOS) but group 2 - NOWell, no entirely true. You CAN create custom Notifications (Toast) on Windows via PS and deploy, but not "send" themI was wrong! NO, NO, YES!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...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.but the notification was sent to the group 1 not the usersIt'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 20 times

krzysztofbr 3 years, 2 months ago

so many wrong answers again:)! custom doesnt work for Windows and MacOS DEVICE 1 (Windows) NO Device 2 (Android) YES Device 3 (IOS) but group 2 - NO

upvoted 20 times

Le_Patriarche2025 9 months ago

ser1 receives Notification1 on Device1NonDevice1 est Windows 10 — les notifications personnalisées ne sont pas supportées sur WindowsUser2 receives Notification1 on Device2NonUser2 est dans Group2, pas dans Group1 — la notification ne lui est pas destinéeUser1 receives Notification1 on Device3NonDevice3 (iOS) est dans Group2, pas Group1 — et User1 n'est pas associé à Device3

upvoted 1 times

hlundin16 11 months, 3 weeks ago

I think it's NNY, this put my mind in a blender but I rarely read carefully.

User 1 receives notification on device 1: No - According the article, this only targets iOS/iPadOS and Android devices

https://learn.microsoft.com/en-us/intune/intune-service/remote-actions/custom-notifications?pivots=ios

User 2 receives notification on device 2: No - User 2 is not a member of Group 1

User 1 receives notification on device 3: Yes - User 1 is in Group 1, will receive the notification

upvoted 3 times

Robert69 1 year, 1 month ago

No, No, No

Device1 is Windows 10 and a member of Group1. Windows 10 does not support custom notifications.

User2 is not in Group1. Even though Device2 is Android (which supports notifications), only members of Group1 receive it.

Device3 is in Group2, and notification was sent to Group1.

upvoted 1 times

AdamRachel 2 years, 10 months 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

AdamRachel 2 years, 10 months 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...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.but the notification was sent to the group 1 not the users

upvoted 4 times

henil_154762 1 year, 2 months ago

User1 receives Notification1 on Device1 (Windows 10): No

User2 receives Notification1 on Device2 (Android): Yes

User1 receives Notification1 on Device3 (iOS): No

Why: Intune custom notifications are only delivered to iOS/iPadOS and Android devices via the Company Portal/Intune app. Windows devices aren't supported, so Device1 won't receive it. You sent the notification to Group1, which contains Device2 (Android), so that device receives it. Device3 (iOS) is in Group2, which wasn't targeted, so it doesn't receive the message.

upvoted 1 times

captainspork 2 years, 1 month 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

captainspork 2 years, 1 month 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.but the notification was sent to the group 1 not the users

upvoted 3 times

nhmh90 1 year, 4 months ago

No, No, Yes.

Custom notification only targeted to user. Hence, the device must meet iOS/Android. Then check whether user in the group or not. Group for devices does not affected.

upvoted 1 times

theptr 1 year, 4 months ago

I think the correct answer is NYN

upvoted 1 times

ExamBud 1 year, 9 months ago

No-No-Yes.

1) No because it is a Windows device.

2) No because User2 is not targeted. Devices are ignored in these assignments.

3) Yes because User1 is targeted and it is iOS.

upvoted 2 times

Tr619899 1 year, 12 months 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 years 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 3 times

King_shola 2 years, 2 months 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 3 times

93831b0 2 years, 2 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 2 times

Pollosor 2 years, 3 months 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 2 years, 3 months 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 2 years, 4 months 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 5 times

bigdaddyzaddy 1 year, 7 months ago

I was thinking the same thing. Device 3 is not in the targeted group. Why are people assuming that user 1 registered device 3? User 2 could've registered device 3 since they're in the same group which is 2. I believe it is NNN

upvoted 3 times

carl_amadeo 2 years, 5 months 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 2 years, 7 months 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%20devices.,-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 that user.User 2 is not a memeber 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 2 years, 8 months 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 2 years, 8 months ago

no, custom notificstion 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 2 years, 8 months ago

mistake here it should be:

no, custom notificstion not available windows devices

upvoted 1 times

Sergey42 2 years, 8 months ago

But device 3 is in group 2, how did the user 1 receive that notification?

upvoted 2 times

MR_Eliot 2 years, 8 months 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 2 years, 9 months 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%20notifications%20to%20the%20users%20of%20managed%20iOS/iPadOS%20and%20Android%20devices.+

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%20notification%20will%20go%20to%20all%20iOS/iPadOS%20and%20Android%20devices%20enrolled%20by%20that%20user.

upvoted 2 times

Darkfire 2 years, 9 months 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

Merrybob 2 years, 9 months ago

N - Only mobile devices get the notification, not Windows

N - Only Group 1 gets the notifications

Y - User 1 is in Group 1 and on a mobile device

upvoted 1 times

Kifayat 2 years, 11 months ago

No,No,Yes

Custom Notification applicable to Android, iOS

Answers with explanations are below.

1)User 1 receives notification1 on device1 - No

Windows - No (not supported)

2)User 2 receives notification1 on device2 - No

User 2 in Group 2, notification1 sent to group 1 only - No

3)User 1 receives notification1 on device3 - yes

User 1 in Group 1 which is iOS - yes

upvoted 3 times

yosry 2 years, 11 months ago

Seems correct

upvoted 1 times

b0gdan433 2 years, 12 months ago

Correct answ is No,No,Yes, took the exam today.

upvoted 2 times

LionelDerBoven 2 years, 2 months ago

But what I don't undrstand 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 sens.

upvoted 1 times

Chief67 3 years ago

Are we saying that User1 will recieve Notification1 because he/she is in group1 regardless if the device is in Group2?

upvoted 2 times

KarlosFandango 3 years ago

The Correct anwser is NNY

Windows Not Applicable

Android Applicable but out of scope.

IOS Applicable and in scope.

upvoted 3 times

iamforksu 3 years, 1 month ago

NO

NO

YES

upvoted 1 times

Futfuyfyjfj Highly Voted 3 years, 1 month 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 38 times

Friscini 1 year, 11 months 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 3 years, 1 month 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 10 times

LionelDerBoven 2 years, 2 months ago

But what I don't undrstand 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

ashville13 3 years, 2 months ago

correct, 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 4 times

NoursBear 3 years, 2 months ago

Researched on my Intune Tenant and it is correct. Once again a topic not mentioned in the course like most things.

upvoted 3 times

Zied_jouini111 3 years, 2 months ago

Non Oui Non

upvoted 1 times

OyYaGotta 2 years, 8 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 3 times

Satya06 1 year, 5 months ago

but the notification was sent to the group 1 not the users

upvoted 1 times

BJS78 3 years, 1 month ago

Well, no entirely true. You CAN create custom Notifications (Toast) on Windows via PS and deploy, but not "send" them

upvoted 1 times

krzysztofbr 3 years, 2 months ago

I was wrong!

NO, NO, YES!

upvoted 26 times

volto 3 years, 3 months ago

"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."

If Device 3 is enrolled by User 1 than he receive notification. We don't know it.

upvoted 3 times

krzysztofbr 3 years, 2 months ago

device 3 but group 2, We are sending to the group1 ONLY

no, yes, no

upvoted 2 times

krzysztofbr 3 years, 2 months ago

SHOULD be NO NO yes

upvoted 3 times

rmac 3 years, 3 months ago

Correct!

No

No

Yes

upvoted 3 times

krzysztofbr 3 years, 2 months ago

PLEASE if You don't know..say You dont know. or You are not sure:)

upvoted 1 times

Krayzr 3 years ago

What is wrong here? you have corrected your answer to this too :D

upvoted 1 times

sh123df 3 years, 3 months ago

Can you please explain how it is correct?

upvoted 1 times

krzysztofbr 3 years, 2 months ago

You have my explanation on the top

upvoted 3 times

Question #31 *Topic 1*

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%)

ciberdiego Most Recent 1 month, 3 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports

upvoted 1 times

Dinkan 1 year, 2 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/intune/intune-service/developer/reports-nav-create-intune-reports

https://learn.microsoft.com/en-us/intune/intune-service/developer/reports-proc-get-a-link-powerbi

upvoted 1 times

MR_Eliot 2 years, 2 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports

upvoted 2 times

Darkfire 2 years, 2 months 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%20App,-The%20Power%20BI

upvoted 2 times

Krayzr 2 years, 3 months ago

Selected Answer: D

correct

upvoted 1 times

krzysztofbr 2 years, 8 months ago

Microsoft Power BI

upvoted 4 times

krzysztofbr 2 years, 8 months ago

Microsoft Power BIhttps://learn.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

upvoted 4 times

pinda 2 years, 7 months ago

Selected Answer: D

correct

upvoted 3 times

Futfuyfyjfj Highly Voted 2 years, 8 months ago

https://learn.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

upvoted 6 times

Question #32 *Topic 1*

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%)

Eagle-eye Most Recent 3 weeks ago

Selected Answer: A

A is correct. https://learn.microsoft.com/en-us/intune/intune-service/enrollment/apple-mdm-push-certificate-get

upvoted 1 times

Dinkan 1 year, 2 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/intune/intune-service/enrollment/apple-mdm-push-certificate-get

upvoted 1 times

5bd2675 2 years, 1 month ago

A is correct, but shouldn't it say "Apple" not "Apply"

upvoted 4 times

Haider_Raza 2 years, 2 months 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 2 years, 2 months ago

Selected Answer: A

A is correct.

upvoted 1 times

Darkfire 2 years, 2 months 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 2 years, 5 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-ios-ipados

upvoted 1 times

VirtualJP 2 years, 8 months ago

Selected Answer: A

Pre-reqs

upvoted 2 times

krzysztofbr 2 years, 8 months 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 3 times

letters1234 Highly Voted 2 years, 8 months ago

Selected Answer: A

Pre-requisites - https://learn.microsoft.com/en-us/mem/intune/enrollment/apple-configurator-enroll-ios

upvoted 10 times

Question #33 *Topic 1*

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.

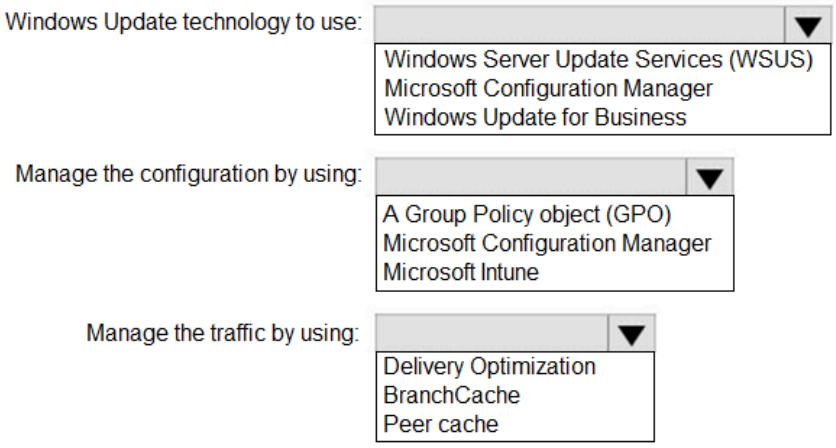
Internet traffic must be minimized.

Costs must be minimized.

How should you configure Windows Update? To answer, select the appropriate options in the answer area.

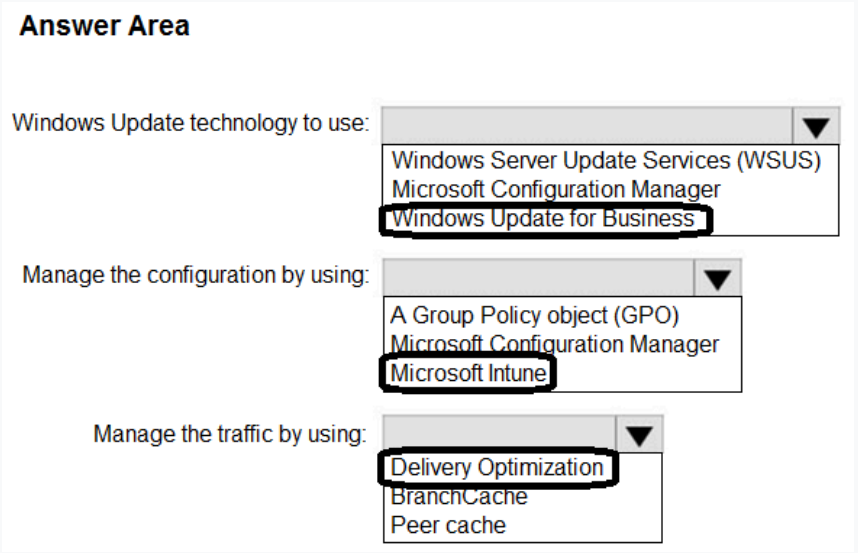
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



NakatomiTower Most Recent 11 months ago

This question is old. It should be Windows Update client policies. Formerly known as Windows Update for Business.

upvoted 2 times

RomanV 2 years, 2 months 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 4 times

oopspruu 2 years, 4 months ago

The key to this question is "You have NO SERVERS".

upvoted 1 times

MR_Eliot 2 years, 8 months ago

answer is correct.

upvoted 1 times

Darkfire 2 years, 9 months ago

Answers are correct.

upvoted 1 times

Murad01 2 years, 9 months ago

Given answers are correct

upvoted 1 times

WilliamsNL 2 years, 9 months 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 3 years, 2 months ago

answers are correct

upvoted 4 times

krzysztofbr Highly Voted 3 years, 2 months ago

"you have no servers" so it must be Intune and Windows update for bussiness

upvoted 22 times

sh123df Highly Voted 3 years, 3 months ago

Answers seems correct out

upvoted 9 times

Question #34 *Topic 1*

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

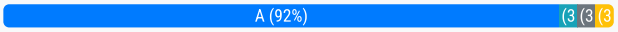
B. a Windows Update for Business Group Policy setting

C. a Microsoft Peer-to-Peer Networking Services Group Policy setting

D. an Update ring for Windows 10 and later profile

Suggested Answer: *A*

Community vote distribution



krzysztofbr Highly Voted 3 years, 3 months ago
answer is wrong should be A "delivery Optimization" https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference
upvoted 26 times

Sango Most Recent 3 months ago
Selected Answer: A
Hybrid joined means both GPO and MDM are possible. However, GPO require line of sight to a domain controller and Intune Configurations do not. This is a significant limitation for roaming devices.
upvoted 1 times

Dinkan 1 year, 2 months ago
You can configure Delivery Optimization using an Intune 'configuration profile' You can also configure delivery optimization using Group policy, but they are not under Windows Update for Business or Microsoft Peer-to-Peer Networking Group Policy Settings. The Delivery Optimization settings in Group Policy are under Configuration\Policies\Administrative Templates\Windows Components\Delivery Optimization

Reference: 1. https://learn.microsoft.com/en-us/intune/intune-service/configuration/delivery-optimization-windows 2. https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference 3. https://support.microsoft.com/en-us/topic/how-to-use-group-policy-to-configure-windows-update-delivery-optimization-in-windows-10-6464960d-d400-0367-be90-02c5a804186a
upvoted 1 times

Dinkan 1 year, 2 months ago
You can configure Delivery Optimization using an Intune 'configuration profile' You can also configure delivery optimization using Group policy, but they are not under Windows Update for Business or Microsoft Peer-to-Peer Networking Group Policy Settings. The Delivery Optimization settings in Group Policy are under Configuration\Policies\Administrative Templates\Windows Components\Delivery Optimization Reference: 1. https://learn.microsoft.com/en-us/intune/intune-service/configuration/delivery-optimization-windows 2. https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference 3. https://support.microsoft.com/en-us/topic/how-to-use-group-policy-to-configure-windows-update-delivery-optimization-in-windows-10-6464960d-d400-0367-be90-02c5a804186aAzure AD doesn't support GPOs
upvoted 1 times

7a9c653 7 months, 3 weeks ago
Selected Answer: A
DO policy can be configured in Intune.
upvoted 1 times

Le_Patriarche2025 9 months, 2 weeks ago
Selected Answer: U
c est la bonne réponse
upvoted 1 times

weslenfranks 1 year, 8 months ago

Irrelevant link.

upvoted 3 times

FemiA55 1 year, 11 months 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

carllaurel 1 year, 9 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups

upvoted 1 times

carllaurel 1 year, 9 months ago

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groupsIrrelevant link.

upvoted 1 times

LionelDerBoven 2 years, 2 months ago

Selected Answer: A

A is right from experiance.

upvoted 3 times

AVN1711 2 years, 4 months 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 2 years, 8 months ago

Selected Answer: A

A it's the correct answer just read the documentation

upvoted 1 times

CJL324 2 years, 6 months 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%.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 2 times

CJL324 2 years, 6 months 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

OyYaGotta 2 years, 8 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 2 years, 8 months ago

Selected Answer: A

A is correct. You can create a configuration for delivery optimization settings.

upvoted 3 times

Darkfire 2 years, 9 months ago

Selected Answer: A

A is correct

https://learn.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-settings#bandwidth

upvoted 1 times

Merrybob 2 years, 9 months ago

Selected Answer: A

A. a configuration profile

upvoted 1 times

Amir1909 2 years, 10 months ago

A is correct

upvoted 1 times

OyYaGotta 2 years, 8 months ago

So does Copilot.

upvoted 1 times

yosry 2 years, 11 months ago

Selected Answer: A

configuration profile > Delivery Optimization > bandwidth oprimazation type = percentage

then select set "Maximum foreground download bandwidth " and "Maximum background download bandwidth " to 50

upvoted 2 times

onepunchkenshin 2 years, 10 months ago

ChatGPT tells you A is correct

upvoted 1 times

onepunchkenshin 2 years, 10 months ago

ChatGPT tells you A is correctSo does Copilot.

upvoted 1 times

madsa 2 years, 11 months ago

This answer is correct, Microsoft Questions can be a bit tricky but with this information, the answer is correct.

upvoted 1 times

chandravamsi 3 years ago

Selected Answer: A

Option A: Configuration Profile

upvoted 1 times

Gentlemanners 3 years ago

Selected Answer: A

The Answer is A.

You need a Configuration profile that allows you to configure the delivery optimazation and its settings.

https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference

upvoted 1 times

fco168 3 years ago

Selected Answer: A

A Configuration Profile allows you to configure Delivery Optimization and its settings.

upvoted 1 times

fco168 3 years ago

A should be the correct answer.

upvoted 1 times

JGMG 3 years ago

Selected Answer: A

Why you sugests C. ?

There are a lot of question that you sugests wrong answers..

upvoted 3 times

NoursBear 2 years, 11 months ago

It is by design and is deliberate, you're supposed to study from the questions

upvoted 1 times

LiamAzure 3 years, 1 month ago

Selected Answer: A

CONFIGURATION PROFILE

upvoted 2 times

4rk4n4 3 years, 1 month ago

Selected Answer: A

Answer should be A

upvoted 3 times

Grg433 3 years, 1 month ago

Selected Answer: A

yes , A is correct !

upvoted 2 times

NoursBear 3 years, 2 months ago

A for me too

upvoted 4 times

letters1234 3 years, 2 months ago

Selected Answer: A

Delivery Optimisation through Configuration Profile in Intune

upvoted 9 times

krzysztofbr Highly Voted 3 years, 3 months ago

answer is wrong should be A "delivery Optimization"

https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference

upvoted 26 times

Onaropus 8 months ago

Azure AD doesn't support GPOs

upvoted 1 times

Buzl 3 years, 3 months ago

A Configuration profile using the "Delivery Optimization" template will allow you to specify the percentage of bandwidth (max) to be used

upvoted 15 times

Question #35 *Topic 1*

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.

Which groups can you add to Group4?

Name	Type	Location
Group1	Universal distribution group	Contoso.com
Group2	Global security group	Contoso.com
Group3	Group	Computer1
Group4	Group	Computer1

A. Group2 only

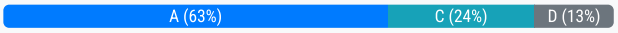
B. Group1 and Group2 only

C. Group2 and Group3 only

D. Group1, Group2, and Group3

Suggested Answer: *A*

Community vote distribution



picho707 Highly Voted 3 years, 1 month ago

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.This is correct!It's not actually.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 en Entra tenant but about on-site AD. And on-site AD allows more complex nesting scenarios compared to Azure AD. There fore i lean towards D.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 32 times

picho707 Highly Voted 3 years, 1 month 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 31 times

Temptset 3 years, 1 month ago

This is correct!It's not actually.

upvoted 3 times

Temptset 3 years, 1 month ago

This is correct!

upvoted 3 times

OyYaGotta 2 years, 8 months ago

It's not actually.

upvoted 2 times

93831b0 2 years, 2 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 en Entra tenant but about on-site AD. And on-site AD allows more complex nesting scenarios compared to Azure AD. There fore i lean towards D.

upvoted 2 times

OyYaGotta 2 years, 8 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 2 times

volto 3 years, 3 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 12 times

volto 3 years, 3 months ago

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.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.I am withdrawing this answer after further research.

upvoted 12 times

picho707 3 years, 2 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 2 times

picho707 3 years, 2 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.I am withdrawing this answer after further research.

upvoted 2 times

picho707 3 years, 1 month ago

I am withdrawing this answer after further research.

upvoted 2 times

TysonBeatty **Most Recent** 6 months ago

Just tested this on a machine and it is most definitely D. This table shows it pretty clearly. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#group-scope

upvoted 1 times

GPPRO 7 months, 3 weeks ago

local group could be added to local group so c is correct.

upvoted 2 times

moluccanvibe 9 months, 2 weeks ago

What Windows allows in a local group A local group on a Windows machine can contain: - User accounts (local or domain) - Domain security groups (Global, Universal, Domain Local) - Other local groups on the same machine A local group cannot contain: - Distribution groups (because they are not security principals)

upvoted 2 times

Robert69 1 year, 1 month ago

Group1 (Universal distribution group): Cannot be added because Group4 is a Security Group. Group2 (Global security group): Can be added. Global security groups can be members of Domain Local groups. Group3 (Domain local security group): Can be added. Domain local groups can contain other Domain Local groups within the same domain.

upvoted 1 times

SheaHask 1 year, 3 months ago

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups

upvoted 1 times

Knight_Of_Peace 1 year, 8 months ago

Selected Answer: D

1) Universal group can be member of: "Local groups on computers in the same forest or trusting forests"

2) Global group can be member of: "Domain Local groups from any domain in the same forest, or from any trusting domain"

3) Domain local group can be member of: "Local groups on computers in the same domain, excluding built-in groups that have well-known security identifiers (SIDs)"

Ref: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#:~:text=Local%20groups%20on%20computers%20in%20the%20same%20forest%20or%20trusting%20forests

upvoted 3 times

f6367e7 1 year, 3 months ago

Group1 (Universal distribution group) □ Cannot be added – not a security group. Group2 (Global security group) □ Can be added – it's from the domain and is a security group. Group3 (Local group on same computer) □ Can be added – local groups can include other local groups on the same machine.

upvoted 1 times

Knight_Of_Peace 1 year, 8 months ago

1) Universal group can be member of: "Local groups on computers in the same forest or trusting forests" 2) Global group can be member of: "Domain Local groups from any domain in the same forest, or from any trusting domain" 3) Domain local group can be member of: "Local groups on computers in the same domain, excluding built-in groups that have well-known security identifiers (SIDs)" Ref: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#:~:text=Local%20groups%20on%20computers%20in%20the%20same%20forest%20or%20trusting%20forestsI'm sorry but it's true for universal security groups, not for distribution groups. Answer is C

upvoted 3 times

cd2cfde 1 year, 4 months ago

I'm sorry but it's true for universal security groups, not for distribution groups. Answer is C

upvoted 1 times

carllaurel 1 year, 9 months ago

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups

upvoted 1 times

TedEx2 1 year, 11 months ago

it' C - you can add a global security group, but not a universal distribution group to a local group

upvoted 1 times

Pisces225 1 year, 12 months ago

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 4 times

LionelDerBoven 2 years, 2 months ago

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 2 years, 2 months ago

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 2 years, 3 months 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 2 years, 3 months ago

Lab tested on company tenant. Only security groups can be added to other groups.

upvoted 2 times

Jt909 2 years, 4 months ago

Selected Answer: A

Correct Answer is A - Lab-tested. Only Domain Security groups (universal, global and domain local) can be addedd. 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 grups and Computer Local groups...

upvoted 4 times

Cezt 2 years, 3 months ago

group nesting is not supported for local groups

upvoted 3 times

Question #36 *Topic 1*

DRAG DROP -

You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune.

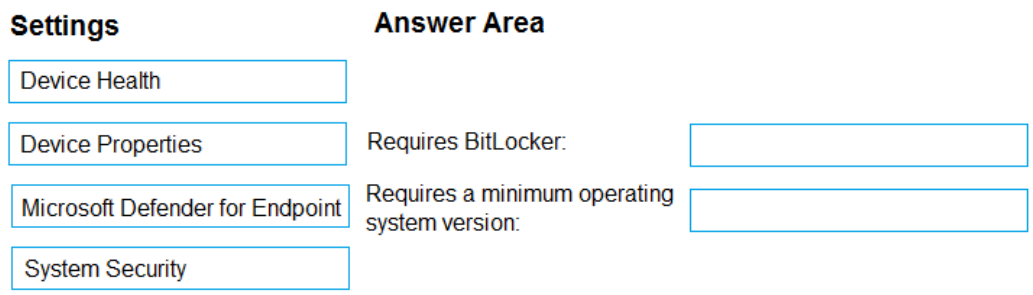
You need to create a compliance policy that meets the following requirements:

Requires BitLocker Drive Encryption (BitLocker) on each device

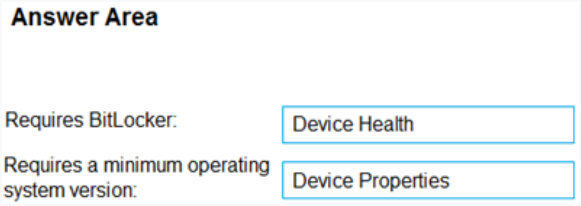
Requires a minimum operating system version

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.



Suggested Answer:



ThomasE Most Recent 1 month, 1 week ago

Minimum OS version is definitely Device Properties. However, seems BitLocker can be either Device Health or System Security. Both have BitLocker settings. Device Health is better for security-first policies where you want to trust TPM attestation and avoid blocking users mid-encryption. System Security is better for completeness-first policies where you require encryption to be fully applied before compliance. If you use conditional access, choose based on whether you want to allow access during encryption (Device Health) or only after it's complete (System Security)

upvoted 1 times

maggie22 Highly Voted 3 years, 1 month ago

it should be system security for bitlocker

upvoted 7 times

maggie22 3 years, 1 month ago

it should be system security for bitlockerIt's not. It is Device Health. https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows#device-healthCorrect: https://www.anoopcnair.com/bitlocker-compliance-policy-using-intune/My comment should be generate dudes Correct With the option posted by Maggie22no, check it in your Tenant

upvoted 7 times

ollyijeh 2 months, 2 weeks ago

Device health allows bitlocker to be configured and Device properties specifies the OS version

upvoted 1 times

Dinkan 1 year, 2 months ago

Requires BitLocker: Device Health

Minimum OS Version: Device Properties

https://learn.microsoft.com/en-us/intune/intune-service/protect/compliance-policy-create-windows#windows-health-attestation-service-evaluation-rules

https://learn.microsoft.com/en-us/intune/intune-service/protect/compliance-policy-create-windows#operating-system-version

upvoted 1 times

Casticod 3 years, 1 month ago

Correct: https://www.anoopcnair.com/bitlocker-compliance-policy-using-intune/My comment should be generate dudes Correct With the option posted by Maggie22

upvoted 1 times

Casticod 3 years, 1 month ago

Correct: https://www.anoopcnair.com/bitlocker-compliance-policy-using-intune/

upvoted 1 times

TylerSivis 1 year, 9 months ago

The Answer Is Device Health > Device Properties.

But I just want to say that this question is dumb as bricks. It basically boils down to "What is the setting syntax called" and no tech I know has this memorized by heart. Pointless Question if you ask me

upvoted 4 times

RomanV 2 years, 2 months 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 3 times

MR_Eliot 2 years, 8 months ago

Answers are correct.

upvoted 4 times

Darkfire 2 years, 9 months ago

Answers are correct idd

https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

upvoted 1 times

Amir1909 2 years, 10 months ago

Correct

upvoted 1 times

Richard_rex 3 years ago

The Answer is correct, Lab tested

upvoted 1 times

Rocky83 3 years, 1 month ago

Correct

upvoted 1 times

NoursBear 2 years, 11 months ago

no, check it in your Tenant

upvoted 1 times

gv_myra 3 years, 1 month 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 3 years, 1 month ago

My comment should be generate dudes Correct With the option posted by Maggie22

upvoted 1 times

krzysztofbr Highly Voted 3 years, 3 months ago

answers are correct

https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

upvoted 30 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You have the Windows 11 devices shown in the following table.

You deploy the device compliance policy shown in the exhibit. (Click the Exhibit tab.)

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

NOTE: Each correct selection is worth one point.

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

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

Answer Area

Statements	Yes	No
Device1 will have Policy assigned and will be marked as compliant.	○	○
Device2 will have Policy assigned and will be marked as compliant.	○	○
Device3 will have Policy assigned and will be marked as compliant.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Device1 will have Policy assigned and will be marked as compliant.	☑	○
Device2 will have Policy assigned and will be marked as compliant.	○	☑
Device3 will have Policy assigned and will be marked as compliant.	○	☑

Kiookr Highly Voted 3 years, 2 months ago

YNN , *** Excluded Groups *** group 2, and per Microsoft "exclusion" take precedence over "inclusion "

upvoted 35 times

ollyijeh Most Recent 2 months, 2 weeks ago

Excluded groups take priority so Device 3 is excluded. Device 2 has bitlocker disabled already so it will fail the compliance check. Device 1 is the only correct answer

upvoted 1 times

riccardo1999 2 years, 10 months ago

if the exclusion win the device has not compliance policy and so is compliance

upvoted 2 times

riccardo1999 2 years, 10 months ago

if the exclusion win the device has not compliance policy and so is compliancethe 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 YNNNo, 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 2 times

Sango 3 months ago

This is not a clear question as it doesn't describe the Compliance Status for devices with no Compliance Policy which is defined under Intune's Compliance Settings.

upvoted 1 times

noa808a 4 months, 3 weeks ago

Answer is correct. Device 1 is included in policy and has bitlocker enabled, making it compliant. Device 2 is included in policy but no bitlocker, so not compliant. Device 3 is excluded from policy but "compliant" if it were included, however question is asking both if the policy applies AND is marked as compliant. Therefore Yes, No, No.

upvoted 1 times

cd2cfde 1 year, 4 months ago

Ynn device 3 will not have a policy assigned because the excluded group takes precedence over the included group

upvoted 1 times

93831b0 2 years, 3 months 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 3 times

letters1234 3 years, 2 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 15 times

veliyath 2 years, 4 months 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

RazielLycas 2 years, 8 months 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 3 times

Kiookr 3 years, 1 month 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

MR_Eliot 2 years, 8 months ago

Answers are correct

upvoted 2 times

Darkfire 2 years, 9 months 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

cserra 3 years, 2 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 13 times

kaushik07 2 years, 9 months 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 2 years, 9 months ago

You can't really know if the given answer is correct, this is purely based on your default Compliane Policy Settings, if no changes have been made, Device3 will be marked compliant.

upvoted 4 times

Engr001 2 years, 10 months ago

Man, i should really read better. Or not try to study when i'm tired. It is YNN

upvoted 1 times

Amir1909 2 years, 10 months ago

Correct

upvoted 1 times

Tonsku 2 years, 11 months 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 2 years, 11 months 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 2 years, 11 months 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

NTNT 2 years, 10 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 3 years, 1 month ago

Yes

No

No

upvoted 2 times

Engr001 2 years, 10 months 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

Suresh_2411 3 years, 1 month ago

Y - policy assigned and compliant

N - policy assigned and not compliant

N - policy not assigned

N

upvoted 4 times

Engr001 2 years, 10 months 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??Man, i should really read better. Or not try to study when i'm tired. It is YNN

upvoted 1 times

Anonymous Highly Voted 3 years, 2 months ago

YNN , *** Excluded Groups *** group 2, and per Microsoft "exclusion" take precedence over "inclusion "

upvoted 36 times

665d390 2 years, 2 months ago

correct

upvoted 1 times

OyYaGotta 2 years, 8 months 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

b0gdan433 2 years, 12 months ago

Yes,No,No correct answ, took the exam today and all the points from the question.

upvoted 1 times

ubiquituz 2 years, 10 months 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 11 times

NoursBear 3 years, 2 months ago

YNY, for Device 3, Exclude wins, although this is not conventional for Microsoft, for everything else normally the most restrictive settings wins but for compliance policies it seems.

upvoted 2 times

b0gdan433 2 years, 12 months ago

Yes,No,No correct answ, took the exam today and all the points from the question.Sure, you must be the first one that gets the score points of the questions. Do not tell usnonsense.

upvoted 1 times

NoursBear 1 year, 10 months ago

changed my mind This is a wording thing re 3 the device does not get a policy at all so won't be marked as compliant but at the same time is compliant. The no is because NO he does not get the policy assigned

I have to revisit all the questions for my update assessment grrr

upvoted 1 times

NoursBear 3 years ago

The problem with this question it's not telling us what was configured under Endpoint Security under Compliance policies | Compliance policy settings, there the following setting is as follows

Mark devices with no compliance policy assigned as (compliant/not compliant). I believe the default is "compliant"

upvoted 4 times

Futfuyfyjfj 3 years, 1 month ago

You can't say whether device 3 is compliant or not. No policy is assigned, so in order to tell if the device is compliant you need to be aware of the default compliance policy, which isn't mentioned. However the question contains two components

-compliance policy assigned

-device is compliant

First one is a No, which makes YNN

upvoted 4 times

letters1234 3 years, 2 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 15 times

WORKHOLIC 2 years, 5 months ago

Y - Applies and Bitlocker enabled

N - Applies and Bitlocker disabled

N - Applies and Bitlocker disabled

upvoted 2 times

AdamRachel 2 years, 10 months 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

Anonymous 3 years, 1 month 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

cserra 3 years, 2 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 13 times

CheMetto 1 year, 6 months ago

Wow gg! i follow with YNN. i was thinkg like letters1234 so YNY because default compliance settings are to mark device as compliant if no compliance policy are assigned, but it's wrong for the question in itself. Thanks!

upvoted 1 times

NoursBear 2 years, 11 months ago

Very good point but tricky though

upvoted 1 times

TheWiz 3 years, 2 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 6 times

krzysztofbr 3 years, 2 months ago

YES

NO (because bitlocker disabled)

YES

upvoted 1 times

Futfuyfyjfj 3 years, 2 months ago

Wrong exclusion takes precedence: https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

Given answer is correct YNN, see cserra

upvoted 7 times

Question #38 *Topic 1*

DRAG DROP -

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

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.

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

Settings

- Require BitLocker
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area

Device1:

Device2:

Device3:

Suggested Answer:

Answer Area

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.

Dinkan Most Recent 1 year, 2 months ago

Device1 : Windows 10 - Require Secure Boot to be enabled on the device

Device2: iOS - Prevent jailbroken devices from having corporate access

Device3: Adnroid Enterprise - Prevent rooted devices from, having corporate access

upvoted 2 times

MR_Eliot 2 years, 8 months ago

Correct!

upvoted 2 times

Darkfire 2 years, 9 months 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 = Decive3

upvoted 2 times

RomanV 2 years, 2 months ago

" access network resources." Read between the lines.

Correct answers are:

Secure Boot --> Windows

Jailbreak --> iOS

Root -> Android

upvoted 1 times

sunil_pal12051989 2 years, 11 months ago

why not require bitlocker

upvoted 3 times

sunil_pal12051989 2 years, 11 months ago

why not require bitlocker" access network resources." Read between the lines. Correct answers are: Secure Boot --> Windows Jailbreak --> iOS Root -> Androidyou need to ensure that only devices running trusted firmware or operating system builds can access network resources.It's about accessing (being able to connect to) resources. Bitlocker doesn't necessarily prevent a connection from happening, it just encrypts data.

upvoted 3 times

Dennizje 2 years, 4 months 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 2 times

NoursBear 2 years, 9 months ago

you need to ensure that only devices running trusted firmware or operating system builds can access network resources.

upvoted 2 times

Crismo Highly Voted 3 years, 1 month ago

rooted is the term used for modified Androids, jailbroken for iOS

upvoted 9 times

krzysztofbr Highly Voted 3 years, 2 months ago

answers are correct

upvoted 15 times

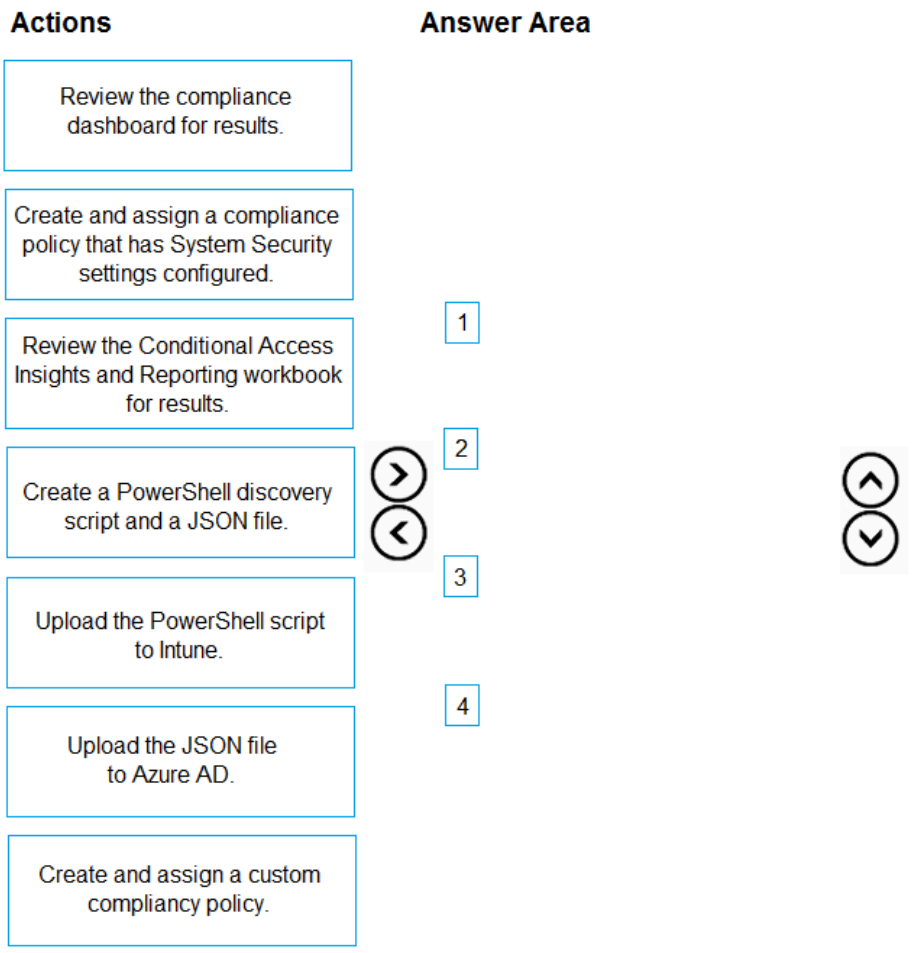
Question #39 *Topic 1*

DRAG DROP -

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.

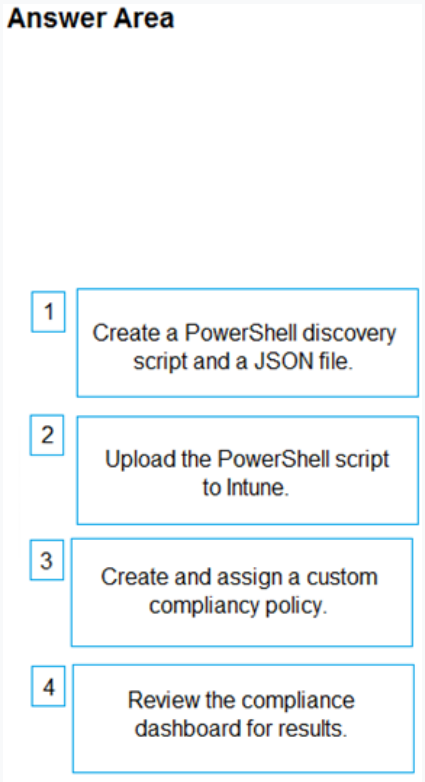
You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices.

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.



Suggested Answer:

Answer Area



ollyijeh Most Recent 2 months, 2 weeks ago

In order

create a powershell discovery script

upload the script to intune

create and assign a custom compliance policy

review the compliance dashboard for results

upvoted 1 times

AK_1234 1 year, 9 months ago

Given answer incorrect - 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 compliance policy -1. Create a PowerShell discovery script and a JSON file. - The PowerShell script is used to discover the BIOS version on the devices and outputs the result in JSON format. The JSON file defines the compliance rule (e.g., expected BIOS version) and remediation messages. 2. Upload the PowerShell script to Intune. - Before you can create the compliance policy, the discovery script must be uploaded to Intune so it can be referenced in the policy. 3. Create and assign a custom compliance policy. - With the script uploaded, you create a custom compliance policy in Intune, reference the uploaded script and the JSON rules file, and assign the policy to the relevant devices. 4. Review the compliance dashboard for results. - After deployment, you monitor the results in the Intune compliance dashboard to see which devices are compliant or noncompliant with the BIOS version requirement

upvoted 2 times

AK_1234 1 year, 9 months ago

Given answer incorrect - 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 compliance policy -

upvoted 2 times

Besxp Highly Voted 1 year, 5 months ago

1. Create a PowerShell discovery script and a JSON file.

- The PowerShell script is used to discover the BIOS version on the devices and outputs the result in JSON format. The JSON file defines the compliance rule (e.g., expected BIOS version) and remediation messages.

2. Upload the PowerShell script to Intune.

- Before you can create the compliance policy, the discovery script must be uploaded to Intune so it can be referenced in the policy.

3. Create and assign a custom compliance policy.

- With the script uploaded, you create a custom compliance policy in Intune, reference the uploaded script and the JSON rules file, and assign the policy to the relevant devices.

4. Review the compliance dashboard for results.

- After deployment, you monitor the results in the Intune compliance dashboard to see which devices are compliant or noncompliant with the BIOS version requirement

upvoted 6 times

MR_Eliot 2 years, 2 months ago

Answers are correct

upvoted 2 times

Darkfire 2 years, 2 months ago

Answers correct idd

https://learn.microsoft.com/en-us/mem/intune/protect/compliance-use-custom-settings#prerequisites

upvoted 1 times

Amir1909 2 years, 4 months ago

- create a powershell discovery script and a JSON file

- upload the powershell script to intune

- Create and assingn a custom complience policy

- upload the JSON file to Azure AD

upvoted 1 times

Alscoran 2 years, 7 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

Alscoran 2 years, 7 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.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."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 2 times

Temptset 2 years, 7 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

Temptset 2 years, 7 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 1 year, 10 months 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

krzysztofbr Highly Voted 2 years, 8 months ago

answers are corect

https://learn.microsoft.com/en-us/mem/intune/protect/compliance-use-custom-settings#prerequisites

upvoted 17 times

Question #40 *Topic 1*

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:

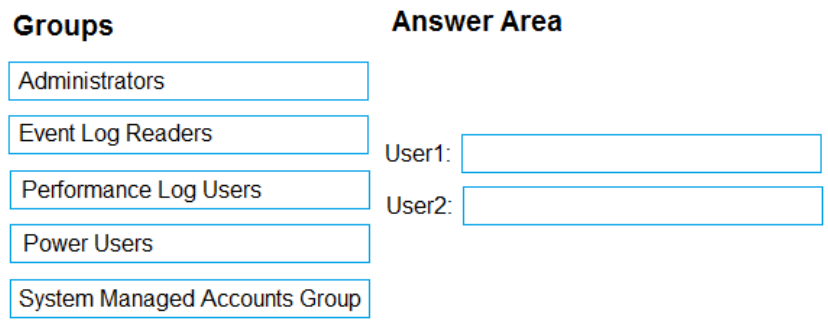
User1 must be able to adjust the date and time.

User2 must be able to clear Windows logs.

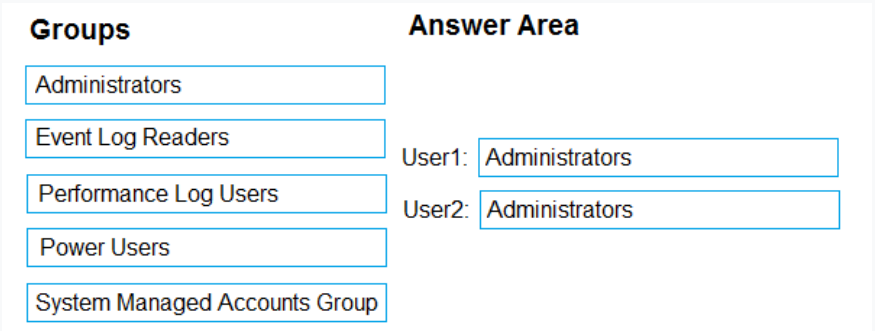
The solution must use the principle of least privilege.

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.



Suggested Answer:



volto Highly Voted 3 years, 3 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 17 times

reyrey Most Recent 9 months ago

this is the correct answer

Adjust date and time User1 Power Users

Clear Windows logscUser2 Administrators

upvoted 4 times

Futfuyfyjfj 3 years, 2 months ago

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/clear-eventlog?view=powershell-5.1That is correct, "you must be a member of the Administrators group on the affected computer."Both Administrators User1: Adjust Date and Time Default Behavior: Only members of the Administrators group can change the system date and time on Windows 10 by default. Power Users cannot change the system time (tested and confirmed). Standard Users and Event Log Readers cannot change the system time. User2: Clear Windows Logs Default Behavior: Only members of the Administrators group can clear event logs (including Security, Application, and System logs). Event Log Readers can read but not clear logs (Microsoft Docs). Performance Log Users and Power Users cannot clear logs.

upvoted 3 times

Futfuyfyjfj 3 years, 2 months ago

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/clear-eventlog?view=powershell-5.1

upvoted 3 times

jayek 1 year, 8 months ago

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771990(v=ws.10)#:~:text=Default%20local%20groups,-Article

upvoted 1 times

Garrick98 3 years, 1 month ago

That is correct, "you must be a member of the Administrators group on the affected computer."

upvoted 2 times

cd2cfde 1 year, 4 months ago

Omg.😷 The Event Log Readers group in Windows allows users to view event logs but does not grant permission to clear or delete them. To clear event logs, a user must have administrative privileges. This is confirmed by multiple sources stating that you must be signed in as an administrator to clear event logs, whether using Event Viewer, Command Prompt, or PowerShell. Standard users and members of the Event Log Readers group cannot perform this action.

upvoted 2 times

yhano 2 years 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 2 times

larry_derby 2 years 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 2 years, 3 months 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 2 years, 4 months ago

Administrators for both. Lab tested on Windows 10 22H2 domain-joined. With Power Users and Performance Log Users always access denied .

upvoted 10 times

LukeXtreme 2 years, 5 months 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

AK_1234 1 year, 9 months ago

Answer incorrect: - User1- Administrator (Members of the Administrators group have the necessary permissions to change system settings, including the date and time.) - User2 -event log readers (Members of the Event Log Readers group have the necessary permissions to read and clear Windows logs.)

upvoted 2 times

AK_1234 1 year, 9 months ago

Answer incorrect: - User1- Administrator (Members of the Administrators group have the necessary permissions to change system settings, including the date and time.) - User2 -event log readers (Members of the Event Log Readers group have the necessary permissions to read and clear Windows logs.)Omg.😳 The Event Log Readers group in Windows allows users to view event logs but does not grant permission to clear or delete them. To clear event logs, a user must have administrative privileges. This is confirmed by multiple sources stating that you must be signed in as an administrator to clear event logs, whether using Event Viewer, Command Prompt, or PowerShell. Standard users and members of the Event Log Readers group cannot perform this action.

upvoted 2 times

mail2bala3011 2 years, 7 months ago

I justed tested on my lab

User1: Administrator

User2 : Administrator

Administrator can perform both action

upvoted 8 times

sergioandreslq 2 years, 8 months 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 2 years, 8 months ago

In Windows 10 & 11 you can change the timezone without any admin priviliges. Hower when you want to change the date and time settings, it will ask you for admin permissions.

So my anwers:

1: Administrators

2: Administrators. Performance log users can only shedule colletion of logs. Not remove the system logs.

upvoted 3 times

Softeng 2 years, 9 months ago

- User 1: Administrator

- User 2: Administrator

https://community.spiceworks.com/topic/2244141-power-users-vs-local-admins

upvoted 1 times

Judith1969 2 years, 9 months 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 2 years, 9 months 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 2 times

Amir1909 2 years, 10 months ago

- Administrators

- Administrators

upvoted 1 times

Tonsku 2 years, 11 months ago

user1: power users

user2: administrators

upvoted 3 times

belyo 2 years, 11 months 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 2 years, 11 months 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

Darkfire 2 years, 9 months 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.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 3 times

Darkfire 2 years, 9 months 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

cpaljchc4 3 years ago
According to Chat GPT

1. For User 1 to adjust the date and time, they typically need to be part of the "Administrators" group or have specific permissions granted for modifying the system time.

2. For User2 to clear Window logs, they usually need to be part of the "Event Log Readers" or "Backup Operators" group to access and manage event logs without elevated privileges.

If there are no better answer and explanation here, I am going to follow ChatGPT...
upvoted 1 times

iTomi 2 years, 11 months ago
ChatGPT is reliable as a Kremlin spokesperson.
upvoted 4 times

NoursBear 2 years, 11 months ago
I sure would not use Chat GPT haha
upvoted 2 times

kay000001 2 years, 12 months ago
haha you will fail for sure!
upvoted 2 times

Daveazure 3 years ago
I think they are mixing it up with 365 RBAC.
upvoted 1 times

Garrick98 3 years ago
Both answers are Administrators
upvoted 1 times

poppinaz 3 years, 1 month ago
Tested in lab: only Administrators can perform the two actions
upvoted 6 times

BoomerangFist 1 year, 11 months ago
I actually tested on my lab and surprisingly the deletion of log can be done by power users

User1: Administrator (adjust the date and time)

User2: Power User (clear Windows logs)
upvoted 1 times

midhunkk 3 years, 1 month ago
Administrator can perform these settings, but is it uses the principle of least privilege?

in my opinion answer given is correct
upvoted 1 times

Rocky83 3 years, 1 month ago
Answers are wrong, both settings need Administrator permission
upvoted 3 times

BJS78 3 years, 1 month ago
https://droidrant.com/what-rights-do-power-users-have-in-windows-10/
upvoted 2 times

NoursBear 3 years, 2 months ago
I think both answers are Administrators. Nothing mentioning the Performance Monitor
upvoted 3 times

NoursBear 3 years, 2 months ago
I will also add "the Power Users Group was made obsolete in Windows Vista" according to an article however I see that Power Users is still on WIndows 10, so for the Date and Time change Power Users would be correct but don't think it is still in use
upvoted 2 times

letters1234 3 years, 2 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 15 times

volto Highly Voted 3 years, 3 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 18 times

Garrick98 3 years, 1 month ago

That is correct, "you must be a member of the Administrators group on the affected computer."

upvoted 2 times

Besxp 1 year, 5 months ago

Both Administrators

User1: Adjust Date and Time

Default Behavior:

Only members of the Administrators group can change the system date and time on Windows 10 by default.

Power Users cannot change the system time (tested and confirmed).

Standard Users and Event Log Readers cannot change the system time.

User2: Clear Windows Logs

Default Behavior:

Only members of the Administrators group can clear event logs (including Security, Application, and System logs).

Event Log Readers can read but not clear logs (Microsoft Docs).

Performance Log Users and Power Users cannot clear logs.

upvoted 2 times

Futfuyfyjfj 3 years, 2 months ago

https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/change-the-system-time#default-values

upvoted 3 times

Question #41 *Topic 1*

HOTSPOT -

You have an Azure AD tenant named contoso.com.

You have the devices shown in the following table.

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.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	Ubuntu Linux

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

Suggested Answer:

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**

krzysztofbr Highly Voted 2 years, 8 months ago

answers are correctAzure 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 15 times

krzysztofbr Highly Voted 2 years, 8 months ago

answers are correct

upvoted 15 times

GarrethM Most Recent 1 year, 4 months ago

Azure AD joined: Device1 and Device2 only

Registered in contoso.com: Device1, Device2, Device3, and Device4

upvoted 2 times

hieunm2411 1 year, 9 months ago

Please take note that as of Feb 2025, Microsoft Entra joined for Apple devices running macOS 13 or newer is in Public preview. https://learn.microsoft.com/en-us/entra/identity/devices/concept-directory-join So the correct answers should be Device 1, 2 and 3 for the first question.Device3 is an iOS, not a MacOS. Only Device1 and Device2 can be joined to Entra AD.Correct! Azure AD joined: Device1 and Device2 only Registered in contoso.com: Device1, Device2, Device3, and Device4

upvoted 2 times

hieunm2411 1 year, 9 months ago

Please take note that as of Feb 2025, Microsoft Entra joined for Apple devices running macOS 13 or newer is in Public preview. https://learn.microsoft.com/en-us/entra/identity/devices/concept-directory-join So the correct answers should be Device 1, 2 and 3 for the first question.

upvoted 2 times

ExamBud 1 year, 8 months ago

Device3 is an iOS, not a MacOS. Only Device1 and Device2 can be joined to Entra AD.Correct! Azure AD joined: Device1 and Device2 only Registered in contoso.com: Device1, Device2, Device3, and Device4

upvoted 3 times

ExamBud 1 year, 8 months ago

Device3 is an iOS, not a MacOS. Only Device1 and Device2 can be joined to Entra AD.

upvoted 3 times

Besxp 1 year, 5 months ago

Correct!

Azure AD joined: Device1 and Device2 only

Registered in contoso.com: Device1, Device2, Device3, and Device4

upvoted 2 times

MR_Eliot 2 years, 2 months 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 4 times

Darkfire 2 years, 2 months 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 2 years, 3 months ago

Correct

upvoted 1 times

Amir1909 2 years, 4 months ago

Correct

upvoted 1 times

yosry 2 years, 4 months ago

seems correct

upvoted 1 times

kay000001 2 years, 6 months ago

Answer are correct.

Can only AD join windows devices.

Can register any device.

upvoted 1 times

krzysztofbr 2 years, 8 months ago

ad join win10 and 11 Ad registered all platforms including linux

upvoted 3 times

krzysztofbr 2 years, 8 months ago

ad join win10 and 11 Ad registered all platforms including linuxshouldnt be opposite then ad join is contoso.com (Directory name) so only 1 and 2 and Azure AD all devices so 1234

upvoted 3 times

Futfuyfyjfj 2 years, 8 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 10 times

mirak123 2 years, 8 months 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

Question #42 *Topic 1*

HOTSPOT -

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

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.

UserA joins Computer1 to Azure AD by using .

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

NOTE: Each correct selection is worth one point.

Name	Role
Admin1@contoso.com	Security Administrator
Admin2@contoso.com	Cloud Device Administrator
User1@contoso.com	*None*

Name	Member of
Administrator1	Network Configuration Operators
Administrator2	Power Users
UserA	Administrators

Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	○	○
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	○	○
Admin2@contoso.com can install software on Computer1.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	○	○
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	○	○
Admin2@contoso.com can install software on Computer1.	○	○

letters1234 Highly Voted 3 years, 2 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 36 times

letters1234 Highly Voted 3 years, 2 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.Yes. When a device is Azure AD joined, the user who performs the join () is automatically added to the local Administrators group. No. Having the Security Administrator role in Azure AD does NOT grant local admin rights on the device, so Admin1 cannot change these settings. No. The Cloud Device Administrator role allows device management in Azure AD, but does NOT provide local admin rights needed to install software.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/2025358The link you provided doesnt clarify anything. In the article is probably reffered to the 'Azure AD Joined Device Local Administrator' role and not the Cloud device Administrator roleThis 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 groupI 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-administratorCloud Device Admin and Device/Global Admin are not same.

upvoted 36 times

ollyijeh Most Recent 2 months, 2 weeks ago

YNN

Cloud Device Administrator is only admin within the Azure portal. To make these changes on the device you would need to be a local adminsitrator which user1 is

Security administrator does not grant local aDMIN EITHER

upvoted 2 times

Besxp 1 year, 5 months ago

Yes. When a device is Azure AD joined, the user who performs the join (user1@contoso.com) is automatically added to the local Administrators group.

No. Having the Security Administrator role in Azure AD does NOT grant local admin rights on the device, so Admin1 cannot change these settings.

No. The Cloud Device Administrator role allows device management in Azure AD, but does NOT provide local admin rights needed to install software.

upvoted 2 times

Le_Patriarche2025 9 months ago

d accord avec la réponse

upvoted 1 times

Futfuyfyjfj 3 years, 2 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 5 times

Futfuyfyjfj 3 years, 2 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/2025358The link you provided doesnt clarify anything. In the article is probably reffered to the 'Azure AD Joined Device Local Administrator' role and not the Cloud device Administrator roleThis 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 groupI 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-administratorCloud Device Admin and Device/Global Admin are not same.

upvoted 5 times

hieunm2411 1 year, 9 months ago

The Security Administrator can indirectly configure the firewall and defender on a device, but the question didn't mention the device enrolled in Intune so the correct answer is YNN.

upvoted 1 times

ExamKiller020 3 years, 1 month ago

The link you provided doesnt clarify anything. In the article is probably reffered to the 'Azure AD Joined Device Local Administrator' role and not the Cloud device Administrator roleThis 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 4 times

ExamKiller020 3 years, 1 month ago

The link you provided doesnt clarify anything. In the article is probably reffered to the 'Azure AD Joined Device Local Administrator' role and not the Cloud device Administrator role

upvoted 4 times

Tr619899 1 year, 12 months ago

YNN is the answer

upvoted 2 times

LionelDerBoven 2 years, 2 months 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 2 years, 3 months ago

YNN

As of now, user peforming 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 2 times

mail2bala3011 2 years, 7 months ago

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#security-administrator

upvoted 1 times

Softeng 2 years, 9 months 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 2 years, 9 months 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 6 times

Merrybob 2 years, 9 months ago

NYN is correct

upvoted 7 times

NoursBear 2 years, 9 months ago

I didn't mean the answers are correct from the question, but with YNN above

upvoted 4 times

NoursBear 2 years, 10 months 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 2 years, 11 months 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 3 times

yosry 2 years, 11 months 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 2 years, 11 months 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 " 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 6 times

NoursBear 2 years, 9 months 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 autocreated user. Users signing in after a device has been joined aren't added to the administrators group. answers are correctI didn't mean the answers are correct from the question, but with YNN above

upvoted 2 times

NoursBear 2 years, 9 months 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 autocreated user. Users signing in after a device has been joined aren't added to the administrators group.

answers are correct

upvoted 2 times

NoursBear 2 years, 11 months ago

Security Administrator

Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.

It is a Priviledged role, but unable to understand what that actually means

upvoted 1 times

benpatto 3 years 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 3 times

NoursBear 2 years, 10 months 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 2 years, 10 months 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.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

benpatto 3 years 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

Contactfornitish 3 years, 1 month ago

YNN

The user performing the join would become local admin by default

ref: https://learn.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin

Security admin would not get local admin and can not change firewall rules.

Cloud device admin can do a number of things at azure end including even adding users to local admin but would not be local admin himself by default

upvoted 4 times

Anonymous 3 years, 2 months ago

Please read carefully " Computer1 is in a workgroup" WORKGROUP " meaning is not joined to domain .. so any member of "local Admin" has full right on Computer1 .. I believe the answer should be NO-NO-NO

upvoted 3 times

iTomi 2 years, 11 months 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

HvD 3 years, 1 month ago

The suer which joins the computer to Azure AD is made local Administrator.

upvoted 1 times

NoursBear 2 years, 11 months 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.Security Administrator Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365. It is a Priviledged role, but unable to understand what that actually means

upvoted 1 times

NoursBear 2 years, 11 months 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

picho707 3 years, 1 month ago

I agree with you on this one based on the article below. Please read the NOTE at the start of the article "This is done during the join operation only. If an administrator makes changes after this point they will need to update the group membership on the device"

https://learn.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin

upvoted 1 times

BJS78 3 years, 1 month ago

Does not matter as UserA joins the device to AAD. User1 has no special local permission.

Cloud Device Admin (usually referred as Device Admin) becomes part of local Admin group after join. Security Admin cannot change firewall rules as I think.

upvoted 4 times

Capital 3 years, 2 months ago

Tested in my lab environment - Security Admin can't edit firewall settings and Cloud Device Admin can install software.

Security Administrator - Can read security information and reports, and manage configuration in Azure AD and Office 365.

Cloud Device Administrator is marked as a privileged role.

upvoted 4 times

NoursBear 3 years, 2 months ago

For me the answers are correct.

upvoted 1 times

NoursBear 3 years ago

Scrap that.. Used to think the second answer was a yes but no, I checked the security admin role and it can manage stuff under Endpoint Security but since firewall settings are under a device configuration profile, the security admin has no rights to create or change such profiles. So it really looks like YNN like letters1234 explains

upvoted 1 times

JP1900 3 years, 2 months ago

letters1234 is correct, it is YNN.

upvoted 14 times

Besxp 1 year, 5 months ago

Yes.

When a device is Azure AD joined, the user who performs the join () is automatically added to the local Administrators group.

No.

Having the Security Administrator role in Azure AD does

NOT grant local admin rights on the device, so Admin1 cannot change these settings.

No.

The Cloud Device Administrator role allows device management in Azure AD, but does NOT provide local admin rights needed to install software.

upvoted 2 times

SajjH 2 years, 3 months ago

Cloud Device Admin and Device/Global Admin are not same.

upvoted 1 times

Alscoran 3 years, 1 month 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

NoursBear 2 years, 9 months 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

letters1234 3 years, 2 months ago

Link - https://learn.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin

Not sure either, there is the possibility in a Deployment Profile to disable AP built devices providing local admin to the signed in user but that's not part of the use case.

(Out-of-box experience: User account type - Standard)

upvoted 1 times

volto 3 years, 3 months ago

"When you connect a Windows device with Azure AD using an Azure AD join, Azure AD adds the following security principals to the local administrators group on the device:

The Azure AD Global Administrator role

The Azure AD joined device local administrator role

The user performing the Azure AD join."

Why is the second answer marked as yes?

upvoted 2 times

NoursBear 2 years, 10 months ago

Same here I cannot see anywhere, where a Security Admin can configure Defender and Firewall on devices.

upvoted 1 times

Question #43 *Topic 1*

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

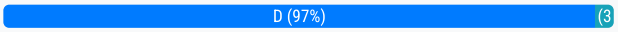
B. Remote Desktop Users

C. Power Users

D. Remote Management Users

Suggested Answer: *D*

Community vote distribution



theptr Most Recent 1 year, 4 months ago

Selected Answer: D

Answer D is correct

upvoted 2 times

SajjH 2 years, 3 months 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 2 years, 6 months 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 2 years, 8 months 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 2 years, 8 months 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 2 years, 8 months 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 2 years, 8 months ago

Selected Answer: D

D for sure

upvoted 1 times

Darkfire 2 years, 8 months ago

Selected Answer: D

D is correct.

See Letters1234 comment..

upvoted 1 times

Krayzr 2 years, 9 months ago

Selected Answer: D

D. Remote Management Users

upvoted 1 times

Merrybob 2 years, 9 months ago

D is right.

upvoted 1 times

Amir1909 2 years, 10 months ago

D is correct

upvoted 1 times

onepunchkenshin 2 years, 10 months ago

ChatGPT tells D

upvoted 1 times

Tonsku 2 years, 11 months ago

Selected Answer: D

D. remote management users

upvoted 1 times

belyo 2 years, 11 months ago

Selected Answer: D

its about PowerShell remoting, not about RDP connections

definitely D

upvoted 1 times

NoursBear 2 years, 11 months ago

I finally found the article proving D https://4sysops.com/archives/powershell-remoting-without-administrator-rights/

upvoted 1 times

NoursBear 2 years, 11 months ago

I finally found the article proving D https://4sysops.com/archives/powershell-remoting-without-administrator-rights/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 1 times

NoursBear 2 years, 11 months 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 2 years, 11 months ago

Answer is correct, it does not say less management it says least privilege.Not quite.. Remote DESKTOP User doesn't give rights to use PowerShell Remote. Two different thing.

upvoted 2 times

madsa 2 years, 11 months ago

Answer is correct, it does not say less management it says least privilege.

upvoted 2 times

iTomi 2 years, 11 months ago

Not quite.. Remote DESKTOP User doesn't give rights to use PowerShell Remote. Two different thing.

upvoted 1 times

chandravamsi 3 years ago

Selected Answer: D

Option: D

upvoted 1 times

fco168 3 years ago

Selected Answer: D

Remote Management Users is the group that allows remoting with PS. RDP is a separate tool than PS.

upvoted 2 times

Contactfornitish 3 years, 1 month ago

Selected Answer: D

RDP is such a nonsense

Remote management users

Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.

upvoted 1 times

NoursBear 3 years, 2 months ago

For me it's D too. On a video with sample questions, this one came up and they are adamant that it is the RDP group. I guess the questions and answers come from the same source

upvoted 1 times

NoursBear 3 years ago

Having a doubt now:

PowerShell Remoting default settings

PowerShell Remoting (and WinRM) listen on the following ports:

HTTP: 5985

HTTPS: 5986

By default, PowerShell Remoting only allows connections from members of the Administrators group. Sessions are launched under the user's context, so all operating system access controls applied to individual users and groups continue to apply to them while connected over PowerShell Remoting.

upvoted 1 times

minasamy 3 years, 2 months ago

Selected Answer: D

A, B, C are not really related to PowerShell

upvoted 3 times

letters1234 Highly Voted 3 years, 2 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

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 19 times

JP1900 3 years, 3 months ago

Selected Answer: B

Read the question carefully, it states: "The solution must use the principle of least privilege."

Use the Remote Management Users group to allow users to manage servers through the Server Manager console.

upvoted 1 times

HvD 3 years, 1 month ago

I think you believe the users will be able to access all servers (remotely). But that's only true if the GPO (also) is applied to the servers(OU). That's not a wise thing to do.

upvoted 1 times

Futfuyfyjfj 3 years, 2 months ago

You selected answer B, but you are telling answer D?

upvoted 4 times

volto 3 years, 3 months ago

Selected Answer: D

@rmac read above

"Members of the Remote Management Users group can access Windows Management Instrumentation (WMI) resources over management protocols like WS-Management via the Windows Remote Management service."

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#remote-management-users

upvoted 1 times

Joe9011 3 years, 3 months ago

D.

https://woshub.com/powershell-remoting-via-winrm-for-non-admin-users/

upvoted 1 times

rmac 3 years, 3 months ago

Not sure if this is the right answer.

"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."

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#remote-management-users

upvoted 1 times

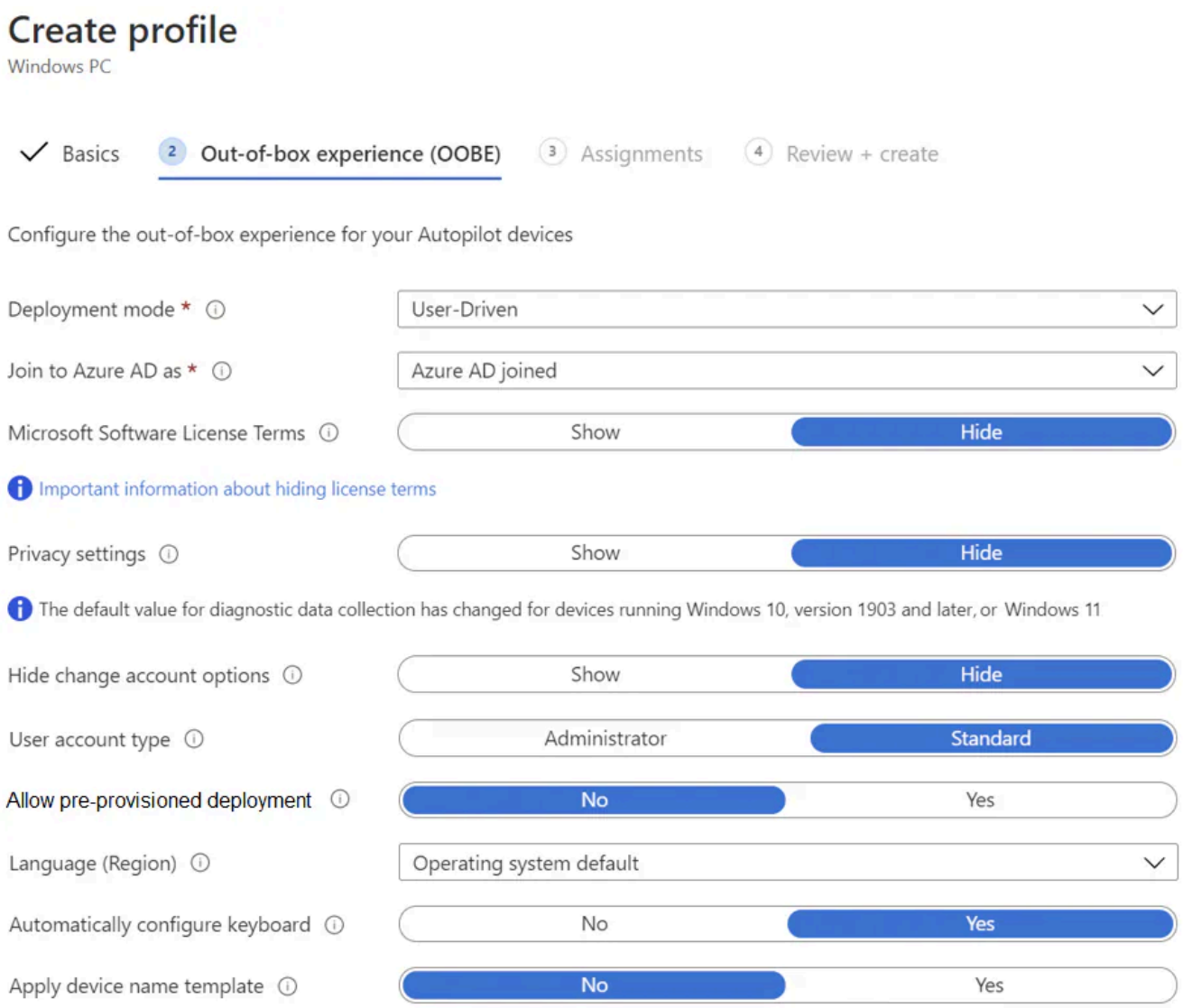
HOTSPOT -

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.

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].**

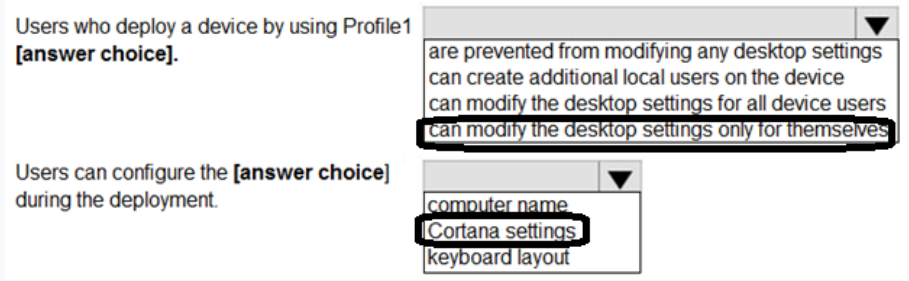
- are prevented from modifying any desktop settings
- can create additional local users on the device
- can modify the desktop settings for all device users
- can modify the desktop settings only for themselves

Users can configure the **[answer choice]** during the deployment.

- computer name
- Cortana settings
- keyboard layout

Suggested Answer:

Answer Area



fco168 Highly Voted 3 years 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 19 times

fco168 Highly Voted 3 years 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.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.You are absolutely wrong!!! It's obvious that some of you have never utilized autopilot. When the device name template is set to no then it allows the user to choose their own name during deployment. I can't believe there are so many wrong answers that people are positive about. The answer to number 2 is without a doubt "computer name"RIP Cortana, they should make a new AI that can make powershell scripts with voice commands lolThey should call it Copilot.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 20 times

NakatomiTower Most Recent 11 months ago

This question is crap. Cortana? Seriously? It was depreciated in 2023. Lift your game examtopics.

upvoted 3 times

LionelDerBoven 2 years, 2 months 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.You are absolutely wrong!!! It's obvious that some of you have never utilized autopilot. When the device name template is set to no then it allows the user to choose their own name during deployment. I can't believe there are so many wrong answers that people are positive about. The answer to number 2 is without a doubt "computer name"

upvoted 1 times

henil_154762 1 year, 2 months ago

Users who deploy a device using Profile1: can modify the desktop settings only for themselves.

Reason: The profile sets User account type = Standard, so the first user is not a local admin and can only change settings that don't affect other users.

Microsoft Learn

+1

Users can configure during the deployment: keyboard layout.

Reason: The profile has Automatically configure keyboard = Yes, but Language (Region) = Operating system default. The keyboard page is skipped only if a specific Language (Region) is selected; otherwise the keyboard selection can still appear during OOBE.

upvoted 2 times

batang_aratan 1 year, 9 months ago

Answer to question 2 should be "computer name"

https://learn.microsoft.com/en-us/autopilot/windows-autopilot-scenarios#cortana-voiceover-and-speech-recognition-during-oobe

upvoted 3 times

F3RRY 3 years ago

RIP Cortana, they should make a new AI that can make powershell scripts with voice commands lolThey should call it Copilot.

upvoted 3 times

F3RRY 3 years ago

RIP Cortana, they should make a new AI that can make powershell scripts with voice commands lol

upvoted 3 times

hieunm2411 1 year, 9 months ago

The answer to the second question is keyboard layout. Windows lets users select and add additional keyboard layouts at the beginning of the installation before the autopilot profile is pushed down to the device.

upvoted 1 times

Tr619899 1 year, 12 months 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 11 times

Besxp 1 year, 5 months ago

Correct! (shorter version)

1. can modify the desktop settings only for themselves

2. "Keyboard layout" is the right answer for the second question, given the settings.

Any answer stating "computer name" is configurable by the user during OOBE is outdated or incorrect.

upvoted 1 times

yhano 2 years 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 3 times

Tr619899 1 year, 12 months 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 10 times

LionelDerBoven 2 years, 2 months 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

RomanV 2 years, 2 months ago

There is.

upvoted 1 times

Burkidur 2 years, 8 months ago

But it says right there on the screenshot "Automatically configure keyboard: Yes"

upvoted 7 times

Merrybob 2 years, 9 months 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 2 years, 10 months ago

- can modify the Desktop settings only for themselves

- Computer Name

upvoted 6 times

oopspruu 2 years, 2 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

oopspruu 2 years, 2 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.There is.

upvoted 1 times

Greatone1 2 years, 11 months ago

Correct answers is only for themselves and keyboard layout.

https://www.examtopics.com/discussions/microsoft/view/64041-exam-md-101-topic-2-question-51-discussion/

upvoted 3 times

madsa 2 years, 11 months ago

Even if keyboard is set, while on the OOE you can modify the Keyboard, as it just highlights it. So prevented from modifying any desktop settings and Keyboard.

upvoted 1 times

MR_Eliot 2 years, 8 months ago

I agree with the first one. Second one should be keyboard layout since cortana is dead and langauge setting are not configured

upvoted 2 times

MR_Eliot 2 years, 8 months ago

I agree with the first one. Second one should be keyboard layout since cortana is dead and langauge setting are not configuredBut it says right there on the screenshot "Automatically configure keyboard: Yes"

upvoted 2 times

cd2cfde 1 year, 5 months ago

You are absolutely wrong!!! It's obvious that some of you have never utilized autopilot. When the device name template is set to no then it allows the user to choose their own name during deployment. I can't believe there are so many wrong answers that people are positive about. The answer to number 2 is without a doubt "computer name"

upvoted 8 times

Valavanchandran 2 years, 9 months 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

OyYaGotta 2 years, 8 months ago

They should call it Copilot.

upvoted 13 times

NoursBear 3 years 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 3 years, 1 month ago

What a bunch are rubbish

upvoted 2 times

ExamKiller020 3 years, 1 month 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

picho707 3 years, 2 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 2 years, 8 months 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

NoursBear 3 years, 2 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 3 years, 1 month ago

This is true only if you set the Region above fixed and not the using the default.

upvoted 2 times

NoursBear 2 years, 11 months 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 3 years, 2 months ago

Agree with prevented from modfiying 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 3 years, 3 months ago

Correct answers: are prevented from modifying any desktop settings

and Keyboard Layout

upvoted 2 times

HvD 3 years, 1 month ago

Why would a normal user not be able to change any setting, like desktop background, volume, default printer, etc?

upvoted 1 times

Question #45 *Topic 1*

HOTSPOT -

You have a server named Server1 and computers that run Windows 10. Server1 has the Microsoft Deployment Toolkit (MDT) installed.

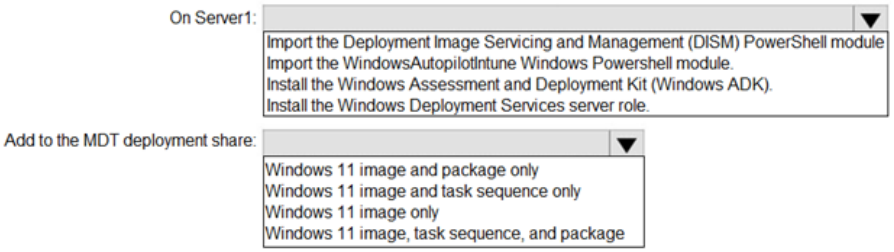
You plan to upgrade the Windows 10 computers to Windows 11 by using the MDT deployment wizard.

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.

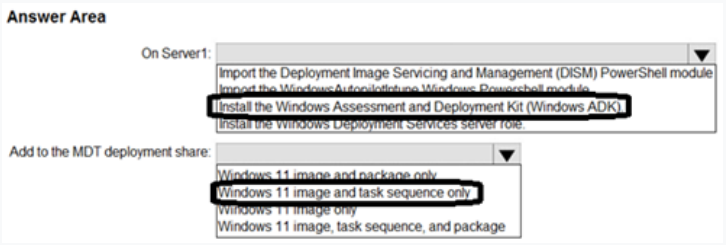
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



650afa5 Highly Voted 2 years, 5 months ago

I took the exam yesterday June 11th. This question was on there.How did it go?

upvoted 7 times

650afa5 Highly Voted 2 years, 5 months ago

I took the exam yesterday June 11th. This question was on there.

upvoted 6 times

ThomasE 4 weeks ago

Just took the MD-102 exam on 10/19/2026. There was not a single question about MDT. Still not a bad technology to know because many customers use it, but it wasn't tested on. There were quite a few questions about CoPilot usage in Intune and Defender.

upvoted 3 times

XxJoshuaxX Most Recent 1 week ago

Thanks for the insights

upvoted 1 times

ExamDumpEnjoyer 2 years, 7 months ago

MDT is being deleted as of 26 April 2024. Question no longer relevant.

upvoted 5 times

ExamDumpEnjoyer 2 years, 7 months ago

MDT is being deleted as of 26 April 2024. Question no longer relevant.What is your source? You can't say something so delicate like that out of nowhere.Actually dude It's true: Is MDT deleted? □ No, MDT is not deleted, but it will no longer be supported after October 10, 2025. Why? Microsoft is phasing out old tools like VBScript and IE components that MDT relies on. MDT won't be updated for future Windows versions. Should I still use it? □ You can use it for now, but it's best to start moving to newer tools like: - SCCM (ConfigMgr) - Windows Autopilot - WDS with PowerShell scripts

upvoted 5 times

Tr619899 1 year, 12 months 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 2 times

Pollosor 2 years, 3 months ago

What is your source?

You can't say something so delicate like that out of nowhere.

upvoted 1 times

Pollosor 2 years, 3 months ago

What is your source? You can't say something so delicate like that out of nowhere.Actually dude It's true: Is MDT deleted? □ No, MDT is not deleted, but it will no longer be supported after October 10, 2025. Why? Microsoft is phasing out old tools like VBScript and IE components that MDT relies on. MDT won't be updated for future Windows versions. Should I still use it? □ You can use it for now, but it's best to start moving to newer tools like: - SCCM (ConfigMgr) - Windows Autopilot - WDS with PowerShell scripts

upvoted 1 times

Zoom2020 2 years, 2 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 anwser.

upvoted 3 times

RomanoSmooth81 2 years, 4 months ago

How did it go?

upvoted 1 times

Besxp 1 year, 5 months ago

Actually dude It's true:

Is MDT deleted?

□ No, MDT is not deleted, but it will no longer be supported after October 10, 2025.

Why?

Microsoft is phasing out old tools like VBScript and IE components that MDT relies on.

MDT won't be updated for future Windows versions.

Should I still use it?

□ You can use it for now, but it's best to start moving to newer tools like:

- SCCM (ConfigMgr)

- Windows Autopilot

- WDS with PowerShell scripts

upvoted 1 times

Softeng 2 years, 9 months 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%20Deployment%20Kit%20(Windows%20ADK)

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#packages (also take a look at the 'Task sequence' section below 'Packages').

upvoted 3 times

Softeng 2 years, 9 months 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%20Deployment%20Kit%20(Windows%20ADK) 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#packages (also take a look at the 'Task sequence' section below 'Packages').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 you can include a package, such as a 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 include a package are wrong. MSFT says 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 3 times

OyYaGotta 2 years, 8 months ago

WDS is not a pre-requisite for ADK. Answer is correct.

upvoted 2 times

MR_Eliot 2 years, 8 months ago

Correct!

upvoted 3 times

Merrybob 2 years, 9 months 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

Merrybob 2 years, 9 months 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-sharesIncorrect: 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 1 times

Darkfire 2 years, 8 months ago

Answers are correct.

upvoted 2 times

Pisces225 1 year, 12 months 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 you can include a package, such as a 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 include a package are wrong. MSFT says 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

krzysztofbr 3 years, 2 months ago

seems to be ok. not 100% sure

upvoted 3 times

krzysztofbr 3 years, 2 months ago

seems to be ok. not 100% sureAgreed: 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-adkWin11 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 3 times

Anonymouse1312 2 years, 9 months 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 2 years, 11 months 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 2 years, 11 months ago

Answer is correct.

upvoted 1 times

Futfuyfyjfj 3 years, 2 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

Futfuyfyjfj 3 years, 2 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

Question #46 *Topic 1*

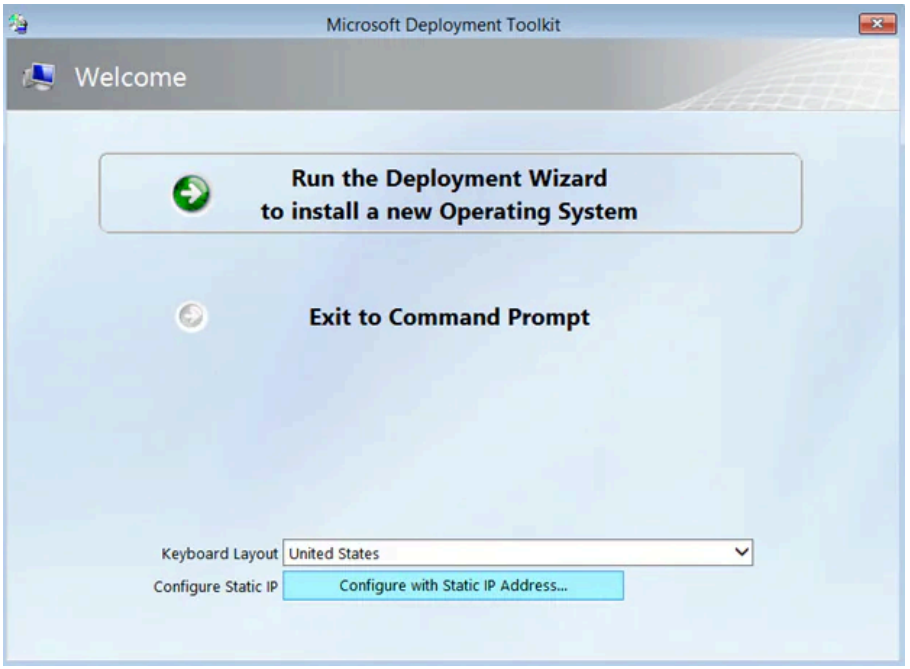
DRAG DROP -

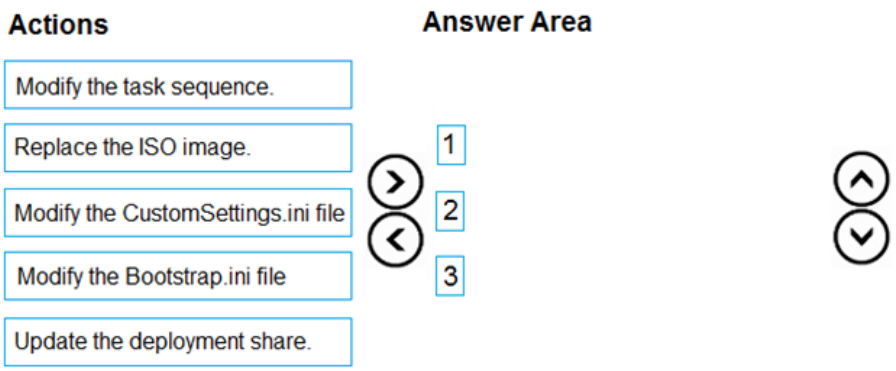
You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

When computers start from the LiteTouchPE_x64.iso image and connect to MDT1, the welcome screen appears as shown in the following exhibit.

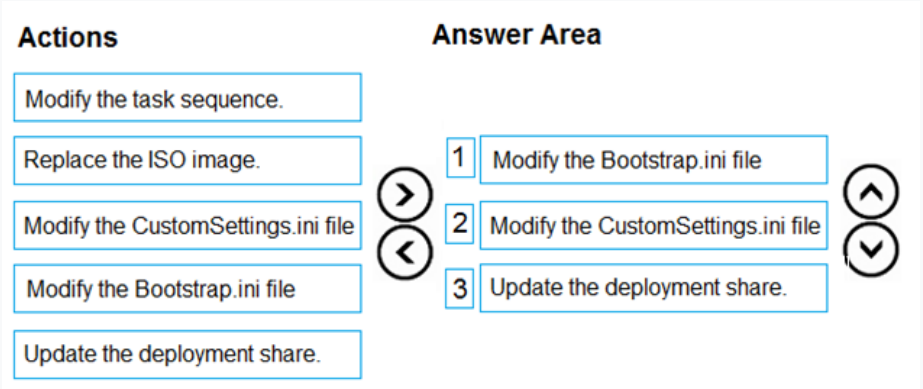
You need to prevent the welcome screen from appearing when the computers connect to MDT1.

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.





Suggested Answer:



JP1900 Highly Voted 3 years, 2 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 34 times

JP1900 Highly Voted 3 years, 2 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.https://www.examtopics.com/discussions/microsoft/view/80401-exam-md-101-topic-2-question-98-discussion/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 itModify 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 35 times

ModernoDecor Most Recent 8 months, 2 weeks ago

question is no longer relevant

upvoted 1 times

Le_Patriarche2025 9 months ago

Réponse exacte

upvoted 1 times

reyrey 9 months ago

correct answer - Modify the Bootstrap.ini file → Update the deployment share → Replace the ISO image

upvoted 1 times

Dinkan 1 year, 2 months ago

1. Modify Bootstrap.ini

2. Modify CustomSettings.ini

3. Update deployment share

SkipBDDWelcome indicates whether the Welcome to Windows Deployment wizard page is skipped. For this property to function properly it must be configured in both CustomSettings.ini and BootStrap.ini. BootStrap.ini is processed before a deployment share (which contains CustomSettings.ini) has been selected.

Reference:

https://learn.microsoft.com/en-us/intune/configmgr/mdt/properties#skipbddwelcome

upvoted 2 times

letters1234 3 years, 2 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).Your reference proves your answer is correct!

upvoted 19 times

letters1234 3 years, 2 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 19 times

f6367e7 1 year, 3 months ago

Correct Sequence

Modify Bootstrap.ini

Update deployment share

Replace the ISO image

CustomSettings.ini is for skipping other wizard panes (like language, computer name, domain join), not the BDD welcome page.

Modify the task sequence has nothing to do with the welcome screen.

upvoted 2 times

Tr619899 1 year, 11 months ago

1. Modify the Bootstrap.ini file

2. Update the Deployment Share

3. Replace the ISO Image

upvoted 3 times

LionelDerBoven 2 years, 2 months 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 6 times

LionelDerBoven 2 years, 2 months ago

Only after september 17 2024

upvoted 3 times

Burkidur 2 years, 8 months 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 2 years, 8 months 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 3 times

Merrybob 2 years, 9 months ago

Boostrap.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 2 years, 10 months ago

- Modify the CustomSettings.ini file

- Modify the BootStrap.ini file

- update the deployment Share

upvoted 3 times

yosry 2 years, 11 months ago

Modify the boostrap.ini file

Modify the CustomStettings.ini file

Update the deployment Share

upvoted 1 times

ExamDumpEnjoyer 2 years, 7 months ago

MDT being deleted from the exam as of 26 April 2024. Question not relevant.Only after september 17 2024

upvoted 11 times

ExamDumpEnjoyer 2 years, 7 months ago

MDT being deleted from the exam as of 26 April 2024. Question not relevant.

upvoted 11 times

Contactfornitish 3 years, 1 month 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 3 years, 1 month ago

1. Modify the Bootstrap.ini file

2. Update the deployment share

3. Replace the ISO image

upvoted 4 times

Futfuyfyjfj 3 years, 2 months ago

Your reference proves your answer is correct!

upvoted 3 times

krzysztofbr 3 years, 2 months ago

answer seems to be wron

should be

Modify the task sequence

Modify the bootsrap 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

iamchoy 1 year, 11 months 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 2 years, 8 months ago

https://www.examtopics.com/discussions/microsoft/view/80401-exam-md-101-topic-2-question-98-discussion/

upvoted 1 times

Valavanchandran 2 years, 9 months ago

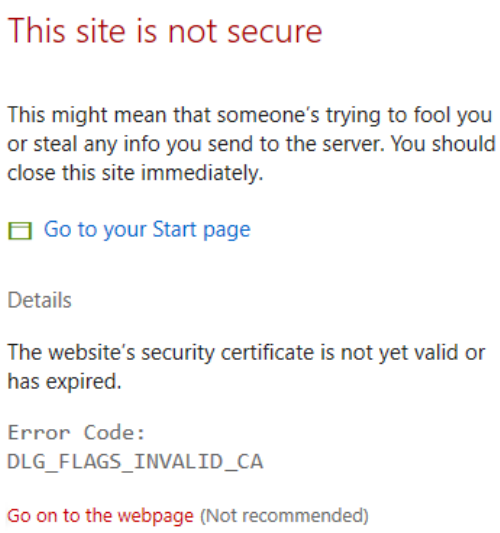
incorrect bootstrap.ini is baked into ISO. Customsettings parses the variables for TS actions , correct answer, Modify bootstrap, update dep share and replace the iso by recreating it

upvoted 4 times

Question #47 *Topic 1*

You use Windows Admin Center to remotely administer computers that run Windows 10.
When connecting to Windows Admin Center, you receive the message shown in the following exhibit.

You need to prevent the message from appearing when you connect to Windows Admin Center.
To which certificate store should you import the certificate?



A. Client Authentication Issuers

B. Personal

C. Trusted Root Certification Authorities

Suggested Answer: *C*

Community vote distribution

C (100%)

Dinkan Most Recent 1 year, 2 months ago
C. Trusted Root Certification Authorities Tested and confirmed
upvoted 1 times

Vlado123 2 years, 3 months ago
Correct answer is B, check on your device after installing Admin Center where is the certificate
upvoted 1 times

MR_Eliot 2 years, 8 months ago
Agreed
upvoted 1 times

Darkfire 2 years, 8 months ago
C is correct. https://learn.microsoft.com/en-us/windows-hardware/drivers/install/trusted-root-certification-authorities-certificate-store
upvoted 1 times

Amir1909 2 years, 10 months ago
C is correct
upvoted 1 times

fco168 3 years ago
C it is!
upvoted 1 times

ZaFletch 3 years, 1 month ago
Error references CA
upvoted 3 times

letters1234 3 years, 2 months ago

Trusted Root

upvoted 2 times

krzysztofbr 3 years, 2 months ago

You need "Certification Authorities" answer C

upvoted 2 times

Question #48 *Topic 1*

HOTSPOT -

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Contoso.com contains the Azure AD groups shown in the following table.

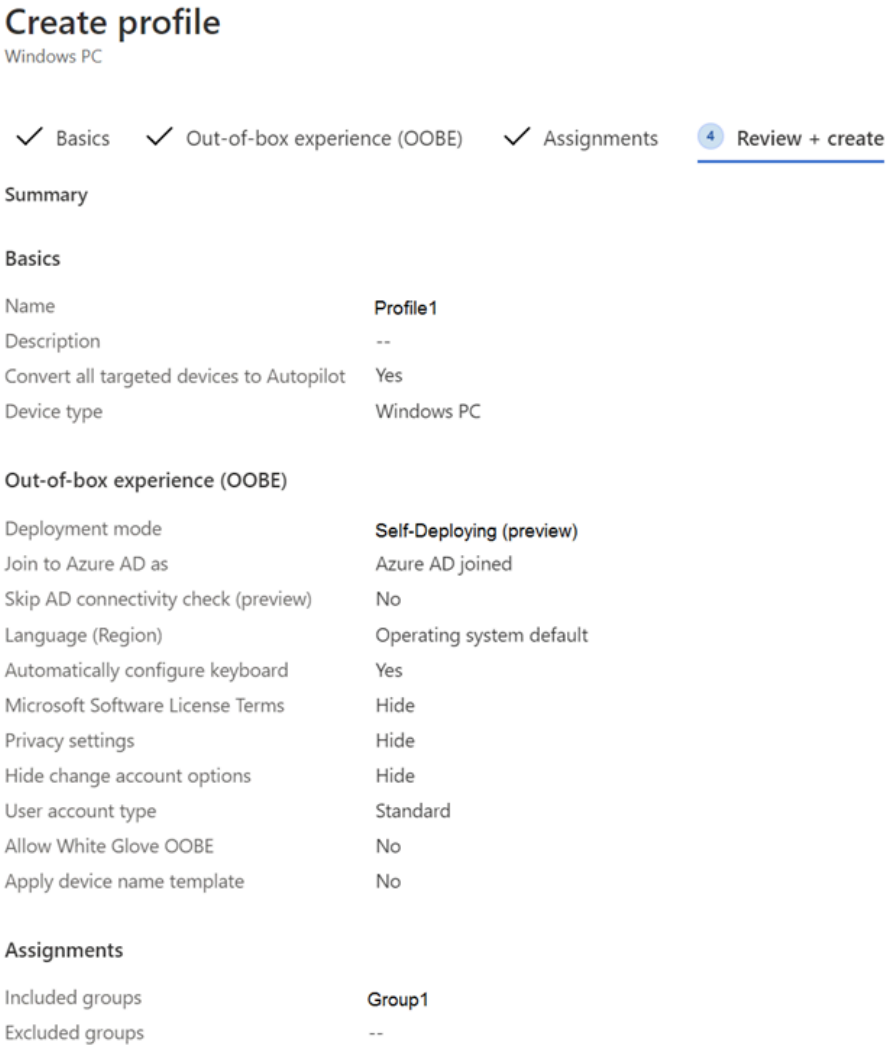
You add a Windows Autopilot deployment profile. The profile is configured as shown in the following exhibit.

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

NOTE: Each correct selection is worth one point.

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

Name	Members
Group1	Group2, Device1, Device3
Group2	Device2



Answer Area

Statements	Yes	No
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	◙
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	◙
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	◙	○

Crismo Highly Voted 3 years, 1 month 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 25 times

Crismo Highly Voted 3 years, 1 month 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.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.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-requirementsIt 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!Let's not confuse people now! It's NNY Comments suggesting YNY or YNY are incorrect because Device1 is only AAD Registered (BYOD-type). Device2 is a toss-up, but due to no Intune + nested group, it should be No. Microsoft's own tools (and testing evidence) support the NNY answer. So yes, most of the upvoted comments are partly or wholly wrong, or at least based on misunderstandings of Autopilot's dependence on device state and group assignment behavior.Device1 is registered = private in Entra (AAD).

upvoted 25 times

Le_Patriarche2025 Most Recent 9 months ago

NNY a l'air correcte. les deux premiers devices non pas enrollés sur Intune , donc ils peuvent pas être pris en compte dans le profil de déploiement.

upvoted 2 times

airmancompsci 3 years, 1 month 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 7 times

airmancompsci 3 years, 1 month 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.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-requirementsIt 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!Let's not confuse people now! It's NNY Comments suggesting YNY or YNY are incorrect because Device1 is only AAD Registered (BYOD-type). Device2 is a toss-up, but due to no Intune + nested group, it should be No. Microsoft's own tools (and testing evidence) support the NNY answer. So yes, most of the upvoted comments are partly or wholly wrong, or at least based on misunderstandings of Autopilot's dependence on device state and group assignment behavior.Device1 is registered = private in Entra (AAD).

upvoted 7 times

cpaljchc4 3 years 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

Dinkan 1 year, 2 months ago

Though there is no official confirmation, intune seems to support nested groups, but the answer still stands as "Convert all targeted devices to Autopilot" requires device to be enrolled in a mobile device management (MDM) service such as Intune as per the documentation

https://learn.microsoft.com/en-us/autopilot/automatic-registration

upvoted 1 times

Drainev 2 years, 10 months 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 4 times

Drainev 2 years, 10 months 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!Let's not confuse people now! It's NNY Comments suggesting YNY or YNY are incorrect because Device1 is only AAD Registered (BYOD-type). Device2 is a toss-up, but due to no Intune + nested group, it should be No. Microsoft's own tools (and testing evidence) support the NNY answer. So yes, most of the upvoted comments are partly or wholly wrong, or at least based on misunderstandings of Autopilot's dependence on device state and group assignment behavior.

upvoted 4 times

hieunm2411 1 year, 9 months ago

The correct answer is NNY.

If the "Convert all targeted devices to Autopilot" option in the Autopilot profile is enabled, then:

When a device is Azure AD Joined or Hybrid Azure AD Joined and managed by Intune, if it is not already in the Autopilot list (does not have a hardware hash), Intune will automatically collect the hardware hash and add the device to the Autopilot list.

Device 1 is Azure AD Registered so if the device is only Azure AD Registered, Intune will not convert it to an Autopilot device, even if the option is enabled.

Device 2 is Azure AD Joined, but it isn't managed by Intune.

upvoted 4 times

CheMetto 1 year, 6 months ago

yes correct. to do so automatically, you need to enable on the entra side: choose as provider MDM intune, enable auto enrollment.

upvoted 2 times

d3a3d8a 2 years 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 2 years, 2 months 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 OOBE. 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 2 years, 2 months ago

You need an MDM. So it's no, no, yes

upvoted 3 times

Dinkan 1 year, 2 months ago

No, No, Yes Automatic registration of existing devices requires the device to be enrolled in a mobile device management (MDM) service such as Intune (Ref: https://learn.microsoft.com/en-us/autopilot/automatic-registration) Hence Device 1 will not be deployed using Autopilot. Device 2 is not Intune Joined, also the policy will not apply to it as Entra/Intune will not honor nested groups.Though there is no official confirmation, intune seems to support nested groups, but the answer still stands as "Convert all targeted devices to Autopilot" requires device to be enrolled in a mobile device management (MDM) service such as Intune as per the documentation https://learn.microsoft.com/en-us/autopilot/automatic-registration

upvoted 1 times

Dinkan 1 year, 2 months ago

No, No, Yes

Automatic registration of existing devices requires the device to be enrolled in a mobile device management (MDM) service such as Intune (Ref: https://learn.microsoft.com/en-us/autopilot/automatic-registration) Hence Device 1 will not be deployed using Autopilot.

Device 2 is not Intune Joined, also the policy will not apply to it as Entra/Intune will not honor nested groups.

upvoted 1 times

MJFT 2 years, 7 months 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 2 years, 8 months 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

hieunm2411 1 year, 9 months ago

The correct answer is NNY. If the "Convert all targeted devices to Autopilot" option in the Autopilot profile is enabled, then: When a device is Azure AD Joined or Hybrid Azure AD Joined and managed by Intune, if it is not already in the Autopilot list (does not have a hardware hash), Intune will automatically collect the hardware hash and add the device to the Autopilot list. Device 1 is Azure AD Registered so if the device is only Azure AD Registered, Intune will not convert it to an Autopilot device, even if the option is enabled. Device 2 is Azure AD Joined, but it isn't managed by Intune.

upvoted 4 times

Darkfire 2 years, 9 months ago

I also think its YNY

https://learn.microsoft.com/en-us/autopilot/automatic-registration#windows-autopilot-for-existing-devices

upvoted 1 times

kaushik07 2 years, 9 months 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 2 years, 9 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 2 years, 10 months ago

So then the given answer is correct....

upvoted 2 times

NoursBear 2 years, 10 months ago

OK this question is still annoying after t he 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 2 years, 10 months ago

YNY!!!

upvoted 1 times

mp34 2 years, 10 months 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 4 times

mp34 2 years, 10 months 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....So then the given answer is correct....

upvoted 4 times

AdamRachel 2 years, 10 months ago

device one it is not register in Intune.

upvoted 2 times

BJS78 2 years, 10 months 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 2 years, 10 months 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

frack 2 years, 10 months 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

frack 2 years, 10 months 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.device one it is not register in Intune.

upvoted 1 times

mhmyz 2 years, 10 months 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 2 years, 9 months 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 2 years, 9 months 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 2 years, 9 months 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 2 years, 11 months 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 belive they are trying to makes 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

Tonsku 2 years, 11 months ago

N, N, Y

Device1 W11 Register None

device2 W10 Joined None

device3 W11 Joined Intune

Group1: Group2, Device1, Device3

Group2: Device2

OOBE:

Azure AD Joined

Include: Group1

Exclude: None

upvoted 2 times

iTomi 2 years, 11 months ago

I think all should be NO.

From book "Exam Ref MD-102 Microsoft Endpoint Administrator" by Warren and Bettany

"Devices to be deployed using Windows Autopilot must be in a generalized state. The OEM vendor normally performs this and allows the device to boot into the OOBE when first turned on. Generalized devices have all user and computer-specific information removed. If you want to generalize a Windows computer or VM, you can use the Sysprep utility, which can be found at C:\windows\system32\sysprep\sysprep.exe. Alternatively, in Windows 11, you can use the Reset your PC option in the Settings app."

upvoted 1 times

NoursBear 2 years, 11 months ago

Maybe this will help:

How does Windows Autopilot work?

Windows Autopilot is included in a large number of Microsoft subscription services, including Microsoft 365 Academic A1, A3 and A5 subscriptions, Microsoft Enterprise E3 and E5 subscriptions. Best of all, Microsoft Autopilot is also included in a Microsoft 365 Business Premium subscription – putting this advanced technology in the hands of even the smallest business.

Autopilot enables the remote set up of devices but, to manage the entire lifecycle of that device remotely, you'll need to pair it with a mobile device management (MDM) solution.

The natural partner to Windows Autopilot is Microsoft Intune (we'll look at Intune in more detail in a subsequent blog). However, contrary to popular understanding, it isn't necessary to use Autopilot with Intune. You can use Autopilot with any MDM solution.

Hence those with no MDM would be a No in any case

upvoted 1 times

madsa 2 years, 11 months ago

Yes No Yes is correct as airman says.

upvoted 1 times

madsa 2 years, 11 months ago

Devices do not need to be enrolled to pick up and autopilot profile, all they need is HID imported and to be assigned to a security group. This question is ambiguous.

upvoted 3 times

DiFortes 3 years ago

NNY seems correct to me

device 1 is registered, personal possibly, therefore autopilot wont work on it?

Windows Autopilot is only for organization-owned devices. For BYOD or personal devices, use Windows automatic enrollment (in this article) or a User enrollment option (in this article).

https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-windows

upvoted 1 times

NoursBear 3 years ago

User-driven mode for Microsoft Entra join

To complete a user-driven deployment using Windows Autopilot, follow these preparation steps:

Make sure that the users performing user-driven mode deployments can join devices to Microsoft Entra ID. For more information, see Configure device settings in the Microsoft Entra documentation.

User-driven mode for Microsoft Entra hybrid join

Windows Autopilot requires that devices be Microsoft Entra joined. If you have an on-premises Active Directory environment, you can join devices to your on-premises domain. To join the devices, configure Autopilot devices to be hybrid-joined to Microsoft Entra ID.

upvoted 1 times

fco168 3 years ago

The devices can be joined or registered with Entra ID. Don't have to be all joined Devices. That's the reason why you have a config option in Autopilot to Join the devices automatically.

upvoted 1 times

VirtualJP 3 years, 1 month ago

This is one of those annoying Microsoft exam questions.

The probelm I have with it is that there is no mention as to whether any of these devices are Autopilot enrolled.

Additionally, if you initiate OOBE the computer name is going to reset, and so with no clarity on the Autopilot enrollment state and the name resetting, unless the same name is reapplied during the OOBE phase the AD group memberships for these devices won't take effect.

With that said, if the computer names did remain the same and the devices matched the AD group memberships, my answer would be:

Y

N - still not sure about this one, as it's a nested group

Y

Overall though, I'm not sure what the 'correct' answer would or should be here.

upvoted 2 times

fco168 3 years ago

It's true, Autopilot does not support nested groups. I agree with

Y

N

Y

upvoted 1 times

VirtualJP 3 years, 1 month ago

I'm revising my answer to NNN

To have a device automatically enrolled in Autopilot, you need to set up Autopilot profiles and initiate the enrollment process during the device's initial setup. Autopilot enrollment requires specific configuration and provisioning during the device's initial setup or a reset, typically using the Autopilot deployment profile.

Further, if a devidce undergoes an Out of Box Experience (OOBE) reboot, it will not automatically enroll with Windows Autopilot, again for the same reasons as above.

upvoted 1 times

picho707 3 years, 1 month ago

Autopilot and Licensing assignment do not support nesting so the policy will not apply to device2. I learned this the hard way during a deployment.

upvoted 2 times

93831b0 2 years, 2 months ago

Device1 is registered = private in Entra (AAD).

upvoted 1 times

cpaljchc4 3 years 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

Dinkan 1 year, 2 months ago

You are wrong.

While Autopilot will work without being enrolled into intue, if you have uploaded the hash or use the autopilot json or provisioning package, the feature mentioned here "Convert all targeted devices to Autopilot" required device to be Enrolled in a mobile device management (MDM) service such as Intune

https://learn.microsoft.com/en-us/autopilot/automatic-registration

upvoted 1 times

Besxp 1 year, 5 months ago

Let's not confuse people now! It's NNY

Comments suggesting YNY or YNY are incorrect because Device1 is only AAD Registered (BYOD-type).

Device2 is a toss-up, but due to no Intune + nested group, it should be No.

Microsoft's own tools (and testing evidence) support the NNY answer.

So yes, most of the upvoted comments are partly or wholly wrong, or at least based on misunderstandings of Autopilot's dependence on device state and group assignment behavior.

upvoted 1 times

krzysztofbr 3 years, 2 months ago

answer C, might be ok. is all about MDM

in the other hand I'm not sure:)

upvoted 1 times

Futfuyfyjfj 3 years, 2 months ago

Answers are correct

upvoted 1 times

Question #49 *Topic 1*

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:

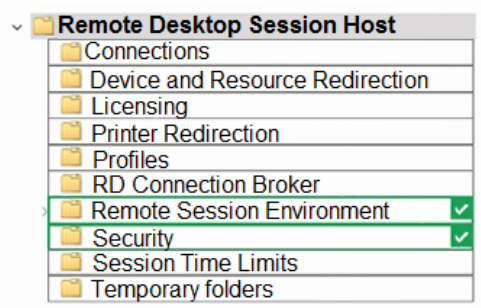
Prevent the sharing of clipboard contents.

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.

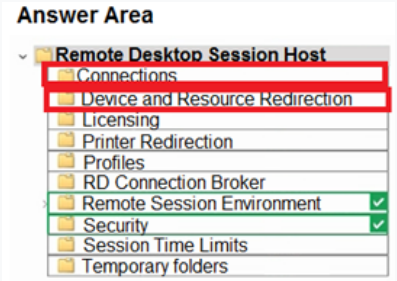
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



Tr619899 Most Recent 1 year, 11 months ago

Answer is: Device and Resource Re-direction and Security

upvoted 5 times

BJS78 3 years, 1 month ago

Clipboard --> Device and Resource Redirection \ Do not allow Clipboard redirection NLA --> Security \ Require user authentication for remote connections by using NLA

upvoted 15 times

Merrybob 2 years, 9 months ago

Device and Resource Redirection (Clipboard Redirection)

Security (NLA)

upvoted 2 times

Amir1909 2 years, 10 months ago

- Device and Resource Redirection

- Security

upvoted 1 times

Krayzr 2 years, 10 months ago

Device and Resource Re-direction

Security

upvoted 2 times

cpaljchc4 3 years 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

BJS78 Highly Voted 3 years, 1 month ago

Clipboard --> Device and Resource Redirection \ Do not allow Clipboard redirection

NLA --> Security \ Require user authentication for remote connections by using NLA

upvoted 16 times

Temptset 3 years, 1 month 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 3 times

letters1234 Highly Voted 3 years, 2 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 29 times

Question #50 *Topic 1*

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.

You are preparing to upgrade the devices to Windows11. 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.

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

Answer Area

Windows Autopilot:
- None of the devices
- Device1 only
- Device1 and Device3 only
- Device1, Device2, and Device3

In-place upgrade:
- None of the devices
- Device1 only
- Device1 and Device3 only
- Device1, Device2, and Device3

Suggested Answer:

Answer Area

Windows Autopilot: None of the devices

In-place upgrade: Device1 and Device3 only

Le_Patriarche2025 Most Recent 9 months ago

Je valide la réponse. cette phrase précise : (Vous devez évaluer Windows Autopilot et la mise à niveau en place comme méthodes de déploiement pour implémenter Windows 11 Pro sur les appareils, tout en conservant tous les paramètres utilisateur et applications) c 'est le piège vu que Win Autopilot fait le reset.

In-Place Upgrade : pas de 32 Bits sur Win11

upvoted 1 times

ExamKiller020 Highly Voted 3 years, 1 month 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 13 times

ExamKiller020 3 years, 1 month 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 wrongIt says all devices is compatible with Win 11 but there is a 32 bit machine..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.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 13 times

386abb2 1 year, 9 months ago

But if the question says "All the devices are compatible with Windows 11." we shouldn't be bothered about device 2 being 32-bit

upvoted 1 times

cpaljchc4 3 years ago

It says all devices is compatible with Win 11 but there is a 32 bit machine..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 3 times

cpaljchc4 3 years ago

It says all devices is compatible with Win 11 but there is a 32 bit machine..

upvoted 3 times

Dinkan 1 year, 2 months ago

They must have been talking about hardware compatability (TPM, SecureBoot, Processor, etc)

upvoted 1 times

Tr619899 1 year, 11 months ago

1. None of the Devices

2. Device 1 and 3 only

upvoted 3 times

AleFCI1908 2 years 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 2 years, 2 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 2 years, 2 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

386abb2 1 year, 9 months ago

But if the question says "All the devices are compatible with Windows 11." we shouldn't be bothered about device 2 being 32-bit

upvoted 1 times

oopspruu 2 years, 4 months 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

RazielLycas 2 years, 8 months 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 2 years, 9 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 10 times

St_Ives 2 years, 8 months ago

it took me a few times to re-read the part on AutoPilot, but I go for this answer.

upvoted 1 times

Pugmohone 2 years, 9 months 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 2 times

AdamRachel 2 years, 10 months 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 2 times

Amir1909 2 years, 10 months ago

- None

- Device1 and Device3 only

upvoted 4 times

mp34 2 years, 10 months 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

Merrybob 2 years, 9 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 10 times

Tati_Oliveira 2 years, 11 months 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 2 years, 11 months ago

The answer is correct due to the line of business app, I overlooked that.

upvoted 1 times

madsa 2 years, 11 months ago

The only possible answer here is 1 and 3 only on both

upvoted 1 times

Tr1v 3 years 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

Contactfornitish 3 years, 1 month ago

Auto pilot doesn't update the device OS version

in place upgrade always possible if upgrade path available, can't do that for 32bit to 64bit so device 1 and device 3

upvoted 3 times

maggie22 3 years, 1 month ago

Windows Autopilot for existing devices lets you reimage and provision a Windows device for Autopilot user-driven mode using a single, native Configuration Manager task sequence. The existing device can be on-premises domain-joined. The end result is a Windows 10 or Windows 11 device joined to either Azure Active Directory (Azure AD) or Active Directory (hybrid Azure AD join).

upvoted 1 times

Casticod Highly Voted 3 years, 1 month 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 33 times

Rocky83 3 years, 1 month ago

"none of the devices" - You cant upgrade windows version through autopilot, you have to use Intune Features Updates

Device 1 and 3 only - In-place Upgrade for 32 bits to 64 is not supported.

Tricky one

upvoted 7 times

Temptset 3 years, 1 month ago

You seem to be right as I can only find references that upgrade from Windows 10 to 11 through WUfB, with that being said:

"Feature updates for Windows 10 and later policies cannot be applied during the Autopilot out of box experience (OOBE). Instead, the policies apply at the first Windows Update scan after a device has finished provisioning, which is typically a day"

https://learn.microsoft.com/en-us/mem/intune/protect/windows-10-feature-updates#limitations-for-feature-updates-for-windows-10-and-later-policy

upvoted 2 times

iTomi 2 years, 11 months 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 3 years, 1 month 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 4 times

BJS78 3 years, 1 month ago

1 - Autopilot requires no existence in AzureAD (Think of OEM devices enrolled), hashID-s needs to be uploaded and that is it. (Works with VMs as well), so all device can work.

https://learn.microsoft.com/en-us/autopilot/software-requirements#next-steps

https://learn.microsoft.com/en-us/autopilot/networking-requirements

2 - 32-bit has no in-place upgrade option as W11 comes only with 64bit version

upvoted 2 times

NoursBear 2 years, 11 months ago

yes but with Hybrid, the devices have to be already joined however it is irrelevant here:

User-driven mode for Microsoft Entra hybrid join

Windows Autopilot requires that devices be Microsoft Entra joined. If you have an on-premises Active Directory environment, you can join devices to your on-premises domain. To join the devices, configure Autopilot devices to be hybrid-joined to Microsoft Entra ID.

upvoted 1 times

cserra 3 years, 2 months ago

1 - Autopilot requires being in AzureAD, other two devices are not joined.

But "All devices are compatible with Windows 11", then all support 64 bit OS. Then:

1, 2 & 3 can be updated.

upvoted 1 times

NoursBear 3 years, 2 months ago

How can devices be Azure AD "joined" in advance for new computers ? I can understand they have to be uploaded into Intune (unique identifier) before staging, if they are Computers already AD joined, existing devices, well they are already known and in Intune, I think Feature Updates would be used and not Autopilot

No devices qualify for Autopilot, Autopilot requires having WIndows 11 already

upvoted 2 times

NoursBear 1 year, 10 months ago

actually they are not new computers lol

upvoted 1 times

Futfuyfyjfj 3 years, 2 months ago

But device 2 has Win10 32 bit installed, in that case an in place upgrade to Win11 64 bit isn't possible right? Regardless whether the hardware supports it?

upvoted 1 times

Fortind1974 3 years, 2 months ago

Correct.

It would need to be a 32-bit in-place upgrade. But Win11 is only available in 64-bit, so a full wipe and install is needed.

upvoted 2 times

letters1234 3 years, 2 months ago

1 - Autopilot requires being in AzureAD, other two devices are not joined.

1 & 3 - CPU requirement is 64bit for windows 11 - https://www.microsoft.com/en-us/windows/windows-11-specifications#table1 -

upvoted 2 times

Question #51 *Topic 1*

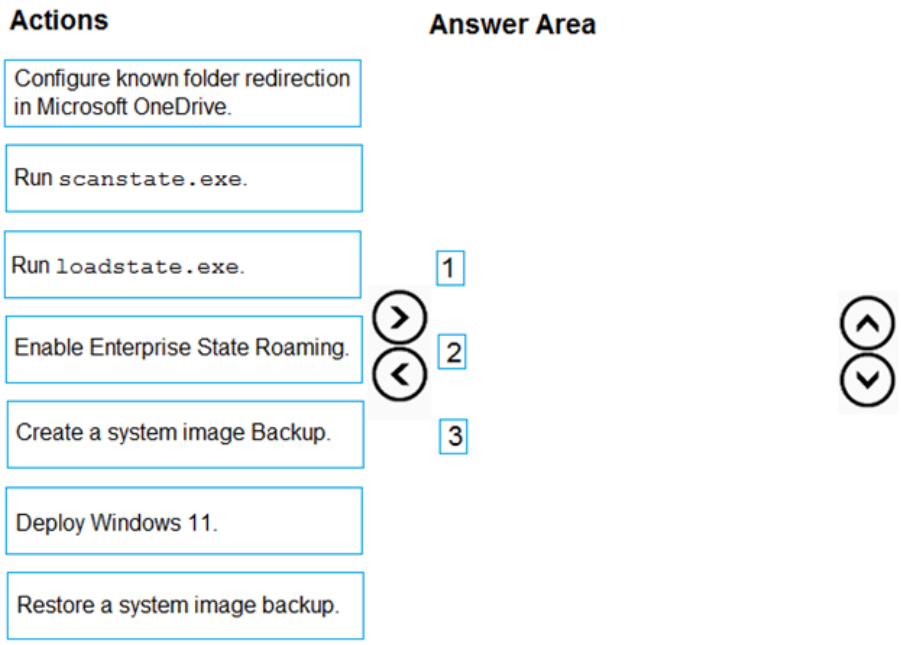
DRAG DROP -

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.



Suggested Answer:

Answer Area

1. Run scanstate.exe.
2. Deploy Windows 11.
3. Run loadstate.exe.

Dinkan 1 year, 2 months ago

1. Run Scanstate

2. Deploy Windows 11

3. Run LoadState.exe

upvoted 2 times

benpatto Highly Voted 3 years 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?This is a microsoft exam. Not a "workplace" exam. Why would microsoft not be testing you on their own programs/services/features? If you want to learn how to do a job function, do some job training instead.

upvoted 9 times

benpatto 3 years 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 9 times

oopspruu 2 years, 4 months 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 2 years, 4 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 2 years, 8 months ago

Provided answer is correct.

upvoted 2 times

Darkfire 2 years, 8 months 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 2 years, 9 months ago

Sounds about right!

upvoted 2 times

frack 2 years, 10 months ago

considering known folder redirection to onedrive was already configured, this is correct

upvoted 1 times

Amir1909 2 years, 10 months ago

Correct

upvoted 1 times

madsa 2 years, 11 months 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

noa808a Most Recent 4 months, 3 weeks ago

This is a microsoft exam. Not a "workplace" exam. Why would microsoft not be testing you on their own programs/services/features? If you want to learn how to do a job function, do some job training instead.

upvoted 1 times

krzysztofbr Highly Voted 3 years, 2 months ago

answers are correct

https://learn.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax

upvoted 10 times

letters1234 3 years, 2 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

Question #52 *Topic 1*

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 Most Recent 2 years, 4 months ago

Selected Answer: C

"Turn on log collection and diagnostics page for end users" set to YES in ESP settings.

upvoted 3 times

veliyath 2 years, 4 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 2 years, 8 months ago

Answer is correct.

upvoted 1 times

Darkfire 2 years, 9 months 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 2 years, 9 months ago

Selected Answer: C

C

ESP allows users to collect troubleshooting logs

upvoted 1 times

Amir1909 2 years, 10 months ago

Correct

upvoted 1 times

madsa 2 years, 11 months ago

Turn on log collection and diagnostics page for end users

Yes, the answer is correct.

upvoted 1 times

cpaljchc4 3 years 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

cpaljchc4 3 years 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 2 years, 10 months 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 3 years 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 3 years, 2 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 3 years, 2 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

Question #53 *Topic 1*

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 Devic1 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.

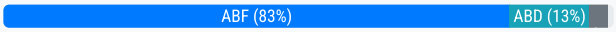
D. Assign a Microsoft 365 E5 license to User1.

E. Rerun device onboarding on Device1.

F. Assign the Remote Help add-on license to User1.

Suggested Answer: *A, B, F*

Community vote distribution



rmac Highly Voted 3 years, 3 months ago

From my point of view, the solution is: A,B,Freference: https://learn.microsoft.com/en-us/mem/intune/fundamentals/remote-help#prerequisitesThe license is already assigned in the statement of the question.Disregard my previous comment. The license assigned is the O365, not the Intune Remote Help!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-onsMicrosoft 365 E5 subscription include Intune Plan 1, so add-on is required. https://www.microsoft.com/en-us/security/business/microsoft-intune-pricing#:~:text=Microsoft%20Intune%20Remote%20Help!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?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?Let's stop confusing people, ABF is correct! A. Deploy the Remote Help app to Device1. The app must be installed for Remote Help to work. B. Assign the Help Desk Operator role to User1. This role gives User1 permission to start Remote Help sessions in Intune. F. Assign the Remote Help add-on license to User1. Remote Help requires a specific license, even if you already have E5. Why not the others? C. Intune Administrator role is not needed—Help Desk Operator is enough. D. Microsoft 365 E5 license is required for Intune, but not specifically for Remote Help (the add-on is what matters). E. Rerun device onboarding is not needed if the device is already enrolled.

upvoted 14 times

rmac Highly Voted 3 years, 3 months ago

From my point of view, the solution is: A,B,F

upvoted 14 times

shamier234 Most Recent 2 months, 1 week ago

Selected Answer: ABF

many question banks were written when Remote Help was still a separate add-on and haven't been updated since the July 2026 licensing changes.

upvoted 1 times

a405051 1 year, 2 months ago

Selected Answer: ABF

Correct.

upvoted 1 times

hasibulhossain275 1 year, 8 months ago

Selected Answer: ABF

1. Deploy the Remote Help app to Device1 (A)

The Remote Help app must be installed on the device for remote assistance to work.

You can deploy the app using Intune or manually install it.

2. Assign the Remote Help add-on license to User1 (F)

Remote Help requires a specific add-on license in addition to the Microsoft 365 E5 license.

This license must be assigned to the user who will provide assistance (User1).

3. Assign the Help Desk Operator role to User1 (B)

To use Remote Help from the Intune admin center, User1 must have permissions to initiate remote sessions.

The Help Desk Operator role provides the required Remote Help permissions in Intune.

upvoted 2 times

Twindragon 1 year, 11 months ago

Selected Answer: ABF

i will go with ABF

upvoted 1 times

SajjH 2 years, 3 months 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 2 years, 3 months 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-onsMicrosoft 365 E5 subscription include Intune Plan 1, so add-on is required. https://www.microsoft.com/en-us/security/business/microsoft-intune-pricing#:~:text=Microsoft%20Intune%20Remote%20HelpI'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?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?Let's stop confusing people, ABF is correct! A. Deploy the Remote Help app to Device1. The app must be installed for Remote Help to work. B. Assign the Help Desk Operator role to User1. This role gives User1 permission to start Remote Help sessions in Intune. F. Assign the Remote Help add-on license to User1. Remote Help requires a specific license, even if you already have E5. Why not the others? C. Intune Administrator role is not needed—Help Desk Operator is enough. D. Microsoft 365 E5 license is required for Intune, but not specifically for Remote Help (the add-on is what matters). E. Rerun device onboarding is not needed if the device is already enrolled.

upvoted 2 times

Tr619899 1 year, 11 months 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 2 years, 2 months ago

Selected Answer: ABF

This is the only correct answer

upvoted 1 times

SajjH 2 years, 3 months 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 2 years, 3 months 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?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

oopspruu 2 years, 4 months 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 priviledge so we go for F.

upvoted 2 times

veliyath 2 years, 4 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

Haider_Raza 2 years, 8 months ago

Selected Answer: ABF

CORRECT ANSWER

upvoted 2 times

mestorrent86 2 years, 8 months 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 2 years, 8 months 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

MR_Eliot 2 years, 8 months 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-windowsE5 includes the Remote help license. You don't need an additional license for remote help. A,B,E is correct.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

LionelDerBoven 2 years, 2 months 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

OyYaGotta 2 years, 8 months 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

OyYaGotta 2 years, 8 months ago

E5 includes the Remote help license. You don't need an additional license for remote help. A,B,E is correct.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 2 years, 9 months ago

Ref: https://www.prajwaldesai.com/intune-remote-help/

upvoted 1 times

Merrybob 2 years, 9 months 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/remote-help#prerequisites)

upvoted 1 times

Merrybob 2 years, 9 months ago

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/remote-help#prerequisites)Ref: https://www.prajwaldesai.com/intune-remote-help/Ref: 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%20Remote%20Help.%20If%20you%20choose%20to%20turn%20on%20Remote%20Help%2C%20its%20use%20is%20enabled%20tenant%2Dwide.%20Remote%20Help%20must%20be%20enabled%20before%20users%20can%20be%20authenticated%20through%20your%20tenant%20when%20using%20Remote%20Help.

upvoted 1 times

Merrybob 2 years, 9 months ago

Ref: 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%20Remote%20Help.%20If%20you%20choose%20to%20turn%20on%20Remote%20Help%2C%20its%20use%20is%20enabled%20tenant%2Dwide.%20Remote%20Help%20must%20be%20enabled%20before%20users%20can%20be%20authenticated%20through%20your%20tenant%20when%20using%20Remote%20Help.

upvoted 1 times

GlobalS 2 years, 10 months ago

I read the question that User1 needs help rather then will be assisting others?

upvoted 1 times

Amir1909 2 years, 10 months ago

A and B and F is correct

upvoted 1 times

kilat 2 years, 11 months ago

Selected Answer: ABF

ABF - looks good for me

upvoted 1 times

NoursBear 2 years, 11 months ago

In case this helps anyone

https://ctsdemos.azureedge.net/microsoft/Intune/remotehelp/RemoteHelpDemo.html

upvoted 3 times

mks_academy 2 years, 11 months 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 2 years, 11 months ago

AB and F is correct, here you have the full deployment https://www.prajwaldesai.com/intune-remote-help/

upvoted 1 times

mks_academy 2 years, 11 months 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

iamforksu 3 years, 1 month ago

Selected Answer: ABF

comment no longer too short

upvoted 1 times

picho707 3 years, 1 month ago

Selected Answer: ABD

I am leaning towards A, B, D.

The question reads: You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite.

I guess it is understood that User1 already has assigned or will be assigned the Microsoft 365 E5 license.

upvoted 2 times

Mekkel 3 years, 1 month ago

Selected Answer: ABF

Agree with rmac

upvoted 2 times

Casticod 3 years, 1 month ago

Selected Answer: ABF

Vote for ABF

upvoted 3 times

Anonymous 3 years, 1 month ago

Agree With rmac .. A,B,F

upvoted 1 times

krzysztofbr 3 years, 2 months ago

Selected Answer: ABF

agree with RMAC

upvoted 4 times

letters1234 3 years, 2 months ago

E5 is not necessary as remote help license can be assigned as addon to other licenses, E5 is 'over-licensing' the user/device.

upvoted 1 times

letters1234 3 years, 2 months ago

Selected Answer: ABF

Agree with RMAC, no need to re-onboard the device to MDM when it's already enrolled.

upvoted 1 times

Besxp 1 year, 5 months ago

Let's stop confusing people, ABF is correct!

A. Deploy the Remote Help app to Device1.

The app must be installed for Remote Help to work.

B. Assign the Help Desk Operator role to User1.

This role gives User1 permission to start Remote Help sessions in Intune.

F. Assign the Remote Help add-on license to User1.

Remote Help requires a specific license, even if you already have E5.

Why not the others?

C. Intune Administrator role is not needed—Help Desk Operator is enough.

D. Microsoft 365 E5 license is required for Intune, but not specifically for Remote Help (the add-on is what matters).

E. Rerun device onboarding is not needed if the device is already enrolled.

upvoted 2 times

justITtopics 1 year, 8 months ago

Microsoft 365 E5 subscription include Intune Plan 1, so add-on is required.

https://www.microsoft.com/en-us/security/business/microsoft-intune-pricing#:~:text=Microsoft%20Intune%20Remote%20Help

upvoted 1 times

SajjH 2 years, 3 months 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

fco168 3 years ago

Disregard my previous comment. The license assigned is the O365, not the Intune Remote Help!

upvoted 1 times

fco168 3 years ago

The license is already assigned in the statement of the question.

upvoted 1 times

rmac 3 years, 3 months ago

reference:

https://learn.microsoft.com/en-us/mem/intune/fundamentals/remote-help#prerequisites

upvoted 2 times

Question #54 *Topic 1*

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.

Which images can be used to perform an in-place upgrade of Device1?

Name	Platform	Description
Image1	x64	Custom Windows 11 image that has Office 2021 installed
Image2	x64	Default Windows 11 image created by Microsoft

A. Image1 only

B. Image2 only

C. Image1 and Image2

Suggested Answer: *B*

Community vote distribution

B (100%)

letters1234 Highly Voted 3 years, 2 months ago

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 23 times

Dinkan Most Recent 1 year, 2 months ago

B. Image2 only https://learn.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios#in-place-upgrade

upvoted 1 times

a405051 1 year, 2 months ago

Only default images can be upgraded on Microsoft intune using the Upgrade Task Sequence.

upvoted 1 times

oopspruu 2 years, 4 months ago

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 2 times

veliyath 2 years, 4 months ago

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 2 years, 8 months ago

You can perform in-place upgrade, only with de default Windows image. Anything else is not supported.

upvoted 4 times

Darkfire 2 years, 8 months ago

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 2 years, 9 months ago

Ref: https://learn.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios#in-place-upgrade

upvoted 1 times

Amir1909 2 years, 10 months ago

B is correct

upvoted 1 times

poppinaz 3 years, 1 month ago

Totaly agree with you. Tried it in my Lab

upvoted 3 times

Question #55 *Topic 1*

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.

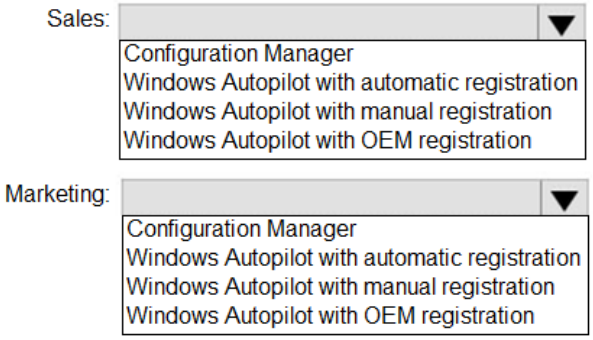
Devices for the sales department must be Azure AD joined. The devices will be shipped directly from the manufacturer to the homes of the sales department users.

Administrative effort must be minimized.

Which deployment method should you recommend for each department? To answer, select the appropriate options in the answer area.

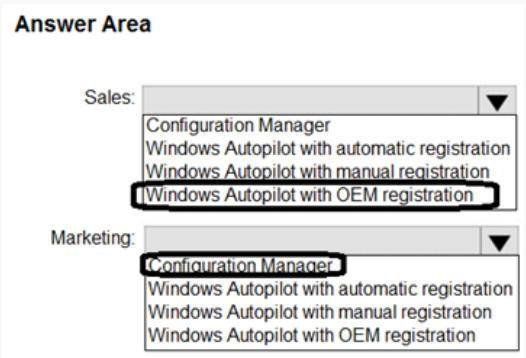
NOTE: Each correct selection is worth point.

Answer Area



Suggested Answer:

Answer Area



letters1234 Highly Voted 2 years, 9 months ago

Correct, Configuration manager doesn't require AAD connectivity and Autopilot with OEM registration means you can send the devices direct to user.AgreedAgreed

upvoted 26 times

letters1234 Highly Voted 2 years, 9 months ago

Correct, Configuration manager doesn't require AAD connectivity and Autopilot with OEM registration means you can send the devices direct to user.

upvoted 26 times

Dinkan Most Recent 1 year, 2 months ago

Sales Dept: Windows Autopilot with OEM registration

Marketing Dept: Configuration Manager

upvoted 1 times

b3c32d7 2 years ago

If all agree then..

upvoted 1 times

MR_Eliot 2 years, 2 months ago

Answer is correct. Also the Marketing team computers, will also be able to join Entra ID with hybrid enrollment.

upvoted 2 times

Darkfire 2 years, 3 months ago

Answers are correct

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

upvoted 2 times

Merrybob 2 years, 3 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 3 times

Amir1909 2 years, 4 months ago

Correct

upvoted 1 times

Krayzr 2 years, 4 months ago

55. Given answer is Correct

upvoted 1 times

cpaljchc4 2 years, 6 months ago

ChatGPT agreed too

upvoted 2 times

Rocky83 2 years, 7 months ago

Agreed

upvoted 1 times

Futfuyfyjfj 2 years, 8 months ago

Agreed

upvoted 1 times

Question #56 *Topic 1*

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 Highly Voted 2 years, 5 months ago

MDT was removed from the Exam in April 2024. Irrelevant to the examFor the purpose of the MD-102 certification, it is important to continue training on MDT to meet the exam objectives and understand its functionality in deployment scenarios.(28 Jan 2025, 2:37 pm)
https://learn.microsoft.com/en-au/answers/questions/2151812/md102-microsoft-deployment-toolkit-course-obsolete

upvoted 7 times

da_terminator Highly Voted 2 years, 5 months ago

MDT was removed from the Exam in April 2024. Irrelevant to the exam

upvoted 7 times

honey919 Most Recent 1 year, 9 months ago

For the purpose of the MD-102 certification, it is important to continue training on MDT to meet the exam objectives and understand its functionality in deployment scenarios.(28 Jan 2025, 2:37 pm)

https://learn.microsoft.com/en-au/answers/questions/2151812/md102-microsoft-deployment-toolkit-course-obsolete

upvoted 2 times

GreenJPGSandRAM 2 years, 6 months ago

MDT will be removed from the exam on Apr 26, 2024, so this question is no longer relevant

upvoted 5 times

GreenJPGSandRAM 2 years, 6 months ago

MDT will be removed from the exam on Apr 26, 2024, so this question is no longer relevantFor the purpose of the MD-102 certification, it is important to continue training on MDT to meet the exam objectives and understand its functionality in deployment scenarios.(28 Jan 2025, 2:37 pm)
https://learn.microsoft.com/en-au/answers/questions/2151812/md102-microsoft-deployment-toolkit-course-obsoleteSeptember 17 it wil.

upvoted 5 times

CJL324 2 years, 6 months 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

LionelDerBoven 2 years, 2 months ago

September 17 it wil.

upvoted 2 times

rcristiano 2 years, 8 months ago

Selected Answer: B

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 2 times

MR_Eliot 2 years, 8 months ago

Question is so vauge, but answer is correct.

You can use selection profile in MDT workbench.

upvoted 1 times

Darkfire 2 years, 9 months ago

Selected Answer: B

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 2 years, 9 months ago

Selected Answer: B

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 2 years, 11 months 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 3 years, 1 month ago

Selected Answer: B

B is correct I believe

upvoted 1 times

krzysztofbr 3 years, 2 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

Question #57 *Topic 1*

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%)

Dinkan Most Recent 1 year, 2 months ago

Selected Answer: C

C. Windows Deployment Services (WDS)

Multicast requires that Windows Deployment Services (WDS) is running on Windows Server 2008 or later.

Reference:

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt#multicast-deployments

upvoted 1 times

letters1234 Highly Voted 3 years, 2 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 8 times

letters1234 Highly Voted 3 years, 2 months ago

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-psThis is the article: https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt#multicast-deployments

upvoted 8 times

veliyath 2 years, 4 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

GreenJPGSandRAM 2 years, 6 months ago

MDT will be removed from the exam on Apr 26, 2024, so this question is no longer relevant

upvoted 8 times

MR_Eliot 2 years, 8 months ago

Selected Answer: C

Answer is correct.

upvoted 1 times

Besxp 1 year, 5 months ago

official Microsoft documentation confirms that MDT was removed from the MD-102 exam objectives in the April 2024 update. This comes from the Microsoft Exam Resource Guide for MD-102, which states: “The Plan and implement a Windows client deployment by using Microsoft Deployment Toolkit (MDT) section has been removed from the exam” That’s an official source (Microsoft Learn / exam guide), not a third-party guess. So you can be confident MDT is no longer tested on MD-102.

upvoted 2 times

Besxp 1 year, 5 months ago

Selected Answer: C

official Microsoft documentation confirms that MDT was removed from the MD-102 exam objectives in the April 2024 update. This comes from the Microsoft Exam Resource Guide for MD-102, which states:

“The Plan and implement a Windows client deployment by using Microsoft Deployment Toolkit (MDT) section has been removed from the exam”

That’s an official source (Microsoft Learn / exam guide), not a third-party guess. So you can be confident MDT is no longer tested on MD-102.

upvoted 2 times

Darkfire 2 years, 9 months 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 2 years, 9 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.

upvoted 1 times

Tonsku 2 years, 11 months 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 3 years, 2 months ago

the answer is correct. multicast in this case requires WDS

upvoted 2 times

Futfuyfyjfj 3 years, 2 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

Question #58 *Topic 1*

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

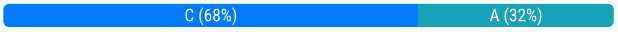
B. Microsoft Deployment Toolkit (MDT)

C. a Windows Configuration Designer provisioning package

D. Windows Deployment Services (WDS)

Suggested Answer: *C*

Community vote distribution



letters1234 Highly Voted 3 years, 2 months ago

Autopilot would require resetting the device, provisioning package can be loaded during normal use of the OS. Doesn't require resetting/wiping etc.In my exprience all the new devices use out-of-box exprience. from out-of-box experience you should be able to enroll the device in Intune by using Autopilot.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.That is not correct, Sysprep dont delete apps, its only prepering you computer unregistering and cleaning some regkeys autopilot is the best way to go and has the least administrative afort

upvoted 18 times

letters1234 Highly Voted 3 years, 2 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 18 times

Le_Patriarche2025 Most Recent 9 months ago

Selected Answer: C

C est la bonne reponse

A. Windows Autopilot : Bien que ce soit une excellente solution moderne, Autopilot est généralement conçu pour les nouveaux appareils sortis d'usine (OOBE - Out of Box Experience). Pour des appareils déjà configurés et utilisés en magasin de détail, le provisionnement est plus direct.

B. Microsoft Deployment Toolkit (MDT) : MDT est utilisé pour le "Wipe and Load" (effacer et charger). Cela supprimerait les applications déjà installées par les utilisateurs.

D. Windows Deployment Services (WDS) : Comme MDT, WDS est une solution de déploiement d'images système (PXE). Cela nécessite de formater l'ordinateur, ce qui contredit l'exigence de conserver les applications utilisateur.

upvoted 1 times

reyrey 9 months ago

Selected Answer: A

Autopilot is the correct answer

upvoted 1 times

benpatto 3 years 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.That is not correct, Sysprep dont delete apps, its only prepering you computer unregistering and cleaning some regkeys autopilot is the best way to go and has the least administrative afort

upvoted 1 times

benpatto 3 years 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

moluccanvibe 9 months, 2 weeks ago

Selected Answer: C

A provisioning package created with Windows Configuration Designer (WCD) is specifically designed for in-place upgrades and light-touch provisioning of devices that users already own.

Autopilot requires a reset (OOBE) to apply the profile.

upvoted 1 times

hieunm2411 1 year, 9 months ago

Selected Answer: A

When new Windows devices are initially deployed, Windows Autopilot uses the OEM-optimized version of Windows client. This version is preinstalled on the device, so custom images and drivers for every device model don't have to be maintained. Instead of re-imaging the device, the existing Windows installation can be transformed into a "business-ready" state that can:

Apply settings and policies.

Install apps.

Change the edition of Windows being used to support advanced features. For example, from Windows Pro to Windows Enterprise.

Ref:https://learn.microsoft.com/en-us/autopilot/overview#process-overview

upvoted 2 times

Tr619899 1 year, 10 months 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 2 times

458184c 1 year, 11 months 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 1 year, 11 months ago

Selected Answer: C

Ensure any application from user is retained, must be C, as autopilot requires full reset

upvoted 2 times

NoursBear 1 year, 10 months ago

I don't think users with BYOD will be happy with autopilot as they own their own computers and the apps must be retained. Read again

upvoted 2 times

Alboo007_rs007 1 year, 12 months ago

Selected Answer: A

"The best" solution is Autopilot

upvoted 1 times

AleFCI1908 2 years ago

Selected Answer: A

if intune joined, can do this with minimal effort

upvoted 1 times

Nav90 2 years ago

Selected Answer: C

https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provision-pcs-for-initial-deployment

upvoted 1 times

Tr619899 1 year, 11 months ago

A. Windows Autopilot

upvoted 1 times

Tr619899 1 year, 11 months ago

A. Windows AutopilotI don't think users with BYOD will be happy with autopilot as they own their own computers and the apps must be retained. Read again

upvoted 1 times

SSL2 2 years 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 2 years, 2 months 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

SajjH 2 years, 3 months 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 2 years, 8 months 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 2 years, 8 months 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 2 years, 9 months ago

Selected Answer: C

Deffinitly C

https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages

upvoted 1 times

veliyath 2 years, 4 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.The question didn't mention anything about availability of Intune whereas Autopilot requires Intune. Based on this, using Autopilot is not a solution.

upvoted 3 times

veliyath 2 years, 4 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

Merrybob 2 years, 9 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 2 years, 11 months ago

Selected Answer: A

More than one answer choice may achieve the goal. Select the BEST answer.

A & C

upvoted 1 times

belyo 2 years, 11 months 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

BJS78 2 years, 12 months ago

Autopilot SHOULD NOT be used for BYOD devices. WCD can do all - including the PRO-->ENT upgrade via UpgradeEditionWithProductKey.

upvoted 3 times

cpaljchc4 3 years ago

The best recommendation to achieve the goal of upgrading the computers to Windows 10 Enterprise, joining them to Azure AD, and installing several Microsoft Store apps while retaining user-installed applications and minimizing user intervention is Windows Autopilot (Option A).

Windows Autopilot is designed for streamlined and user-driven deployment scenarios. With Autopilot, you can configure the devices to upgrade to Windows 10 Enterprise, join Azure AD, and also include the installation of specified Microsoft Store apps. It allows for minimal user intervention, ensuring a smooth upgrade process while retaining user-installed applications and providing a seamless out-of-box experience for users.

upvoted 1 times

cpaljchc4 3 years ago

Since it is almost 50/50 here, I will go with gpt.

Using a **Windows Configuration Designer provisioning package (Option C)** could also potentially achieve parts of the requirements, like joining the computers to Azure AD and installing Microsoft Store apps. However, it might not directly address the upgrade from Windows 10 Pro to Windows 10 Enterprise, which is a significant part of the scenario.

The Configuration Designer provisioning package is more focused on configuring settings, policies, and deploying apps to devices. While it could help join the computers to Azure AD and install apps, it might not handle the OS upgrade and the retention of user-installed applications as effectively as Windows Autopilot. Autopilot offers a more holistic approach that covers the entire deployment process, including the OS upgrade, user data retention, Azure AD joining, and app installation, providing a smoother and more comprehensive deployment experience.

upvoted 1 times

ckmay 2 years, 9 months ago

"[WCD] it might not handle the OS upgrade and the retention of user-installed applications as effectively as Windows Autopilot".

2 big issues with Autopilot is it requires and full device wipe and reload every time you deploy with it and also Microsoft constantly mentions that the purpose of Autopilot is for corporate owned Entra joined or Entra Hybrid joined devices and should not be used to enroll BYOD devices

upvoted 1 times

chandravamsi 3 years ago

Selected Answer: A

Option A: Windows Auto Pilot

upvoted 1 times

pinda 3 years ago

Selected Answer: C

Correct

upvoted 1 times

When_you_know_you_know 3 years ago

Answer is C

Use the Windows Configuration Designer tool to create provisioning packages to easily configure devices running Windows client. Windows Configuration Designer is primarily used by IT departments for business and educational institutions who need to provision bring-your-own-device (BYOD) and business-supplied devices.

Benefits of provisioning packages

Provisioning packages let you:

Quickly configure a new device without going through the process of installing a new image.

Save time by configuring multiple devices using one provisioning package.

Quickly configure employee-owned devices in an organization without a mobile device management (MDM) infrastructure.

Set up a device without the device having network connectivity.

Provisioning packages can be:

Installed using removable media such as an SD card or USB flash drive.

Attached to an email.

Downloaded from a network share.

Deployed in NFC tags or barcodes.

upvoted 3 times

picho707 3 years, 1 month ago

Selected Answer: A

I am leaning towards "A" since the "Windows Configuration Designer provisioning package" answer does not provide the level of automation and user intervention that the question requires.

upvoted 2 times

ckmay 2 years, 9 months ago

"[WCD] does not provide the level of automation and user intervention that the question requires."

huh?

You can literally email every user a small provisioning package file they double click and it begins to do all of that.

Autopilot requires backing up all their stuff and settings, wiping/resetting the computer to factory, registering and enrolling to Autopilot, then reinstalling Windows and only then will it be able to do any of those other things and that's only IF the org has an Intune subscription and licensing. After all that, users would have to restore their backed up apps and files.

upvoted 1 times

ckmay 2 years, 9 months ago

oh also, Autopilot is not meant to enroll BYOD personally owned devices, only corporate owned managed devices.

upvoted 1 times

Temptset 3 years, 1 month ago

Selected Answer: C

It's Windows Configuration Designer (WCD) as it can ADD packages (provisioning), hence retain user data, which AutoPilot cannot.

https://learn.microsoft.com/en-us/windows/configuration/wcd/wcd-editionupgrade

upvoted 2 times

MR_Eliot 2 years, 8 months ago

In my exprience all the new devices use out-of-box exprience. from out-of-box experience you should be able to enroll the device in Intune by using Autopilot.

upvoted 1 times

Rylz 2 years, 3 months ago

That is not correct, Sysprep dont delete apps, its only prepering you computer unregistering and cleaning some regkeys

autopilot is the best way to go and has the least administrative afort

upvoted 1 times

JP1900 3 years, 3 months ago

Selected Answer: A

Minimize user intervention.

upvoted 4 times

Futfuyfyjfj 3 years, 2 months ago

Furthermore Autopilot isn't designed for BYOD

upvoted 3 times

krzysztofbr 3 years, 2 months ago

can't be a "any applications installed by the users are retained."

autopilot removes all APPS

upvoted 4 times

Question #59 *Topic 1*

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

hieunm2411 Most Recent 1 year, 9 months ago

Selected Answer: B

B is the correct answer

upvoted 1 times

veliyath 2 years, 4 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 2 years, 8 months ago

Selected Answer: B

B for sure

upvoted 1 times

MR_Eliot 2 years, 8 months ago

Selected Answer: B

Easy no.

upvoted 1 times

iTomi Highly Voted 2 years, 11 months ago

Selected Answer: B

NO!

Intune > Devices > Configuration profiles > Create > New Policy > Windows 10 or later > Settings Catalog > Create > Windows Hello for Business.

upvoted 8 times

krzysztofbr 3 years, 2 months ago

Selected Answer: B

agrree with letters1234

upvoted 1 times

letters1234 Highly Voted 3 years, 2 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 15 times

Question #60 *Topic 1*

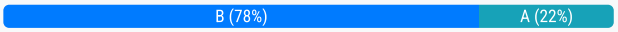
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer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



veliyath Highly Voted 2 years, 4 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 8 times

MR_Eliot Highly Voted 2 years, 8 months 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 settins, you will need to configure Windows hello for Business.

upvoted 6 times

Merrybob 2 years, 9 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%20Intune%20configuration%20policies%20you%20set%20to%20control%20the%20device%20PIN%2C%20and%20additionally%2C%20any%20Windows%20Hello%20for%20Business%20policies%20you%20configured%2C%20now%20both%20set%20this%20new%20PIN%20value.

upvoted 3 times

yosry 2 years, 11 months ago

Selected Answer: B

No

the answer is B

upvoted 1 times

iTomi 2 years, 11 months 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 2 years, 11 months ago

I also agree A yes is correct

upvoted 1 times

NoursBear 2 years, 11 months ago

I also agree A yes is correctNope.. the correct way is in question 61. So this is a No now

upvoted 1 times

NoursBear 2 years, 11 months ago

Nope.. the correct way is in question 61. So this is a No now

upvoted 1 times

madsa 2 years, 11 months 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

madsa 2 years, 11 months 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 2 years, 10 months ago

device configuration profile not restriction profile, correct. I agree, the answer is No.

upvoted 1 times

Krayzr 3 years 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 3 years 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 3 years ago

Correction, Question says Intune admin center.

Answer "A"

upvoted 2 times

sbermejor 3 years 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 3 years 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 3 years 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 3 years, 1 month ago

Selected Answer: A

should be Yes

upvoted 1 times

suresh08 3 years, 1 month ago

Yes, we can achieve it from device restriction.NO! Intune > Devices > Configuration profiles > Create > New Policy > Windows 10 or later > Settings Catalog > Create > Windows Hello for Business.

upvoted 3 times

suresh08 3 years, 1 month ago

Selected Answer: A

Yes, we can achieve it from device restriction.

upvoted 3 times

letters1234 3 years, 2 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

letters1234 3 years, 2 months ago

Correct, would need to be Enroll Devices \ Windows Enrollment \ Windows Hello for Business \ Minimum PIN Length. Or possibly a Device Configuration Policy.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#passwordWrong. You can set PIN for iOS/Android, but for Windows only the password (not the PIN) can be controlled via Device restrictions.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……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 4 times

Futfuyfyjfj 3 years, 2 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#passwordWrong. You can set PIN for iOS/Android, but for Windows only the password (not the PIN) can be controlled via Device restrictions.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……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

Futfuyfyjfj 3 years, 2 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 3 years, 1 month ago

Wrong. You can set PIN for iOS/Android, but for Windows only the password (not the PIN) can be controlled via Device restrictions.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……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 1 times

BJS78 3 years, 1 month 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

Futfuyfyjfj 3 years, 1 month 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……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 3 times

Futfuyfyjfj 3 years, 1 month 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 2 years, 11 months 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

Question #61 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your 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 Highly Voted 2 years, 9 months ago
Correct, confirmed Intune 2308 environment.yes is correct
upvoted 9 times

letters1234 Highly Voted 2 years, 9 months ago
Correct, confirmed Intune 2308 environment.
upvoted 9 times

Jeff777 Most Recent 2 years, 1 month ago
A is correct
upvoted 2 times

Haider_Raza 2 years, 2 months ago
Selected Answer: A
YES, IT is correct
upvoted 1 times

Haider_Raza 2 years, 2 months ago
Selected Answer: A
ANSWER IS CORRECT
upvoted 1 times

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

ckmay 2 years, 3 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 2 years, 4 months ago
Selected Answer: A
A is Good
upvoted 1 times

NoursBear 2 years, 5 months ago
OK so the previous question with No was correct
upvoted 2 times

fco168 2 years, 6 months ago

Selected Answer: A

YES.....

upvoted 2 times

yosry 2 years, 6 months ago

Selected Answer: A

allah yarhmou walla rabi m3ah

upvoted 2 times

Hadilsa 2 years, 1 month ago

yes is correct

upvoted 1 times

Question #62 *Topic 1*

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.

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.

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

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

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

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

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?

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

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

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

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%)

cd2cfde 1 year, 5 months ago

They actually made this question wayyyy longer than it had to be. Unbelievable 😂😂😂

upvoted 2 times

MR_Eliot 2 years, 2 months ago

Selected Answer: C

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

MR_Eliot 2 years, 2 months ago

A: NO, because it just deployment profile. B: NO C: Correct D: easy no. It's just for compliancy. does nothing else.In order to Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot, don't you have to create a Deployment Profile?

upvoted 1 times

e70d081 Most Recent 5 months, 3 weeks ago

In order to Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot, don't you have to create a Deployment Profile?

upvoted 1 times

Darkfire 2 years, 3 months ago

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 2 years, 3 months ago

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%20diagnostic%20and%20usage%20data%20to%20Apple.%20When%20set%20to%20Not%20configured%20(default)%2C%20Intune%20doesn%27t%20change%20or%20update%20this%20setting.%20By%20default%2C%20the%20OS%20might%20allow%20this%20data%20to%20be%20sent.

upvoted 3 times

Tonsku 2 years, 5 months ago

C. a device configuration profile

upvoted 1 times

iamforksu 2 years, 7 months ago

Seem like C

upvoted 1 times

Futfuyfyjfj 2 years, 8 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.

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.

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

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

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

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

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.

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

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

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Answer Area

Statements	Yes	No
Device1 is compliant.	○	○
Device3 is compliant.	○	○
Device4 is compliant.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Device1 is compliant.	○	◉
Device3 is compliant.	◉	○
Device4 is compliant.	◉	○

MR_Eliot Highly Voted 2 years, 8 months 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 16 times

Tonsku Highly Voted 2 years, 11 months 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 5 times

Tr619899 Most Recent 1 year, 11 months ago

Answer is: No, Yes, Yes

upvoted 1 times

Engr001 2 years, 8 months ago

I will go with N, N, Y Device 3 will be a NO because it is an android device. Policy 2 wil 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?Device 3 is i 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 3 times

Engr001 2 years, 8 months ago

I will go with N, N, Y Device 3 will be a NO because it is an android device. Policy 2 wil 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 3 times

b47afda 2 years, 6 months ago

Device 3 is i 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 2 years, 8 months ago

Answer is correct. (NYY) Device3 > member of group 2 & 3. Least previliges override, so Group3 = Policy1 > Is compliant

upvoted 4 times

madsa 2 years, 11 months ago

No Yes Yes is correct, sorry, Futfuyfyjfj is 100% correct, this device will be affected by policy 1.

upvoted 1 times

madsa 2 years, 11 months 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 3 years, 1 month ago

NO YES YES

upvoted 2 times

picho707 3 years, 1 month 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 NOQuestion 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 YesQuestion 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

picho707 3 years, 1 month 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 3 years, 1 month 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 3 years, 1 month 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 YesQuestion 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 3 times

picho707 3 years, 1 month 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 3 years, 1 month ago

NO YES YES

upvoted 4 times

sh123df 3 years, 2 months ago

No ? = Will the exclude or include over ride? Yes

upvoted 1 times

sh123df 3 years, 2 months ago

No ? = Will the exclude or include over ride? YesDoesn't matter, the policy (2) is for iOS, the Devices is Android. So policy is not applicableWrong. Device 3 will be excluded from Policy2 due to ex: Group3 setting. The device will receive. N-Y-Y, answer is correctYou 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.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

Futfuyfyjfj 3 years, 2 months ago

Doesn't matter, the policy (2) is for iOS, the Devices is Android. So policy is not applicableWrong. Device 3 will be excluded from Policy2 due to ex: Group3 setting. The device will receive. N-Y-Y, answer is correctYou 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.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 3 times

Futfuyfyjfj 3 years, 2 months ago

Doesn't matter, the policy (2) is for iOS, the Devices is Android. So policy is not applicable

upvoted 3 times

BJS78 3 years, 1 month 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

BJS78 3 years, 1 month ago

Wrong. Device 3 will be excluded from Policy2 due to ex: Group3 setting. The device will receive. N-Y-Y, answer is correctYou 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.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

Futfuyfyjfj 3 years, 1 month 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

Futfuyfyjfj 3 years, 1 month 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.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 3 times

BJS78 2 years, 11 months 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.

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.

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

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

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

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

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?

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

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

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

A. Generalize the computers and configure the Device settings from the Microsoft Entra admin center.

B. Extract the serial number of each computer to an XML file and upload the file from the Microsoft Intune admin center.

C. Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune admin center.

D. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Microsoft Entra admin center.

E. 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 Most Recent 2 years, 2 months ago

C it is

upvoted 1 times

MR_Eliot 2 years, 2 months ago

Answer is correct.

upvoted 1 times

Darkfire 2 years, 3 months ago

C is correct https://learn.microsoft.com/en-us/autopilot/add-devices

upvoted 1 times

ckmay 2 years, 3 months ago

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 2 times

Tonsku 2 years, 5 months ago

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 2 years, 6 months ago

Get the Hash IDs to provision using Autopilot.

upvoted 1 times

Kiookr 2 years, 8 months 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 4 times

[Removed] 2 years, 8 months 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.CorrectThe 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 4 times

Futfuyfyjfj 2 years, 8 months ago

Correct

upvoted 1 times

Oslaf_PSN 2 years, 7 months 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 3 times

Futfuyfyjfj 2 years, 8 months 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.

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.

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

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

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

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

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.

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

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

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

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

Suggested Answer:

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

Fortind1974 Highly Voted 3 years, 2 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-restrictionsDevice 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.Source?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-enrollAzure 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-enrollThat's Entra device limit restrictions, not Intune. The question says nothing about Entra restrictions, so it's safe to assume it's unlimited.The device enrollment restriction takes precedence over the privileges granted by the DEM role.

upvoted 36 times

Fortind1974 Highly Voted 3 years, 2 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 36 times

picho707 3 years, 2 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.Source?

upvoted 4 times

picho707 3 years, 2 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 4 times

Pablosanchez 4 months, 3 weeks ago

I doubt this question will be on the exam, and even if it is, the limit for a regular user is no longer 10 but 15, and DEM is still 1,000.
https://learn.microsoft.com/en-us/intune/device-enrollment/limits-intune-entra#intune-device-limit-restrictions

upvoted 1 times

b8142ea 1 year, 2 months ago

Can someone please confirm if these Q are still present on the exam recently ?

upvoted 1 times

batang_aratan 1 year, 9 months ago

I think:

User 1: 10 devices

User 2: 1000

According to this: https://learn.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure#intune-device-limit-restrictions

upvoted 1 times

picho707 3 years, 2 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-enrollThat's Entra device limit restrictions, not Intune. The question says nothing about Entra restrictions, so it's safe to assume it's unlimited.

upvoted 5 times

picho707 3 years, 2 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

Tr619899 1 year, 11 months 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 year, 12 months 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 2 years 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 2 years, 2 months 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 2 years, 2 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 2 years, 7 months ago

Usuario 1: 15 dispositivos e usuário 2: 1000 - DEM (gerenciador de registro de dispositivos) no Intune

upvoted 1 times

Jeff777 2 years, 7 months ago

User1: 10

User2: 15

User1 GroupA

User2 GroupB & DEM

Device limit 15 GroupB

Device limit 10 GroupA

upvoted 1 times

ckmay 2 years, 8 months 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

sergioandreslq 2 years, 8 months ago

User 1: 10 Devices because, user 1 belong to group A which has a restriction of device limit 10.

upvoted 2 times

Darkfire 2 years, 8 months 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

Anonymouse1312 2 years, 9 months 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 4 times

ckmay 2 years, 8 months 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

onepunchkenshin 2 years, 10 months ago

I will vote 1000 devices for User2 as Windows devices are being deployed

upvoted 2 times

ckmay 2 years, 8 months ago

CORRECTION- User 1: 10 Devices User 2: 1000

upvoted 4 times

Tonsku 2 years, 11 months ago

User1: 10

User2: 15

User1 GroupA

User2 GroupB & DEM

Device limit 15 GroupB

Device limit 10 GroupA

upvoted 5 times

ckmay 2 years, 8 months ago

CORRECTION- User 1: 10 Devices User 2: 1000User 1: 10 Devices because, user 1 belong to group A which has a restriction of device limit 10.

upvoted 4 times

mks_academy 2 years, 11 months 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

Merrybob 2 years, 9 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.%20You%20can%20allow%20a%20user%20to%20enroll%20up%20to%2015%20devices.)

upvoted 1 times

Merrybob 2 years, 9 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.%20You%20can%20allow%20a%20user%20to%20enroll%20up%20to%2015%20devices.)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 1 times

NoursBear 2 years, 11 months 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 2 years, 11 months ago

OK here we are working with mobile devices, where die DEM would be limited

upvoted 1 times

iTomi 2 years, 11 months 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

madsa 2 years, 11 months ago

The correct answer is 10 and 15. Restrictions overrule DEM.

upvoted 3 times

iTomi 2 years, 11 months 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.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 3 times

NoursBear 2 years, 11 months ago

Comment in wrong place

upvoted 1 times

kay000001 2 years, 12 months 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 2 years, 12 months ago

Apolgies, User 2: is also under Restriction1 (15 devices), so their limit will be 15 anyway.

upvoted 1 times

HawkieEyes 3 years ago

User1 is 15

https://learn.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure

>Intune device limit restrictions

>Intune device limit restrictions set the maximum number of devices that a user can enroll. >You can allow a user to enroll up to 15 devices

upvoted 1 times

BlackCat9588 3 years ago

User2 = 15

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 3 times

Contactfornitish 3 years, 1 month ago

User1 in group A so 10 devices

User2 is DEM so 1000 devices

upvoted 2 times

VirtualJP 3 years, 1 month ago

I'm going with this answer being correct.

upvoted 3 times

VirtualJP 3 years, 1 month ago

I revise. User2 = 1000 becuase of DEM.

I did not read the question properly the first time.

upvoted 1 times

VirtualJP 3 years, 1 month ago

I revert to my original assumption of answer being correct

Here's why:

Device limit restrictions in Intune override DEM if the DEM user is assigned a restriction. This means that if a DEM user is assigned a device limit restriction in Intune, the user will not be able to enroll more devices than the limit specified in the restriction, even if the DEM account allows for more devices to be enrolled.

upvoted 4 times

Casticod 3 years, 1 month ago

User 1 10 Devices : https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll#device-limit-restrictions

User 2 1000 devices: https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll#device-limit-restrictions

upvoted 2 times

Casticod 3 years, 1 month ago

Sorry user 1: 15

upvoted 1 times

majerzg 3 years, 1 month ago

Why user1: 15? not 10?

upvoted 1 times

ExamKiller020 3 years, 1 month ago

User 1: 15

user 2: 1000

DEM enrolls Windows 10/11 devices in shared device mode, so device limit restrictions won't work on them. Instead, you can configure a hard limit for these devices in the Azure AD admin center.

ref: https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll#device-limit-restrictions

upvoted 1 times

Futfuyfyjfj 3 years, 1 month ago

This source says when using automatic enrollment on Win10 and using DEM at the same time won't apply a maximum based on the limit restrictions to a DEM

https://learn.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure

upvoted 1 times

rus10 3 years, 2 months ago

user 1 is 15 and user 2 is 1000

upvoted 1 times

Futfuyfyjfj 3 years, 2 months ago

Why do you think so?

upvoted 1 times

NoursBear 3 years, 2 months ago

User 1 is 15 devices

upvoted 1 times

NoursBear 3 years ago

scrap that I meant 10 and user 2 15 because the restriction on a DEM user overrides his DEM capacity.

upvoted 2 times

Victor3 3 months ago

To further support this: https://learn.microsoft.com/en-us/intune/device-enrollment/limits-intune-entra

Intune device limit restrictions don't apply to devices enrolled via:

Android device administrator + device enrollment manager

Android Enterprise dedicated device

Co-management with Configuration Manager

Automatic enrollment + group policy

Automatic enrollment + device enrollment manager

Automatic enrollment + bulk device enrollment

Automatic enrollment initiated by user through desktop (for example, when they connect a work or school account in the Windows Settings app)

Windows Autopilot

upvoted 1 times

Victor3 Most Recent 3 months ago

Actually, the case studies states: Implement co-management for the computers and my above statement says does not apply to Co-management with Configuration Manager. Does not mean the max limit for both User 1 and User 2?

upvoted 1 times

Savior99 2 years, 8 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

SaiK1234 2 years, 8 months ago

User 2: - 1000 devices.

If you're bulk enrolling devices, consider creating the Device enrollment manager (DEM) account. The DEM account can enroll up to 1,000 mobile devices

https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment

upvoted 1 times

fco168 3 years ago

The device enrollment restriction takes precedence over the privileges granted by the DEM role.

upvoted 5 times

Burkidur 2 years, 8 months 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

Futfuyfyjfj 3 years, 2 months ago

Source?

upvoted 4 times

sh123df 3 years, 2 months ago

If thinking at role so answer is not correct.

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.

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.

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

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

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

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

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.

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

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

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

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

Suggested Answer:

Answer Area

Policy1: Device3 only

Policy2: Device4 only

Futfuyfyjfj Highly Voted 3 years, 2 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 22 times

DiligentSam Most Recent 2 years ago

Given Answer is correct.

upvoted 1 times

Darkfire 2 years, 9 months ago

Answer is correct.

upvoted 4 times

Tonsku 2 years, 11 months ago

Device3: Group2 & Group3 Policy1: Group3. Exclude None Device4: Group2 Policy2: Group2. Exclude Group3

upvoted 1 times

yosry 2 years, 11 months ago

seems correct

upvoted 1 times

madsa 2 years, 11 months ago

The given answer is correct.

upvoted 1 times

sh123df 3 years ago

Policy 1=device 3 Policy 2=device 2 and 4Device2 is in Group3, which is excluded by Policy2, so Policy2 is Device4 onlyPolicy 2 = Device 4 Only. Device 2 is in group 3 as well and Policy 2 excludes that group.

upvoted 3 times

sh123df 3 years ago

Policy 1=device 3 Policy 2=device 2 and 4

upvoted 2 times

HawkieEyes Highly Voted 3 years ago

Device2 is in Group3, which is excluded by Policy2, so Policy2 is Device4 only

upvoted 8 times

fco168 3 years ago

Policy 2 = Device 4 Only. Device 2 is in group 3 as well and Policy 2 excludes that group.

upvoted 5 times

Question #67 *Topic 1*

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.

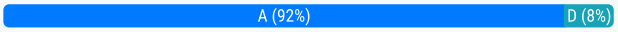
B. On Computer2, add Computer1 to the Remote Management Users group.

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



Jz23 Most Recent 1 year, 9 months ago

Selected Answer: A

A. On Computer2, run the Enable-PSRemoting cmdlet.

Explanation:

To use the Invoke-Command cmdlet for remote management, PowerShell Remoting must be enabled on the target computer (in this case, Computer2).

Enable-PSRemoting configures the necessary settings, including starting the WinRM service, setting up listeners, and configuring the firewall rules to allow remote PowerShell commands.

Why not the others?

B. Add Computer1 to the Remote Management Users group:

This is useful for non-administrator accounts, but it's not the first step. Remoting must be enabled first.

C. Configure Trusted for Delegation:

This is used for Kerberos delegation scenarios, not basic PowerShell Remoting.

D. Run New-PSSession on Computer1:

This initiates a remote session, but it will fail if PowerShell Remoting is not enabled on Computer2.

upvoted 2 times

Darkfire 2 years, 3 months 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 2 years, 5 months ago

Selected Answer: A

A. On Computer2, run the Enable-PSRemoting cmdlet.

upvoted 1 times

belyo 2 years, 5 months 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 2 years, 7 months ago

Selected Answer: A

Answer is correct

upvoted 2 times

Temptset 2 years, 7 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

Alscoran 2 years, 7 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

upvoted 1 times

Rocky83 2 years, 7 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

Rocky83 2 years, 7 months ago

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.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 1 times

picho707 2 years, 7 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

Futfuyfyjfj 2 years, 8 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

upvoted 3 times

Futfuyfyjfj 2 years, 8 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-7.3same here

upvoted 3 times

Rocky83 2 years, 7 months ago

same here

upvoted 1 times

Question #68 *Topic 1*

You have an Azure AD tenant that contains the devices shown in the following table.

Which devices can be activated by using subscription activation?

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

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%)

Futfuyfyjfj Highly Voted 3 years, 2 months ago

Answer is correct: https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#requirements

upvoted 11 times

Dinkan Most Recent 1 year, 2 months ago

C. Device1 and Device3 only * Devices must be Microsoft Entra joined or Microsoft Entra hybrid joined. Workgroup-joined or Microsoft Entra registered devices aren't supported Ref: https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivots=windows-11#requirements

upvoted 1 times

GarrethM 1 year, 4 months ago

Devices must be Microsoft Entra joined or Microsoft Entra hybrid joined. Workgroup-joined or Microsoft Entra registered devices aren't supported

upvoted 1 times

Twindragon 1 year, 11 months ago

Agree with C

upvoted 1 times

Tr619899 1 year, 11 months ago

Agrees with the WORKHOLIC answer

upvoted 3 times

Pollosor 2 years, 4 months ago

Automatic subscription?

upvoted 1 times

WORKHOLIC 2 years, 6 months 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 2 years, 9 months ago

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 2 years, 9 months 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. Con guration Manager C. subscription activation (Correct Answer) D. Microsoft Deployment Toolkit (MDT)

upvoted 1 times

Tonsku 2 years, 11 months ago

C. Device1 and Device3 only

upvoted 1 times

iTomi 2 years, 11 months ago

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 3 years ago

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 3 years, 1 month ago

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

Question #69 *Topic 1*

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 3 years, 1 month ago

Autopilot does not upgrade Windows version. The only approach listed to perform upgrade in-place is MDT with DEFAULT imageAutopilot 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.Subscription activation cannot upgrade between versions, ie 10 to 11The answers is B - Configuration manager

upvoted 28 times

Sas2003 Highly Voted 3 years, 1 month 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 27 times

noa808a Most Recent 4 months, 3 weeks ago

Selected Answer: D

A is depricated, B is not possible via Intune, C cannot be used for "in place upgrades". D is the correct answer.

upvoted 1 times

OyYaGotta 2 years, 8 months 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.Subscription activation cannot upgrade between versions, ie 10 to 11

upvoted 5 times

OyYaGotta 2 years, 8 months 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 5 times

ModernoDecor 8 months, 2 weeks ago

Selected Answer: D

Subscription activation allows a device to automatically upgrade from Windows Pro to Windows Enterprise simply by having a licensed user sign in.

In 2026 MD-102 Exam, the focus is on the Cloud. So, it will be MOST of the time the right answer.

upvoted 2 times

Dinkan 1 year, 2 months ago

Selected Answer: A

A. Microsoft Deployment Toolkit (MDT) and a default image of Windows 11 Enterprise

* You can't use a custom image to perform the in-place upgrade.

* You can't do in-place upgrade using Autopilot

* Subscription activation can't be used to upgrade to a newer version of Windows.

Reference:

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit

https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivots=windows-11

upvoted 3 times

yoyoyo99 1 year, 4 months ago

Selected Answer: D

MDT□Windows11□□□□□□□□□□

upvoted 1 times

GarrethM 1 year, 4 months ago

Selected Answer: D

What Subscription Activation does:

Automatically upgrades eligible Windows 10/11 Pro devices to Enterprise edition.

No reimaging or manual key entry required.

Works seamlessly with Azure AD join or Hybrid Azure AD join.

Completely zero-touch after device is enrolled in Intune and licensed.

upvoted 1 times

cd2cfde 1 year, 5 months ago

Selected Answer: A

Can't be d because subscription activation cannot update to a newer version of windows

upvoted 3 times

CheMetto 1 year, 5 months ago

Selected Answer: D

A - it can't be. Officialy MDT doesn't support W11, so it's excluded! Also, it can't change edition from Pro to Enterprise

B. the second reason of A, so it can't change from Pro to Enterprise within an in-place upgrade

C- does nothing, neither upgrade OS nor change edition. You need to reinstall OS / do sysprep to get into the oobe for activate autopilot, however, it doesn't do anything autopilot in itself.

D- it's the only option who allow change edition from pro to enterprise, then do an in-place upgrade with iso/MDT/script/MCM.

upvoted 1 times

Mekenna 1 year, 7 months ago

Selected Answer: D

Lots of debate on this one, but I think D is correct. Here's why (with the help of chat GBT)

-You have Windows 10 Pro devices

-You have Microsoft 365 E5 (which includes Windows 11 Enterprise licensing)

-You want to upgrade to Windows 11 Enterprise

-You want to minimize admin effort (I think this piece is key here)

-You want to do an in-place upgrade (keep files, apps, settings)

Subscription Activation allows devices with Windows 10/11 Pro to automatically upgrade to Enterprise edition without reinstalling the OS — as long as:

-The device is Azure AD-joined or hybrid joined

-The user has an M365 E3 or E5 license

-The base OS is Windows Pro (which your 25 devices already have)

The other options are wrong because they either don't support in place upgrades, or have too many steps/too complex to be considered the least effort solution

upvoted 1 times

ExamBud 1 year, 8 months ago

Selected Answer: A

It is A for me. But for me the easiest way would be to use a feature update profile from Intune (Autopilot is not required). As it is not an option, I think it is A.

upvoted 1 times

sorinaccio 1 year, 9 months ago

Selected Answer: A

Autopilot does not upgrade Windows versions. MDT + DEFAULT image -> A is the correct answer.

upvoted 1 times

mersaine 1 year, 9 months ago

Selected Answer: D

ChatGpt answer not sure if it's correct or not :

The correct answer is D. Subscription Activation.

Explanation:

Subscription Activation is a feature that allows you to upgrade Windows 10 Pro installations to Windows Enterprise using the rights granted by a Microsoft 365 subscription (such as your E5 subscription).

This method performs an in-place upgrade without requiring the deployment of new images or additional configuration tools.

As a result, it minimizes administrative effort compared to solutions like MDT, Configuration Manager, or Windows Autopilot.

Thus, with your setup (25 Windows 10 Pro computers managed via Microsoft Intune under a Microsoft 365 E5 subscription), Subscription Activation is the optimal choice to upgrade to Windows 11 Enterprise.

upvoted 2 times

hieunm2411 1 year, 9 months ago

Selected Answer: D

I think D is correct.

upvoted 2 times

Doug77 1 year, 9 months ago

Selected Answer: A

The answer is correct, Autopilot won't upgrade versions, just like Subscription activation won't upgrade from 10 to 11 enterprise

upvoted 1 times

TylerSivis 1 year, 9 months ago

Selected Answer: A

This question has a most even split of answers I've seen yet. I think the answer is A but I KNOW the answer isn't D because of this line at https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivots=windows-10

Note

Subscription activation is available for qualifying devices running currently supported versions of Windows. Subscription activation can't be used to upgrade to a newer version of Windows.

upvoted 2 times

diazed 1 year, 10 months ago

Selected Answer: A

Subscription activation is available for qualifying devices running currently supported versions of Windows. Subscription activation can't be used to upgrade to a newer version of Windows. This leaves only the option A as a correct answer.

upvoted 1 times

458184c 1 year, 11 months ago

Selected Answer: D

The correct answer is D. Subscription Activation.

upvoted 2 times

BigTone 1 year, 11 months 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/autopilot/existing-devices

So for me, the only possible correct answer is A

upvoted 2 times

Abitek007 1 year, 11 months ago

Selected Answer: D

Subscription activation can upgrade from pro to enterprise. hence D is right

upvoted 2 times

Tr619899 1 year, 11 months 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 2 times

1655b71 2 years 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 years ago

Selected Answer: D

minimal effort

upvoted 2 times

AleFCI1908 2 years ago

Selected Answer: D

minimal administrative effort

upvoted 3 times

d3a3d8a 2 years 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?pivots=windows-11#subscription-activation-for-enterprise

upvoted 3 times

SSL2 2 years 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 2 times

RomanV 2 years, 2 months 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 3 times

EUC_PRO 2 years, 2 months 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 2 years, 2 months 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 2 years, 2 months ago

https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivots=windows-11

This may lessen the confusion.

upvoted 2 times

Zoom2020 2 years, 2 months ago

This only update the Windows edtion on th same OS level, it does not IPU the device!

upvoted 1 times

oopspruu 2 years, 4 months 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 10 times

ergacharsk 2 years, 4 months 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 2 years, 5 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

Maclouis116 2 years, 5 months ago

Should be D. Subscription Activation

upvoted 2 times

Jaqueplakzaque 2 years, 5 months ago

Selected Answer: D

Least Administrative effort. So D.

upvoted 1 times

Ruchira007 2 years, 5 months ago

I think answer is correct. For customization , MDT is a best choice. But in this scenario with minimal setup is the concern , subscription activation should be the best option.

upvoted 1 times

Frank9020 2 years, 5 months ago

Selected Answer: D

Subscription Activation provides the most efficient and least administratively intensive method to upgrade existing Windows 10 Pro devices to Windows 11 Enterprise in an organization using Microsoft 365 E5 and Intune

upvoted 1 times

mark2525 2 years, 6 months ago

Selected Answer: C

The online assessment from ms says it's C. Not sure why we paid for this.

upvoted 2 times

TristanForest 2 years, 6 months ago

Selected Answer: A

Autopilot does not upgrade Windows version

upvoted 1 times

ejonesy80 2 years, 6 months ago

Because the solution must minimize administrative effort. The best answer is:

D. Subscription Activation

See documentation from Microsoft:

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 subscriptions.

https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivots=windows-10

upvoted 2 times

ejonesy80 2 years, 6 months ago

I'm sorry guys for the wrong answer, after more research, the only answer that is valid is: A.

The only approach listed to perform upgrade in-place is MDT with DEFAULT image.

upvoted 1 times

3661de6 2 years, 7 months ago

Selected Answer: A

AUTOPILOT DOES NOT IN-PLACE UPGRADE

upvoted 1 times

kerimnl 2 years, 7 months ago

Selected Answer: A

A for sure -> In pllace upgrade

upvoted 1 times

Cheban 2 years, 7 months ago

Windows Autopilot can be used to deploy and upgrade devices in an organization. However, the question specifically asked for an in-place upgrade from Windows 10 Pro to Windows 11 Enterprise with minimal administrative effort. In this context, Subscription Activation is a feature that can automatically upgrade Windows 10 Pro to Windows 11 Enterprise when a user signs in with a Microsoft 365 E5 license, which aligns with the requirements specified in the question.

upvoted 1 times

Rooza 2 years, 8 months ago

Selected Answer: D

The most suitable option for upgrading your 25 computers from Windows 10 Pro to Windows 11 Enterprise while minimizing administrative effort is D. Subscription Activation. Here's why:

Subscription Activation:

Allows a seamless transition from Windows Pro to Enterprise.

No manual key entry or image deployment required.

Low administrative effort.

Integration with Microsoft 365 E3/E5 licenses.

upvoted 3 times

RomanV 2 years, 2 months ago

Your chatgpt text is against your choice of answer. "Allows a seamless transition from Windows Pro to Enterprise." It's not from 1 Win version to another one (10 -> 11) but from Windows Pro to Enterprise within the SAME version.

upvoted 1 times

mestorrent86 2 years, 8 months ago

Selected Answer: C

Windows Autopilot: It allows you to set up new devices automatically, including upgrading existing devices to Win11, you can reduce manual intervention and streamline the upgrade process. This option aligns well with your Microsoft 365 E5 subscription and Microsoft Intune usage.

MECM: You can create a custom image of Win11 Ent and use MECM for an in-place upgrade.While this approach provides flexibility, it may involve more administrative effort.Not the most efficient choice for minimizing administrative tasks.

MDT it can be used for in-place upgrades, it requires creating a custom image of Win11 Ent. This approach involves additional steps and manual effort. Not the optimal choice for minimizing administrative workload.

Subscription Activation is related to licensing and activation, not the actual upgrade process.It doesn't directly address the in-place upgrade task. Not applicable for this scenario.

upvoted 1 times

RazielLycas 2 years, 8 months ago

Selected Answer: A

Autopilot is not an in-place upgrade method neither is able to upgrade windows version in any scenario. This is done via clud with feature update or update ring and the upgrade to win 11 option

upvoted 1 times

RazielLycas 2 years, 8 months ago

what I mean for "windows version" is the build (win 10 to win 11) not the version like home,pro,enterprise

upvoted 1 times

suman95 2 years, 8 months ago

Answer Should be B. Autopilot can not upgrade from 10 to 11, MDT doesn't support Windows 11, and Subscription Activation can only do 10 pro to 10 E. Only left that can do is SCCM

upvoted 1 times

OyYaGotta 2 years, 8 months ago

Sorry, but none of what you said is correct. Autopilot can be used to upgrade Win 10 Pro to Win 11, MDT does support Win 11 and Subscription Activation does support the upgrade. But the least administrator effort is Subscription Activation, so the answer is D.

upvoted 1 times

MR_Eliot 2 years, 8 months ago

For people who are thinking to choose another answer than A, you're wrong!

Question is not asking about licence upgrade, it's asking for in-place upgrade of Windows 10 PRO devices. MDT with a default image is sufficient.

upvoted 1 times

BigStan82 2 years, 8 months ago

Selected Answer: D

Subscription Activation allows you to upgrade Windows 10 Pro devices to Windows 11 Enterprise automatically without the need for re-imaging or manual upgrade processes. This method leverages your existing Microsoft 365 E5 subscription, which includes licensing for Windows 11 Enterprise. It uses the Azure AD join of your devices and their connection to Microsoft Intune to manage the upgrade process, aligning with the requirements of minimizing administrative effort. This method is more efficient and streamlined than using deployment tools or manual upgrades for a relatively small number of devices.

upvoted 3 times

Dariooo 2 years, 8 months ago

Subscription activation is available for qualifying devices running currently supported versions of Windows. Subscription activation can't be used to upgrade to a newer version of Windows

upvoted 1 times

mhmyz 2 years, 8 months ago

Selected Answer: B

Modern deployment methods

....

In-place upgrade

..... Control is accomplished by using tools like Microsoft Configuration Manager to completely automate the upgrade process through simple task sequences.

https://learn.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios

upvoted 1 times

Softeng 2 years, 9 months ago

Selected Answer: B

- MDT does not support Windows 11.

- Configuration Manager supports Windows 11.

- Autopilot wipes device, so It's not really an 'in-place upgrade' :)

- Subscription Activation will update from Pro to Enterprise, but not from W10 to W11.

Therefore only logical answer is B.

upvoted 1 times

Judith1969 2 years, 9 months ago

Selected Answer: B

Merrybob seems to have it right.

upvoted 1 times

Merrybob 2 years, 9 months ago

Selected Answer: B

B. Microsoft Configuration Manager and a custom image of Windows 11 Enterprise

This goes against the grain for the responses received below but here are my findings:

upvoted 2 times

Merrybob 2 years, 9 months ago

MDT does NOT support deployment of Windows 11.

Ref 1: https://learn.microsoft.com/en-us/mem/configmgr/mdt/release-notes#supported-platforms:~:text=MDT%20doesn%27t%20support%20Windows%2010%20ARM64%20devices%2C%20Windows%2011%20and%20Windows%20Server%202022%20operating%20systems.)

Ref 2: [Read Simon Ren-MSFT's comment] https://learn.microsoft.com/en-us/answers/questions/1325234/why-is-there-no-mdt-support-for-windows-11

Ref 3: https://learn.microsoft.com/en-us/mem/configmgr/mdt/release-notes#latest-release

.

upvoted 1 times

Merrybob 2 years, 9 months ago

Config Manager does support all Windows 11 editions.

(Ref: https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/support-for-windows-11#:~:text=Support%20for%20Windows%2011%20versions%20includes%20the%20following%20editions%3A%20Enterprise%2C%20Pro%2C%20Education%2C%20Pro%20Education%2C%20and%20Pro%20for%20Workstation.)

.

upvoted 2 times

vijay0715 2 years, 9 months ago

Selected Answer: D

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.

upvoted 2 times

frack 2 years, 10 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios

upvoted 1 times

onepunchkenshin 2 years, 10 months ago

Selected Answer: C

The solution must minimize administrative effort.

upvoted 2 times

norelissme 2 years, 11 months ago

Autopilot & Subscription activation ==> Do not support in-place upgrade

Config Manager (SCCM) ==> Does support in-place upgrade (via MDT). But in-place upgrade does not support custom image

A is the right answer

upvoted 3 times

Tonsku 2 years, 11 months ago

Selected Answer: C

C. Windows Autopilot

This will minimize the administrative effort required upgrade to Windows 11 Enterprise.

upvoted 1 times

belyo 2 years, 11 months ago

Selected Answer: A

where is autopilot you can configure to update from 10 to 11 ?

this option isnt available, PC's must have win 10 or 11 already installed

Its just another trap question that makes you pick autopilot due to the administrative effort requirement

A seems to be the only option, as subscription activation does not upgrade from 10 to 11

upvoted 1 times

yosry 2 years, 11 months ago

Selected Answer: A

answer A seems correct

upvoted 1 times

madsa 2 years, 11 months ago

C. Windows Autopilot

Windows Autopilot is a modern deployment method that leverages the capabilities of Microsoft Intune for managing and deploying Windows devices. With Windows Autopilot, you can perform in-place upgrades to Windows 11 without the need for extensive manual intervention or imaging.

upvoted 1 times

madsa 2 years, 11 months ago

This one is C guys, I've done it ant the correct answer is on the MD-102 self-learning practice questions.

upvoted 1 times

LiamAzure 3 years ago

Selected Answer: A

MDT, to upgrade from windows 10 to 11, you need to install the OS. Autopilot can't do this

upvoted 2 times

chandravamsi 3 years ago

Windows Autopilot

upvoted 1 times

chandravamsi 3 years ago

My Appoogy, It is option A

upvoted 2 times

benpatto 3 years ago

Realistically speaking, A. can't work because no mention of any physical infrastructure. Autopilot isn't an in-place upgrade so also doesn't work.

Only choice is Sub-activation as the 'starting point', once on enterprise, other options can be looking into.

upvoted 1 times

NoursBear 3 years ago

Initially I was all for the MDT way. I think they want you to chose "subscritption activation" first to get them to an Enterprise edition and then use an update ring to upgrade to 11. Bad question as no details about infrastructure given etc..

upvoted 1 times

fco168 3 years ago

Selected Answer: D

The microsoft 365 license comes with a Win Enterprise license and comes with an O365 License as well. Which means that when a user logs into Outlook or any app on the suite, the windows license will kick in and will upgrade the windows edition automatically, keeping the user's data and programs.

upvoted 1 times

iTomi 2 years, 11 months ago

Wrong wrong wrong!

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#subscription-activation-for-enterprise

upvoted 2 times

egg651 2 years, 12 months ago

The question states that we need to go from Windows 10 Pro to Windows 11 Enteprrise, so we need to update the OS as well as switch edition. In practice I would absolutely do subscription activation + Windows Update for Business, but the question doesn't give us that option. The only choice that allows both in-place OS upgrade *and* edition switch to Enterprise in one go is MDT with the default image (A).

upvoted 1 times

sh123df 3 years ago

Selected Answer: C

Yes, possible by using intune feature update deployment policy.

upvoted 2 times

Zelda78 3 years ago

as it states "in-place upgrade", autopilot does not do in-place to my knowledgde. so to me it's A

upvoted 3 times

ZaFletch 3 years, 1 month ago

Selected Answer: D

D seems correct to me:

It's designed to seamlessly upgrade from Pro to Enterprise. There's no need to re-image the device. They meet the licensing requirements so it's by far the least admin overhead. There seems to be no requirement to update from 10 to 11 just an edition change.

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

upvoted 4 times

iTomi 2 years, 11 months ago

Your source says: "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."

upvoted 1 times

Monades 3 years, 1 month ago

Selected Answer: A

https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit

upvoted 2 times

4rk4n4 3 years, 1 month ago

Selected Answer: C

I think its option C.

Option A (using Microsoft Deployment Toolkit and a default image) may require more manual effort, like a custom image creation.

upvoted 2 times

VirtualJP 3 years, 1 month ago

Selected Answer: C

Here's why:

Windows Autopilot is a modern deployment method for Windows 10 and Windows 11 that streamlines the setup and configuration of new devices and the upgrading of existing devices. It's designed to simplify the deployment process and reduce administrative overhead.

Since we already have a Microsoft 365 E5 subscription that uses Microsoft Intune, you can leverage these services to manage and configure Windows Autopilot deployments.

Windows Autopilot supports both new device provisioning and in-place upgrades. In this scenario, you want to perform an in-place upgrade from Windows 10 Pro to Windows 11 Enterprise, which can be accomplished through Windows Autopilot.

Windows Autopilot minimizes administrative effort by automating many of the deployment and configuration tasks. Once you set up the Autopilot profile and enrollment settings in Microsoft Intune, the rest of the process can be largely hands-off for administrators and end-users.

upvoted 2 times

iTomi 2 years, 11 months ago

Question is about IN-PLACE upgrade. You cannot do that with autopilot.

upvoted 1 times

picho707 3 years, 1 month ago

Selected Answer: C

I am leaning towards "C" due to the fact that there is no mention of on-premise servers.

upvoted 1 times

iTomi 2 years, 11 months ago

Great, but there is mention of IN-PLACE upgrade.

upvoted 1 times

Cheban 2 years, 7 months ago

The answers is B - Configuration manager

upvoted 3 times

pxdPhil2 2 years, 7 months ago

Subscription activation cannot upgrade between versions, ie 10 to 11

upvoted 4 times

Nozuka 3 years, 2 months ago

Autopilot doesn't do an "in-place upgrade", it deletes everything. Subscription activation can't do it either. SCCM doesn't seem to be present yet, so it's too much effort. I guess that only leaves MDT, but it is not very satisfying solution for "low effort" either.

upvoted 4 times

JustinHadwin 3 years, 2 months ago

"Subscription activation doesn't update a device from Windows 10 to Windows 11. Only the edition is updated."

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

upvoted 3 times

rus10 3 years, 2 months ago

Selected Answer: C

Autopilot and update rings so the PC will be forced in-place upgrade to windows 11

upvoted 2 times

Futfuyfyjfj 3 years, 2 months ago

Well knowing Microsoft and the way they write down exam questions, I doubt whether C is correct, since Autopilot on it’s own can’t update anything. And wiping all the devices to enroll them through Autopilot and then update by using WUfB in Intune is quite some effort as well. Just updating in place by MDT might be easier anyway.

upvoted 2 times

picho707 3 years, 1 month ago

There is no mention of on-premise servers in the wording of this question.

upvoted 1 times

usmansyed23 3 years, 2 months ago

Selected Answer: C

I am guessing its C because Autopilot will help with the 'minimize administrative effort' bit.

A and B dont apply as this is an Intune focused question.

upvoted 3 times

NoursBear 3 years, 2 months ago

For me MDT is the only correct answer

upvoted 3 times

Futfuyfyjfj 3 years, 2 months ago

Answer is correct, subscription activation is based on the license assigned in AAD and only requires a Windows sign off and sign in.

upvoted 3 times

picho707 3 years, 1 month ago

Subscription activation cannot upgrade from Windows 10 to Windows 11.

upvoted 2 times

Crismo 3 years, 1 month ago

Weird question. To me all answers don't make sense. There's a statement in the Microsoft documentation that says you can't use subscription activation to upgrade from W10 to W11, https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#subscription-activation-for-enterprise

But it's needed to get from Pro to Enterprise, therefore it seems be the best choice anyhow.

upvoted 1 times

picho707 3 years, 2 months ago

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 3 times

Futfuyfyjfj 3 years, 2 months ago

I think you are wrong, the question states the device are now on Win 10 Pro and need to upgrade to Win11Ent. Subscription activation only upgrades the edition, not the version

upvoted 2 times

Question #70 *Topic 1*

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



Tr619899 Most Recent 1 year, 11 months 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 2 years, 2 months ago

Answer is A

upvoted 2 times

Ruchira007 2 years, 5 months ago

A is correct

upvoted 1 times

GreenJPGSandRAM Highly Voted 2 years, 6 months ago

MDT is being removed from the exam on Apr 26, 2024. This question is no longer relevant

upvoted 11 times

mestorrent86 2 years, 8 months 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 2 years, 8 months ago

Selected Answer: B

B is correct. Trust me on this one.

upvoted 2 times

MR_Eliot 2 years, 8 months ago

B is correct. Trust me on this one.In a world of anonymity, trust is absent; only proof and evidence matter.Thanks, I trust you

upvoted 2 times

RomanV 2 years, 2 months ago

In a world of anonymity, trust is absent; only proof and evidence matter.

upvoted 4 times

ten1ton 2 years, 6 months ago

Thanks, I trust you

upvoted 2 times

Darkfire 2 years, 9 months 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 2 years, 11 months 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 2 years, 11 months ago

Selected Answer: A

seems correct

upvoted 1 times

NoursBear 2 years, 11 months ago

According to this question in MD 101 everyone voted the same "update deployment share"

https://www.examtopics.com/discussions/microsoft/view/86938-exam-md-101-topic-2-question-97-discussion/

upvoted 2 times

Linkin27 3 years ago

Selected Answer: B

I think it's B

upvoted 1 times

fco168 3 years ago

Selected Answer: A

A is correct. And then replace the image in WDS.

upvoted 4 times

LiamAzure 3 years ago

Selected Answer: A

Right click deployment share -> Update

upvoted 3 times

Dropkick 3 years 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 3 years, 1 month 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 3 years, 1 month 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

Support_Compu 3 years, 1 month 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

cpaljchc4 3 years ago

Agreed

upvoted 1 times

BJS78 3 years, 1 month 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

novaCapta 3 years, 1 month ago

I am not sure of the answer!

upvoted 1 times

Question #71 *Topic 1*

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 Highly Voted 2 years ago

MDT is being removed from the exam on Apr 26, 2024. This question is no longer relevant

upvoted 8 times

mestorrent86 Highly Voted 2 years, 2 months 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 5 times

MR_Eliot 2 years, 2 months 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 2 years, 3 months 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 2 years, 5 months ago

Selected Answer: B

B. Standard Client Replace Task Sequence

upvoted 1 times

Wonder55 2 years, 6 months 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 2 years, 6 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 2 years, 8 months 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 2 years, 8 months ago

I think the right response is the A

The "Standard Client Replace Task Sequence" don't prreserve the user state.

upvoted 1 times

cserra 2 years, 8 months ago

I think the right response is the A The "Standard Client Replace Task Sequence" don't prreserve the user state.

upvoted 1 times

4rk4n4 2 years, 7 months ago

Option A ("Standard Client Task Sequence") is used for clean installations, not for replacing existing devices or migrating user data.

upvoted 1 times

Futfuyfyjfj 2 years, 8 months 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

Question #72 *Topic 1*

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%)

Dinkan Most Recent 1 year, 2 months ago

Selected Answer: B

B. Enable-PSRemoting

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.

Reference: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting

upvoted 1 times

ergacharsk 2 years, 4 months ago

Selected Answer: B

B is correct

upvoted 1 times

MR_Eliot 2 years, 8 months ago

Selected Answer: B

Correct

upvoted 1 times

Darkfire 2 years, 9 months 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 2 times

neki99 Highly Voted 3 years, 1 month 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 9 times

BJS78 3 years, 1 month ago

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-7.3

upvoted 1 times

Question #73 *Topic 1*

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.

You assign Windows 10/11 Enterprise E5 licenses to Group1 and User2.

You deploy the devices shown in the following table.

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

NOTE: Each correct selection is worth one point.

Name	Member of	On-premises sync
User1	Group1	Disabled
User2	Group2	Enabled

Name	Operating system	Joined to
Device1	Windows 11 Pro	Azure AD
Device2	Windows 11 Pro	AD DS
Device2	Windows 10 Pro	Azure AD

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.	○	○
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	○	○
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.	○	○
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	○	○
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.	○	○

Grg433 Highly Voted 3 years, 2 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 28 times

Grg433 Highly Voted 3 years, 2 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.Agree: Y,N,N User1 signs in to Device1 (Win11 Pro, Azure AD Joined): User1 is in Azure AD and licensed. Device1 is Azure AD joined. Result: Yes. Meets all requirements for automatic edition upgrade to Windows 11 Enterprise. User2 signs in to Device2 (Win11 Pro, AD DS Joined): Device2 is only AD DS joined, not Azure AD joined or Hybrid Azure AD joined. Result: No. Does not meet the device join type requirement for subscription activation. User2 signs in to Device3 (Win10 Pro, Azure AD Joined): User2 is licensed. Device3 is Azure AD joined. Result: No. The device will automatically upgrade to Windows 10 Enterprise. However, the question asks for an upgrade to Windows 11 Enterprise automatically. While the license provides the right to Windows 11 Enterprise, the version upgrade from Windows 10 to Windows 11 is a separate, non-automatic step.until User1 is synced it is not licensed with the E5 license and therefore the device is not upgraded to W11 N,N,NThe first line of Q says the users are in Entra. So....?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.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.Or User1 is AD-onprem only and thus not available in AzureAD.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 28 times

reyrey Most Recent 9 months ago

the correct answer is YNY

upvoted 2 times

justITtopics 1 year, 7 months ago

YNN

Box 1: user 1 is a cloud user with a licence and device 1 is Azure AD joined.

Box 2: we cannot asume that is a hybrid-joined device even though they say "(AD DS) domain that syncs with an Azure AD tenant", because they don't say and maybe, there's no gpo for hybrid enrolment.

Hybrid-joined devices are valid.

Deploy Windows Enterprise Licenses

Devices must be joined to Microsoft Entra ID, or hybrid domain joined with Microsoft Entra Connect.

https://learn.microsoft.com/en-us/windows/deployment/deploy-enterprise-licenses?pivots=windows-11#review-requirements-on-devices:~:text=Devices%20must%20be%20joined%20to%20Microsoft%20Entra%20ID%2C%20or%20hybrid%20domain%20joined%20with%20Microsoft%20Entra%20Connect.

Box 3: you cannot upgrade directly from Windows 10 Pro, to Windows 11 Enterprise. Licensing will upgrade from Win 10 pro to Win 10 Ent

upvoted 1 times

Stuckbear 3 years, 1 month 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 13 times

Stuckbear 3 years, 1 month ago

until User1 is synced it is not licensed with the E5 license and therefore the device is not upgraded to W11 N,N,NThe first line of Q says the users are in Entra. So....?

upvoted 13 times

JRD88 1 year, 8 months ago

Where is Device 3?

upvoted 3 times

Tr619899 1 year, 11 months 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 4 times

[Removed] 2 years, 10 months 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 2 years, 9 months 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.Or User1 is AD-onprem only and thus not available in AzureAD.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 3 times

Anonymouse1312 2 years, 9 months 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

AleFCI1908 2 years ago

the 3rd is win10, you can't upgrade win 10 to 11 wind subs activation, so NO

upvoted 3 times

HvD 2 years, 2 months ago

Or User1 is AD-onprem only and thus not available in AzureAD.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

HvD 2 years, 2 months ago

Or User1 is AD-onprem only and thus not available in AzureAD.

upvoted 1 times

Cezt 2 years, 3 months ago

Microsoft Entra available for identity management. is a requirement to upgrada

upvoted 1 times

Vlad99 3 years, 1 month 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.For number 2, the device is already in Azure AD, so it doesnt matter if the sync is disabled?For number 1 I mean

upvoted 17 times

Vlad99 3 years, 1 month 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 17 times

oopspruu 2 years, 4 months ago

Y N N

Subscription will simply upgrade Windows 10 Pro to Windows 10 Enteprise. You have to do the upgrade from Windows 10 to 11 manually.

upvoted 2 times

LiamAzure 2 years, 12 months ago

For number 2, the device is already in Azure AD, so it doesnt matter if the sync is disabled?For number 1 I mean

upvoted 1 times

LiamAzure 2 years, 12 months ago

For number 2, the device is already in Azure AD, so it doesnt matter if the sync is disabled?

upvoted 1 times

CJL324 2 years, 6 months 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 2 years, 9 months ago

I think correct answer should be YNN.

upvoted 2 times

FDMR 1 year, 8 months ago

you cannot assume that Hybrid Azure AD join is configured

upvoted 1 times

Mattia8 2 years, 9 months ago

Seems correct

upvoted 1 times

1655b71 2 years 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 3 times

1655b71 2 years 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.the 3rd is win10, you can't upgrade win 10 to 11 wind subs activation, so NO

upvoted 3 times

arsh807 2 years, 9 months ago

1. User not synced BUT Device1 is already joined to Azure AD

Y Y N

upvoted 1 times

Krayzr 2 years, 11 months 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 5 times

mertak 2 years, 9 months 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.examtopics.com/discussions/microsoft/view/52384-exam-md-101-topic-2-question-48-discussion/you cannot assume that Hybrid Azure AD join is configured

upvoted 2 times

mertak 2 years, 9 months 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.examtopics.com/discussions/microsoft/view/52384-exam-md-101-topic-2-question-48-discussion/

upvoted 2 times

madsa 2 years, 11 months 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 2 years, 11 months ago

Actually, the answer is correct.

upvoted 1 times

kay000001 2 years, 12 months 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 Enteprise (if the device is running 'supported' versions of Win10 Pro).

Please correct me if I am wrong.

upvoted 1 times

belyo 2 years, 11 months ago

1.NO user not synced 2.YES [it looks to me like a hybrid joined device, given the question statements] 3.NO definitely1. User not synced BUT Device1 is already joined to Azure AD Y Y N

upvoted 1 times

belyo 2 years, 11 months 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

Krayzr 2 years, 11 months ago

Read the question line one. It says users are on the (Azure) Tenant (already)

upvoted 1 times

fco168 3 years 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. Howeeeveeeeer, Device3 is windows 10 pro, CANNOT UPGRADE TO WINDOWS 11 ENT. Only to Win10 Ent.

That was the trick.

upvoted 1 times

benpatto 3 years ago

As far as I'm aware, you can't 'automatically' update windows 10 to windows 11, you can only do small in place upgrades. AD DS synced devices require a manual input to update the version of windows whereas device 1, it should be very possible to happen automatically

upvoted 1 times

VirtualJP 3 years, 1 month ago

Have to agree with Vlad99

upvoted 1 times

LiamAzure 2 years, 12 months ago

For number 1 I mean

upvoted 1 times

picho707 3 years, 1 month ago

The answer is No, No, No:

Question 1: User1 is not synced to Azure AD.

Question 2: The device is not Azure AD joined.

Question 3: It is not possible to upgrade Windows 10 pro to Windows 10 Ent via subscription upgrades.

upvoted 6 times

Casticod 3 years, 1 month ago

According to your comment, in cloud-only companies (without synchronized AD) it would never work, right?

The products and licenses, with very few exceptions (for example SSPR), are exactly the same for Hybrid and cloud-only users.

upvoted 1 times

BJS78 3 years, 1 month ago

https://xenit.se/blog/2017/12/27/windows-10-subscription-activation-hybrid-azure-ad-joined-devices/

According to this, IF the AD DS device is AAD registered as well, it will also upgrade. If not, no.

upvoted 1 times

Besxp 1 year, 5 months ago

Agree: Y,N,N

User1 signs in to Device1 (Win11 Pro, Azure AD Joined):

User1 is in Azure AD and licensed. Device1 is Azure AD joined.

Result: Yes. Meets all requirements for automatic edition upgrade to Windows 11 Enterprise.

User2 signs in to Device2 (Win11 Pro, AD DS Joined):

Device2 is only AD DS joined, not Azure AD joined or Hybrid Azure AD joined.

Result: No. Does not meet the device join type requirement for subscription activation.

User2 signs in to Device3 (Win10 Pro, Azure AD Joined):

User2 is licensed. Device3 is Azure AD joined.

Result: No. The device will automatically upgrade to Windows 10 Enterprise. However, the question asks for an upgrade to Windows 11 Enterprise automatically. While the license provides the right to Windows 11 Enterprise, the version upgrade from Windows 10 to Windows 11 is a separate, non-automatic step.

upvoted 2 times

Anonymous 2 years, 10 months 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

FemiA55 1 year, 11 months 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

Krayzr 2 years, 11 months ago

The first line of Q says the users are in Entra. So....?

upvoted 3 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.

The local Administrator accounts on Computer1, Computer2, and Computer3 have the same user name and password.

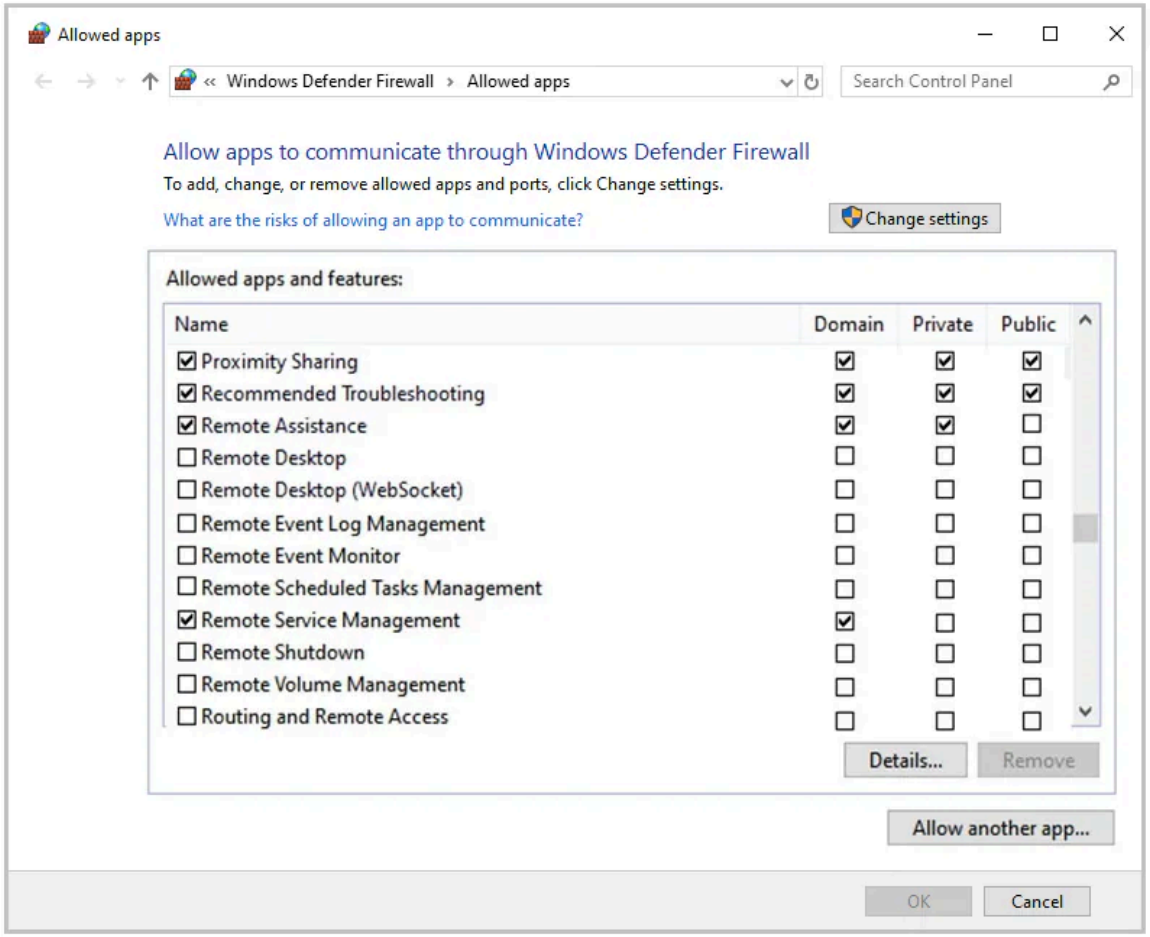
On Computer1, Windows Defender Firewall is configured as shown in the following exhibit.

The services on Computer1 have the following states.

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

NOTE: Each correct selection is worth one point.

Name	Member of	Active Windows Defender Firewall profile
Computer1	Adatum.com	Domain
Computer2	Adatum.com	Domain
Computer3	Workgroup	Public



```
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)
```

Answer Area

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.	○	○
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	○	○
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.	○	◉
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	○	◉
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.	○	◉

fco168 Highly Voted 3 years ago

You need Remote Registry Service to be running for Disk Management, Performance Monitor and Registry itself. That's required. N N NBut 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 by YNNActually YYN 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 managedWrong it's still N,N,N Don't confuse the people: while many comments arrived at the correct answer (N, N, N), their underlying technical explanations for why were often flawed, incomplete, or based on incorrect readings of the provided firewall configuration. The most critical factors are the explicitly disabled firewall rules for the specific remote management features and the stopped RemoteRegistry service for its respective function.

upvoted 13 times

fco168 Highly Voted 3 years ago

You need Remote Registry Service to be running for Disk Management, Performance Monitor and Registry itself. That's required.

N N N

upvoted 13 times

ckmay 2 years, 9 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 by YNNActually YYN 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 managedWrong it's still N,N,N Don't confuse the people: while many comments arrived at the correct answer (N, N, N), their underlying technical explanations for why were often flawed, incomplete, or based on incorrect readings of the provided firewall configuration. The most critical factors are the explicitly disabled firewall rules for the specific remote management features and the stopped RemoteRegistry service for its respective function.

upvoted 1 times

ckmay 2 years, 9 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 by YNN

upvoted 1 times

ckmay 2 years, 9 months ago

Actually YYN 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

ckmay 2 years, 9 months ago

Actually YYN 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 managedWrong it's still N,N,N Don't confuse the people: while many comments arrived at the correct answer (N, N, N), their underlying technical explanations for why were often flawed, incomplete, or based on incorrect readings of the provided firewall configuration. The most critical factors are the explicitly disabled firewall rules for the specific remote management features and the stopped RemoteRegistry service for its respective function.

upvoted 1 times

Besxp Most Recent 1 year, 5 months ago

Wrong it's still N,N,N Don't confuse the people: while many comments arrived at the correct answer (N, N, N), their underlying technical explanations for why were often flawed, incomplete, or based on incorrect readings of the provided firewall configuration. The most critical factors are the explicitly disabled firewall rules for the specific remote management features and the stopped RemoteRegistry service for its respective function.

upvoted 2 times

Tr619899 1 year, 11 months ago

Answer is: NO, NO, NO

upvoted 1 times

Engr001 2 years, 8 months ago

Remote Access Service is stopped. So no remote access is available? Therefor it's N, N, N ?

upvoted 3 times

yosry 2 years, 11 months ago

seems correct

upvoted 2 times

pirate84 3 years ago

No,No,No

upvoted 1 times

NoursBear 3 years 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 3 years 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

BJS78 3 years, 1 month 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

Question #75 *Topic 1*

You have a Hyper-V host that contains the virtual machines shown in the following table.

On which virtual machines can you install Windows 11?

Name	Generation	Virtual processors	Memory
VM1	1	4	16 GB
VM2	2	1	8 GB
VM3	2	2	4 GB

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%)

Dinkan Most Recent 1 year, 2 months ago

B. VM3 only -- Windows 11 minimum requirements include 4GB RAM, 2 Core Processor, TPM & SecureBoot. Only Gen 2 VMs will have TPM support, hence cannot be installed on VM1 VM2 does not have 2 CPU Cores https://learn.microsoft.com/en-us/windows/whats-new/windows-11-requirements#hardware-requirements

upvoted 1 times

Jz23 1 year, 9 months ago

Windows 11 Minimum Requirements for VMs in Hyper-V To install Windows 11, the VM must meet these key requirements: Processor: 1 GHz or faster, 2 or more cores, 64-bit compatible RAM: At least 4 GB Storage: At least 64 GB TPM (Trusted Platform Module) 2.0: Must be enabled (can be emulated in Hyper-V) Secure Boot: Must be enabled UEFI Firmware (instead of legacy BIOS)

upvoted 2 times

Twindragon 1 year, 11 months ago

Answer B is correct windows 11 is not supported by generation1.

upvoted 1 times

Tr619899 1 year, 11 months ago

Answer seems correct.

upvoted 2 times

oopspruu 2 years, 4 months ago

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 4 times

MR_Eliot 2 years, 8 months ago

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 2 times

Darkfire 2 years, 9 months ago

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 3 times

Amir1909 2 years, 10 months ago

Correct

upvoted 1 times

yosry 2 years, 11 months ago

seems correct

upvoted 1 times

fco168 3 years ago

Win11 minimum requirements, 2 cores and 4GB Ram

upvoted 3 times

Casticod 3 years, 1 month ago

Picho707 Right

upvoted 1 times

Grg433 3 years, 2 months ago

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).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://learn.microsoft.com/en-us/windows/whats-new/windows-11-requirements#virtual-machine-support It seems that's right

upvoted 2 times

Grg433 3 years, 2 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 Highly Voted 3 years, 2 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.https://learn.microsoft.com/en-us/windows/whats-new/windows-11-requirements#virtual-machine-support It seems that's right

upvoted 6 times

picho707 Highly Voted 3 years, 2 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 3 years, 1 month ago

https://learn.microsoft.com/en-us/windows/whats-new/windows-11-requirements#virtual-machine-support It seems that's right

upvoted 2 times

Question #76 *Topic 1*

HOTSPOT

-

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

Group2 has been assigned in the Enrollment Status Page.

You have the devices shown in the following table.

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.

Name	Member of	License
User1	Group1	*None*
User2	Group1	Microsoft 365 E3
User3	Group2	Microsoft 365 E5

Name	Operating system	Department
Device1	Windows 10 Pro	Marketing
Device2	Windows 10 Home	Research
Device3	Windows 10	Marketing

Answer Area

Statements	Yes	No
User1 can complete the Autopilot process on Device1.	○	○
User2 can complete the Autopilot process on Device1.	○	○
User3 can view device setup information during the enrollment phase of Device1.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can complete the Autopilot process on Device1.	○	◉
User2 can complete the Autopilot process on Device1.	◉	○
User3 can view device setup information during the enrollment phase of Device1.	◉	○

ExamKiller020 Highly Voted 3 years, 1 month 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 configuredN,N,Y O dispositivo 02 não pertence ao departamento de marketing, ID de hardware não foi carregado.

upvoted 19 times

ExamKiller020 Highly Voted 3 years, 1 month 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 19 times

ExamBud 1 year, 8 months ago

If it is self-deploying mode, it is userless. The question implies it is user-driven.

upvoted 1 times

Casticod 3 years, 1 month 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/1438719Very true option 2, Its Windows HOME. ===> Thus NOQuestion 2 also is about Device1, Windows Pro. Not Home.Fully Agree !! answer 2 is NO because Windows HOME is not supported by Autopilot N Y Ymistyped sorry correct answers are N N YCorrect. Windows Autopilot is not available for Windows 10 Home edition. It requires Windows 10 Pro, Enterprice, or Education editons to utilize Autopilot.You do realize it's talking about DEVICE 1 right? So answer is YES.I correct NYY and the second question talks about device 1 (not 2)There is no mention of device 2. Correct me, but No, Yes, Yes.

upvoted 14 times

Casticod 3 years, 1 month 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 14 times

c54796e 2 years, 6 months ago

Correct. Windows Autopilot is not available for Windows 10 Home edition. It requires Windows 10 Pro, Enterprice, or Education editons to utilize Autopilot.

upvoted 3 times

MCI 1 year, 7 months ago

That's shows how much experience you have with intune. In a user driven scenario you need to log on with an account that has a intune license. So N Y Y.

upvoted 1 times

ExamBud 1 year, 8 months ago

The hardware ID is just to register the computer in Autopilot. But you need an Intune license to deploy the device.

upvoted 1 times

VLAG 2 years, 8 months ago

Fully Agree !! answer 2 is NO because Windows HOME is not supported by Autopilot N Y Ymistyped sorry correct answers are N N Y

upvoted 1 times

Tr619899 1 year, 11 months ago

Answer is: No, Yes, Yes

upvoted 1 times

Kiookr 3 years ago

Very true option 2, Its Windows HOME. ===> Thus NO

upvoted 2 times

Xillar 2 years ago

NYY is correct.

All questions about Device 1

upvoted 2 times

c54796e 2 years, 6 months ago

Correct. Windows Autopilot is not available for Windows 10 Home edition. It requires Windows 10 Pro, Enterprice, or Education editons to utilize Autopilot.You do realize it's talking about DEVICE 1 right? So answer is YES.

upvoted 3 times

EUC_PRO 2 years, 2 months ago

NYY is correct

upvoted 1 times

VLAG 2 years, 8 months ago

Fully Agree !! answer 2 is NO because Windows HOME is not supported by Autopilot N Y Y

upvoted 1 times

oopspruu 2 years, 4 months 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 5 times

KakTak 2 years, 4 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

hieunm2411 1 year, 9 months ago

I think the question wasn't clear. The license for user1 is unnecessary if the Deployment mode in the autopilot profile is Self-Deploying. So maybe Y Y Y could the the correct answer also.If it is self-deploying mode, it is userless. The question implies it is user-driven.

upvoted 1 times

hieunm2411 1 year, 9 months ago

I think the question wasn't clear. The license for user1 is unnecessary if the Deployment mode in the autopilot profile is Self-Deploying. So maybe Y Y Y could the the correct answer also.

upvoted 1 times

MR_Eliot 2 years, 8 months ago

NYY

https://learn.microsoft.com/en-us/autopilot/software-requirements

upvoted 4 times

nlnick 2 years, 9 months ago

User 2 isnt a member of group to so should be N-N-Y

upvoted 1 times

GamingFuntime1985 1 year, 9 months ago

Y Y Y 1. no license , but who cares since hardware ID already in the Intune. It will join even without user ID. 2. MS E3 and if no ESP config is assigned the default ESP will take place 3. MS E5 And ESP has been configuredThat's shows how much experience you have with intune. In a user driven scenario you need to log on with an account that has a intune license. So N Y Y.The hardware ID is just to register the computer in Autopilot. But you need an Intune license to deploy the device.

upvoted 1 times

GamingFuntime1985 1 year, 9 months ago

Y Y Y 1. no license , but who cares since hardware ID already in the Intune. It will join even without user ID. 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 1 times

Murad01 2 years, 9 months ago

It is definetly NYY.

upvoted 1 times

AdamRachel 2 years, 10 months ago

it is device1 Windows 10 Pro not device 2.

upvoted 1 times

abill 2 years, 11 months ago

Sorry it's NYY - no mention of device 2

upvoted 2 times

LiamAzure 3 years ago

So it's N Y Y

upvoted 1 times

abill 2 years, 11 months ago

NNY - Windows home is not supported for autopilotit is device1 Windows 10 Pro not device 2.Sorry it's NYY - no mention of device 2

upvoted 1 times

abill 2 years, 11 months ago

NNY - Windows home is not supported for autopilot

upvoted 1 times

Newboy Most Recent 1 year, 2 months ago

There is no mention of device 2. Correct me, but No, Yes, Yes.

upvoted 2 times

LiamAzure 3 years ago

N N Y Windows 10 Home edition is not supported for autopilot

upvoted 1 times

LiamAzure 3 years ago

N N Y Windows 10 Home edition is not supported for autopilotSorry, it doesn't mention device 2, only device 1So it's N Y Y

upvoted 1 times

LiamAzure 3 years ago

Sorry, it doesn't mention device 2, only device 1

upvoted 2 times

LiamAzure 3 years ago

Sorry, it doesn't mention device 2, only device 1So it's N Y Y

upvoted 2 times

RomanV 2 years, 2 months ago

You do realize it's talking about DEVICE 1 right? So answer is YES.

upvoted 8 times

Savior99 2 years, 8 months ago

All 3 questions refer to Device1, so N Y Y is correct

upvoted 4 times

Anonymous 3 years ago

Very true option 2, Its Windows HOME. ===> Thus NO

upvoted 2 times

HvD 2 years, 2 months ago

Question 2 also is about Device1, Windows Pro. Not Home.

upvoted 3 times

VLAG 2 years, 8 months ago

mistyped sorry

correct answers are

N

N

Y

upvoted 1 times

Casticod 3 years, 1 month ago

I correct NYY and the second question talks about device 1 (not 2)

upvoted 6 times

rcristiano 2 years, 6 months ago

N,N,Y O dispositivo 02 não pertence ao departamento de marketing, ID de hardware não foi carregado.

upvoted 1 times

sh123df 3 years, 2 months ago

Correct answer

upvoted 3 times

Question #77 *Topic 1*

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 (90%) D (10%)

martin451 Most Recent 4 months, 4 weeks ago

Selected Answer: D

The question is testing the Windows Enterprise per-user activation limit, not Microsoft 365 Apps activation which is 5 devices. So: Activated = 3 Maximum = 11 Remaining = 8

The key is the specific license mentioned: Windows 10/11 Enterprise E3 license Microsoft's Windows Enterprise per-user licensing allows a licensed user to activate Enterprise on up to 11 devices.

So: User1 has activated 3 devices:

Device1

Device2

Device3

Maximum allowed = 11

11 − 3 = 8

upvoted 1 times

Dinkan 1 year, 2 months ago

Selected Answer: A

A. User1 can activate 2 more devices as he has already activated 3 devices.

Up to five devices can be upgraded for each user license. If the user license is used for a sixth device, the computer where the user hasn't signed in for the longest time reverts to Pro or Pro Education.

https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation?pivots=windows-11#licenses

upvoted 1 times

Xillar 2 years 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 2 times

oopspruu 2 years, 4 months ago

Selected Answer: A

"How many more" is they key pointer in the question. Given answer is correct.

upvoted 1 times

Pollosor 2 years, 5 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 2 years, 7 months ago

Selected Answer: A

Total 5, Answer is 2

upvoted 1 times

Haider_Raza 2 years, 7 months ago

Selected Answer: A

A is correct.

upvoted 1 times

MR_Eliot 2 years, 8 months ago

Selected Answer: A

A is correct.

https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation#licenses

upvoted 2 times

vijay0715 2 years, 9 months 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 2 years, 11 months ago

Selected Answer: A

Normal user's limit is 5 devices

upvoted 1 times

NoursBear 2 years, 11 months ago

It seems with an E5 license it is also 5

upvoted 1 times

NoursBear 3 years 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

upvoted 1 times

fco168 3 years ago

Selected Answer: A

With this subscription you obtain a license to activate up to 5 devices.

upvoted 2 times

Kiookr 3 years, 1 month 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

Casticod 3 years, 1 month 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 3 years, 1 month ago

Disregard please.. I see _ how many more _

upvoted 2 times

Anonymous 3 years, 1 month 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

Anonymous 3 years, 1 month ago

Disregard please.. I see _ how many more _

upvoted 2 times

picho707 3 years, 2 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

Question #78 *Topic 1*

DRAG DROP

-

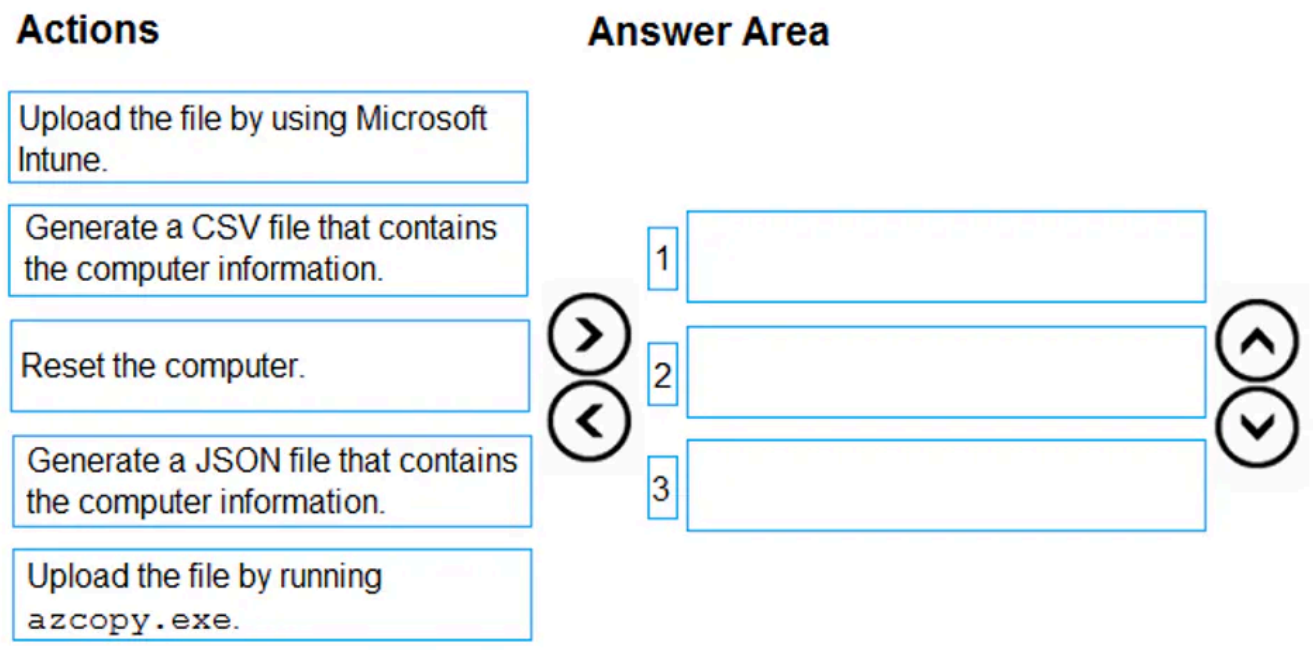
Your company has a computer named Computer1 that runs Windows 10.

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.



Suggested Answer:

Answer Area

Generate a CSV file that contains the computer information.

Upload the file by using Microsoft Intune.

Reset the computer.

TysonBeatty Most Recent 6 months ago

Typical not enough info.

The given answer is correct if we make the assumption that the computer was NOT in Intune and Autopilot for the prior owner. For this to be truly correct it should say something like you need to enroll this device in Autopilot and reset before you redeploy.

upvoted 2 times

ModernoDecor 8 months, 2 weeks ago

The question is outdated. Repurposing a device with Autopilot: Device stays enrolled in Intune. No need to get a CSV or hardware har, as it is already in Intune. Just need to click Autopilot reset

upvoted 2 times

TylerSivis 1 year, 9 months ago

I don't understand. There are instructions in Microsoft learn that contradict this entire process now.

https://learn.microsoft.com/en-us/autopilot/tutorial/reset/local-autopilot-reset https://learn.microsoft.com/en-us/autopilot/tutorial/reset/remote-autopilot-reset

upvoted 1 times

Dinkan 1 year, 2 months ago

1. Generate CSV file that contain computer information (Get-WindowsAutopilotInfo -OutputFile C:\AutopilotHWID.csv)

2. Uploading the file to Microsoft Intune

3. Reset the computer

Reference:

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

https://learn.microsoft.com/en-us/intune/intune-service/enrollment/corporate-identifiers-add#upload-csv-file

upvoted 2 times

TylerSivis 1 year, 9 months ago

I don't understand. There are instructions in Microsoft learn that contradict this entire process now. https://learn.microsoft.com/en-us/autopilot/tutorial/reset/local-autopilot-reset https://learn.microsoft.com/en-us/autopilot/tutorial/reset/remote-autopilot-resethttps://learn.microsoft.com/en-us/autopilot/tutorial/pre-provisioning/azure-ad-join-register-device

upvoted 1 times

Dinkan 1 year, 2 months ago

https://learn.microsoft.com/en-us/autopilot/tutorial/pre-provisioning/azure-ad-join-register-device

upvoted 1 times

Moot2 1 year, 12 months ago

Answer is correct

upvoted 3 times

Xillar 2 years ago

Given answer is the correct one.

upvoted 2 times

den5_pepito83 2 years, 7 months ago

Reset Computer Create CSV File Import CSV into Intune

upvoted 3 times

Josete1106 2 years, 1 month ago

The answer are correct:

Generate a CSV file that contains the computer information

Upload the file by ussing Microsft Intune

Reset the computer

upvoted 2 times

den5_pepito83 2 years, 7 months ago

Reset Computer Create CSV File Import CSV into IntuneNO 1. Create 2. Import 3. ResetI 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 policiies so you are expected to wipe it before importing the hash, but in this case the hash would normallly 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.You forget about LAPS.Assuming they have LAPS implemented

upvoted 3 times

3661de6 2 years, 7 months ago

NO

1. Create 2. Import 3. Reset

upvoted 4 times

3661de6 2 years, 7 months ago

NO 1. Create 2. Import 3. ResetI 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 policiies so you are expected to wipe it before importing the hash, but in this case the hash would normallly 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.You forget about LAPS.Assuming they have LAPS implemented

upvoted 4 times

captainspork 2 years, 2 months 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 policiies so you are expected to wipe it before importing the hash, but in this case the hash would normallly 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

oopspruu 2 years, 4 months ago

Given answer is correct.

1. Collect Hardwasre 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

captainspork 2 years, 2 months 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 policiies so you are expected to wipe it before importing the hash, but in this case the hash would normallly 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.You forget about LAPS.Assuming they have LAPS implemented

upvoted 1 times

MCI 1 year, 7 months ago

You forget about LAPS.

upvoted 1 times

MCI 1 year, 7 months ago

You forget about LAPS.Assuming they have LAPS implemented

upvoted 1 times

Casticod 3 years, 1 month ago

Ja Ja Ja, I have repeated this operation more than 1000 times, its correct

upvoted 4 times

Casticod 3 years, 1 month ago

Ja Ja Ja, I have repeated this operation more than 1000 times, its correctThe device detail should already be in intune if it is used by a past employee so why repeat it again? Why is there not a option to wipe the device and login using new users details?

upvoted 4 times

IStudyforRaizes 1 year, 6 months ago

Assuming they have LAPS implemented

upvoted 1 times

MR_Eliot 2 years, 8 months ago

coorect

upvoted 1 times

abill 2 years, 11 months ago

Correct

upvoted 1 times

HawkieEyes 3 years ago

Answer is correct

upvoted 2 times

fco168 3 years ago

That's correct.

upvoted 1 times

Sherpa23 2 years, 3 months 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 a option to wipe the device and login using new users details?

upvoted 3 times

ExamKiller020 3 years, 1 month ago

Given answer is correct.

ref: https://learn.microsoft.com/en-us/autopilot/add-devices

upvoted 3 times

Question #79 *Topic 1*

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%)

marcomartinez Highly Voted 1 year, 10 months ago

Selected Answer: C

MDT is being removed from the exam on Apr 26, 2024. This question is no longer relevant

upvoted 5 times

Twindragon 1 year, 11 months ago

Selected Answer: C

C is the correct answer.

upvoted 1 times

ergacharsk 2 years, 4 months ago

Selected Answer: C

preinstall

upvoted 2 times

MR_Eliot 2 years, 8 months ago

Selected Answer: C

Just checked this. C is correct.

upvoted 1 times

fco168 3 years ago

Selected Answer: C

Correct!

upvoted 2 times

Grg433 Highly Voted 3 years, 2 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 8 times

Question #80 *Topic 1*

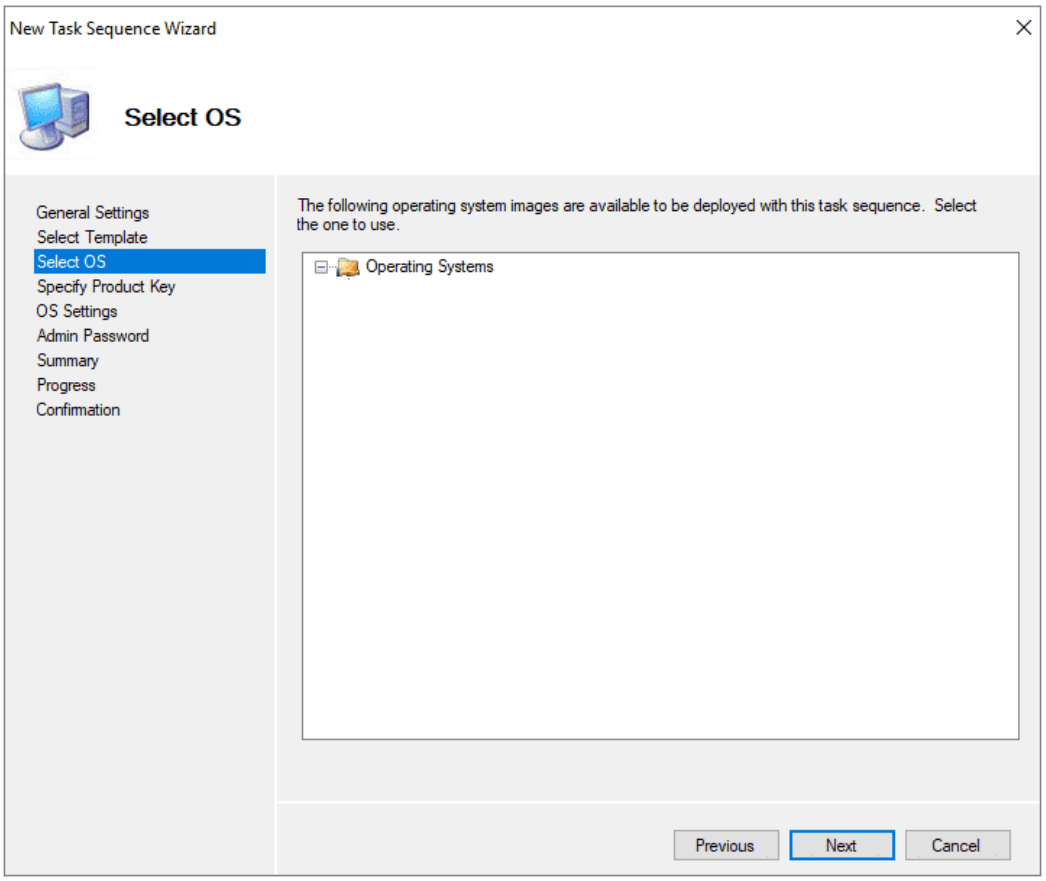
You have a Microsoft Deployment Toolkit (MDT) deployment share.

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: *B*

Community vote distribution

B (94%)

Krayzr Highly Voted 2 years, 9 months ago

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

marcomartinez Highly Voted 1 year, 10 months ago

MDT is being removed from the exam on Apr 26, 2024. This question is no longer relevant

upvoted 5 times

Jt909 2 years, 4 months ago

Upgrade with custom image can't be done. Only vanilla full source files

upvoted 3 times

MR_Eliot 2 years, 8 months ago

B is correct

upvoted 3 times

Anonymouse1312 2 years, 9 months ago

The keyword here is "perform a Windows 11 in-place upgrade" Cannot upgrade using custom images

upvoted 2 times

yosry 2 years, 11 months ago

B is the correct answer

upvoted 3 times

NoursBear 2 years, 11 months 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 3 years ago

- 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 3 years ago

Import custom image file, Although option B is Correct as Windows is not Open source it is not viable

upvoted 2 times

fco168 3 years ago

Agree with VirtualJP

upvoted 2 times

VirtualJP 3 years, 1 month ago

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 3 years, 2 months ago

indeed B to me.Thank you for your confidence, BUT can you back up your choice with documentation?

upvoted 1 times

Zelda78 3 years, 2 months ago

indeed B to me.

upvoted 1 times

[Removed] 3 years, 1 month ago

Thank you for your confidence, BUT can you back up your choice with documentation?

upvoted 1 times

Kiookr 3 years, 1 month ago

Thank you for your confidence, BUT can you back up your choice with documentation?

upvoted 1 times

Nozuka 3 years, 2 months ago

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

Question #81 *Topic 1*

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%)

Dinkan Most Recent 1 year, 2 months ago

Selected Answer: D

D. an app protection policy from the Microsoft Intune admin center

https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/manage-apps#protect-apps-on-organization-owned-and-personal-devices

upvoted 1 times

theptr 1 year, 4 months ago

Selected Answer: D

D targets the app

upvoted 1 times

ergacharsk 2 years, 4 months ago

Selected Answer: D

D is correct

upvoted 1 times

MR_Eliot 2 years, 8 months ago

Selected Answer: D

D is correct. done this many times

upvoted 1 times

Darkfire 2 years, 9 months 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 2 years, 9 months ago

Selected Answer: D

D. an app protection policy from the Microsoft Intune admin center

upvoted 1 times

Tonsku 2 years, 11 months ago

Selected Answer: D

D. an app protection policy from the Microsoft Intune admin center

upvoted 1 times

Nivla 3 years, 1 month 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 3 years, 2 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

Question #82 *Topic 1*

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: *D*

Community vote distribution



Dinkan Most Recent 1 year, 2 months ago

Selected Answer: D

D. an app configuration policy

Tested and confirmed in LAB

https://learn.microsoft.com/en-us/intune/intune-service/apps/apps-configure-chrome-android#add-app-configuration-for-managed-ae-devices

upvoted 1 times

edo1803 1 year, 11 months ago

Selected Answer: D

D is correct

upvoted 1 times

Pollosor 2 years, 4 months ago

Selected Answer: D

The answer is D because it is the most direct method, I suppose.

upvoted 1 times

MR_Eliot 2 years, 8 months ago

Selected Answer: D

D is correct.

upvoted 1 times

BigStan82 2 years, 8 months 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 2 years, 9 months 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 2 years, 9 months ago

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.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.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 3 times

Krayzr 2 years, 9 months 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 2 years, 9 months 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 2 years, 9 months 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.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 2 years, 9 months 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 2 years, 10 months 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 2 years, 10 months ago

Selected Answer: D

Is correct

upvoted 1 times

Tonsku 2 years, 11 months 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 2 years, 11 months ago

C. an app protection policy https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-androidmy mistake, D. an app configuration policy https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android

upvoted 2 times

Tonsku 2 years, 11 months ago

my mistake, D. an app configuration policy

https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android

upvoted 4 times

belyo 2 years, 11 months 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 2 years, 12 months ago

Selected Answer: D

Answer is D:

https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android

upvoted 1 times

chandravamsi 3 years ago

Selected Answer: D

Option : D

upvoted 1 times

fco168 3 years ago

Selected Answer: D

agree with VirtualJP

upvoted 1 times

LiamAzure 3 years ago

Selected Answer: D

Its android so app configuration

upvoted 1 times

4rk4n4 3 years, 1 month ago

Selected Answer: D

Answer is D.

upvoted 1 times

iamforksu 3 years, 1 month ago

Selected Answer: D

Answer is D

upvoted 1 times

VirtualJP 3 years, 1 month ago

Selected Answer: D

Here's why:

An app configuration policy is a better way to deliver bookmarks to the Chrome browser on Android devices than a configuration profile.

To deliver bookmarks to the Chrome browser on Android devices, you would create an app configuration policy that specifies the bookmarks that you want to be added to the browser. The policy would then be assigned to your managed devices. Once the policy is applied, the bookmarks will be added to Chrome automatically.

To deliver bookmarks using a configuration profile, you would need to create a file that contains the bookmark data. The file would then be pushed to your managed devices. Once the file is on the device, you would need to use a script to import the bookmarks into Chrome.

This process is more complex and time-consuming than using an app configuration policy. It also requires you to create and maintain a bookmark file, which can be cumbersome if you have a large number of bookmarks or if you need to frequently update them.

upvoted 3 times

ZaFletch 3 years, 1 month ago

Selected Answer: D

Plenty of links already in discussion, answer is D

upvoted 1 times

Rocky83 3 years, 1 month ago

Selected Answer: D

Should be D

upvoted 1 times

Gillactus 3 years, 2 months ago

Selected Answer: D

Answer is D App Config Policy.

https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android

upvoted 3 times

Nozuka Highly Voted 3 years, 2 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 18 times

Grg433 3 years, 2 months ago

Selected Answer: B

I think B is correct

A configuration profile in Microsoft Intune allows you to configure settings and features on enrolled devices, including configuring bookmarks in the Chrome browser. You can use this profile to define the bookmarks you want to push to the devices' Chrome browsers.

The other options (A, C, D) are used for different purposes and wouldn't be the appropriate choice for delivering bookmarks to the browser.

https://www.anoopcnair.com/configure-google-chrome-bookmarks-using-intune/

upvoted 1 times

sh123df 3 years, 2 months ago

Selected Answer: B

Answer is wrong.

Devices > Windows > Configuration profiles > Create profile.

Create a profile using Administrative templates: Computer Configuration > Google > Google Chrome

upvoted 4 times

sh123df 3 years ago

My this answer was wrong. Look away from this. Sorry.

upvoted 1 times

Kaasstengelss123 3 years, 1 month ago

the question is about android devices

upvoted 1 times

Question #83 *Topic 1*

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%)

Dinkan Most Recent 1 year, 2 months ago

Selected Answer: D

D. the Microsoft 365 Apps admin center

https://learn.microsoft.com/en-us/microsoft-365-apps/admin-center/overview-office-customization-tool

upvoted 1 times

06152f0 2 years, 3 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

06152f0 2 years, 3 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

Besxp 1 year, 5 months ago

 Correct Answer: D. Microsoft 365 Apps admin center

Why right? It has the Office Customization Tool (config.office.com), which creates the XML file used by ODT.

Why not wrong? This is the only tool made specifically for generating the config file for ODT.

 B. Microsoft Intune admin center

Why wrong? Intune is used to deploy and manage Office apps, but it does not generate the XML customization file.

Why it seems right sometimes? You can deploy Office using policies in Intune — but you still need to create the config file elsewhere (D) if using ODT.

upvoted 1 times

MR_Eliot 2 years, 8 months ago

Selected Answer: D

Correct.

upvoted 1 times

Darkfire 2 years, 9 months ago

Selected Answer: D

D is correct

https://learn.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options

upvoted 1 times

Mattia8 2 years, 10 months ago

D is the correct one

upvoted 1 times

Tonsku 2 years, 11 months ago

Selected Answer: D

D. the Microsoft 365 Apps admin center

upvoted 1 times

fco168 3 years 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 3 years, 1 month ago

Selected Answer: D

Given answer is correct.

https://config.office.com/

upvoted 3 times

picho707 3 years, 2 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

picho707 3 years, 2 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.the Microsoft Intune admin center can manage all devices including desktop devices however

upvoted 4 times

NoursBear 3 years ago

the Microsoft Intune admin center can manage all devices including desktop devices however

upvoted 1 times

Question #84 *Topic 1*

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: *A*

Community vote distribution

A (95%) (5%

Dinkan Most Recent 1 year, 2 months ago

Selected Answer: A

A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.

Before you can add a Win32 app to Microsoft Intune, you must prepare the app by using the Microsoft Win32 Content Prep Tool.

https://learn.microsoft.com/en-us/intune/intune-service/apps/apps-win32-prepare

upvoted 1 times

edo1803 1 year, 11 months 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 2 years, 4 months 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 2 years, 6 months 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 Intunereviewed 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 .intunewin format.had this one on the exam yesterday. I went with A. Still scored a 662, but obviously not sure if A was correct

upvoted 2 times

Michael_010 2 years, 6 months 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 2 years, 5 months 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 2 years, 6 months 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 .intunewin format.

upvoted 1 times

MR_Eliot 2 years, 8 months ago

Selected Answer: A

its A.

upvoted 1 times

BigStan82 2 years, 8 months 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 2 years, 9 months 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 2 years, 9 months ago

Selected Answer: C

C is correct Win32 app is not mentioned in the question. So it's an normal app.

upvoted 2 times

Darkfire 2 years, 9 months ago

C is correct Win32 app is not mentioned in the question. So it's an normal app.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 2 times

OyYaGotta 2 years, 8 months 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 2 years, 9 months 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 2 years, 9 months ago

Selected Answer: A

A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.

upvoted 2 times

Pugmohone 2 years, 9 months ago

Selected Answer: A

Multiple files. Must be A. Need to wrap all the files as an intunewin

upvoted 2 times

Tonsku 2 years, 11 months 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 2 years, 11 months 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 2 years, 11 months ago

It doesn't mention at all that we are deploying a legacy application; how did people get to that conclusion?

upvoted 1 times

ZaFletch 3 years, 1 month 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 3 years, 1 month 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

Rocky83 3 years, 1 month ago

Selected Answer: A

A of course

upvoted 1 times

Anonymous 3 years, 1 month ago

I think is "A"

upvoted 1 times

Nozuka Highly Voted 3 years, 2 months ago

Selected Answer: A

Should be A.

https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-prepare

upvoted 11 times

Grg433 3 years, 2 months ago

Selected Answer: A

please let me know if this is wrong.

To deploy an application that contains multiple installation files in Microsoft Intune, you should:

A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.

The Microsoft Win32 Content Prep Tool is used to package and prepare Win32 applications (legacy desktop applications) for deployment through Microsoft Intune. It helps you create the necessary installation files and metadata that Intune requires to distribute and install the application on Windows devices.

upvoted 3 times

HOTSPOT

-

You have groups that use the Dynamic Device membership type as shown in the following table.

You are deploying Microsoft 365 apps.

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

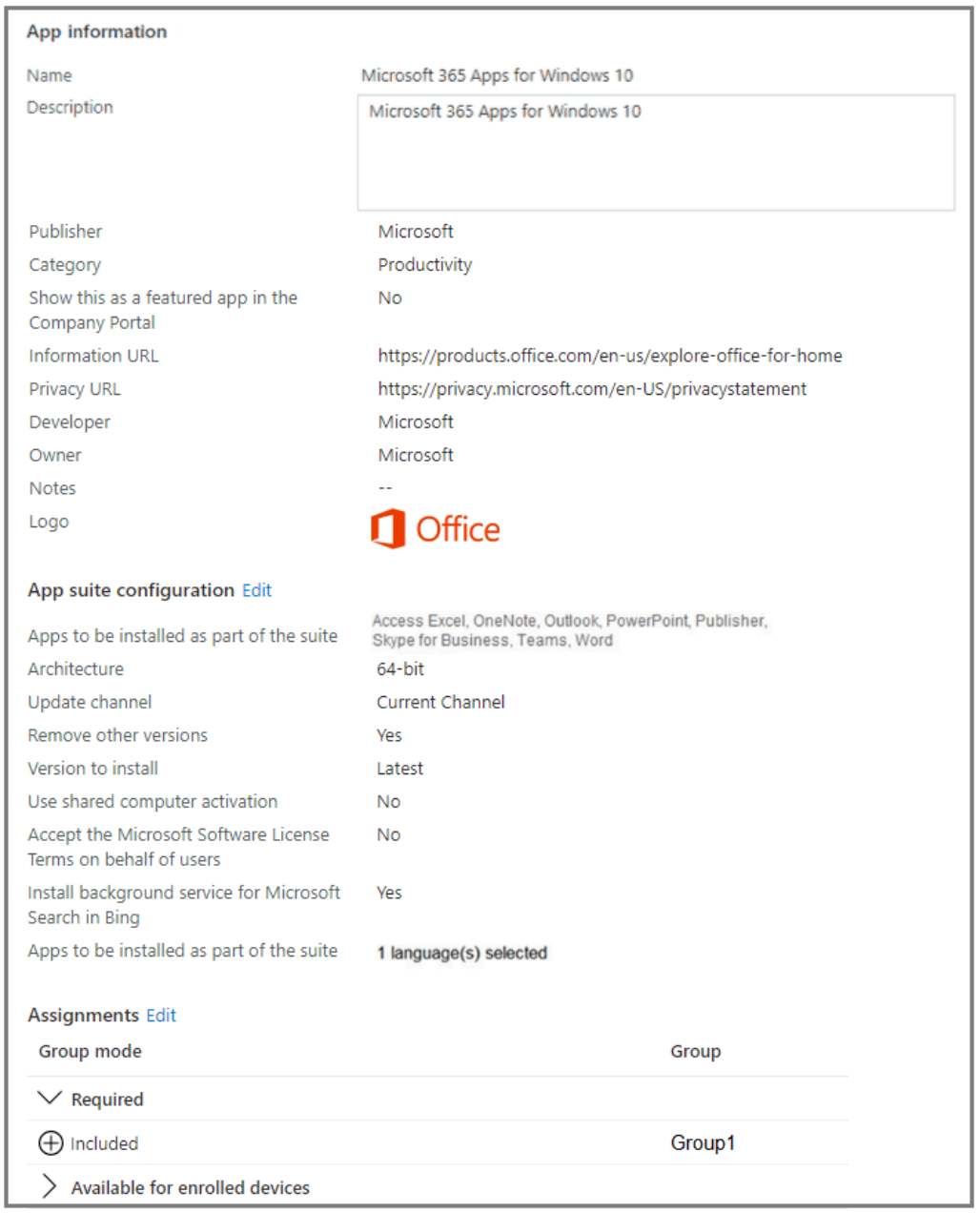
In the Microsoft Intune admin center, you create a Microsoft 365 Apps app as shown in the exhibit. (Click the Exhibit tab.)

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

NOTE: Each correct selection is worth one point.

Name	Syntax
Group1	(device.deviceOwnership -eq "Company")
Group2	(device.deviceOwnership -eq "Personal")

Name	Ownership	Platform
LT1	Company	Windows 10 Enterprise x64
LT2	Personal	Windows 10 Enterprise x64
LT3	Company	MacOS Big Sur



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	Office

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

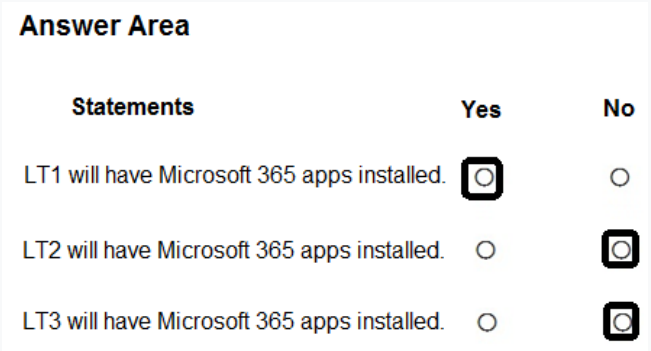
Assignments Edit

Group mode	Group
Required	
Included	Group1
Available for enrolled devices	

Answer Area

Statements	Yes	No
LT1 will have Microsoft 365 apps installed.	○	○
LT2 will have Microsoft 365 apps installed.	○	○
LT3 will have Microsoft 365 apps installed.	○	○

Suggested Answer:



BJS78 Highly Voted 3 years, 1 month 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 13 times

Cezt Most Recent 2 years, 3 months ago

YNN this portal only supports w10/11 and some wserver

upvoted 1 times

Haider_Raza 2 years, 8 months ago

Answer correct...

upvoted 1 times

MR_Eliot 2 years, 8 months ago

YNN.

for mac you will need to create another application.

upvoted 3 times

Darkfire 2 years, 9 months ago

Answer is correct.

upvoted 1 times

Tonsku 2 years, 11 months 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 3 times

benpatto 3 years 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 8 times

LiamAzure 3 years ago

Its correct, it will install only on Corporate Windows Devices

upvoted 1 times

Rocky83 3 years, 1 month ago

I think the answer is correct

upvoted 1 times

BJS78 Highly Voted 3 years, 1 month 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 13 times

Casticod 3 years, 1 month ago

I´m Agree

upvoted 1 times

Question #86 *Topic 1*

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: *D, E*

Community vote distribution



ThomasE 1 month ago

Selected Answer: DE

Custom device configuration profile: Windows Update for Business setting then Manage Preview Builds.

Update Rings

upvoted 1 times

7a9c653 7 months, 3 weeks ago

Selected Answer: DE

There is nothing related to Windows Insider on Device Restrictions.

upvoted 1 times

ModernoDecor 8 months, 2 weeks ago

Selected Answer: AE

Question is outdated.

Windows update rings: You can only enable "Enable pre-release builds" or leave it as not configured, but it doesn't block.

To disable: Configuration Profile > Settings Catalog > Manage preview builds > set to "Disable preview builds"

upvoted 3 times

fartphilosopher89 10 months, 2 weeks ago

Selected Answer: AE

A and E

upvoted 3 times

Dinkan 1 year, 1 month ago

Selected Answer: DE

D. a custom device configuration profile

E. a Windows 10 and later update ring

https://learn.microsoft.com/en-us/intune/intune-service/protect/windows-update-settings

https://learn.microsoft.com/en-us/intune/intune-service/protect/windows-update-settings#update-settings

upvoted 1 times

cd2cfde 1 year, 5 months ago

Selected Answer: DE

Originally thought it was A but I checked device restriction and there was no option there for this. So it is DE

upvoted 2 times

aj.davies01 1 year, 5 months ago

Selected Answer: AE

A + E is the most correct and recommended answer, as it:

Blocks user interaction with Insider settings (A)

Enforces update policies to prevent Insider builds (E)

Uses official and supported Intune methods

Requires less effort and is more maintainable than using custom profiles

upvoted 5 times

theptr 1 year, 7 months ago

Selected Answer: AE

A and E is correct

upvoted 2 times

MCI 1 year, 7 months ago

Selected Answer: AE

A. a device restrictions device configuration profile

E. a Windows 10 and later update ring

upvoted 2 times

b3c32d7 1 year, 8 months ago

Selected Answer: DE

DE are the only ways I can see in intune, in device restrictions there's no windows update options to select, but can in settings catalog, which is not an option here.

In custome device config you can use following

Name: Block Windows Insider Program

OMA-URI: ./Vendor/MSFT/Policy/Config/Update/AllowBuildPreview

Data type: Integer

Value: 0 (to disable)

upvoted 2 times

RJTW070 1 year, 9 months ago

Selected Answer: AE

This allows you to disable access to the Windows Insider settings in the Settings app, preventing users from enrolling in the program.

E. A Windows 10 and later update ring

In Intune, you can configure an update ring to control Windows Update settings, including preventing devices from receiving Windows Insider builds.

upvoted 2 times

458184c 1 year, 10 months 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 year, 11 months 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 3 times

ThomasE Most Recent 1 month ago

Looks like they've removed this option from the General section.

upvoted 1 times

1655b71 2 years 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 2 years, 2 months ago

Selected Answer: AE

A and E are correct

upvoted 1 times

Cezt 2 years, 3 months 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 2 years, 4 months ago

Selected Answer: AE

A : If you set Telemetery to required in Device Restrictions, they cannot get preview builds as it needs Optional Telemetery.

E: Use update ring to block preview builds.

Source:

I just implemented this last week.

upvoted 3 times

Prasis 2 years, 4 months 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 2 years, 8 months 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 4 times

MR_Eliot 2 years, 8 months ago

Selected Answer: DE

DE is correct.

upvoted 2 times

Krayzr 2 years, 9 months 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 2 years, 9 months ago

The 30 days represents an upgrade of Windows Version through a feature update not a standard feature update

upvoted 1 times

Merrybob 2 years, 9 months ago

Selected Answer: DE

DE

Ref: https://www.petervanderwoude.nl/post/managing-windows-insider-preview-builds-within-the-organization/

upvoted 1 times

Murad01 2 years, 9 months ago

I would go for A and D.

upvoted 1 times

frack 2 years, 10 months ago

Selected Answer: AE

custom is almost legacy as it requires OMA-URI, always the last resort

upvoted 1 times

Tonsku 2 years, 11 months ago

Selected Answer: AE

A. Create a device restrictions device configuration profile

E. Create a Windows 10 and later update ring

upvoted 2 times

yosry 2 years, 11 months ago

seems correct

upvoted 1 times

chandravamsi 3 years ago

Selected Answer: AC

Option A,C

upvoted 1 times

NoursBear 3 years ago

D can be used in two ways either with a custom setting and OMA-URI or using the settings catalog /Windows Update for Business/Manage Preview Builds. Nothing found under Device Restrictions

upvoted 1 times

ExamKiller020 Highly Voted 3 years, 1 month 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

upvoted 15 times

BJS78 3 years, 1 month ago

Device restriction: no windows update reference, so no Insider

App policy has no business here

Security baseline has no Insider setting

Custom profile: CSP/OMA-RUI for Update/ManagePreviewBuilds

Update ring: "Enable pre-release builds"

So, DE is correct

upvoted 3 times

picho707 3 years, 2 months ago

To prevent users from enrolling their devices in the Windows Insider Program using Microsoft Intune, you should perform the following two configurations from the Microsoft Intune admin center:

A. Create a device restrictions device configuration profile: This profile allows you to enforce restrictions and settings on Windows 10 devices. You can use this to prevent users from joining the Windows Insider Program.

E. Create a Windows 10 and later update ring: By configuring an update ring, you can control the release of Windows updates to devices. By setting the update ring to a stable release channel, you can prevent users from receiving Insider Preview builds, which are part of the Windows Insider Program.

upvoted 6 times

Grg433 Highly Voted 3 years, 2 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 9 times

Question #87 *Topic 1*

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



picho707 Highly Voted 3 years, 2 months ago

To create baseline metrics in Endpoint analytics, you should start by: C. Create a Log Analytics workspace. B. Onboard 10 devices to Endpoint analytics – Correct You must onboard at least 5–10 devices for Endpoint Analytics to start collecting data and generating baseline metrics. This is the required first step. A. Modify the Baseline regression threshold This is only possible after baseline metrics exist. You can't modify thresholds before any data is collected. C. Create a Log Analytics workspace This is not needed for Endpoint Analytics. It's only required for services like Azure Monitor or Update Compliance — not for creating baselines in Intune. D. Create an Azure Monitor workbook Used for custom dashboards and advanced reporting, but not required to start Endpoint Analytics or create baselines.

upvoted 16 times

picho707 Highly Voted 3 years, 2 months ago

To create baseline metrics in Endpoint analytics, you should start by:

C. Create a Log Analytics workspace.

upvoted 16 times

Dinkan Most Recent 1 year, 2 months ago

Selected Answer: B

Endpoint Analytics > Baseline page shows "You need at least 10 devices to create a baseline" in my lab

upvoted 1 times

theptr 1 year, 4 months ago

Selected Answer: B

Tested this, answer B seems correct

upvoted 1 times

JayHall 1 year, 11 months 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 definately satisfies this requirement

https://learn.microsoft.com/en-us/mem/analytics/enroll-intune#bkmk_onboard

upvoted 1 times

GyanPoudyal 2 years, 3 months 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

oopspruu 2 years, 4 months 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 13 times

GreenJPGSandRAM 2 years, 6 months ago

Selected Answer: C

You need a Log Analytics Workspace before you can start collecting information

upvoted 1 times

Rastova 2 years, 8 months 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

RazielLycas 2 years, 8 months 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

RomanV 2 years, 1 month 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 2 years, 9 months ago

Selected Answer: B

B. as there is definitely a minimum requirement for getting a baseline in endpoint analytics

upvoted 1 times

MR_Eliot 2 years, 8 months ago

c is the answers. you need log analtics workspace before you can collect the informaion. quesion also asls for what should you do first!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

MR_Eliot 2 years, 8 months ago

Selected Answer: C

c is the answers. you need log analtics workspace before you can collect the informaion. quesion also asls for what should you do first!

upvoted 1 times

Darkfire 2 years, 9 months 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 2 years, 10 months 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-us/mem/analytics/scores#:~:text=A%20status%20of%20insufficient%20data%20means%20you%20don%27t%20have%20enough%20devices%20reporting%20to%20provide%20a%20meaningful%20score.%20Currently%2C%20at%20least%20five%20devices%20are%20required.

upvoted 2 times

Tonsku 2 years, 11 months ago

Selected Answer: B

B. Onboard 10 devices to Endpoint analytics.

https://learn.microsoft.com/en-us/mem/analytics/scores

upvoted 1 times

frack 2 years, 10 months 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 2 years, 11 months ago

Selected Answer: B

B seems to correct

upvoted 1 times

GeekGizmo 2 years, 11 months 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

GeekGizmo 2 years, 11 months 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 CEndpoint 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

iTomi 2 years, 11 months 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 2 years, 11 months ago

B seems correct

upvoted 3 times

iTomi 2 years, 11 months ago

Selected Answer: B

B is right answer

https://learn.microsoft.com/en-us/mem/analytics/enroll-configmgr#bkmk_onboard

upvoted 1 times

iTomi 2 years, 11 months ago

B is right answer https://learn.microsoft.com/en-us/mem/analytics/enroll-configmgr#bkmk_onboardOnboarding 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

madsa 2 years, 11 months ago

Before enrolling you need to Create a Log Analytics workspace.

upvoted 2 times

NoursBear 3 years ago

This one is debatable and it's all in the question. Of course a Workspace needs to be created but here it's not enough to just have a workspace, to create the actual baseline you need 10 devices.

upvoted 1 times

siffy 2 years, 5 months ago

but what should you do first? historically in all ms exams log analytics workspace is always the first choice answer

upvoted 2 times

VirtualJP 3 years, 1 month ago

Selected Answer: B

I think answer is correct

upvoted 3 times

iTomi 2 years, 11 months 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.

https://learn.microsoft.com/en-us/mem/analytics/enroll-configmgr#bkmk_onboard

upvoted 1 times

Casticod 3 years, 1 month ago

Selected Answer: C

"Once you have more than 10 devices enrolled in to Endpoint Analytics you will be able to create new baselines."

C for Me

https://timmyit.com/2020/07/15/scheduled-creation-of-baselines-for-endpoint-analytics/

upvoted 2 times

cpaljchc4 3 years ago

The questions only mentioned 10 devices are enrolled to Intune, not Endpoint Analytics.

upvoted 1 times

cpaljchc4 3 years ago

100* Win 10 devices

upvoted 1 times

Rocky83 3 years, 1 month ago

Selected Answer: C

Before onboard devices you need to create the Log Analytics Workspace

upvoted 2 times

iTomi 2 years, 11 months ago

No, right answer is B.

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. https://learn.microsoft.com/en-us/mem/analytics/enroll-configmgr#bkmk_onboard

upvoted 1 times

ExamKiller020 3 years, 1 month ago

Just noticed in my own test tenant: 'You need at least 10 devices to create a baseline.'

upvoted 4 times

Casticod 3 years, 1 month ago

This is a prerequisite, therefore it must come first

upvoted 3 times

Anonymous 3 years, 1 month ago

I agree with Picho707... "C. Create a Log Analytics workspace.

upvoted 1 times

BJS78 3 years, 1 month ago

If the very first selection "Collect device data from" equals onboarding, then onboarding is the first step.

upvoted 1 times

Besxp 1 year, 5 months ago

 B. Onboard 10 devices to Endpoint analytics – Correct

You must onboard at least 5–10 devices for Endpoint Analytics to start collecting data and generating baseline metrics. This is the required first step.

 A. Modify the Baseline regression threshold

This is only possible after baseline metrics exist. You can't modify thresholds before any data is collected.

 C. Create a Log Analytics workspace

This is not needed for Endpoint Analytics. It's only required for services like Azure Monitor or Update Compliance — not for creating baselines in Intune.

 D. Create an Azure Monitor workbook

Used for custom dashboards and advanced reporting, but not required to start Endpoint Analytics or create baselines.

upvoted 1 times

Question #88 *Topic 1*

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%)

Dinkan Most Recent 1 year, 1 month ago

Selected Answer: B

B. 10 (Default is 10 days, can be chan ged to between 2 to 60days)

https://learn.microsoft.com/en-us/intune/intune-service/protect/windows-update-settings#update-settings:~:text=Set%20feature%20update%20uninstall%20period%20(2%20%E2%80%93%2060%20days)%20Default%3A%2010%20Windows%20Update%20CSP%3A

upvoted 1 times

oopspruu 2 years, 4 months 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 2 years, 8 months 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 2 times

Tonsku 2 years, 11 months 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 2 years, 11 months 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 2 years, 11 months 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 2 years, 12 months ago

Selected Answer: B

You have 10 days to roll back a feature update

upvoted 1 times

VirtualJP 3 years, 1 month 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

BJS78 3 years, 1 month ago

https://www.itechtics.com/rollback-windows-updates-after-10-days/

upvoted 2 times

Question #89 *Topic 1*

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: *A*

Community vote distribution



reastman66 Highly Voted 2 years, 11 months ago

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 2 years, 11 months ago

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

HueCumber Most Recent 7 months, 4 weeks ago

copilot says D

upvoted 1 times

reyrey 9 months ago

The Azure Monitor Agent is the current, recommended agent (replacing the legacy Log Analytics agent/MMA, which is deprecated) for collecting logs and metrics from Windows machines and sending them to a Log Analytics workspace.

upvoted 2 times

fartphilosopher89 10 months, 2 weeks ago

It is D

upvoted 1 times

henil_154762 1 year, 2 months ago

D. Install the Azure Monitor Agent To query events from a Windows 10 client in a Log Analytics workspace, the required step on the device is to install the Azure Monitor Agent (AMA). AMA sends Windows event logs to the workspace (via a Data Collection Rule). It does not require the PC to join Azure AD or a domain. Microsoft Learn +1 Options A/B/C don't achieve this: Join Azure AD — not required for Log Analytics ingestion. Configure Windows Defender Firewall — not the mechanism for log collection. Create an event subscription — that's Windows Event Forwarding, not Log Analytics.

upvoted 3 times

02dc19c 1 year, 7 months ago

The answer i s D: The Azure Monitor Agent works on both domain-joined and non-domain-joined devices (including workgroup computers). After installing the agent, you can configure it to send data to your Log Analytics workspace. Azure AD joining is not a prerequisite for using the agent or querying data from the workspace.

upvoted 2 times

RomanV 2 years, 1 month 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

RomanV 2 years, 1 month 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#prerequisitesThe Azure Monitor Agent works on both domain-joined and non-domain-joined devices (including workgroup computers). After installing the agent, you can configure it to send data to your Log Analytics workspace. Azure AD joining is not a prerequisite for using the agent or querying data from the workspace.Prerequisites for Azure Monitor Agent for Windows Clients demads the machine to be domain-joined to a Microsoft Entra tenant (joined or hybrid joined machines). https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client#prerequisites

upvoted 1 times

02dc19c 1 year, 7 months ago

The Azure Monitor Agent works on both domain-joined and non-domain-joined devices (including workgroup computers). After installing the agent, you can configure it to send data to your Log Analytics workspace. Azure AD joining is not a prerequisite for using the agent or querying data from the workspace.Prerequisites for Azure Monitor Agent for Windows Clients demads the machine to be domain-joined to a Microsoft Entra tenant (joined or hybrid joined machines). https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client#prerequisites

upvoted 1 times

02dc19c 1 year, 7 months ago

The Azure Monitor Agent works on both domain-joined and non-domain-joined devices (including workgroup computers). After installing the agent, you can configure it to send data to your Log Analytics workspace. Azure AD joining is not a prerequisite for using the agent or querying data from the workspace.

upvoted 1 times

Dinkan 1 year, 1 month ago

Prerequisites for Azure Monitor Agent for Windows Clients demads the machine to be domain-joined to a Microsoft Entra tenant (joined or hybrid joined machines). https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client#prerequisites

upvoted 2 times

Frank9020 2 years, 2 months ago

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 3 times

Prasis 2 years, 4 months 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 3 times

mark2525 2 years, 6 months ago

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 2 years, 8 months ago

D is must, A can be done later

upvoted 1 times

MR_Eliot 2 years, 8 months ago

A is correct. with the old agent joning the domain/ aad is not needed.

upvoted 1 times

BigStan82 2 years, 8 months ago

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 2 years, 9 months ago

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 2 years, 9 months ago

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 2 years, 9 months ago

I would choose answer D, install Azure monitor Agent

upvoted 2 times

Question #90 *Topic 1*

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: *A, E*

Community vote distribution

AE (91%) AB (9%)

Besxp Most Recent 1 year, 5 months ago

Selected Answer: AE

A. Create a device configuration profile – to control the OS version and restrict updates.

E. Enroll devices via Apple Business Manager – to enable supervision and enforce update policies.

B is wrong because enrolling iPads using the Intune Company Portal does not make them supervised, and only supervised devices can:

Receive iOS update policies from Intune.

Be prevented from manually installing newer iOS versions.

upvoted 2 times

1655b71 2 years 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 2 years, 4 months ago

A and E

https://learn.microsoft.com/en-us/mem/intune/protect/software-updates-ios

upvoted 1 times

MR_Eliot 2 years, 8 months ago

Selected Answer: AE

The answer is correct. However it sucks for users since they need to reset their device.

upvoted 1 times

Darkfire 2 years, 9 months ago

Selected Answer: AE

AE is correct

https://learn.microsoft.com/en-us/mem/intune/protect/software-updates-ios

upvoted 1 times

ckmay 2 years, 9 months ago

Config profiles sill 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.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 specifics 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

ckmay 2 years, 9 months ago

Selected Answer: AE

Config profiles sill 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 2 years, 9 months 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 specifics 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 2 years, 10 months ago

Correct

upvoted 1 times

Tonsku 2 years, 11 months 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 2 years, 11 months ago

AE seems correct

upvoted 2 times

fco168 3 years 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 3 years 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 3 years, 1 month 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 3 years, 1 month 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

Question #91 *Topic 1*

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 3 years, 1 month ago

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#uninstallThanks for the Microsoft link and clarification!Very much correct :)

upvoted 18 times

ExamKiller020 Highly Voted 3 years, 1 month 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 17 times

Dinkan Most Recent 1 year, 1 month ago

Selected Answer: B

B. As soon as the policy is received

When you use the Uninstall option, Intune passes the uninstall request to devices immediately.

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.

If the update removal requires a device restart, the device restarts without offering device users an option to delay.

https://learn.microsoft.com/en-us/intune/intune-service/protect/windows-10-update-rings#uninstall

upvoted 2 times

oopspruu 2 years, 4 months 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 2 years, 9 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%20immediately.

upvoted 1 times

Darkfire 2 years, 9 months ago

Very much correct :)

upvoted 1 times

kay000001 2 years, 12 months ago

Thanks for the Microsoft link and clarification!

upvoted 2 times

Question #92 *Topic 1*

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



VirtualJP Highly Voted 3 years, 1 month ago

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.That's it, you can look it up in Intune > Device Configuration Profiles > Administrative Templates > Turn off Local Group Policy Objects processing.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 13 times

VirtualJP Highly Voted 3 years, 1 month 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 12 times

Tom_y2k Most Recent 6 months ago

Selected Answer: C

The only Intune policy type that can override GPO is Administrative Templates.

upvoted 1 times

7a9c653 7 months, 3 weeks ago

Selected Answer: C

I go in C once in the custom we should configure individually all the policies one by one to the MDM wins.

upvoted 1 times

NakatomiTower 10 months, 3 weeks ago

Selected Answer: B

Another outdated question? The setting for this is MDM Wins Over GP. Which is found - Devices > Windows > Configuration profiles > Settings catalog > Control Policy Conflict > MDM Wins Over GP.

upvoted 3 times

ExamKiller020 3 years, 1 month ago

Given answer is correct. REF: https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict#mdmwinsovergptested in intune !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 11 times

ExamKiller020 3 years, 1 month 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

Besxp 1 year, 5 months ago

Selected Answer: B

 Why?

You must configure the MDMWinsOverGP setting (via Settings Catalog or custom OMA-URI) to let Intune take priority over Group Policy.

Administrative Templates (Option C) can't configure this setting.

GPO settings (Options A & D) only reinforce Group Policy, not fix the conflict.

upvoted 1 times

yoha1558 3 years ago

tested in intune !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

yoha1558 3 years ago

tested in intune !

upvoted 1 times

Knight_Of_Peace 1 year, 8 months ago

Selected Answer: B

Intune --> Devices --> Configuration --> Create New Policy --> Windows 10- and later --> Setting catalog --> Create --> Add settings --> search for (Control Policy Conflict) --> Tick (MDM Wins Over GP) --> Select (The MDM policy is used and the GP policy us blocked).

upvoted 3 times

sorinaccio 1 year, 9 months ago

Selected Answer: C

C. From the Microsoft Intune admin center, create an Administrative Templates device profile.

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 1 times

Seek12 1 year, 10 months ago

Selected Answer: A

GPO: Computer Configuration > Administrative Templates > Windows Components > MDM

> "MDM Policy Refresh" > "Enable MDM Wins Over GPO"

upvoted 1 times

59c6be3_111 1 year, 11 months ago

Agreed, just checked. It's not in the Administrative Templates, but it is available in the settings catalogue.

upvoted 1 times

1655b71 2 years 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 2 years, 3 months ago

currently found in settings catalog

upvoted 1 times

oopspruu 2 years, 4 months 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 2 years, 4 months 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

yhano 2 years 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

CJL324 2 years, 6 months 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

yhano 2 years 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.Agreed, just checked. It's not in the Administrative Templates, but it is available in the settings catalogue.

upvoted 2 times

MR_Eliot 2 years, 8 months ago

https://www.anoopcnair.com/mdm-wins-over-gpo-group-policy-intune-policy/

upvoted 1 times

Darkfire 2 years, 9 months ago

Selected Answer: B

B is correct

Sign in to the Microsoft Endpoint Manager admin center (Endpoint.Microsoft.coom)

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 policy from the list.

https://www.anoopcnair.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%20GPO%20Policy

upvoted 3 times

smart008 2 years, 9 months 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 2 years, 9 months ago

Selected Answer: B

B. From the Microsoft Intune admin center, create a custom device profile.

Ref: https://www.anoopcnair.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%20GPO%20Policy

upvoted 1 times

BJS78 2 years, 10 months 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 5 times

MR_Eliot 2 years, 8 months ago

Selected Answer: B

B is correct.

upvoted 2 times

CyberBuck_92 2 years, 11 months 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

MR_Eliot 2 years, 8 months ago

B is correct.https://www.anoopcnair.com/mdm-wins-over-gpo-group-policy-intune-policy/

upvoted 2 times

yosry 2 years, 11 months ago

Selected Answer: B

B seems correct

upvoted 2 times

chandravamsi 3 years ago

Selected Answer: B

Although B can do the same , A standard template is available in C

upvoted 1 times

Tr1v 3 years ago

Selected Answer: C

To ensure that the settings configured in Microsoft Intune take precedence, you can create an Administrative Templates device profile in the Microsoft Intune admin center. This allows you to configure the settings and policies for Windows 10 devices directly through Intune, ensuring that they override any conflicting Group Policy settings.

upvoted 1 times

benpatto 3 years ago

Admin templates > control policy conflict > MDM Wins over GP (The MDM policy is used and the GP policy is blocked)

upvoted 2 times

cpaljchc4 3 years ago

MDM Wins over GP is below Admin Templates, but it is not under the Admin templates tree though.

upvoted 1 times

MR_Eliot 2 years, 8 months 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

conartistique 3 years 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

smart008 2 years, 9 months 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

picho707 3 years, 2 months ago

To ensure that the settings configured in Microsoft Intune policies override the Group Policy settings for Windows 10 devices enrolled in Intune, you should do the following:

C. From the Microsoft Intune admin center, create an Administrative Templates device profile.

upvoted 2 times

Question #93 *Topic 1*

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: *D*

Community vote distribution

D (100%)

Besxp Most Recent 1 year, 5 months ago

Selected Answer: D

Why?

This policy enables Endpoint analytics, which collects and shows startup performance and other device health metrics in the Intune admin center.

It's the required setting to view startup times for managed Windows 11 devices.

 Why Not the Others?

A. Azure Monitor agent

➤ Used for log collection and Azure Monitor, not for Endpoint analytics in Intune.

B. Device compliance policy

➤ Used to assess device health and enforce access rules, not for performance data.

C. Conditional Access policy

➤ Controls access to apps and services based on conditions, unrelated to performance data.

upvoted 3 times

027ea51 2 years, 3 months 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 3 times

Cezt 2 years, 3 months ago

currently is called windows health monitoring policy -> endpoint analytics

upvoted 2 times

OyYaGotta 2 years, 8 months 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 data1. However, it doesn't directly monitor or display the startup performance of a device21.

upvoted 3 times

MR_Eliot 2 years, 8 months ago

Selected Answer: D

D is correct.

Keyword to look for: "for review in the Intune admin center".

upvoted 1 times

Krayzr 2 years, 9 months 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 2 years, 9 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-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 2 years, 11 months 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 2 years, 12 months 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 3 years ago

Option : A

upvoted 1 times

ExamKiller020 3 years, 1 month 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 3 years, 2 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 3 years, 2 months ago

Selected Answer: D

D. an Intune data collection policy

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.

The devices are the members of groups as shown in the following table.

You create an iOS/iPadOS update profile as shown in the following exhibit.

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

NOTE: Each correct selection is worth one point.

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

Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

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

Start day	Start time	End day	End time
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

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.	○	○
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	○	○
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	○	○

Suggested Answer:

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.	◉	○
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	○	◉
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	○	◉

picho707 2 years, 7 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.and for device 3 can not be enrolled in Sunday as policy finish S.aturday

upvoted 15 times

picho707 2 years, 7 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 15 times

MR_Eliot 2 years, 2 months ago

I agree with the answer.

Second device, does not recieve the policy because of exclusion group.

Third device, is not supervised, so you cannot control updates.

upvoted 3 times

Darkfire 2 years, 3 months 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 2 years, 4 months ago

can anyone explain why the answer 1 is yes please? why not update immediately on Tuesday?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)its because it can only install outside of the schedules time which is untill wednesday

upvoted 1 times

onepunchkenshin 2 years, 4 months ago

can anyone explain why the answer 1 is yes please? why not update immediately on Tuesday?

upvoted 1 times

ClaudiuR2023 2 years, 3 months 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)its because it can only install outside of the schedules time which is untill wednesday

upvoted 2 times

ClaudiuR2023 2 years, 3 months 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 2 times

Engr001 Most Recent 2 years, 2 months ago

its because it can only install outside of the schedules time which is untill wednesday

upvoted 2 times

Grg433 2 years, 8 months ago

can anyone please explain this : why second and third is No ?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).Agree +1

upvoted 2 times

Grg433 2 years, 8 months ago

can anyone please explain this : why second and third is No ?

upvoted 2 times

AdamRachel 2 years, 4 months ago

and for device 3 can not be enrolled in Sunday as policy finish S.aturday

upvoted 3 times

Fortind1974 Highly Voted 2 years, 8 months 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

Fortind1974 Highly Voted 2 years, 8 months 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).Agree +1

upvoted 18 times

Casticod 2 years, 7 months ago

Agree +1

upvoted 3 times

Question #95 *Topic 1*

You have a Microsoft Intune deployment that contains the resources shown in the following table.

You create a policy set named Set1 and add Comply1 to Set1.

Which additional resources can you add to Set1?

Name	Type	Platform
Comply1	Device compliance policy	Windows 10 and later
Comply2	Device compliance policy	iOS/iPadOS
CA1	Conditional Access policy	*Not applicable*
Conf1	Device configuration profile	Windows 10 and later
Office1	Office app policy	*Not applicable*

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 3 years, 2 months ago

C. Comply2 and Conf1 only https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets

upvoted 7 times

Merrybob Highly Voted 2 years, 9 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 5 times

7a9c653 Most Recent 7 months, 3 weeks ago

What can I use policy sets for? A policy set is an assignable collection of apps, policies, and other management objects you've created. Creating a policy set enables you to select many different objects at once, and assign them from a single place. As your organization changes, you can revisit a policy set to add or remove its objects and assignments. You can use policy sets to: Group objects that need to be assigned together Assign your organization's minimum configuration requirements on all managed devices Assign commonly used or relevant apps to all users What can be included in a policy set? Apps App configuration policies App protection policies Device configuration profiles Device compliance policies Windows autopilot deployment profiles Enrollment status page

upvoted 1 times

Dinkan 1 year, 1 month ago

C. Comply2 and Conf1 only https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/policy-sets

upvoted 1 times

GoombaLMAO 1 year, 9 months ago

You can add all types of policies and they can be cross platform, however. "Policy sets supports a subset of Intune App, Policy and Platform types. If an app or policy type is not available in the Policy Set picker experience, it is not officially supported." https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets

upvoted 1 times

Crille 2 years ago

it say additional resources is not conf1 include in comply1?

upvoted 1 times

matrixuser 2 years, 8 months 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 orignal 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

matrixuser 2 years, 8 months 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 orignal set 1 includes win10 and later already added . is it possible to create set with compliance policys of two different OS ? please comment .. thankyou :)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.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

Jaqueplakzaque 2 years, 5 months 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

oopspruu 2 years, 4 months 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

MR_Eliot 2 years, 8 months ago

After my own research in my test tenant, C is the answer.

upvoted 2 times

Darkfire 2 years, 9 months ago

C is correct https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets#:~:text=You%20can%20include,Settings%20catalog%20policies

upvoted 1 times

belyo 2 years, 11 months ago

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 2 years, 11 months ago

C - can't add CA1 or Office policies to sets according to MS Learn materials

upvoted 1 times

yosry 2 years, 11 months ago

C seems correct

upvoted 1 times

Question #96 *Topic 1*

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: *B*

Community vote distribution



2938b52 Most Recent 10 months, 2 weeks ago

Selected Answer: B

Microsoft's Security Baselines are pre-configured, recommended security settings for products like Windows and M365 Apps, providing a starting blueprint for admins, while the Microsoft Secure Score is a dynamic measurement TOOL in the Defender Portal that quantifies your overall security posture against these best practices, helping you track improvements & align with frameworks like NIST and CIS by reducing security gaps and vulnerabilities.

upvoted 2 times

Dinkan 1 year, 1 month ago

B. Microsoft Secure Score Most Voted https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-scoreThe wordings in the question will tempt you to think the answer should be Security baselines assessment, which is in Defender portal (SecureScore also is in Defender portal). But To Security Baseline Assessment feature, you'll require Microsoft Defender Vulnerability Management Standalone or if you're already a Microsoft Defender for Endpoint Plan 2 customer, the Defender Vulnerability Management add-on. As the question does not states whether the additional license is present, we assume the default as it is not preset. We also do not have the Secusity Baseline Assessment as an option in the question. I chose to select the best available option

upvoted 1 times

Dinkan 1 year, 1 month ago

Selected Answer: B

B. Microsoft Secure Score Most Voted

https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score

upvoted 1 times

Dinkan 1 year, 1 month ago

The wordings in the question will tempt you to think the answer should be Security baselines assessment, which is in Defender portal (SecureScore also is in Defender portal). But To Security Baseline Assessment feature, you'll require Microsoft Defender Vulnerability Management Standalone or if you're already a Microsoft Defender for Endpoint Plan 2 customer, the Defender Vulnerability Management add-on. As the question does not states whether the additional license is present, we assume the default as it is not preset. We also do not have the Secusity Baseline Assessment as an option in the question. I chose to select the best available option

upvoted 1 times

henil_154762 1 year, 2 months ago

Selected Answer: D

D. Microsoft 365 Defender portal

Use Threat & Vulnerability Management (TVM) → Security baselines assessment in the Microsoft 365 Defender portal to compare your devices' Defender configuration against Microsoft-recommended baselines and see the gaps/differences

upvoted 1 times

henil_154762 1 year, 2 months ago

Selected Answer: D

D. Microsoft 365 Defender portal

Use Threat & Vulnerability Management (TVM) → Security baselines assessment in the Microsoft 365 Defender portal to compare your devices' Defender configuration against Microsoft-recommended baselines and see the gaps/differences

upvoted 1 times

Dinkan 1 year, 1 month ago

To use Security Baseline Assessment feature, you'll require Microsoft Defender Vulnerability Management Standalone or if you're already a Microsoft Defender for Endpoint Plan 2 customer, the Defender Vulnerability Management add-on. The question does not states that we have the license. If you don't have the license, this option will not be visible in the portal

upvoted 1 times

d832958 1 year, 8 months ago

Selected Answer: B

The question is about what tool you use. The Microsoft 365 Defender portal is not a tool, secure score is a tool ;-) Its all in the question because Mickeyflop wants those.

upvoted 2 times

Pisces225 1 year, 12 months 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 years 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

1655b71 2 years 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.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

nsss 1 year, 11 months 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 2 years, 1 month 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 2 years, 4 months 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 2 years, 6 months 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 2 years, 6 months 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 2 years, 6 months 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 2 years, 8 months 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 2 years, 8 months ago

Selected Answer: B

B is correct.

upvoted 1 times

Darkfire 2 years, 9 months ago

I think B should be the answer as well. https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwideWhere does that article mention Security Baselines? Answer is D where you look to assess the custom security policies over Security Policies.

upvoted 2 times

Darkfire 2 years, 9 months 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 2 years, 8 months 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 2 years, 11 months ago

Selected Answer: B

B. Microsoft Secure Score

upvoted 2 times

chandravamsi 3 years ago

Selected Answer: B

Option B: Microsoft Secure score

upvoted 1 times

cpaljchc4 3 years ago

Secure score is stated in MD101 exam topics

https://www.examtopics.com/discussions/microsoft/view/65809-exam-md-101-topic-4-question-48-discussion/

upvoted 2 times

iamforksu 3 years, 1 month ago

Selected Answer: B

As other's stated.

upvoted 2 times

Fortind1974 3 years, 2 months ago

B. Microsoft Secure Score https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-scoreI 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

Fortind1974 3 years, 2 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 3 years, 1 month 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

Question #97 *Topic 1*

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



Dinkan Most Recent 1 year, 2 months ago

Selected Answer: B

B. Connectors and tokens

Intune Admin Center > Tenant Administration > Connectors & tokens > Cross platform > Microsoft Defender for Endpoint

upvoted 1 times

Moot2 1 year, 12 months ago

Selected Answer: B

is correct

upvoted 1 times

RomanV 2 years, 1 month 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 3 times

CJL324 2 years, 6 months 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 4 times

MR_Eliot 2 years, 8 months ago

Selected Answer: B

B is correct.

upvoted 1 times

Darkfire 2 years, 9 months ago

Selected Answer: B

B is correct

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

upvoted 2 times

Merrybob 2 years, 9 months ago

Selected Answer: B

B. Connectors and tokens

upvoted 2 times

Tonsku 2 years, 11 months ago

Selected Answer: B

B. Connectors and tokens

upvoted 3 times

HawkieEyes 3 years ago

Andrew is BSorry, Answer is B

upvoted 4 times

HawkieEyes 3 years ago

Selected Answer: B

Andrew is B

upvoted 4 times

HawkieEyes 3 years ago

Sorry, Answer is B

upvoted 3 times

cpaljchc4 3 years ago

MD101 has the same answer

https://www.examtopics.com/discussions/microsoft/view/98243-exam-md-101-topic-5-question-40-discussion/

upvoted 3 times

h38jhd38k 3 years 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 3 years, 1 month 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 3 years, 1 month ago

I go with B

upvoted 2 times

Question #98 *Topic 1*

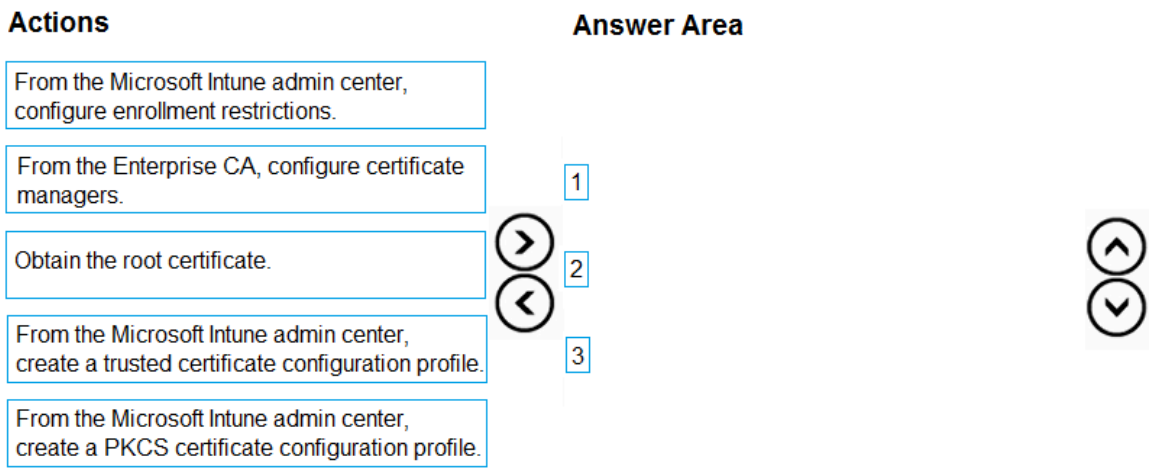
DRAG DROP

-

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.



Suggested Answer:

Answer Area

Obtain the root certificate.

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 3 years, 1 month 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-profileWhy the heck does it say Intune though????? Intune = MS Endpoint ManagerIf 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 8 times

Casticod Highly Voted 3 years, 1 month 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

reyrey Most Recent 9 months ago

this is the correct answer

Obtain the root certificate

From the Microsoft Intune admin center, create a trusted certificate configuration profile3From the Microsoft Intune admin center, create a PKCS certificate configuration profile

upvoted 1 times

1125BravadoGuy 2 years, 10 months ago

Why the heck does it say Intune though????? Intune = MS Endpoint ManagerIf 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 2 times

1125BravadoGuy 2 years, 10 months ago

Why the heck does it say Intune though???

upvoted 2 times

Moot2 1 year, 12 months ago

Answer correct - https://learn.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure

upvoted 2 times

oopspruu 2 years, 4 months 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 6 times

NoursBear 2 years, 10 months ago

?? Intune = MS Endpoint Manager

upvoted 1 times

Question #99 *Topic 1*

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

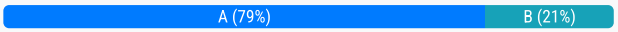
B. Device categories in Intune

C. Corporate device identifiers in Intune

D. Device settings in Azure AD

Suggested Answer: *A*

Community vote distribution



oopspruu Highly Voted 2 years, 3 months 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 12 times

Cezt 2 years, 3 months ago

Selected Answer: A

A is correct

upvoted 2 times

Prasis 2 years, 4 months 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 2 years, 6 months ago

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.thanks for the gpt answer bro

upvoted 2 times

CJL324 2 years, 6 months 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

8choxo Most Recent 1 year, 4 months ago

thanks for the gpt answer bro

upvoted 1 times

Darkfire 2 years, 9 months 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 2 years, 9 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

NoursBear 2 years, 11 months 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

NoursBear 2 years, 11 months 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 questionCorrect. 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.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 4 times

Tonsku 2 years, 11 months 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

ckmay 2 years, 9 months 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 2 years, 9 months 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 2 years, 9 months 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

Kiookr 3 years 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

HawkieEyes 3 years ago

Selected Answer: A

Answer is A

upvoted 3 times

Anonymous 3 years 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 3 years ago

Selected Answer: A

A - https://www.examtopics.com/discussions/microsoft/view/5327-exam-md-101-topic-3-question-4-discussion/

upvoted 3 times

cpaljchc4 3 years ago

Answer and discussion in MD101 goes with Dynamic groups

https://www.examtopics.com/discussions/microsoft/view/5327-exam-md-101-topic-3-question-4-discussion/

upvoted 3 times

NoursBear 3 years ago

I am with A, in a Dynamic Groups you use query expressions to group models etc...

upvoted 1 times

Mahi_444 3 years ago

Question is what should we configure first?!!Device categories didn't mention anything related to device version though. Whereas under the dynamic device group, there is a function of that

upvoted 1 times

Mahi_444 3 years ago

Selected Answer: B

Question is what should we configure first?!!

upvoted 1 times

fco168 3 years ago

Selected Answer: A

In dynamic groups you can query the devices by OS versions.

upvoted 1 times

cpaljchc4 3 years 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 3 years, 1 month 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

Rocky83 3 years, 1 month ago

Selected Answer: B

You must create the categories first and use them in the dynamic group.

upvoted 1 times

VirtualJP 3 years, 1 month ago

Selected Answer: B

B, because: Device categories allow you to group devices based on criteria such as device platform (e.g., Android, iOS) or other properties. By defining device categories for Android and iOS devices, you can apply policies selectively to each category based on the version of Android or iOS installed.

Not A, because: Groups with dynamic membership rules in Azure AD are used for creating Azure AD security groups with dynamic membership based on user or device attributes. While these can be used for targeting policies, they are more focused on user attributes and may not directly address the need to target based on device platform and version.

upvoted 2 times

picho707 3 years, 1 month ago

Selected Answer: B

Devices must be categorized first and then the devices can be grouped statically or dynamically.

upvoted 1 times

Casticod 3 years, 1 month ago

Selected Answer: A

To create Device category you also create a dynamic/s Group/s

I Think A as a correct response (but with doubts)

upvoted 1 times

ExamKiller020 3 years, 1 month ago

Selected Answer: A

Given answer is 100% correct.

Just tested in my own test tenant. You can create a dynamic rule based on 'DeviceOSVersion'. And groups can be assigned to a policy.

REF: https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#rules-for-devices

upvoted 3 times

Zelda78 3 years, 2 months ago

device categories are linked to a dynamic group, not directly to a policy. dynamic groups you can apply to a policy right? so A to me.

upvoted 3 times

Grg433 3 years, 2 months ago

Selected Answer: B

should be B no ?

Device categories in Intune allow you to group devices based on certain criteria.By creating device categories, we can target policies to specific groups of devices, including those running different versions of Android or iOS.

upvoted 1 times

Ferric 3 years, 1 month ago

I agree. This learn article describes configuring the Device Category first:

https://learn.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

upvoted 1 times

Question #100 *Topic 1*

DRAG DROP
-

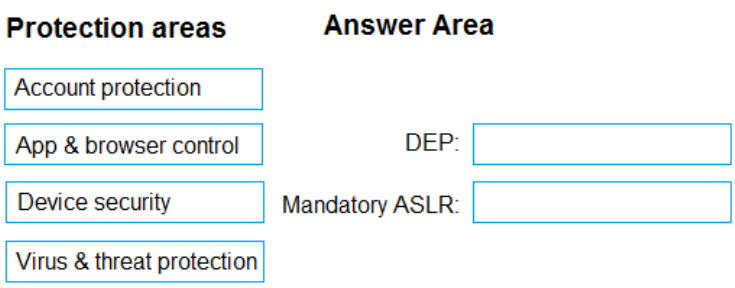
You have 500 Windows 10 devices enrolled in Microsoft Intune.

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)

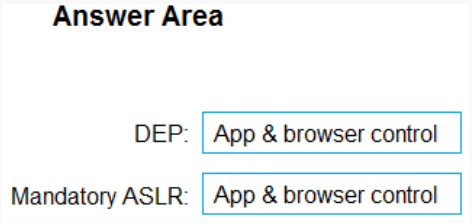
You need to configure a Windows 10 device that will be used to create a template file.

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.



Suggested Answer:



TestTaker09876 Highly Voted 2 years, 7 months ago
Congrats if you made it this far. Keep on Going!
upvoted 70 times

TestTaker09876 Highly Voted 2 years, 7 months ago
Congrats if you made it this far. Keep on Going!Everytime I go through all the questions from scratch and I get here I want to upvote again hahacorrecto
upvoted 75 times

1f85a58 2 years, 7 months ago
Everytime I go through all the questions from scratch and I get here I want to upvote again haha
upvoted 9 times

665d390 2 years, 2 months ago
correcto
upvoted 3 times

Dinkan Most Recent 1 year, 1 month ago
DEP: App & Browser Control Mandatory ASLR: App & Browser Control Tested and confirmed on Windows 11 (Windows Security app > App & browser control > Exploit protection)
upvoted 2 times

oopspruu 2 years, 4 months 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 2 years, 9 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

upvoted 4 times

reastman66 2 years, 12 months ago

App & Browser https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwideControl

upvoted 1 times

BJS78 3 years, 1 month 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 3 years, 2 months ago

Should be this no ? Virus & Threat Protection for DEP. App & Browser Control for Mandatory ASLR.

upvoted 1 times

Grg433 3 years, 2 months ago

Should be this no ? Virus & Threat Protection for DEP. App & Browser Control for Mandatory ASLR.sorry, I was wrong - answer is correct both can be found in - windows security > App & Browser Control

upvoted 1 times

Grg433 3 years, 1 month ago

sorry, I was wrong - answer is correct both can be found in - windows security > App & Browser Control

upvoted 8 times

Question #101 *Topic 1*

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



Dinkan Most Recent 1 year, 1 month ago

Selected Answer: D

D. the Settings app

Settings > Accounts > Access work or School > Connect > Join this device to Microsoft Entra ID

Reference: https://support.microsoft.com/en-us/account-billing/join-your-work-device-to-your-work-or-school-network-ef4d6adb-5095-4e51-829e-5457430f3973

upvoted 1 times

ergacharsk 2 years, 3 months 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 2 years, 9 months ago

Selected Answer: D

D is correct

Settings > System > About > Domain or Workgroup > Change > Select Member of, Domain.

upvoted 3 times

Merrybob 2 years, 9 months ago

Selected Answer: D

D. the Settings app

upvoted 2 times

belyo 2 years, 11 months 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 2 years, 12 months ago

Selected Answer: D

Question is in regard to Entra ID, so it is via Settings app

upvoted 1 times

Rocky83 3 years, 1 month ago

Selected Answer: D

Should be D

upvoted 2 times

firefox15 3 years, 1 month 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 3 years, 1 month 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 3 years, 1 month 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)

upvoted 1 times

majerzg 3 years, 1 month ago

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc788018(v=ws.11)Incorrect. This link pertains to windows server 2012, not windows 11 which is what the question is asking about.

upvoted 1 times

ckmay 2 years, 9 months ago

Incorrect. This link pertains to windows server 2012, not windows 11 which is what the question is asking about.

upvoted 1 times

Kiookr 3 years, 1 month 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

Anonymous 3 years, 1 month 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

Question #102 *Topic 1*

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%)

Dinkan Most Recent 1 year, 1 month ago

Selected Answer: A

A. Microsoft Authenticator

https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-mfa-number-match

upvoted 2 times

Merrybob 2 years, 3 months ago

Selected Answer: A

A. Microsoft Authenticator

upvoted 2 times

fco168 2 years, 6 months ago

Selected Answer: A

Microsoft Authenticator. Passwordless auth typing the number on your phone.

upvoted 1 times

picho707 2 years, 8 months 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

picho707 2 years, 8 months 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.but the authenticator popup comes usually only after user enters the password?

upvoted 3 times

Aji03 2 years, 4 months ago

but the authenticator popup comes usually only after user enters the password?

upvoted 1 times

Question #103 *Topic 1*

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



Emmanexam Most Recent 1 month, 2 weeks ago

Selected Answer: D

D. Configuration Profile

It clearly says you have a compliance policy already.

where do you enable the enhance jailbreak detection?

upvoted 1 times

HueCumber 7 months, 3 weeks ago

Selected Answer: A

Intune admin center → Devices → Device compliance → Compliance policy settings

upvoted 1 times

moluccanvibe 9 months, 2 weeks ago

Selected Answer: A

The device compliance policy defines what you check (e.g., block jailbroken devices).

The Compliance policy settings define how Intune performs certain advanced checks, including Enhanced jailbreak detection for iOS/iPadOS.

upvoted 2 times

2938b52 10 months, 2 weeks ago

Selected Answer: A

This is a tenant-wide setting that applies to all iOS devices with compliance policies targeting jailbroken devices, making the detection more frequent & thorough. In contrast, a device compliance policy is platform-specific & defines the rules devices must meet to be compliant.

Intune admin center > Navigate to Devices > Compliance policies > Compliance policy settings > Enable the setting for Enhanced jailbreak detection.

upvoted 2 times

NakatomiTower 10 months, 3 weeks ago

Selected Answer: B

Another outdated question

upvoted 1 times

Besxp 1 year, 5 months ago

Selected Answer: B

Stop commenting the wrong answer and do some research!

 So what's the correct answer now (current Intune)?

➡ B. the device compliance policy

 That's where you set jailbroken detection today (there is no separate enhanced detection toggle anymore).

 Why are some answers still A?

- Some people are answering based on older exam versions or older portal experience, where Enhanced jailbreak detection was in Compliance policy settings.

- In the past (before ~May 2023), Enhanced jailbreak detection was indeed configured in Compliance policy settings in Intune.

upvoted 4 times

02dc19c 1 year, 7 months ago

Selected Answer: A

it's not the device compliance policy itself where you enable Enhanced jailbreak detection. Instead, you configure it in the Compliance policy settings. This is a broader, tenant-wide setting in Microsoft Intune that enhances how compliance policies detect jailbroken devices

upvoted 4 times

02dc19c 1 year, 7 months ago

Selected Answer: A

The Compliance policy settings allow you to enable additional options like Enhanced jailbreak detection, which provides a more robust mechanism to identify jailbroken devices. O

upvoted 2 times

mhmyz 2 years, 2 months ago

Selected Answer: B

https://learn.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-create-ios

upvoted 1 times

Darkfire 2 years, 3 months 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%20you%E2%80%99ve%20integrated%20with%20Intune.

upvoted 1 times

NoursBear 2 years, 3 months ago

It would be A before May

upvoted 1 times

NoursBear 2 years, 3 months ago

It would be A before Mayhuh I already replied two months ago lolI checked an app protection policy for iOS and in the Conditional Launch blade, there is indeed a Jailbroken setting

upvoted 1 times

NoursBear 2 years, 3 months 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 2 years, 3 months ago

huh I already replied two months ago lol

upvoted 1 times

NoursBear 2 years, 6 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 2 years, 6 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: 'Bock'

upvoted 4 times

fco168 2 years, 6 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: 'Bock'

upvoted 4 times

BJS78 2 years, 6 months ago

It is about Enhanced detection, which was in the device compliance settings until May and then it was removed.

upvoted 1 times

ExamKiller020 Highly Voted 2 years, 7 months 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 9 times

Question #104 *Topic 1*

DRAG DROP
-

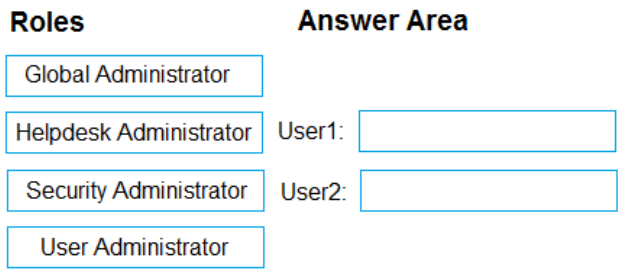
You have a Microsoft 365 subscription that contains two users named User1 and User2.

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.

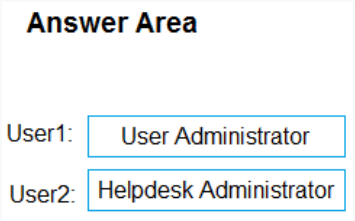
The solution must use the principle of least privilege.

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.



Suggested Answer:



Dinkan Most Recent 1 year, 1 month ago

User1 : User Administrator (https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#user-administrator)

User2 : Helpdesk Administrator (https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#helpdesk-administrator)

upvoted 1 times

Darkfire Highly Voted 2 years, 3 months 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 7 times

yosry 2 years, 4 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 2 years, 5 months 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 2 years, 6 months ago

User Administrator

Helpdesk Administrator

upvoted 2 times

JBV85 2 years, 7 months 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 January1, you enroll Windows 10 devices in Intune as shown in the following table.

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.

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group1

Answer Area

Statements	Yes	No
On January 7, Device1 is marked as compliant.	○	○
On January 8, Device1 is marked as compliant.	○	○
On January 8, Device2 is marked as compliant.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
On January 7, Device1 is marked as compliant.	○	◉
On January 8, Device1 is marked as compliant.	○	◉
On January 8, Device2 is marked as compliant.	◉	○

HawkieEyes Highly Voted 3 years ago

N - no firewall, policy 2 marks it non compliant immediately N - see above Y - will be set to not compliant on the 10thY,Y,Y! ➡ Device1: Matches Policy1 (Tag1) BitLocker: Enabled → meets requirement No noncompliance → still compliant ➡ No Policy2 applies → Device1 has no Tag2 Device1 is compliant → YES ➡ Same as above: Still meets Policy1 requirement (BitLocker enabled) No firewall requirement (Policy2 doesn't apply because no Tag2) Device1 is compliant → YES ➡ Device2: Matches Policy2 (Tag2) Firewall: On → meets Policy2 requirement Policy1 doesn't apply (no Tag1) Device2 is compliant → YES Many commenters assumed: Both policies apply to both devices (ignores scope tags). Device1 fails because its firewall is off (but no applicable policy requires firewall). Device2 fails because BitLocker is disabled (but no applicable policy requires BitLocker).

upvoted 26 times

HawkieEyes Highly Voted 3 years ago

N - no firewall, policy 2 marks it non compliant immediately N - see above Y - will be set to not compliant on the 10th

upvoted 26 times

HelloItsSam Most Recent 4 weeks ago

Answers are correct!

Both devices belong to Group1, so both devices receive both rules:

- Policy1: BitLocker must be enabled. If it isn't, allow 5 days to fix it.

- Policy2: Firewall must be enabled. If it isn't, mark the device noncompliant immediately.

upvoted 2 times

Oekoe 12 months ago

Scope tags have no impact.

NO Policy2 marks the device as non compliant immediately (Firewall Off -> fails Policy2 immediately)

NO Still not compliant and never will be (Still failing Firewall requirement)

NO Is in grace period ("In grace period" is not the same as "marked as compliant")

upvoted 2 times

mhmyz 2 years, 8 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 15 times

mhmyz 2 years, 8 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-policyOn January 5, you assign Policy1 and Policy2 to Group1 Scope tags doesn't override group assignmentsOn January 5, you assign Policy1 and Policy2 to Group1Assignment of Groups is how these are assigned...Scope tags mean nothing in this case.Policy Assignment for Device1: Policy1 applies (because it is assigned to Group1 and has Scope Tag1). Policy2 does NOT apply (Device1 does not have Scope Tag2). Policy1 requires BitLocker enabled → Device1 meets this requirement □. Policy1 does not enforce firewall settings (so, the firewall being off does not make it noncompliant). Policy1 marks a device noncompliant after 5 days of noncompliance, but Device1 is already compliant. ➡ Device1 remains compliant throughout. On January 7, Device1 is marked as compliant? □ Yes On January 8, Device1 is marked as compliant? □ YesDevice2: BitLocker is disabled □ (Fails Policy1 requirement) Firewall is on □ (Meets Policy2 requirement) Scope Tag: Tag2 (Matches Policy2, but not Policy1) Group Membership: Group2 Policy Assignment for Device2: Policy1 does NOT apply (not in Group1 or Scope Tag1). Policy2 does NOT apply (only assigned to Group1, but Device2 is in Group2). Since no compliance policy is assigned to Device2, and the setting "Mark devices with no compliance policy assigned as: Compliant" is enabled, Device2 is automatically considered compliant. ➡ On January 9, Device2 is marked as compliant? □ Yes

upvoted 15 times

Oekoe 12 months ago

Please ignore my comment.

Grace period is the same as the compliant.

Tag is what the device sees.

YYY

upvoted 2 times

Dinkan 1 year, 1 month ago

Scope Tags are used for RBAC. Only an admin with both these tags assigned (or Intune administrator role) can assign a Tag1 policy to Tag2 device. But once applied, they will just work, hence we don't haver to consider about them when evaluating the policies. Just ignore them.

upvoted 2 times

nickdb70 1 year, 4 months ago

Correct, scope tags have no impact to the answers in this question - "Scope tags are used to restrict what Intune admins can see and manage"

upvoted 1 times

jzmirus2 1 year, 9 months ago

Policy Assignment for Device1: Policy1 applies (because it is assigned to Group1 and has Scope Tag1). Policy2 does NOT apply (Device1 does not have Scope Tag2). Policy1 requires BitLocker enabled → Device1 meets this requirement □. Policy1 does not enforce firewall settings (so, the firewall being off does not make it noncompliant). Policy1 marks a device noncompliant after 5 days of noncompliance, but Device1 is already compliant. ➡ Device1 remains compliant throughout. On January 7, Device1 is marked as compliant? □ Yes On January 8, Device1 is marked as compliant? □ YesDevice2: BitLocker is disabled □ (Fails Policy1 requirement) Firewall is on □ (Meets Policy2 requirement) Scope Tag: Tag2 (Matches Policy2, but not Policy1) Group Membership: Group2 Policy Assignment for Device2: Policy1 does NOT apply (not in Group1 or Scope Tag1). Policy2 does NOT apply (only assigned to Group1, but Device2 is in Group2). Since no compliance policy is assigned to Device2, and the setting "Mark devices with no compliance policy assigned as: Compliant" is enabled, Device2 is automatically considered compliant. ➡ On January 9, Device2 is marked as compliant? □ Yes

upvoted 3 times

jzmirus2 1 year, 9 months ago

Policy Assignment for Device1: Policy1 applies (because it is assigned to Group1 and has Scope Tag1). Policy2 does NOT apply (Device1 does not have Scope Tag2). Policy1 requires BitLocker enabled → Device1 meets this requirement □. Policy1 does not enforce firewall settings (so, the firewall being off does not make it noncompliant). Policy1 marks a device noncompliant after 5 days of noncompliance, but Device1 is already compliant. ➡ Device1 remains compliant throughout.

On January 7, Device1 is marked as compliant? □ Yes On January 8, Device1 is marked as compliant? □ Yes

upvoted 3 times

02dc19c 1 year, 7 months ago

the answers are YYY: Scope tags act as a filter, ensuring that only devices with the designated tags are impacted by the policy. This provides a way to refine and control the assignment of policies within broader groups.

This means that Device 1 is only subject to the first policy and is compliant immediately regardless of grace period, and Device 2 is only subject to the 2nd policy and again, is compliant immediately. Hence, YYY

upvoted 2 times

batang_aratan 1 year, 8 months ago

Answers are correct

No - because the firewall rule applies immediately

No - for the same reason, firewall rule

Yes - because although BitLocker is disabled on Device 2, Policy1 hasn't kicked in yet. On January 10, Device 2 will be non-compliant.

upvoted 3 times

Oekoe 12 months ago

Scope tags have no impact.

NO Policy2 marks the device as non compliant immediately (Firewall Off -> fails Policy2 immediately) NO Still not compliant and never will be (Still failing Firewall requirement) NO Is in grace period ("In grace period" is not the same as "marked as compliant")

upvoted 1 times

JayHall 1 year, 9 months ago

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) - Although firewall is off, Device 2 IS compliant on Jan 8th but it will go into non-compliant statis on Jan 10th (due to firewall being off, 5 days after non-compliance)

upvoted 5 times

AleFCI1908 2 years 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 3 times

Faceless_Void 2 years, 3 months 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

PXAbstraction 1 year, 4 months ago

There is a lot of debate on this, but I've just spent a half hours reading up on it and am confident in saying that scope tags do NOT have any impacts on how policies are applied to devices, only what users can view them for administrator. Which means that the given answers are in fact correct.

upvoted 2 times

PXAbstraction 1 year, 4 months ago

There is a lot of debate on this, but I've just spent a half hours reading up on it and am confident in saying that scope tags do NOT have any impacts on how policies are applied to devices, only what users can view them for administrator. Which means that the given answers are in fact correct.Correct, scope tags have no impact to the answers in this question - "Scope tags are used to restrict what Intune admins can see and manage"

upvoted 2 times

ergacharsk 2 years, 3 months ago

According to the Chat GPT correct answer is Y,Y,Y

upvoted 1 times

oopspruu 2 years, 4 months 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

moluccanvibe 9 months, 2 weeks ago

On January 5, you assign Policy1 and Policy2 to Group1

Scope tags doesn't override group assignments

upvoted 1 times

jzmirus2 1 year, 9 months ago

Device2:

BitLocker is disabled □ (Fails Policy1 requirement)

Firewall is on □ (Meets Policy2 requirement)

Scope Tag: Tag2 (Matches Policy2, but not Policy1)

Group Membership: Group2

Policy Assignment for Device2:

Policy1 does NOT apply (not in Group1 or Scope Tag1).

Policy2 does NOT apply (only assigned to Group1, but Device2 is in Group2).

Since no compliance policy is assigned to Device2, and the setting "Mark devices with no compliance policy assigned as: Compliant" is enabled, Device2 is automatically considered compliant.

➡ On January 9, Device2 is marked as compliant? □ Yes

upvoted 2 times

2c57d1c 2 years, 5 months ago

Assignment of Groups is how these are assigned...Scope tags mean nothing in this case.

upvoted 4 times

Irism 2 years, 6 months ago

On January 5, you assign Policy1 and Policy2 to Group1

upvoted 1 times

MR_Eliot 2 years, 8 months ago

NNY for sure.

upvoted 4 times

Darkfire 2 years, 9 months ago

I think NNN

Because both policies will mark devices as non-compliant. Eventhough some variables pass the criteria.

upvoted 2 times

Manojkl1206 2 years, 11 months 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 2 times

Manojkl1206 2 years, 11 months 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 NDevice 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.But it will not be marked "compliant", it will have "evaluating" or something like that till 10th.

upvoted 2 times

AdamRachel 2 years, 10 months 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.But it will not be marked "compliant", it will have "evaluating" or something like that till 10th.

upvoted 2 times

AdamRachel 2 years, 10 months 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

ZaFletch 3 years 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. NNYCorrect, but it says "On January 5, you assign Policy1 and Policy2 to Group1."

upvoted 5 times

ZaFletch 3 years 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 5 times

Krayzr 2 years, 9 months ago

But it will not be marked "compliant", it will have "evaluating" or something like that till 10th.

upvoted 2 times

RabbitB 3 years, 1 month 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

Besxp 1 year, 5 months ago

Y,Y,Y!

➡ Device1:

Matches Policy1 (Tag1)

BitLocker: Enabled → meets requirement

No noncompliance → still compliant

➡ No Policy2 applies → Device1 has no Tag2

 Device1 is compliant → YES

➡ Same as above:

Still meets Policy1 requirement (BitLocker enabled)

No firewall requirement (Policy2 doesn't apply because no Tag2)

 Device1 is compliant → YES

➡ Device2:

Matches Policy2 (Tag2)

Firewall: On → meets Policy2 requirement

Policy1 doesn't apply (no Tag1)

 Device2 is compliant → YES

Many commenters assumed:

 Both policies apply to both devices (ignores scope tags).

 Device1 fails because its firewall is off (but no applicable policy requires firewall).

 Device2 fails because BitLocker is disabled (but no applicable policy requires BitLocker).

upvoted 7 times

RabbitB 3 years ago

Mistake, YYY

upvoted 1 times

RabbitB 3 years ago

Mistake, YYYWho you?

upvoted 1 times

Tr1v 3 years ago

Correct, but it says "On January 5, you assign Policy1 and Policy2 to Group1."

upvoted 1 times

RabbitB 3 years, 1 month 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 2 years, 11 months 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

ubiquituz 2 years, 10 months ago

Who you?

upvoted 1 times

iamforksu 3 years, 1 month ago

NNY for the win

upvoted 1 times

reapernam 3 years, 1 month 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 3 years, 1 month 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 5 times

iTomi 2 years, 11 months 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 3 years, 1 month ago

Just remember: Scope (Tags) are used to determine which objects admins can see.

N,N,Y

upvoted 2 times

cserra 3 years, 1 month ago

I think the answer is YYY

Initialy, 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 dont 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 3 times

BJS78 3 years, 1 month ago

Tag is for RBAC. No relevance in configuration implementation.

upvoted 4 times

Grg433 3 years, 2 months ago

can someone please explaing why N,N,Y ?

upvoted 2 times

Fortind1974 3 years, 2 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

Question #106 *Topic 1*

HOTSPOT -

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have computers that run Windows 11 as shown in the following table.

You have the groups shown in the following table.

You create and assign the compliance policies shown in the following table.

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.

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

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

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

Answer Area

Statements	Yes	No
The compliance status of Computer1 is in grace period.	○	○
The compliance status of Computer2 is Compliant.	○	○
The compliance status of Computer3 is Not compliant.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
The compliance status of Computer1 is in grace period.	○	○
The compliance status of Computer2 is Compliant.	○	○
The compliance status of Computer3 is Not compliant.	○	○

MR_Eliot 2 years, 8 months 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 7 times

7a9c653 Most Recent 7 months, 3 weeks ago

Once the device 3 is not communicating with Intune, it will report not compliant by Default Device Compliance Policy > Is active. For me all the answers are correct.

upvoted 1 times

ModernoDecor 8 months, 2 weeks ago

YYN.

A device that is registered (Entra ID Registered) but not enrolled in Intune cannot receive a "complete" policy. So, it will not be either "Compliant" or "Not compliant"

upvoted 1 times

NoursBear 3 years 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 6 times

Dinkan 1 year, 1 month ago

Y

Y

N

upvoted 1 times

MR_Eliot 2 years, 8 months 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.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 7 times

e6d6bf4 1 year, 6 months ago

You are correct. The compliance policy from Intune needs the device to be enrolled so Intune can evaluate the compliancy. Since Computer 3 does not have a record on Intune, Intune will not mark the device noncompliant or compliant whatsover. The question statement said " it will be marked noncomplaint" --> Not true > No

upvoted 2 times

nickdb70 1 year, 4 months ago

Also from ChatGPT - "No, a device that is not enrolled in Intune cannot be marked as Compliant or Noncompliant."

upvoted 1 times

nickdb70 1 year, 4 months ago

YYN

For the third option, an unenrolled device can never be considered compliant, here's what ChatGPT says - "No — if a device is not enrolled in Intune, it cannot be considered compliant, regardless of whether a compliance policy is assigned or not."

upvoted 1 times

386abb2 1 year, 9 months ago

I would say YYY the last question is tricky as it says not compliant

upvoted 1 times

Doug77 1 year, 9 months ago

Answers are correct folks, this is why....first two we agree on, third is stated as not compliant, answering no= compliant for the default settings of devices not enrolled in intune with no device compliance policy applied. So....actually these are correct.

upvoted 1 times

ronniefactor 1 year, 10 months ago

YYY

- comp1-compliant -grace period,

-comp2 - compliant-FW enabled and Bit locker enabled

Comp3-not compliant, not entra joined and FW is disabled

upvoted 1 times

Stu5mmy 2 years, 4 months ago

This a tricky question when it comes to the evaluation of device 2. There's 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 2 years, 6 months ago

resposta correta

upvoted 2 times

MR_Eliot Highly Voted 2 years, 8 months 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 17 times

Bukaj 2 years, 10 months 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 2 years, 11 months 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

mks_academy 2 years, 11 months 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.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.But device 3 is not enrolled to Intune so Policy not apply so will leave device as compliant.computer 3 is not enrolled on Intune.it is registered.

upvoted 4 times

AdamRachel 2 years, 10 months ago

But device 3 is not enrolled to Intune so Policy not apply so will leave device as compliant.

upvoted 1 times

AdamRachel 2 years, 10 months 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

riccardo1999 2 years, 10 months ago

computer 3 is not enrolled on Intune.

upvoted 2 times

riccardo1999 2 years, 10 months ago

computer 3 is not enrolled on Intune.it is registered.

upvoted 2 times

frack 2 years, 10 months ago

it is registered.

upvoted 1 times

madsa 2 years, 11 months ago

amckinson_Android_10/16/2023_4:38 PM

Intune

Personal

Noncompliant

Android (device administrator)

9.0

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

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 3 years 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 7 times

madsa 2 years, 11 months 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

e6d6bf4 1 year, 6 months ago

You are correct. The compliance policy from Intune needs the device to be enrolled so Intune can evaluate the compliancy. Since Computer 3 does not have a record on Intune, Intune will not mark the device noncompliant or compliant whatsover. The question statement said " it will be marked noncomplaint" --> Not true > No

upvoted 3 times

Casticod 3 years, 1 month 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

Casticod 3 years, 1 month 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 questionIt clearly says its registered (computer3) Compliance policy applies on all registered, hybrid, enrolled devices.It can belong a group if it in AAD. But it cannot be compliant or not compliant if it is not in Intune.

upvoted 2 times

CheMetto 1 year, 5 months ago

That's the correct explanation! If you don't have a device in intune, how can you see it inside intune? It's like: I don't have a device into AD. The last time a user logged in was yesterday. On AD, would i see the device last logged in time to yesterday? Of course, not! You don't have AD, how can you? It's No the last one.

upvoted 1 times

benpatto 3 years 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 4 times

Sonia33 2 years, 11 months 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

Contactfornitish 3 years, 1 month ago

It clearly says its registered (computer3)

Compliance policy applies on all registered, hybrid, enrolled devices.

upvoted 2 times

BJS78 3 years, 1 month 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 3 years, 2 months ago

No

Yes

Yes

Looks like is wrong, correct me.

upvoted 2 times

sh123df 3 years ago

My answer is wrong. Look away from this

upvoted 3 times

LiamAzure 3 years ago

Why No for the first one? This is after 1 day, it has 10 days

upvoted 1 times

majerzg 3 years, 1 month ago

I think that you are right.

upvoted 1 times

Grg433 3 years, 2 months ago

should be Y,Y,Y ? no ?

upvoted 4 times

SdovlA Highly Voted 3 years, 2 months ago

The third device is just registered in AAD. The status is N/A.

upvoted 8 times

ExamBud 1 year, 9 months ago

It doesn't mind if it is registered. It is NA because it is not enrolled in Intune.

upvoted 1 times

frack 2 years, 10 months ago

table indicate Device3 as registered

upvoted 1 times

Question #107 *Topic 1*

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

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

Your 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%)

Darkfire Most Recent 2 years, 3 months 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 2 years, 3 months ago

Selected Answer: B

B. No

Should be configured as a Windows Hello for Business policy.

upvoted 1 times

ExamKiller020 Highly Voted 2 years, 7 months ago

Selected Answer: B

Devices > Enroll devices > Windows enrollment > Windows Hello for Business in Intune and configure a desired policy.

upvoted 12 times

Question #108 *Topic 1*

You have a Microsoft 365 tenant that contains the objects shown in the following table.

You are creating a compliance policy named Compliance1.

Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Main-enabled security group
Group4	Security group

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 2 years, 8 months 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 9 times

OyYaGotta Highly Voted 2 years, 8 months ago

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.thanks for clarification

upvoted 9 times

ergacharsk 2 years, 3 months ago

thanks for clarification

upvoted 2 times

MR_Eliot 2 years, 8 months ago

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 6 times

Dinkan 1 year, 2 months ago

C. Group1, Group2, and Group3 only Tested and confirmed in Lab

upvoted 1 times

Tr619899 1 year, 11 months ago

C is Correct

upvoted 1 times

Cezt 2 years, 3 months ago

it can not be sent to users, nor security groups

upvoted 1 times

Darkfire 2 years, 9 months ago

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 2 times

NoursBear 3 years 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 3 years, 1 month ago

This question looks like question 158.sry Question 156

upvoted 1 times

brunolopes01 3 years, 1 month ago

This question looks like question 158.

upvoted 1 times

brunolopes01 3 years, 1 month ago

sry Question 156

upvoted 1 times

Rocky83 3 years, 1 month ago

C is correct

upvoted 1 times

ExamKiller020 3 years, 1 month ago

Given answer is correct. Tested in my own tenant. You can only select groups with email adresses

upvoted 1 times

SdovlA 3 years, 2 months ago

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 3 years, 2 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.Nope, tested it. You can add only groups (groups with e-mail addresses)

upvoted 2 times

picho707 3 years, 2 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 3 years, 1 month ago

Nope, tested it. You can add only groups (groups with e-mail addresses)

upvoted 2 times

Grg433 3 years, 2 months ago

Is this C option even correct ?Yes, tested in lab

upvoted 2 times

Grg433 3 years, 2 months ago

Is this C option even correct ?

upvoted 2 times

Dinkan Most Recent 1 year, 2 months ago

Yes, tested in lab

upvoted 1 times

Question #109 *Topic 1*

HOTSPOT -

You have an Azure AD tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of .

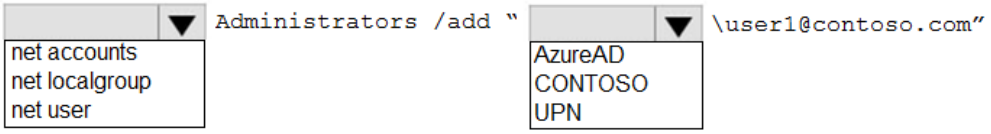
You join a Windows 11 device named Client1 to contoso.com.

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.

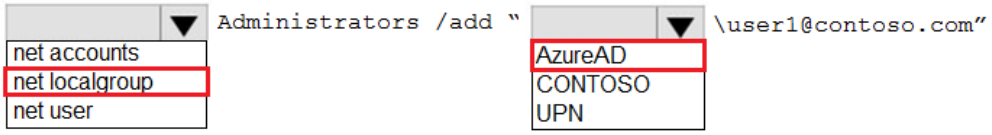
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



Dinkan Most Recent 1 year, 2 months ago

net localgroup administrators /add "AzureAD\UserUpn

Ref: https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin#manually-elevate-a-user-on-a-device

upvoted 1 times

AleFCI1908 2 years ago

net localgroup administrators /add "AzureAD\

upvoted 3 times

MR_Eliot 2 years, 8 months ago

Net localgroup

AzureAD

upvoted 5 times

Darkfire 2 years, 9 months ago

net localgroup administrators /add "AzureAD\"

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

AleFCI1908 2 years ago

net localgroup administrators /add "AzureAD\user1@contoso.com

upvoted 3 times

iTomi 2 years, 11 months 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 2 years, 11 months ago

You can also do like: net localgroup administrators AzureAD\ /add

upvoted 1 times

Darkfire 2 years, 9 months 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

Rocky83 3 years, 1 month ago

AzureAD is the correct answer here

upvoted 4 times

Casticod 3 years, 1 month ago

net localgroup administrators /add "AzureAD\

https://superuser.com/questions/982336/how-do-i-add-azure-active-directory-user-to-local-administrators-group

upvoted 2 times

madsa 2 years, 11 months ago

You can also do like: net localgroup administrators AzureAD\user1@contoso.com /add

upvoted 1 times

Sas2003 Highly Voted 3 years, 2 months ago

AzureAD is the correct answer

upvoted 16 times

Nozuka Highly Voted 3 years, 2 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 34 times

Casticod 3 years, 1 month 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

Question #110 *Topic 1*

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



Stuckbear Highly Voted 3 years, 1 month ago

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.^^^ 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.Microsoft must have changed it, your link now says "To configure security defaults in your directory, you must be assigned at least the Conditional Access Administrator role."

upvoted 15 times

Stuckbear Highly Voted 3 years, 1 month 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 15 times

HueCumber Most Recent 7 months, 3 weeks ago

Selected Answer: C

□ C. Security Administrator □

✔ Can enable/disable Security defaults

✔ Can create and manage Conditional Access policies

✔ Can manage other identity security features (MFA, Identity Protection, security alerts)

□ Meets the requirement using least privilege

This is the lowest-privileged built-in role that satisfies both requirements.

upvoted 1 times

moluccanvibe 9 months, 2 weeks ago

Selected Answer: B

The solution must use the principle of least privilege. Which is B.

upvoted 2 times

Dinkan 1 year, 2 months ago

Selected Answer: B

Disable security defaults in your directory:

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

* Browse to Entra ID > Overview > Properties.

* Select Manage security defaults.

* Set Security defaults to Disabled (not recommended).

* Select Save.

Ref:

https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#disabling-security-defaults

upvoted 3 times

henil_154762 1 year, 2 months ago

Selected Answer: B

B. Conditional Access Administrator

Create/manage Conditional Access policies: explicitly permitted for the Conditional Access Administrator role.

Microsoft Learn

Enable/disable Security defaults: Microsoft states you must be at least Conditional Access Administrator to configure Security defaults.

upvoted 1 times

jzmirus2 1 year, 8 months ago

Selected Answer: B

To provide a user with the ability to manage Security defaults and create Conditional Access policies while adhering to the principle of least privilege, you should assign the Conditional Access Administrator role (Option B). This role grants the necessary permissions without the broader access associated with the Global Administrator role

upvoted 3 times

correction 1 year, 9 months ago

Selected Answer: B

correction "To configure security defaults in your directory, you must be assigned at least the Conditional Access Administrator role."

https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults

upvoted 3 times

6060 1 year, 10 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults?utm_source=chatgpt.com#enabling-security-defaults:~:text=To%20configure%20security%20defaults%20in%20your%20directory%2C%20you%20must%20be%20assigned%20at%20least%20the%20Conditional%20Access%20Administrator%20role.%20By%20default%20the%20first%20account%20in%20any%20directory%20is%20assigned%20a%20higher%20privileged%20role%20known%20as%20Global%20Administrator.

upvoted 1 times

Dinkan 1 year, 2 months ago

Selected Answer: B

Disable security defaults in your directory: * Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator. * Browse to Entra ID > Overview > Properties. * Select Manage security defaults. * Set Security defaults to Disabled (not recommended). * Select Save. Ref: https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#disabling-security-defaults

upvoted 2 times

Seek12 1 year, 10 months ago

Selected Answer: B

security admin cannot create CA policy

upvoted 2 times

Friscini 1 year, 11 months 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 year, 10 months ago

- To Support my answer:

https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults?utm_source=chatgpt.com#enabling-security-defaults

upvoted 1 times

Nav90 2 years 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

Tr619899 1 year, 11 months 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 1 year, 11 months ago

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.- To Support my answer: https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults?utm_source=chatgpt.com#enabling-security-defaults

upvoted 2 times

RomanV 2 years, 1 month 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

martinods 2 years, 1 month 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

martinods 2 years, 1 month 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.correction "To configure security defaults in your directory, you must be assigned at least the Conditional Access Administrator role." https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults

upvoted 1 times

2938b52 10 months, 2 weeks ago

The security administrator has broader permissions than the Conditional Access Admin.

The security administrator manages an org's overall security, handling threat policies, security reports & configurations across Entra ID & Office 365. To assign the user this role you would not be using the principle of LEAST privilege. You'd be using a bazooka when a fly swatter will do.

upvoted 1 times

RomanV 2 years, 1 month 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

Nav90 2 years 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 2 times

EUC_PRO 2 years, 2 months 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

EUC_PRO 2 years, 2 months ago

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-thisTo 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 linkcorrection "To configure security defaults in your directory, you must be assigned at least the Conditional Access Administrator role." https://learn.microsoft.com/en-us/entra/fundamentals/security-defaultsas 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

Pollosor 2 years, 3 months ago

Selected Answer: B

With both it is possible, but the conditional access administrator has fewer privileges.

upvoted 2 times

martinods 2 years, 1 month 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 linkcorrection "To configure security defaults in your directory, you must be assigned at least the Conditional Access Administrator role." https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults

upvoted 1 times

martinods 2 years, 1 month 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

oopspruu 2 years, 4 months 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 2 years, 4 months ago

B

https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

upvoted 1 times

da_terminator 2 years, 5 months 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 2 years, 6 months 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 2 years, 8 months ago

Selected Answer: B

Given answer is correct.

upvoted 1 times

Darkfire 2 years, 9 months 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-defaults#:~:text=If%20your%20organization%20has%20complex%20security%20requirements%2C%20you%20should%20consider%20Conditional%20Access.

upvoted 2 times

belyo 2 years, 11 months ago

Selected Answer: B

B. tested in my tenant

CA admin can turn on/off security defaults

upvoted 2 times

Rocky83 3 years, 1 month ago

Selected Answer: B

To provide a user the ability to manage both security defaults and Conditional Access policies, you should assign them the Conditional Access Administrator role1. This role allows the user to create, edit, and delete Conditional Access policies, as well as enable or disable security defaults.

upvoted 4 times

Casticod 3 years, 1 month ago

Selected Answer: B

100%100 Agree With Examkiller020

Global administrator, Conditional Access Administrator and Security Administrator can change security defaults But CAA Has a lower level of privileges

upvoted 2 times

ExamKiller020 3 years, 1 month ago

Selected Answer: B

Both Conditional Access Administrator and Security Administrator can change security defaults

REF: https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-turn-on-mfa?view=o365-worldwide&tabs=secdefaults#to-enable-security-defaults-or-confirm-theyre-already-enabled

When I look at all the permissions Security Administrator has. Its way more compaired to the Conditional Access Administrator role.

So I guess the answer is B

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

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

upvoted 6 times

Frederikd 1 year, 9 months ago

Microsoft must have changed it, your link now says "To configure security defaults in your directory, you must be assigned at least the Conditional Access Administrator role."

upvoted 9 times

Burkidur 2 years, 8 months 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 3 years, 2 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 9 times

Question #111 *Topic 1*

HOTSPOT -

In Microsoft Intune, you have the device compliance policies shown in the following table.

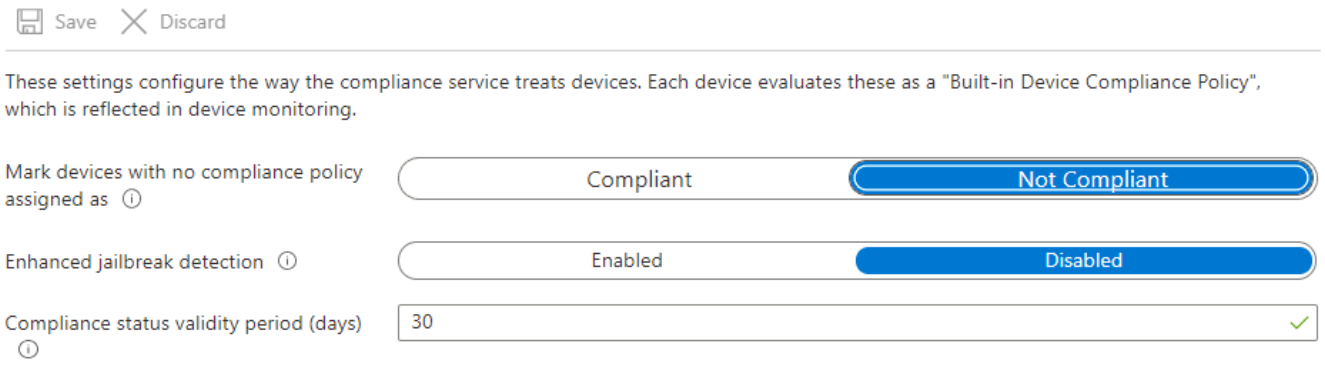
The Intune compliance policy settings are configured as shown in the following exhibit.

On June 1, you enroll Windows 10 devices in Intune as shown in the following table.

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

NOTE: Each correct selection is worth one point.

Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8.1 and later	Require	*Not applicable*	5 days	Group1
Policy2	Windows 10 and later	Not configured	Require	7 days	Group2
Policy3	Windows 10 and later	Require	Require	10 days	Group2

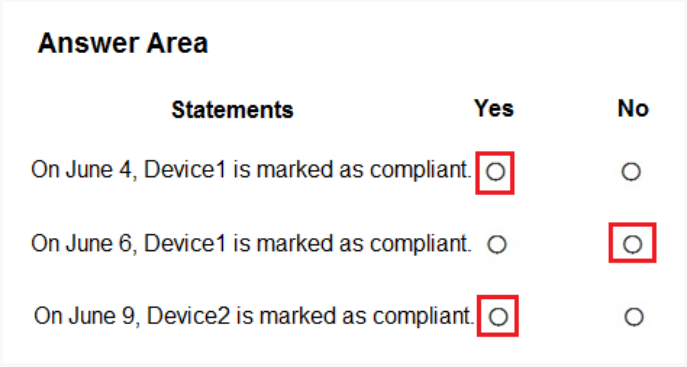


Name	Use BitLocker Drive Encryption (BitLocker)	Windows Defender	Member of
Device1	No	Enabled	Group1
Device2	No	Enabled	Group2

Answer Area

Statements	Yes	No
On June 4, Device1 is marked as compliant.	○	○
On June 6, Device1 is marked as compliant.	○	○
On June 9, Device2 is marked as compliant.	○	○

Suggested Answer:



iamforksu Highly Voted 3 years, 1 month ago

YNY - answer is correct

upvoted 34 times

iamforksu Highly Voted 3 years, 1 month ago

YNY - answer is correctY - 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 daysexplain pleasecorrecto

upvoted 34 times

scrapper_slapper Most Recent 7 months, 2 weeks ago

i agree with this

upvoted 1 times

ModernoDecor 8 months, 2 weeks ago

outdated. Windows 8.1 is no longer supported by Microsoft Intune or Microsoft Entra ID

upvoted 1 times

Dinkan 1 year, 2 months ago

Answer should be NNN nbased on this article: https://learn.microsoft.com/en-us/intune/intune-service/protect/create-compliance-policy#assign-an-ingraceperiod-status

upvoted 4 times

Casticod 3 years, 1 month 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-noncompliancePolicy 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.The third device is marked non-compliant immediately: the grace period does not grant compliance to devices that are missing the policy requirements: the grace period allows you to use a non-compliant device until the policy is ENFORCED at the end of the grace period, therefore the device is marked non-compliant on day 1.

upvoted 22 times

Casticod 3 years, 1 month 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 22 times

02dc19c 1 year, 7 months ago

The answer should be No, No, No: the grace period does not mark devices that are missing a policy requirement as compliant: the devices with missing requirements are marked non-compliant immediately and the grace period allows you to resolve the compliance issue until the policy is ENFORCED at the end of the grace period, therefore the last answer should also be a hard NO.

upvoted 4 times

Roska 1 year, 8 months ago

YYY

==========

Device1 = Windows10

Policy1 -> Windows 8.1 -> No policy assigned -> falls back on Compliance Policy Settings - 30 days

upvoted 1 times

JayHall 1 year, 9 months ago

Slighty modifying MR_Eliot's comment for clarity:

On June 4, device1 is marked as compliant

- YES. Mark device as not compliant after 5 days (which will be June 6). Device is still within non compliance grace period.

On June 6, device1 is marked as compliant

- NO. Grace period is over. So de device is not compliant.

On June 9, device2 is marked as compliant:

- YES. Policy3 makes the device not compliant after 10 days (which is Jun 11). Device is within non complaince grace period.

upvoted 3 times

GoombaLMAO 1 year, 9 months ago

Grace period is not the same as compliant.

N - N - N

upvoted 5 times

ModernoDecor 8 months ago

N,N,N Compliant: The device successfully applied one or more device compliance policy settings. In-grace period: The device is targeted with one or more device compliance policy settings but isn't yet compliant to all of them. Devices with this status are noncompliant, but in the grace period defined by the admin. https://learn.microsoft.com/en-us/intune/intune-service/protect/compliance-policy-monitor

upvoted 2 times

ModernoDecor 8 months ago

N,N,N Compliant: The device successfully applied one or more device compliance policy settings. In-grace period: The device is targeted with one or more device compliance policy settings but isn't yet compliant to all of them. Devices with this status are noncompliant, but in the grace period defined by the admin. https://learn.microsoft.com/en-us/intune/intune-service/protect/compliance-policy-monitori agree with this

upvoted 2 times

METAM 2 years, 2 months ago

NNY. good

upvoted 1 times

Pollosor 2 years, 3 months 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 4 times

HvD 2 years 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 5 times

CJL324 2 years, 6 months 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 2 times

MR_Eliot 2 years, 8 months ago

Y, N, Y

Device1:

Policies: Policy1

Verdict: Not compliant since bitlocker is disabled.

Device2:

Plicies: 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. Whihin grace period.

On June 6, device 1 is marked as compliant

- No. Grace periode is over. So de device is not compliant.

On June 9, device2 is marked as compliant:

- Yes. Policy3 makes the device not compliant after 10 days. Device is whithin grace period.

upvoted 8 times

Krayzr 2 years, 9 months ago

Confused :?

https://www.examtopics.com/discussions/microsoft/view/51834-exam-md-101-topic-3-question-25-discussion/

upvoted 1 times

WORKHOLIC 2 years, 5 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

WORKHOLIC 2 years, 5 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-conflictsBox 1: Yes, because the device is indeed not compliant, but will be marked as such after 5 days, which is June 6.

upvoted 2 times

NoursBear 2 years, 10 months 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

CJL324 2 years, 6 months 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 6 times

CJL324 2 years, 6 months 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: NoDevice1 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: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 6 times

gavorgavin 2 years 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 2 years, 8 months ago

Exactly. Otherwise the screenshot with devices with no compliance setting would make no sense in this question.

upvoted 2 times

CJL324 2 years, 6 months 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: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

CJL324 2 years, 6 months 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

Greatone1 2 years, 11 months ago

NNY this question is on MS 101 exam

upvoted 2 times

abill 2 years, 11 months ago

NNY for me

upvoted 2 times

Kevern 2 years, 11 months 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 5 times

Sonia33 2 years, 11 months ago

For me it should be No, No, No. The third device should be In Grace period.

upvoted 6 times

NoursBear 2 years, 10 months 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

madsa 2 years, 11 months ago

Yes No Yes

upvoted 1 times

Bradministrator 3 years ago

NNY

Device 1 on June 4 isn't compliant as it's in grace period

upvoted 3 times

Rubends 3 years, 1 month ago

I think is NNY because question say put mark not complain without policy

upvoted 3 times

RabbitB 3 years, 1 month ago

YNY - answer is incorrect

upvoted 4 times

NoursBear 2 years, 11 months ago

for me too

upvoted 2 times

AleFCI1908 2 years 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 6 times

665d390 2 years, 2 months ago

correcto

upvoted 2 times

METAM 2 years, 2 months ago

explain please

upvoted 2 times

02dc19c 1 year, 7 months ago

The third device is marked non-compliant immediately: the grace period does not grant compliance to devices that are missing the policy requirements: the grace period allows you to use a non-compliant device until the policy is ENFORCED at the end of the grace period, therefore the device is marked non-compliant on day 1.

upvoted 2 times

firefox15 3 years, 1 month 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 20 times

Question #112 *Topic 1*

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

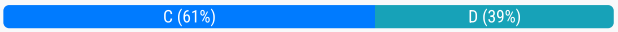
B. a device compliance policy

C. an account protection policy

D. a device configuration profile

Suggested Answer: *C*

Community vote distribution



Fortind1974 Highly Voted 3 years, 2 months ago

C. an account protection policy https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy#manage-local-groups-on-windows-devicesYou 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 19 times

Fortind1974 Highly Voted 3 years, 2 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 18 times

Krayzr 2 years, 9 months 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

scrapper_slapper Most Recent 7 months, 2 weeks ago

i think its D . you are not configuring the account you are adding an account to a local group (of the device) which you can do with Device Configuration Profile

upvoted 1 times

HueCumber 7 months, 3 weeks ago

Intune admin center → Endpoint security → Account protection → Create policy → Profile: Local user group membership → Local group: Remote Desktop Users → Add User1 (or an AAD group containing User1) → Assign to Marketing devices

upvoted 1 times

Le_Patriarche2025 9 months ago

La bonne réponse est D. Un profil de configuration de l'appareil. Raisonnement : Dans Intune, pour ajouter un utilisateur au groupe "Utilisateurs du Bureau à distance" (Remote Desktop Users) sur les appareils locaux, on utilise un profil de configuration d'appareil avec le type "Groupes d'utilisateurs et d'appareils locaux" (Local users and groups). Ce profil permet de : Cibler un groupe local spécifique (ex. Remote Desktop Users) Y ajouter un utilisateur Azure AD (User1) Déployer cela automatiquement sur les 75 appareils du département marketing

upvoted 1 times

Robert69 1 year, 1 month ago

A. An app configuration policy: This is used to configure settings inside mobile apps (like Outlook or Teams) on iOS/Android devices. It has no capability to manage Windows local system groups. B. A device compliance policy: This defines security standards (e.g., must have a PIN, firewall enabled) a device must meet to be considered "compliant." It is used for reporting and conditional access, not for applying configuration settings like adding a user to a local group. C. An account protection policy: This policy is part of Endpoint Security and focuses on protecting user credentials and accounts, primarily by managing settings like Windows Hello for Business, Credential Guard, and Local Security Authority (LSA) protection. It is not the standard or correct tool for managing local user group membership.

upvoted 3 times

Dinkan 1 year, 2 months ago

C. an account protection policy Tested in LAB. Intune Admin Center > Endpoint Security > Account Protection > Create Policy > Platform: Windows, Profile: Local user group Membership Reference: https://learn.microsoft.com/en-us/intune/intune-service/protect/endpoint-security-account-protection-policy#manage-local-groups-on-windows-devices

upvoted 3 times

henil_154762 1 year, 3 months ago

Selected Answer: D

Ans - D checked on Microsoft

upvoted 2 times

henil_154762 1 year, 3 months ago

Ans - D checked on MicrosoftOnly the Device configuration profile supports managing local group membership.

upvoted 2 times

henil_154762 1 year, 3 months ago

Only the Device configuration profile supports managing local group membership.

upvoted 1 times

Besxp 1 year, 5 months ago

Selected Answer: D

 Correct exam answer: D. Device Configuration Profile

It's the fully supported, general availability (GA) method to add a user to the Remote Desktop Users group.

C (Account Protection Policy) can also work, but it's still in preview, and Microsoft exams typically avoid preview features.

Use a Device Configuration Profile with the Settings Catalog or Custom OMA-URI to configure local group membership.

https://learn.microsoft.com/en-us/mem/intune/configuration/local-users-groups-settings-windows

upvoted 2 times

Besxp 1 year, 5 months ago

 Correct exam answer: D. Device Configuration Profile It's the fully supported, general availability (GA) method to add a user to the Remote Desktop Users group. C (Account Protection Policy) can also work, but it's still in preview, and Microsoft exams typically avoid preview features. Use a Device Configuration Profile with the Settings Catalog or Custom OMA-URI to configure local group membership. https://learn.microsoft.com/en-us/mem/intune/configuration/local-users-groups-settings-windowsSorry, the link didn't work, but did some deeper research: Both D (Device Configuration Profile) and C (Account Protection policy) work technically. But for exam clarity and production best practices, D is the recommended answer. You can confidently base this on Microsoft documentation.

upvoted 2 times

Besxp 1 year, 5 months ago

Sorry, the link didn't work, but did some deeper research: Both D (Device Configuration Profile) and C (Account Protection policy) work technically. But for exam clarity and production best practices, D is the recommended answer. You can confidently base this on Microsoft documentation.

upvoted 1 times

02dc19c 1 year, 7 months ago

To add User1 to the Remote Desktop Users group on the Windows 11 devices, you would use a device configuration profile in Microsoft Intune. Specifically, you can configure a Group Policy Object (GPO) or use a custom configuration profile to add User1 to the Remote Desktop Users group across multiple devices. This approach ensures the policy is applied to all relevant devices in the marketing department.

upvoted 4 times

02dc19c 1 year, 7 months ago

account protection policy isn't the correct choice in this scenario. Account protection policies in Intune are generally used to configure security-related settings, such as enforcing password policies or managing Windows Hello for Business.

upvoted 2 times

Tr619899 1 year, 11 months ago

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 3 times

EUC_PRO 2 years, 2 months ago

https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy#manage-local-groups-on-windows-devices

upvoted 1 times

METAM 2 years, 2 months ago

C good

upvoted 1 times

Frank_2022 2 years, 3 months ago

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 2 years, 3 months ago

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 2 times

oopspruu 2 years, 4 months ago

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 2 years, 4 months 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

Question #113 *Topic 1*

HOTSPOT -

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

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:

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

Name	Member of	License
User1	Group1	Microsoft 365 E5
User2	Group2	Microsoft 365 E5

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android

Answer Area

Statements	Yes	No
If User1 registers Device1 in contoso.com, Device1 is enrolled automatically in Microsoft Intune.	○	○
If User1 joins Device1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	○	○
If User2 registers Device3 in contoso.com, Device3 is enrolled automatically in Microsoft Intune.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
If User1 registers Device1 in contoso.com, Device1 is enrolled automatically in Microsoft Intune.	○	●
If User1 joins Device1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	●	○
If User2 registers Device3 in contoso.com, Device3 is enrolled automatically in Microsoft Intune.	○	●

benpatto Highly Voted 3 years ago

It really helps to read the question people!!!! Option 2 says user1 joins device1 to contoso.com - why would Device2 be affacted by this?

upvoted 20 times

benpatto Highly Voted 3 years ago

It really helps to read the question people!!!! Option 2 says user1 joins device1 to contoso.com - why would Device2 be affacted by this?the question is incorrect. For me, option two talks about device 2 and for me is "yes"

upvoted 20 times

Le_Patriarche2025 Most Recent 8 months, 2 weeks ago

Y: Portée MDM

N: l enregistrement de l'un n a rien avoir avec l'autre

N: Android necessite autre chose

upvoted 1 times

Robert69 1 year, 1 month ago

Y, Y, N

For a device to be "enrolled automatically in Microsoft Intune" (MDM), three conditions must be met:

The user has a license that includes Intune (Both User1 and User2 do).

The user is in the MDM user scope (Only User1 is).

The user performs an action (register/join) that triggers the enrollment process.

upvoted 4 times

MR_Eliot 2 years, 8 months 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.Automatic enrollment occurs when you join or register a device.

upvoted 13 times

MR_Eliot 2 years, 8 months 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 13 times

ExamBud 1 year, 8 months ago

Registering also enroll the device in Intune: https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enroll?source=recommendations#:~:text=This%20enrollment%20method%20enables%20devices%20to%20enroll%20automatically%20when%20they%20join%20or%20register%20in%20Microsoft%20Entra%20ID

upvoted 3 times

Doug77 1 year, 9 months ago

Should be N,Y,N, if question 2 is actually a typo, otherwise

Device 1...N registering will not automatically enroll in intune/ Entra ID registered

Device 1, if typo, yes, if Device 2, No

Device 3 ....No, User 2 does not have MDM, MAM has nothing to do with this, so No

upvoted 1 times

Faceless_Void 2 years, 3 months ago

Y - Group1 - MDM user scope

N - NO MDM

N - NO MDM

upvoted 1 times

ergacharsk 2 years, 3 months ago

The given answer is correct Y, N, N

Y - because automatic enrollment occurs when you join or register a device.

N - beause 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 9 times

Doug77 1 year, 9 months ago

Should be N,Y,N, if question 2 is actually a typo, otherwise Device 1...N registering will not automatically enroll in intune/ Entra ID registered Device 1, if typo, yes, if Device 2, No Device 3 ....No, User 2 does not have MDM, MAM has nothing to do with this, so NoRegistering also enroll the device in Intune: https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enroll?source=recommendations#:~:text=This%20enrollment%20method%20enables%20devices%20to%20enroll%20automatically%20when%20they%20join%20or%20register%20in%20Microsoft%20Entra%20ID

upvoted 1 times

oopspruu 2 years, 4 months 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 5 times

e6d6bf4 1 year, 6 months ago

This is the best answer by far!

upvoted 1 times

Maclouis116 2 years, 4 months ago

Automatic enrollment occurs when you join or register a device.

upvoted 9 times

cuber 2 years, 4 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 4 times

cuber 2 years, 4 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.This is the best answer by far!

upvoted 4 times

Burkidur 2 years, 8 months ago

It's likely a typo by ET. The key difference between Q1 and Q2 is "joined" vs "registered".

upvoted 3 times

NoursBear 2 years, 10 months ago

Attention !!! the second option is a trick, read it carefully

upvoted 3 times

NoursBear 2 years, 10 months ago

Attention !!! the second option is a trick, read it carefullyIt's likely a typo by ET. The key difference between Q1 and Q2 is "joined" vs "registered".

upvoted 3 times

Sonia33 2 years, 11 months 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 2 years, 11 months 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.I read it wrong... Yes, No, No.why? For me, user 1 can enroll the device 2It says that if User1 joines Device1 (not 2), that enrolls Device2. It doesn't make any sense so it is a NO, if there is not a typo.

upvoted 3 times

Sonia33 2 years, 11 months ago

I read it wrong... Yes, No, No.why? For me, user 1 can enroll the device 2It says that if User1 joines Device1 (not 2), that enrolls Device2. It doesn't make any sense so it is a NO, if there is not a typo.

upvoted 1 times

Sonia33 2 years, 11 months ago

I read it wrong... Yes, No, No.

upvoted 1 times

riccardo1999 2 years, 10 months ago

why? For me, user 1 can enroll the device 2

upvoted 1 times

riccardo1999 2 years, 10 months ago

why? For me, user 1 can enroll the device 2It says that if User1 joines Device1 (not 2), that enrolls Device2. It doesn't make any sense so it is a NO, if there is not a typo.

upvoted 1 times

Contactfornitish 3 years, 1 month 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.Second option talking about device 2 and thit is targeted to group 2 which is MAM user scope so ans is Ndevice 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 YESSorry, 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 2 times

Contactfornitish 3 years, 1 month 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 2 times

ExamBud 1 year, 9 months ago

It says that if User1 joines Device1 (not 2), that enrolls Device2. It doesn't make any sense so it is a NO, if there is not a typo.

upvoted 1 times

Mahi_444 3 years ago

Second option talking about device 2 and thit is targeted to group 2 which is MAM user scope so ans is Ndevice 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 YESSorry, 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

Mahi_444 3 years 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

madsa 2 years, 11 months 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 enrol the device in Intune.

upvoted 3 times

riccardo1999 2 years, 10 months 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

riccardo1999 2 years, 10 months 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 YESSorry, 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

riccardo1999 2 years, 10 months ago

the question is incorrect. For me, option two talks about device 2 and for me is "yes"

upvoted 8 times

VirtualJP 3 years, 1 month ago

I'm thinking N,N,N

upvoted 5 times

VirtualJP 3 years, 1 month ago

I'm thinking N,N,NNot sure why I said N for all 3. I retract my original answer in favour of: Y Y N.Can you explain?

upvoted 5 times

VirtualJP 3 years, 1 month ago

Not sure why I said N for all 3. I retract my original answer in favour of: Y Y N.

upvoted 2 times

VirtualJP 3 years, 1 month ago

Not sure why I said N for all 3. I retract my original answer in favour of: Y Y N.Can you explain?

upvoted 2 times

BJS78 2 years, 10 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 3 years, 1 month ago

Seems correct:

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

upvoted 2 times

LiamAzure 3 years ago

Can you explain?

upvoted 2 times

BJS78 3 years, 1 month ago

https://call4cloud.nl/2021/08/the-battle-between-aadj-and-aadr/

upvoted 1 times

Question #114 *Topic 1*

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%)

Dinkan Most Recent 1 year, 2 months ago

Selected Answer: B

B. Perform a Windows Autopilot reset on the devices.

Performing clean install will also remove all the data and applications installed by the previous users, but this required a lot more administrative effort than doing autopilot reset

upvoted 1 times

WORKHOLIC 1 year, 11 months ago

Selected Answer: B

Windows Pilot Reset, removes user data but retains device enrollment

upvoted 1 times

MR_Eliot 2 years, 2 months ago

Selected Answer: B

Answer is correct.

upvoted 1 times

Darkfire 2 years, 3 months ago

Selected Answer: B

B is correct

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

upvoted 1 times

Amir1909 2 years, 4 months ago

Correct

upvoted 1 times

kay000001 2 years, 5 months ago

Selected Answer: B

Answer is B:

https://learn.microsoft.com/en-us/education/windows/autopilot-reset

upvoted 1 times

LiamAzure 2 years, 6 months ago

B Windows Pilot Reset, removes user data but retains device enrollment

upvoted 1 times

iamforksu 2 years, 7 months ago

Selected Answer: B

B seems solid

upvoted 1 times

HOTSPOT
-

You create a Windows Autopilot deployment profile.

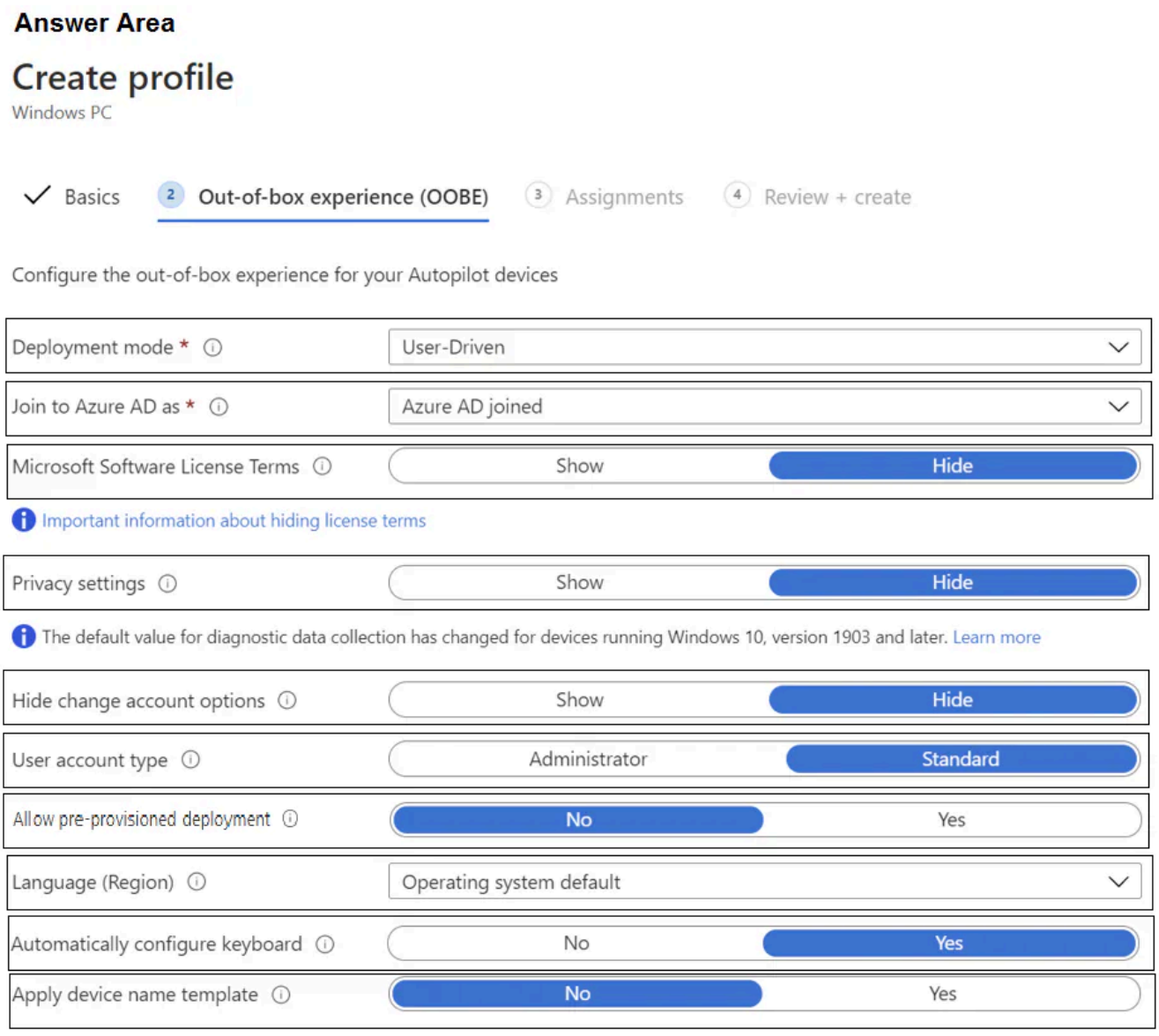
You need to configure the profile settings to meet the following requirements:

• 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



Suggested Answer:



solitudewriter Most Recent 5 months ago

The answer is Allow pre-provisioned deployment. The description of Allow pre-provisioned deployment in the tenant says, 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. The queston says "system-apps". The description of self-deploying mode in the tenant says Self-Deploying (preview): Devices are not associated with the user enrolling the device and user credentials are not required to provision the device

Because of the word "system apps" in the question, it is pre-provisioned deployment and MS documentation says, self-deploying mode allows deployment of a Windows device as a kiosk, digital signage device, or a shared device.

upvoted 1 times

HueCumber 7 months, 3 weeks ago

□ Final Answer (what the exam wants)

□ Allow pre-provisioned deployment → Yes

□ Apply device name template → Yes

Those two settings fully satisfy both requirements.

upvoted 2 times

Dinkan 1 year, 2 months ago

Deplyment Mode: Self-Deploying

Apply device name template: Yes (Use the %SERIAL% macro to add a hardware-specific serial number)

upvoted 1 times

dnt91 2 years, 2 months ago

Answer is :

1. Allow pre-provisionned deployment

2. Apply Device name template

upvoted 3 times

CJL324 2 years, 6 months 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 2 years, 7 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

flc 2 years, 7 months ago

Surreeee!!

upvoted 1 times

kerimnl 2 years, 7 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 templateSurreeee!!

upvoted 4 times

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

https://learn.microsoft.com/en-us/autopilot/self-deploying

upvoted 1 times

MR_Eliot 2 years, 8 months ago

https://learn.microsoft.com/en-us/autopilot/self-deployingFrom your link: 1. Create an Autopilot profile for self-deploying mode with the desired settings.

upvoted 1 times

chafe 2 years, 4 months ago

From your link:

1. Create an Autopilot profile for self-deploying mode with the desired settings.

upvoted 1 times

Darkfire 2 years, 9 months 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 2 years, 10 months 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 user %SERIAL% variable.

upvoted 4 times

Romke_en_Tomke 2 years, 10 months 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 user %SERIAL% variable.I agree but then it would have needed 3 options to changegreat!!!

upvoted 4 times

NoursBear 2 years, 10 months ago

I agree but then it would have needed 3 options to change

upvoted 1 times

NoursBear 2 years, 10 months ago

I agree but then it would have needed 3 options to changegreat!!!

upvoted 1 times

abigailcarol 2 years, 6 months ago

great!!!

upvoted 1 times

VirtualJP Highly Voted 3 years, 1 month ago

Agree answer is correct

upvoted 6 times

ExamKiller020 Highly Voted 3 years, 1 month ago

Given answer is correct.

For deployment mode you can use self-deploying mode.

upvoted 9 times

Question #116 *Topic 1*

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%)

Dinkan Most Recent 1 year, 2 months ago

Selected Answer: B

With NLA enabled, users must authenticate themselves before a remote session is established

https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/remotepc/remote-desktop-allow-access#why-allow-connections-only-with-network-level-authentication

upvoted 1 times

ergacharsk 2 years, 3 months 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 2 years, 8 months ago

B is correct.

upvoted 1 times

Darkfire 2 years, 9 months 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%20from%20outside%20of%20that%20network%2C%20don%27t%20select%20this%20option.,-Feedback

upvoted 1 times

Amir1909 2 years, 10 months ago

Correct

upvoted 1 times

kay000001 2 years, 12 months ago

Selected Answer: B

Answer is B:

Here is a good article: https://zappedia.com/network-level-authentication/

upvoted 1 times

fco168 3 years ago

Selected Answer: B

B it is!

upvoted 1 times

VirtualJP 3 years, 1 month ago

Selected Answer: B

Given answer is correct.

upvoted 1 times

BJS78 3 years, 1 month ago

https://itcompanies.net/blog/network-level-authentication

upvoted 1 times

Question #117 *Topic 1*

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.

Which devices can be changed to Windows 11 Enterprise by using subscription activation?

Name	Operating system	Activation type
Device1	Windows 10 Pro for Workstation	Key
Device2	Windows 11 Pro	Key
Device3	Windows 11 Pro	Subscription

A. Device3 only

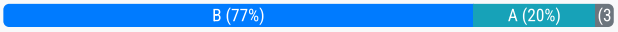
B. Device2 and Device3 only

C. Device1 and Device2 only

D. Device1, Device2, and Device3

Suggested Answer: *B*

Community vote distribution



Gillactus Highly Voted 3 years, 2 months ago

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 17 times

HueCumber Most Recent 7 months, 3 weeks ago

I checked google and copilot all three can be upgraded because they are Pro or Pro for Workstations. Enterprise is still a step up.

upvoted 1 times

Dinkan 1 year, 2 months ago

B. Device2 and Device3 only * Product key-based Windows Enterprise software licenses can be transitioned to Windows Enterprise subscriptions. * 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

upvoted 1 times

henil_154762 1 year, 3 months ago

A. Device3 onlythis is the most recent comment I saw so far, if you took the exam can you please let us know if these Questions are on the exam recently or not?

upvoted 1 times

henil_154762 1 year, 3 months ago

Selected Answer: A

A. Device3 only

upvoted 1 times

b8142ea 1 year, 2 months ago

this is the most recent comment I saw so far, if you took the exam can you please let us know if these Questions are on the exam recently or not?

upvoted 1 times

nhmh90 1 year, 4 months ago

only activation type = subscription is entitle for version upgrade

upvoted 2 times

Omerozb 1 year, 11 months ago

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?pivots=windows-11

upvoted 3 times

1655b71 2 years ago

Only device 3

upvoted 1 times

RomanV 2 years, 1 month 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 2 years, 4 months ago

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 2 years, 7 months ago

Wouldn't this be A? since device3 is the only one with subscription?

upvoted 1 times

OyYaGotta 2 years, 8 months 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

OyYaGotta 2 years, 8 months 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.The question though is asking to upgrade devices to 11 enterprise with subscription activation, not pro to pro.

upvoted 1 times

Doug77 1 year, 9 months ago

The question though is asking to upgrade devices to 11 enterprise with subscription activation, not pro to pro.

upvoted 1 times

MR_Eliot 2 years, 8 months ago

B is correct. Device one, needst to be upgraded to Windows 11 first and activated using a Windows 11 key.

upvoted 1 times

Darkfire 2 years, 9 months ago

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 Enterprise newer than Windows 10. 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%20first%20be%20required%2C%20followed%20by%20upgrading%20to%20the%20version%20of%20Windows%20Enterprise%20newer%20than%20Windows%2010

upvoted 1 times

Amir1909 2 years, 10 months ago

B is correct

upvoted 1 times

yosry 2 years, 12 months ago

SEEMS CORRECT

upvoted 1 times

fco168 3 years ago

B. Because the subscription cannot upgrade from Windows 10 to 11.

upvoted 1 times

LiamAzure 3 years ago

2 and 3

upvoted 1 times