



Microsoft Endpoint MD-102 Exam Questions

Total Questions: 350+

Demo Questions: 35

Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

**For Access to the full set of Updated Questions – Visit:
[MD-102 Exam Dumps](#) by Cert Empire**

Question: 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.

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

ADatum has a hybrid Azure AD tenant named adatum.com. **Users and Groups -** The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license. Enterprise State Roaming is enabled for Group1 and GroupA. Group1 and Group2 have a Membership type of Assigned. **Devices -** ADatum has the Windows 10 devices shown in the following table.

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

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune. The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1. Microsoft Intune Configuration - Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

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

Mark devices with no compliance policy assigned as ☒ **Compliant** ☐ Not Compliant

Enhanced jailbreak detection ☐ Enabled ☒ Disabled

Compliance status validity period (days) ☒

The Automatic Enrollment settings have the following configurations: MDM user scope: GroupA - MAM user scope: GroupB - You have an Endpoint protection configuration profile that has the following Controlled folder access settings: Name: Protection1 - Folder protection: Enable - List of apps that have access to protected folders: C:*\AppA.exe List of additional folders that need to be protected: D:\Folder1 Assignments: Included groups: Group2, GroupB - Windows Autopilot Configuration - ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments **4 Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot. The Intune connector for Active Directory is installed on Server1. Requirements - Planned Changes - ADatum plans to implement the following changes: Purchase a new Windows 10 device named Device6 and enroll the device in Intune New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined. Deployed a network boundary configuration profile that will have the

following settings: Name: Boundary1 - Network boundary: 192.168.1.0/24 Scope tags: Tag1 - Assignments: Included groups: Group1, Group2 - Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings: Name: Connection1 - Connection name: VPN1 - Connection type: L2TP - Assignments: Included groups: Group1, Group2, GroupA Excluded groups: -- Name: Connection2 - Connection name: VPN2 - Connection type: IKEv2 - Assignments: Included groups: GroupA - Excluded groups: GroupB - Technical Requirements - ADatum must meet the following technical requirements: Users in GroupA must be able to deploy new computers. Administrative effort must be minimized. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

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

Answer:

Statement 1: No Statement 2: No Statement 3: No

Explanation:

Statement 1: User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.

Answer: No Explanation: The Endpoint protection profile, Protection1, enables "Controlled folder access" and is assigned to Group2. Device4 is a member of Group2, so this policy applies to it. The policy explicitly adds D:\Folder1 to the list of protected folders. The only application allowed to access protected folders is C:*\AppA.exe. Since Notepad is not on this allowlist, it will be blocked by Controlled folder access when trying to create a file in the protected D:\Folder1 folder.

Statement 2: User2 can remove D:\Folder1 from the list of protected folders on Device2. Answer: No Explanation: The configuration for Controlled folder access on Device2 is enforced by the Protection1 profile from Microsoft Intune, as Device2 is in Group2. While User2 has the "Azure AD Joined Device Local Administrator" role, which grants local administrator privileges, settings managed and enforced by an MDM authority like Intune cannot be changed by a local administrator on the device itself. The option to modify the list of protected folders would be grayed out in the Windows Security settings, indicating it is managed by an administrator (in this

case, Intune). Statement 3: User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script. Answer: No Explanation: Device2 is subject to the Protection1 policy, which enables Controlled folder access. By default, Controlled folder access protects common system folders, including the user's Desktop (C:\Users*\Desktop). The policy's allowlist only permits C:*\AppA.exe to make changes in these protected locations. Windows PowerShell is not on this list. Therefore, when User3 runs a script attempting to create a file on their own desktop, the action will be blocked by Controlled folder access.

References:

1. Controlled Folder Access:

Microsoft Documentation: Protect important folders with controlled folder access. This document explains that CFA protects default folders (like Desktop) and can be configured to protect additional folders. It also describes how only allowed apps can access these folders. Microsoft Documentation: Customize controlled folder access. This details how to specify which applications are allowed to bypass CFA restrictions.

2. Intune Policy Enforcement:

Microsoft Documentation: Policy conflict. This resource explains the hierarchy and precedence of policies, noting that MDM policies (from Intune) typically override locally configured settings.

CertEmpire

3. Azure AD Roles:

Microsoft Documentation: Azure AD built-in roles - Azure AD Joined Device Local Administrator. This clarifies that the role adds the user to the local administrators' group on Azure AD joined devices, but this does not grant rights to override MDM policies.

Question: 2

Case study - Overview - ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. ADatum has a Microsoft 365 E5 subscription. Environment - Network Environment - The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

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

ADatum has a hybrid Azure AD tenant named adatum.com. Users and Groups - The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license. Enterprise State Roaming is enabled for Group1 and GroupA. Group1 and Group2 have a Membership type of Assigned. Devices - ADatum has the Windows 10 devices shown in the following table.

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

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune. The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1. Microsoft Intune Configuration - Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

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

Mark devices with no compliance policy assigned as ☒ **Compliant** ☐ Not Compliant

Enhanced jailbreak detection ☐ Enabled ☒ Disabled

Compliance status validity period (days) ☒

The Automatic Enrollment settings have the following configurations: MDM user scope: GroupA - MAM user scope: GroupB - You have an Endpoint protection configuration profile that has the following Controlled folder access settings: Name: Protection1 - Folder protection: Enable - List of apps that have access to protected folders: C:*\AppA.exe List of additional folders that need to be protected: D:\Folder1 Assignments: Included groups: Group2, GroupB - Windows Autopilot Configuration - ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments **4 Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot. The Intune connector for Active Directory is installed on Server1. Requirements - Planned Changes - ADatum plans to implement the following changes: Purchase a new Windows 10 device named Device6 and enroll the device in Intune New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined. Deployed a network boundary configuration profile that will have the

following settings: Name: Boundary1 - Network boundary: 192.168.1.0/24 Scope tags: Tag1 - Assignments: Included groups: Group1, Group2 - Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings: Name: Connection1 - Connection name: VPN1 - Connection type: L2TP - Assignments: Included groups: Group1, Group2, GroupA Excluded groups: -- Name: Connection2 - Connection name: VPN2 - Connection type: IKEv2 - Assignments: Included groups: GroupA - Excluded groups: GroupB - Technical Requirements - ADatum must meet the following technical requirements: Users in GroupA must be able to deploy new computers. Administrative effort must be minimized. Which devices are registered by using the Windows Autopilot deployment service?

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

Answer:

C

Explanation:

The technical requirements explicitly state, "Users in GroupA must be able to deploy new computers." This identifies GroupA as the designated group for handling Windows Autopilot deployments. According to the user table, User1 and User3 are members of GroupA. The device table indicates that User1 is the primary user of Device1, and User3 is the primary user of Device3. User2, the primary user of Device2, is not in GroupA. Therefore, it is logical to infer that the devices associated with the designated deployment users (Device1 and Device3) are the ones registered with the Windows Autopilot service. The case study note that "no devices deployed" refers to the final provisioning process, not the prerequisite registration of the device hardware IDs.

Why Incorrect Options are Wrong:

A. Device1 only: This is incorrect because User3 is also in GroupA, making Device3 a registered device as well. B. Device3 only: This is incorrect because User1 is also in GroupA, making Device1 a registered device as well. D. Device1, Device2, and Device3: This is incorrect because User2, the primary user of Device2, is not a member of GroupA and is therefore not designated to perform Autopilot deployments.

References:

Microsoft. (2024). Overview of Windows Autopilot. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/autopilot/overview>. (This document outlines the Autopilot process, distinguishing between device registration and deployment.)

Microsoft. (2023). Manually register devices with Windows Autopilot. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/autopilot/manual-register>. (This reference clarifies that registration is a distinct administrative step that precedes device deployment.)

Microsoft. (2023). Assign a user to a specific device. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/autopilot/enrollment-auth#assign-a-user-to-a-specificdevice>. (This explains the association between a user and a device within the Autopilot context, which is central to solving this scenario.)

CertEmpire

Question: 3

HOTSPOT - Case study - Overview - ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. ADatum has a Microsoft 365 E5 subscription. **Environment - Network Environment -** The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

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

ADatum has a hybrid Azure AD tenant named adatum.com. **Users and Groups -** The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license. Enterprise State Roaming is enabled for Group1 and GroupA. Group1 and Group2 have a Membership type of Assigned. **Devices -** ADatum has the Windows 10 devices shown in the following table.

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

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune. The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1. Microsoft Intune Configuration - Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

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

Mark devices with no compliance policy assigned as ☒ **Compliant** ☐ Not Compliant

Enhanced jailbreak detection ☐ Enabled ☒ Disabled

Compliance status validity period (days) ☒

The Automatic Enrollment settings have the following configurations: MDM user scope: GroupA - MAM user scope: GroupB - You have an Endpoint protection configuration profile that has the following Controlled folder access settings: Name: Protection1 - Folder protection: Enable - List of apps that have access to protected folders: C:*\AppA.exe List of additional folders that need to be protected: D:\Folder1 Assignments: Included groups: Group2, GroupB - Windows Autopilot Configuration - ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments **4 Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot. The Intune connector for Active Directory is installed on Server1. Requirements - Planned Changes - ADatum plans to implement the following changes: Purchase a new Windows 10 device named Device6 and enroll the device in Intune New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined. Deployed a network boundary configuration profile that will have the

following settings: Name: Boundary1 - Network boundary: 192.168.1.0/24 Scope tags: Tag1 - Assignments: Included groups: Group1, Group2 - Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings: Name: Connection1 - Connection name: VPN1 - Connection type: L2TP - Assignments: Included groups: Group1, Group2, GroupA Excluded groups: -- Name: Connection2 - Connection name: VPN2 - Connection type: IKEv2 - Assignments: Included groups: GroupA - Excluded groups: GroupB - Technical Requirements - ADatum must meet the following technical requirements: Users in GroupA must be able to deploy new computers. Administrative effort must be minimized. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

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

Answer:

Statement 1: No Statement 2: No Statement 3: Yes

Explanation:

Device1: Not Compliant Device1 is a member of Group1. It is therefore assigned Policy1 (Require BitLocker) and Policy2 (Require Secure Boot). For a device to be compliant, it must meet the requirements of all assigned policies. Device1 meets the condition for Policy1 (BitLocker is enabled). However, Device1 fails to meet the condition for Policy2 because Secure Boot is not enabled. Since it fails one of the assigned policies, Device1 is marked as Not Compliant. Device4: Not Compliant Device4 is a member of Group2. It is assigned Policy3, which requires both BitLocker and Secure Boot. Device4 has Secure Boot enabled but does not have BitLocker enabled. Because it fails to meet the BitLocker requirement of Policy3, Device4 is marked as Not Compliant. Device5: Compliant Device5 is a member of Group3. There are no compliance policies assigned to Group3. According to the compliance policy settings exhibit, devices with "no compliance policy assigned" are marked as Compliant. Therefore, Device5 is considered

Compliant.

References:

1. Microsoft Intune Documentation: Get started with device compliance policies in Intune - This document explains that if a device has multiple compliance policies assigned, it must be compliant with every policy to be compliant.
2. Microsoft Intune Documentation: Configure compliance policy settings - This section details the "Mark devices with no compliance policy assigned as" setting, which dictates the compliance state for devices not targeted by any specific policy.

CertEmpire

Question: 4

Case study - Overview - ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. ADatum has a Microsoft 365 E5 subscription. Environment - Network Environment - The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

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

ADatum has a hybrid Azure AD tenant named adatum.com. Users and Groups - The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license. Enterprise State Roaming is enabled for Group1 and GroupA. Group1 and Group2 have a Membership type of Assigned. Devices - ADatum has the Windows 10 devices shown in the following table.

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

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune. The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1. Microsoft Intune Configuration - Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

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

Mark devices with no compliance policy assigned as ☒ **Compliant** ☐ Not Compliant

Enhanced jailbreak detection ☐ Enabled ☒ Disabled

Compliance status validity period (days) ☒

The Automatic Enrollment settings have the following configurations: MDM user scope: GroupA - MAM user scope: GroupB - You have an Endpoint protection configuration profile that has the following Controlled folder access settings: Name: Protection1 - Folder protection: Enable - List of apps that have access to protected folders: C:*\AppA.exe List of additional folders that need to be protected: D:\Folder1 Assignments: Included groups: Group2, GroupB - Windows Autopilot Configuration - ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments **4 Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot. The Intune connector for Active Directory is installed on Server1. Requirements - Planned Changes - ADatum plans to implement the following changes: Purchase a new Windows 10 device named Device6 and enroll the device in Intune New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined. Deployed a network boundary configuration profile that will have the

following settings: Name: Boundary1 - Network boundary: 192.168.1.0/24 Scope tags: Tag1 - Assignments: Included groups: Group1, Group2 - Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings: Name: Connection1 - Connection name: VPN1 - Connection type: L2TP - Assignments: Included groups: Group1, Group2, GroupA Excluded groups: -- Name: Connection2 - Connection name: VPN2 - Connection type: IKEv2 - Assignments: Included groups: GroupA - Excluded groups: GroupB - Technical Requirements - ADatum must meet the following technical requirements: Users in GroupA must be able to deploy new computers. Administrative effort must be minimized. You implement Boundary1 based on the planned changes. Which devices have a network boundary of 192.168.1.0/24 applied?

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

Answer:

D

Explanation:

CertEmpire

The Boundary1 configuration profile is assigned to user groups Group1 and Group2. In Microsoft Intune, when a device configuration profile is assigned to user groups, the settings apply to the devices associated with those users. According to the case study: Group1 contains User1 and User2. Group2 contains User3 and User4. The primary users for the devices are: Device1: User1 Device2: User2 Device3: User3 Device4: User4 Therefore, the Boundary1 profile will be applied to Device1, Device2, Device3, and Device4. Device5 is not affected because its primary user, User5, is not a member of either Group1 or Group2.

Why Incorrect Options are Wrong:

A. Device2 only: This is incorrect because the policy also applies to the devices of User1, User3, and User4, who are members of the targeted groups. B. Device3 only: This is incorrect because the policy also applies to the devices of User1, User2, and User4, who are members of the targeted groups. C. Device1, Device2, and Device5 only: This is incorrect because Device5 is not targeted as its primary user (User5) is not in Group1 or Group2.

References:

Microsoft Learn (Official Vendor Documentation): "Assign device profiles in Microsoft Intune." This document explains that when you assign a profile to a user group, the settings within that profile apply to the user on any device they enroll and sign in to. The policy

targets the user, and by extension, their devices.

URL: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign>

Microsoft Learn (Official Vendor Documentation): "Create a device profile in Microsoft Intune." This article details the process of creating and assigning profiles, confirming that assignments are made to user or device groups to apply settings.

URL: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-profiles-create>

CertEmpire

Question: 5

HOTSPOT - You have a Microsoft 365 subscription. You use Microsoft Intune Suite to manage devices. You have the iOS app protection policy shown in the following exhibit.

Access requirements

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

Conditional launch

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

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

Answer Area

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

▼

account credentials only

PIN only

PIN and account credentials

Entering the wrong PIN five times will

▼

block access

reset the app PIN

reset the device PIN

wipe company data

Answer:

After 30 minutes of inactivity, a user will be prompted for their: PIN and account credentials

Entering the wrong PIN five times will: reset the app PIN

Explanation:

Based on the provided iOS app protection policy settings: The Access requirements section has both PIN for access and Work or school account credentials for access set to Require. The setting Recheck the access requirements after /minutes of inactivity is configured for 30 minutes. Therefore, after 30 minutes of inactivity, the user must satisfy all the required access settings, which includes providing both their PIN and their work or school account credentials. The Conditional launch section specifies the actions taken based on certain conditions. The setting Max PIN attempts is set to 5, and the corresponding Action is explicitly defined as Reset PIN. This means that after five incorrect PIN attempts, the system will force a reset of the application PIN.

References:

Source: Microsoft Learn Official Microsoft Intune Documentation

Reference 1: iOS/iPadOS app protection policy settings - Access requirements. This document details the access settings for Intune app protection policies. It specifies that when multiple access requirements like 'PIN for access' and 'Work or school account credentials for access' are set to 'Require', and the 'Recheck the access requirements after (minutes of inactivity)' timer expires, the user will be prompted to satisfy those requirements.

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

Section: Access requirements "Recheck the access requirements after (minutes of inactivity)"

Reference 2: iOS/iPadOS app protection policy settings - Conditional launch. This

document explains the conditional launch settings. It confirms that the Max PIN attempts setting, when reached, triggers the configured action. The available actions are Reset PIN or Wipe data. The exhibit shows Reset PIN is the configured action.

URL: <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settingsios#conditional-launch>

Section: Conditional launch "App PIN" settings "Max PIN attempts"

[/apps/app-protection-policy-settings-ios#restrict-cut-copy-and-paste-between-other-apps](https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settingsios#restrict-cut-copy-and-paste-between-other-apps)

CertEmpire

Question: 6

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

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

On which devices can you apply app configuration policies?

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

Answer:

E

CertEmpire

Explanation:

Microsoft Intune supports the deployment of app configuration policies to all the operating systems listed in the table. These policies can be applied to managed apps on devices enrolled in Intune, which includes Windows 10, Android Enterprise, iOS/iPadOS, and macOS. The purpose of these policies is to pre-configure app settings for users, simplifying the app setup process. Since all four devices are enrolled in Intune, they are all capable of receiving app configuration policies for compatible applications.

Why Incorrect Options are Wrong:

A. Device2 only: This is incorrect. While Android Enterprise is a primary use case, Windows, iOS/iPadOS, and macOS also support these policies. B. Device1 and Device2 only: This is incorrect as it omits iOS/iPadOS and macOS, which are both supported platforms for app configuration policies. C. Device3 and Device4 only: This is incorrect as it omits Windows and Android Enterprise, which are also supported platforms. D. Device2, Device3, and Device4 only: This is incorrect because it excludes Windows 10, which supports app configuration policies for managed devices.

References:

1. App configuration policies for Microsoft Intune: Microsoft Learn. "App configuration policies can be used on devices that are enrolled or not enrolled in a mobile device management (MDM) solution. App configuration policies are supported on iOS/iPadOS, Android, Windows, and macOS devices."

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

2. Add app configuration policies for managed Windows devices: Microsoft Learn. "Use app configuration policies in Microsoft Intune to supply configuration settings for your Windows apps."

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

3. Add app configuration policies for managed macOS devices: Microsoft Learn. "Use app configuration policies in Microsoft Intune to provide custom configuration settings for your macOS apps."

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

4. Add app configuration policies for managed Android Enterprise devices: Microsoft Learn. "This article describes how to create an app configuration policy for managed Android Enterprise devices."

URL:

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

CertEmpire

Question: 7

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

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

All devices contain an app named App1 and are enrolled in Microsoft Intune. You need to prevent users from copying data from App1 and pasting the data into other apps. Which type of policy and how many policies should you create in Intune? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

▼

App configuration policy

App protection policy

Conditional access policy

Device compliance policy

Minimum number of policies:

▼

1

2

3

4

5

Answer:

Policy type: App protection policy Number of policies: 3

Explanation:

App Protection Policies (APP) are used to manage and protect organizational data within an application. A key feature of APP is restricting data transfer actions, such as cut, copy, and paste, from managed applications like App1 to unmanaged applications. This directly addresses the requirement to prevent data leakage. Because App Protection Policies are platform-specific, a separate policy must be created for each operating system. The scenario includes devices running Windows, iOS, and Android. Therefore, three distinct App Protection Policies are required: one for Windows, one for iOS, and one for Android.

References:

1. Microsoft Learn App protection policies overview: "App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app... You can create app protection policies for apps running on devices that are... Enrolled in Intune... You create app protection policies for either iOS/iPadOS, Android, or Windows apps." This confirms that APP is the correct policy type and that policies are created per platform.

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

2. Microsoft Learn How to create and assign app protection policies: The procedural steps for creating a policy begin with selecting a platform: "In the Microsoft Intune admin center, select Apps App protection policies Create policy and select a platform for your policy." This demonstrates that a separate policy is necessary for each of the three platforms (Windows, iOS, Android) in the scenario.

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

3. Microsoft Learn App protection policy settings for Android/iOS/Windows: The documentation details specific data protection settings, including "Restrict cut, copy, and paste between other apps." This setting is available for each platform, confirming its use to meet the requirement.

Android: <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settingsandroid#data-protection>

iOS: <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settingsios#data-protection>

Windows: <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policysettings-windows#data-protection>

Question: 8

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

Answer:

D

Explanation:

Microsoft Intune allows for the creation of dependencies for Win32 apps to control the installation order. To ensure App1 is installed before App2, you must edit the properties of App2 and configure App1 as a dependency. This setting instructs the Intune Management Extension on the client device to verify that the dependent app (App1) is successfully installed before it begins the installation of the parent app (App2). This is the designated feature for managing installation prerequisites between Win32 applications.

Why Incorrect Options are Wrong:

A. the App1 deployment configurations: The configuration for App1 defines its own installation and requirements, but it cannot dictate the behavior or prerequisites of other applications like App2. B. a dynamic device group: A dynamic group is used for targeting assignments based on device properties (e.g., OS version, model). It does not control the sequence of application installations. C. a detection rule: A detection rule is configured for an app to determine if that specific app is already present on a device. It does not check for the presence of other prerequisite apps.

References:

Microsoft Learn. (2024). Win32 app management in Microsoft Intune. Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-appmanagement#add-win32-app-dependencies>

This document explicitly states, "When you deploy a Win32 app, you can specify other apps that must be installed before your Win32 app is installed. This feature is called dependencies... You configure the dependency relationship when you are adding or editing

<https://certempire.com>

a Win32 app." This confirms the setting is on the app that has the dependency (App2).

CertEmpire

Question: 9

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

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

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

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

CertEmpire

Answer:

B

Explanation:

Microsoft Intune applies app configuration policies based on the device's operating system (OS) platform. The policies for different OS platforms, such as iOS/iPadOS and Android, are not interchangeable. To manage the same application (App1) across different OS types, a separate app configuration policy must be created for each platform. In this scenario, the devices belong to two distinct OS platforms: 1. Android: Device1 (Android 8.1.0) and Device2 (Android 9). 2. iOS: Device3 (iOS 11.4.1), Device4 (iOS 12.3.1), and Device5 (iOS 12.3.2). Therefore, a minimum of two separate policies are required: • One policy targeting the Android platform to manage App1 on Device1 and Device2. • A second policy targeting the iOS/iPadOS platform to manage App1 on Device3, Device4, and Device5.

Why Incorrect Options are Wrong:

A: 1: This is incorrect. A single app configuration policy cannot be applied to both Android and iOS/iPadOS devices simultaneously. Intune requires platform-specific policies. C: 3, D: 4, and E: 5: These options are incorrect because Intune does not require a separate policy for each device

or for each minor version of an operating system. A single policy for a specific platform (like iOS/iPadOS) can target all devices running that OS, regardless of the version.

References:

Microsoft Learn: App configuration policies for Microsoft Intune.

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

Reference: In the "Create an app configuration policy" section, it states, "App configuration policies can be created and assigned for a specific app. When you create the policy, you'll associate it with a specific app... you'll also assign the policy to groups of users and/or devices." The platform-specific nature is detailed in the linked articles for iOS and Android.

Microsoft Learn: Add app configuration policies for managed iOS/iPadOS devices.

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

Reference: Step 3 in the "Create an app configuration policy" section explicitly requires selecting iOS/iPadOS for the Platform. This demonstrates that the policy is specific to this OS.

Microsoft Learn: Add app configuration policies for managed Android Enterprise devices.

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

Reference: Step 3 in the "Create a new app configuration policy from the Apps pane" section requires selecting Android Enterprise for the Platform. This confirms a separate policy type is needed for Android devices.

CertEmpire

Question: 10

DRAG DROP - You have a Microsoft 365 E5 subscription and a computer that runs Windows 11. You need to create a customized installation of Microsoft 365 Apps for enterprise. Which four actions should you perform in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Actions

Run `setup.exe` and specify the `/packager` switch.

Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.

Edit the XML configuration file.

Run `setup.exe` and specify the `/download` switch.

Run `setup.exe` and specify the `/configure` switch.

Answer Area

1

2

3

4



Answer:

Actions

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

Answer Area

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

Actions

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

Answer Area

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

Explanation:

The deployment of Microsoft 365 Apps using the Office Deployment Tool (ODT) follows a logical, multi-step process. Download the ODT: The first step is to acquire the necessary toolset from the Microsoft Download Center. Running the self-extracting file unpacks the setup.exe executable and sample configuration.xml files. Edit the XML file: To customize the installation, you must

modify the configuration.xml file. This file dictates which products and languages to install, the update channel, architecture (32-bit or 64-bit), and other deployment settings. Download Installation Files: Next, you run `setup.exe /download`. This command reads the configuration file and downloads the necessary source files from the Office Content Delivery Network (CDN) to the location specified in the XML. This step allows you to stage the installation files on a local network share. Configure (Install) Apps: The final step is to run `setup.exe /configure` on the client computers. This command uses the settings in the XML file and the previously downloaded source files to install Microsoft 365 Apps. Incorrect Options: Run `setup.exe` and specify the `/packager` switch: This switch is used to create an App-V package for virtualized environments. It is not part of the standard Click-to-Run installation workflow that is implied by the other steps. The `/packager` mode is a distinct function of the ODT for a different deployment scenario.

References:

Microsoft Documentation: "Deploy Microsoft 365 Apps with the Office Deployment Tool". This official guide explicitly outlines the procedure.

URL: <https://learn.microsoft.com/en-us/deployoffice/officedeploymenttool-microsoft-365apps>

Reference: Review the sections "Step 1: Download the Office Deployment Tool," "Step 2: Create the configuration file," "Step 3: Download the installation files for Microsoft 365 Apps," and "Step 4: Install Microsoft 365 Apps." These sections directly correspond to the correct answer sequence.

Microsoft Documentation: "Overview of the Office Deployment Tool". This document provides a summary of the ODT's purpose and modes.

URL: <https://learn.microsoft.com/en-us/deployoffice/overview-office-deployment-tool>

Reference: The section "Download and install Microsoft 365 Apps" describes the two main modes: `/download` and `/configure`. The section "ODT command line" lists `/packager` as a separate mode used to "create an App-V package."

Question: 11

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

Answer:

B

Explanation:

To deploy a custom line-of-business (LOB) app to iOS or iPadOS devices using Microsoft Intune, the app package file must be in the .ipa format. This is the standard application archive file used by Apple's iOS operating system. Intune specifically requires this file type to be uploaded to the admin center for distribution to managed iOS devices. The other file extensions listed are for different operating systems and are incompatible with iOS.

CertEmpire

Why Incorrect Options are Wrong:

A. .intunemac: This file extension is used for wrapping and deploying line-of-business apps to macOS devices, not iOS devices. C. .apk: This is the Android Package Kit file format used for distributing and installing apps on Android devices. D. .appx: This is the application package format used for distributing and installing apps on modern Windows platforms (Windows 10/11).

References:

Microsoft Learn. (2024). Add an iOS/iPadOS line-of-business app to Microsoft Intune.

Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/mem/intune/apps/lobapps-ios>

Quote: "When you add a line-of-business (LOB) app to Microsoft Intune, you use the Microsoft Intune admin center. You upload the LOB app to Intune by first selecting the app package file (extension .ipa)."

Question: 12

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

Answer:

E

Explanation:

To block legacy authentication, the Client apps condition must be used in the Conditional Access policy. This condition allows administrators to distinguish between applications that use modern authentication and those that use legacy protocols (e.g., POP3, SMTP, IMAP, MAPI over HTTP). By configuring the policy to target "Legacy authentication clients" under the Client apps condition and setting the access control to "Block," you can specifically prevent these older, less secure sign-in methods for App1, while still permitting modern authentication.

Why Incorrect Options are Wrong:

A. Filter for devices: This condition targets devices based on their attributes (e.g., model, OS version), not the authentication protocol being used. B. Device platforms: This condition targets the device's operating system (e.g., Windows, iOS), not the specific authentication method. C. User risk: This condition is part of Microsoft Entra ID Protection and targets users whose identities are suspected to be compromised, not the authentication protocol. D. Sign-in risk: This condition, also from ID Protection, evaluates the real-time risk of a sign-in attempt, but it does not directly filter by authentication type.

References:

1. Microsoft Entra documentation, "Conditional Access: Conditions": This document details the available conditions. For "Client apps," it states, "This condition allows a Conditional Access policy to target specific client applications... Due to their risk, you might choose to

apply a policy to legacy authentication clients."

URL: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/conceptconditional-access-conditions#client-apps>

2. Microsoft Entra documentation, "Common Conditional Access policy: Block legacy authentication": This guide provides a step-by-step tutorial for creating a policy to block legacy authentication, explicitly using the "Client apps" condition.

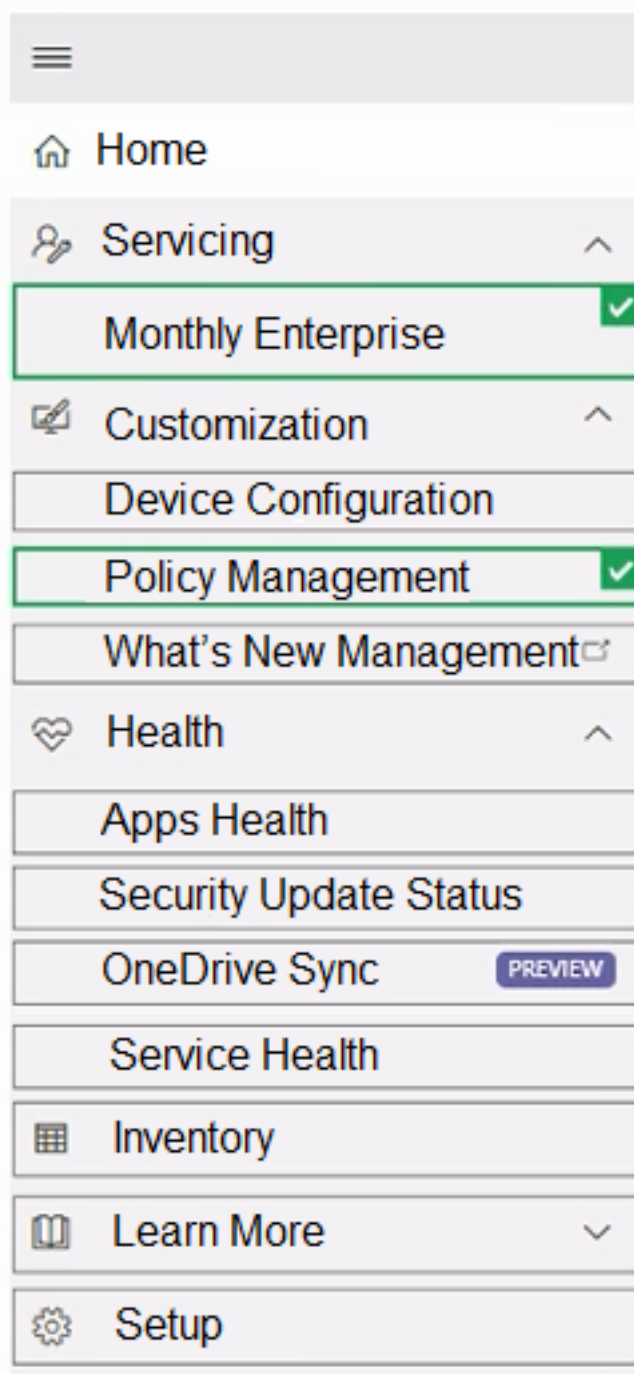
URL: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditionalaccess-policy-block-legacy>

CertEmpire

Question: 13

HOTSPOT - All users have Microsoft 365 apps deployed. You need to configure Microsoft 365 apps to meet the following requirements: Enable the automatic installation of WebView2 Runtime. Prevent users from submitting feedback. Which two settings should you configure in the Microsoft 365 Apps admin center? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Automatically install WebView2 Runtime: On Allow users to submit feedback: Off

Explanation:

To meet the specified requirements using the Microsoft 365 Apps admin center, you must configure two specific policy settings. First, to ensure WebView2 Runtime is installed automatically, the "Automatically install WebView2 Runtime" setting must be enabled by setting it to "On". This component is necessary for modern add-ins and features within Microsoft 365 Apps. Second, to prevent users from sending feedback to Microsoft through the applications, the "Allow users to submit feedback" policy must be disabled by setting it to "Off". This removes the feedback submission functionality from the user interface of the Office applications.

References:

1. Microsoft Learn: Overview of cloud policy service for Microsoft 365. This document explains how to use the Microsoft 365 Apps admin center to create and manage app configuration policies.

URL: <https://learn.microsoft.com/en-us/deployoffice/admincenter/overview-cloud-policy>

2. Microsoft Learn: Use policy settings to manage privacy controls for Microsoft 365 Apps for enterprise. This source details the "Allow users to submit feedback" policy, confirming that disabling it prevents users from submitting feedback.

URL: <https://learn.microsoft.com/en-us/deployoffice/privacy/manage-privacycontrols#policy-setting-for-allowing-users-to-submit-feedback>

3. Microsoft Learn: Microsoft Edge WebView2 and Microsoft 365 Apps. This document explains that WebView2 is automatically installed with Microsoft 365 Apps, but its installation can be managed by an administrator. The "Automatically install WebView2 Runtime" policy in the cloud policy service directly controls this behavior.

URL: <https://learn.microsoft.com/en-us/deployoffice/webview2-install#managing-thewebview2-runtime-installation>

Question: 14

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.

Answer:

D

Explanation:

To deploy software to devices managed by Microsoft Intune, the correct procedure is to use the "Apps" workload within the Microsoft Intune admin center. Intune has a specific, built-in app type named "Microsoft 365 Apps for Windows 10 and later" designed for this exact purpose. This allows an administrator to configure the application suite, select which apps to install (e.g., Word, Excel), choose the update channel, and then assign the deployment to specific groups of users or devices.

Why Incorrect Options are Wrong:

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.

References:

1. Microsoft Intune Documentation. "Add Microsoft 365 apps to Windows 10/11 devices with Microsoft Intune." This official guide explicitly states, "You can use Intune to add Microsoft 365 apps to Windows 10/11 devices." The procedure begins in the Microsoft Intune admin center by navigating to Apps All apps Add.

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

2. Microsoft Intune Documentation. "What are Microsoft Intune device profiles?" This document clarifies that device profiles are used to "add and configure settings" for devices, distinguishing them from application deployment.

URL: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-profiles>

3. Microsoft Entra Documentation. "Quickstart: Register an application with the Microsoft identity platform." This document describes the purpose of app registration, which is unrelated to software deployment via MDM.

URL: <https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app>

<https://certempire.com>

Question: 15

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

Answer:

B

Explanation:

The Retire action is the correct choice because it is specifically designed to remove company data and apps provisioned by Intune while leaving the user's personal data, user-installed applications, and OEM-installed apps untouched. When the Retire action is initiated for an offline device, the command is queued. The next time the device connects to the internet and checks in with the Intune service, it will process the command, unenroll from Intune, and remove the managed content. This directly meets all the requirements of the scenario.

Why Incorrect Options are Wrong:

A. a Delete action: While the Delete action also removes the device from Intune management and can trigger a retire, the Retire action is more specific to the described data handling requirements. C. a Fresh Start action: This action removes all installed applications (including user-installed ones), which contradicts the requirement to retain them. It is used to return a device to a clean state. D. an Autopilot Reset action: This action resets the device to a business-ready state but explicitly keeps it managed by Intune and enrolled in Azure AD, which is the opposite of the goal.

References:

Microsoft Learn. (2024). Retire devices from Intune management. "The Retire action removes managed app data, settings, and email profiles that were assigned by using Intune... Retirement leaves the user's personal data on the device." URL:

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

Microsoft Learn. (2024). Remove devices by using wipe, retire, or manually unenrolling the device. "Retire: Removes managed app data... The device is removed from Intune

<https://certempire.com>

management. This action leaves the user's personal data on the device." URL:

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

Microsoft Learn. (2024). Use Fresh Start to reset Windows 10/11 devices with Intune. "The Fresh Start device action removes any apps that are installed on a PC running Windows 10, version 1709 or later and Windows 11." URL:

<https://learn.microsoft.com/enus/mem/intune/remote-actions/device-fresh-start>

Microsoft Learn. (2024). Reset devices with Windows Autopilot Reset. "Windows Autopilot Reset takes the device back to a business-ready state... It maintains the device's identity connection to Azure AD and its management connection to Intune." URL:

<https://learn.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset>

CertEmpire

Question: 16

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

Answer:

D

Explanation:

Endpoint analytics, a feature within the Microsoft Intune product family, is specifically designed to provide insights into the performance and health of managed endpoints. It includes dedicated reports for Startup performance, which analyzes boot and sign-in times, and tracks restart frequencies to help identify devices with abnormal restart patterns. This allows administrators to proactively identify and resolve issues that impact user productivity, directly addressing the requirements of the question.

CertEmpire

Why Incorrect Options are Wrong:

A. Azure Monitor: This is a broad monitoring service for Azure resources and applications. It is not the specialized tool for analyzing detailed endpoint performance metrics like startup times within Intune. B. Intune Data Warehouse: This service stores historical Intune data for custom reporting and trend analysis, but it is not the primary, built-in tool for real-time performance analytics and proactive insights. C. Microsoft Defender for Endpoint: This is an endpoint security platform focused on threat detection and response (EDR), not on measuring and improving device performance metrics like startup times.

References:

1. Microsoft Learn. (2024). What is Endpoint analytics? "Endpoint analytics is part of Microsoft Intune. The service provides insights and intelligence for you to make informed decisions about the health and performance of your Windows endpoints... Key features include scores and insights for Startup performance..."

URL: <https://learn.microsoft.com/en-us/mem/analytics/overview>

2. Microsoft Learn. (2024). Startup performance in Endpoint analytics. "The Startup performance score helps IT get users from power-on to productivity quickly, without lengthy boot and sign-in delays."

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

3. Microsoft Learn. (2024). Device restarts in Endpoint analytics. "The restart frequency metric in Endpoint analytics helps IT admins find devices that are having restart issues. An abnormal restart can indicate a problem with the device..."

URL: <https://learn.microsoft.com/en-us/mem/analytics/device-restarts>

CertEmpire

Question: 17

HOTSPOT - You have a Microsoft 365 E5 subscription. You create a new update rings policy named Policy1 as shown in the following exhibit.

Update ring settings [Edit](#)

Update settings

Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Servicing channel	General Availability channel
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

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

Answer Area

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

▼

can be deferred indefinitely

can be deferred for 30 days

will be installed immediately

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

▼

1 day

30 days

60 days

Answer:

Updates that contain fixes and improvements to existing Windows functionality will be installed immediately. Updates that contain new Windows functionality will be installed within 60 days of release.

Explanation:

Updates with fixes and improvements are known as Quality Updates. The policy shows the Quality update deferral period (days) is set to 0. Additionally, the Deadline for quality updates is also set to 0 days. A zero-day deadline enforces the installation of the update as soon as the device checks in. Therefore, these updates are installed immediately upon availability. Updates with new functionality are known as Feature Updates. The policy configures a Feature update deferral period (days) of 30. This means the update will not be offered to the device until 30 days after Microsoft releases it. After this deferral period, a Deadline for feature updates of 30 days begins. The total time from the update's release until the mandatory installation is the sum of the deferral period and the deadline period ($30 + 30 = 60$ days).

References:

1. Microsoft Learn: This official documentation details the settings for Windows Update rings in Intune. It explains that a deadline starts after the update is first offered to a device, which happens after any configured deferral period.

Source: Microsoft, "Update rings for Windows 10 and later policy in Intune". Sections on "Feature update deferral period", "Quality update deferral period", and "Use deadline settings".

URL: <https://learn.microsoft.com/en-us/mem/intune/protect/update-rings-for-windows-10and-later>

2. Microsoft Learn (Windows Update for Business): This document clarifies how deferral and deadline policies work together. It specifies that the deadline compliance clock starts when the update is offered, which is determined by the deferral policy.

Source: Microsoft, "What is Windows Update for Business?". Section on "Deadlines".

URL: <https://learn.microsoft.com/en-us/windows/deployment/update/waas-manageupdates-wufb#deadlines>

CertEmpire

Question: 18

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

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

Which events are collected in the Log Analytics workspace?

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

Answer:

CertEmpire

E

Explanation:

The configuration specifies collecting "all available events from the Windows event logs." The Windows event logging system includes both standard logs (Application, Security, System) and Applications and Services Logs. The AppLocker log (Microsoft-Windows- AppLocker/EXE and DLL) is part of the Applications and Services Logs. A policy to collect "all available events" implies a comprehensive data collection rule that ingests events from all log sources on the endpoint, not just the default ones. Therefore, events from the Application, Security, System, and the specified AppLocker log will all be collected by the Log Analytics workspace.

Why Incorrect Options are Wrong:

A: This is incorrect because the collection policy is for all logs, not just the Application log. The System and Security logs are also standard logs that would be included. B: This is incorrect as it omits the Application log, which is a standard log, and the AppLocker log, which is included under the "all available" policy. C: This is incorrect as it omits the Security log, a standard log, and the AppLocker log, which is covered by the comprehensive collection policy. D: This is incorrect because it omits the System log (Event 3), which is a standard Windows event log and would be

included in any comprehensive collection strategy.

References:

1. Microsoft Documentation: Collect events and performance counters from virtual machines with Azure Monitor Agent. This document explains that Data Collection Rules (DCRs) are used to specify which event logs to collect. You can specify any log by name, including standard logs and those under Applications and Services. A configuration for "all available events" would be set up to include all these sources.

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

2. Microsoft Documentation: Windows Event Log. This documentation outlines the structure of Windows Event Logs, clarifying that it includes categories like "Windows Logs" (containing Application, Security, System) and "Applications and Services Logs" (containing logs like AppLocker). This confirms all four logs in the question are part of the "Windows event logs" system.

URL: <https://learn.microsoft.com/en-us/windows/win32/wes/windows-event-log>

CertEmpire

Question: 19

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

Answer:

D

Explanation:

To configure an Android Enterprise device to operate in a single-app kiosk mode, an administrator must create a device restrictions profile in Microsoft Intune. Within the configuration settings of this profile, the Device experience category contains the necessary options. Specifically, the "Dedicated device" setting is found here, which can be configured for "Single app" mode to lock the device to a specific application, effectively turning it into a kiosk. CertEmpire

Why Incorrect Options are Wrong:

A. Users and Accounts: This section manages settings related to user account management, such as adding or removing accounts, not the device's operational mode. B. General: This section contains broad device restrictions like disabling the camera or screen capture, but it does not include the primary kiosk mode configuration. C. System security: This section is focused on security policies such as password requirements, encryption, and Google Play Protect, not on locking down the user interface.

References:

Microsoft Learn: "Android Enterprise device settings to allow or restrict features using Intune". This official documentation details the configuration settings for Android Enterprise device restriction profiles. Under the "Device experience" section for Fully Managed, Dedicated, and Corporate-Owned Work Profile devices, it lists the "Dedicated device" setting, which is used to configure single-app or multi-app kiosk mode.

URL: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictionsandroid-enterprise#device-experience>

Question: 20

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.

Answer:

D

Explanation:

To apply and manage Microsoft Defender for Endpoint antivirus policies on macOS devices via Microsoft Intune, the standard and most direct method is to create a configuration profile. Using the Settings Catalog in the Microsoft Intune admin center, administrators can configure a wide range of Defender for Endpoint settings, such as real-time protection, threat and virus protection, and exclusions. This profile is then deployed to the targeted group of macOS devices, allowing for centralized management and enforcement of antivirus policies with minimal administrative effort.

Why Incorrect Options are Wrong:

A: The Microsoft Purview compliance portal is primarily for data governance, risk, and compliance management, not for configuring and deploying endpoint antivirus policies. B: Security baselines in Microsoft Intune are pre-configured security settings templates that are only available for Windows devices and Microsoft Edge, not for macOS. C: Installing the Defender for Endpoint agent is a necessary prerequisite. However, the installation itself does not apply or configure the specific antivirus policies; it only enables the device to receive them.

References:

1. Microsoft Learn. "Set preferences for Microsoft Defender for Endpoint on macOS." This document explicitly states, "In Microsoft Intune, you can create a device configuration profile to set Microsoft Defender for Endpoint settings for macOS devices... Use the Settings catalog to configure Microsoft Defender for Endpoint on macOS."
URL: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/macpreferences?view=o365-worldwide>
2. Microsoft Learn. "Create a device profile in Microsoft Intune." This guide details the process of creating configuration profiles, including using the Settings Catalog, which is the recommended method for configuring Defender on macOS.

URL: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-profiles-create>

3. Microsoft Learn. "Use security baselines to configure Windows devices in Intune." This source confirms that security baselines apply to Windows 10/11 and Microsoft Edge, not macOS.

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

CertEmpire

Question: 21

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.

- 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.

CertEmpire

Answer:

C, E

Explanation:

For Azure AD joined and Intune-managed devices, the most efficient method to configure security settings is by using Microsoft Intune's configuration profiles. The Endpoint protection profile template is specifically designed for this purpose. It provides a centralized location within the Intune console to configure settings for both Microsoft Defender Antivirus (e.g., real-time protection, scan settings, exclusions) and Microsoft Defender Firewall (e.g., domain, private, and public network rules). Using this single profile type for both components streamlines administration, fulfilling the requirement to minimize administrative effort.

Why Incorrect Options are Wrong:

References: 1. Microsoft Learn Windows 10/11 (and later) settings to protect devices using Intune: This official documentation details the settings available in an Endpoint Protection device configuration profile. It explicitly lists "Microsoft Defender Firewall" and "Microsoft Defender Antivirus" as categories that can be configured using this profile type. URL: <https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10> 2. Microsoft Learn Overview of device profiles in Microsoft Intune: This document explains that device

configuration profiles are the primary tool in Intune for managing settings and features on devices. It distinguishes between different profile types, reinforcing that "Endpoint protection" is the correct template for security components. URL:

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profiles>

References:

1. Microsoft Learn Windows 10/11 (and later) settings to protect devices using Intune: This official documentation details the settings available in an Endpoint Protection device configuration profile. It explicitly lists "Microsoft Defender Firewall" and "Microsoft Defender Antivirus" as categories that can be configured using this profile type.

URL: <https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10>

2. Microsoft Learn Overview of device profiles in Microsoft Intune: This document explains that device configuration profiles are the primary tool in Intune for managing settings and features on devices. It distinguishes between different profile types, reinforcing that "Endpoint protection" is the correct template for security components.

URL: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-profiles>

Question: 22

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

Answer:

A

Explanation:

An Intune device-configuration profile is delivered only to the Azure AD groups that are included in its Assignments. By editing Profile1's Assignments and either 1) including a group that contains only Device1 or 2) excluding a group that contains Device2, the profile will target Device1 alone. No other fields (settings, scope tags, applicability rules) change which individual devices receive the profile.

Why Incorrect Options are Wrong:

B. Settings " alters the configuration that is applied, not the set of devices that receive it. C. Scope (Tags) " limit admin visibility; they do not influence profile deployment to devices. D. Applicability Rules " filter by OS edition/version/ownership, not by specific device objects such as Device1.

References:

1. Microsoft Intune documentation Assign device profiles " include and exclude groups:
<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#useinclude-and-exclude-groups>
2. Microsoft Intune documentation Scope tags:
<https://learn.microsoft.com/enus/mem/intune/fundamentals/scope-tags>
3. Microsoft Intune documentation Applicability rules for device profiles:
<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-apply>

Question: 23

Your network contains an on-premises Active Directory domain and an Azure AD tenant. The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

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

You need to migrate the existing Default Domain Policy GPO settings to a device configuration profile. Which device configuration profile type template should you use?

- A. Administrative Templates
- B. Endpoint protection
- C. Device restrictions
- D. Custom

CertEmpire

Answer:

C

Explanation:

The Device restrictions profile template in Microsoft Intune is the correct choice for migrating the specified Group Policy settings. This template provides a dedicated "Password" section that allows administrators to configure the exact settings shown in the GPO, such as password complexity, minimum length, maximum age (expiration), and history. Using this template is the most direct and intended method for managing these specific device-level security policies in Intune, providing a clear user interface that maps directly to the legacy GPO settings.

Why Incorrect Options are Wrong:

A. Administrative Templates: This profile type is used for configuring ADMX-backed policies, which correspond to the "Administrative Templates" section in GPO, not the "Security Settings Account Policies" section. B. Endpoint protection: This profile is for configuring security features like Microsoft Defender Antivirus, BitLocker encryption, and firewalls, not for user account password policies. D. Custom: A custom profile using OMA-URLs is a valid but more complex method. It should only be used when a setting is not available in a standard template, which is not

the case here.

References:

1. Microsoft Intune Documentation - Device restrictions settings for Windows 10/11: This document explicitly lists the password settings available within the Device Restriction profile, which directly match the GPO settings in the question.

URL: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictionswindows-10#password>

Relevant Section: "Password" section details settings for Password, Minimum password length, Password expiration (days), and Number of previous passwords to prevent reuse.

2. Microsoft Intune Documentation - Use Windows 10/11 templates to configure Group Policy settings: This source clarifies that Administrative Templates in Intune are for configuring ADMX-backed GPO settings, differentiating them from other policy types.

URL:

<https://learn.microsoft.com/en-us/mem/intune/configuration/administrative-templateswindows>

Relevant Section: Overview section explaining the purpose of Administrative Templates.

3. Microsoft Intune Documentation - Endpoint security policies in Microsoft Intune: This document outlines the purpose of Endpoint security policies, showing they are focused on threat protection components like Antivirus and Firewall, not account password policies.

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

Relevant Section: "Manage security policies" table, which lists policy types like Antivirus, Disk encryption, and Firewall.

Question: 24

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.

- 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

Answer:

C, D, E

Explanation:

The Log Analytics (LA) agent for Windows can be configured to ingest three native data classes:

1. Windows performance counters " e.g., Processor(Total)\% Processor Time, which yields average CPU utilisation (C).
2. Windows event logs " the agent supports Application and System channels, so System- level Error events are collectible (D).
3. Custom text-based log files " LATMs Custom Logs feature lets you ingest any third-party application log stored as a text file (E).

The agent does not natively inventory running processes, and Windows Security-audit (failure) events require the separate Microsoft Sentinel/Defender connector, not the base LA configuration.

Why Incorrect Options are Wrong:

A. Security-audit failures need Sentinel/Defender; the base LA event-log data source cannot be configured for the Security channel. B. Listing processes/execution times is only available when the optional VM Insights/Service Map solution is added, not from the default agent.

References:

1. Microsoft Azure Monitor " Windows event logs (System, Application supported; Security not supported)
<https://learn.microsoft.com/azure/azure-monitor/agents/agent-data-sources#event-logs>
2. Microsoft Azure Monitor " Windows Performance Counters
<https://learn.microsoft.com/azure/azure-monitor/agents/agent-data-sources#performancecounters>
3. Microsoft Azure Monitor " Collect custom logs (text files) from Windows and Linux
<https://learn.microsoft.com/azure/azure-monitor/agents/data-sources-custom-logs>
4. Microsoft Sentinel connector " Windows Security Events via AMA (required for Security log collection)

<https://learn.microsoft.com/azure/sentinel/connect-windows-security-events>

CertEmpire

<https://certempire.com>

Question: 25

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

Answer:

C

Explanation:

To onboard Windows devices to Microsoft Defender for Endpoint using Microsoft Intune, the correct and most direct method is to create an Endpoint Detection and Response (EDR) policy. This policy type is specifically designed to deploy the onboarding configuration package to targeted devices. Once applied, the policy connects the endpoint to the Defender for Endpoint service, enabling its detection, investigation, and response capabilities. This is the designated pathway within the Intune Endpoint Security workload for this specific task.

Why Incorrect Options are Wrong:

A. an attack surface reduction (ASR) policy: ASR policies are used to configure security controls on devices that are already onboarded to Defender for Endpoint, not to perform the initial onboarding. B. a security baseline: While a security baseline applies a broad set of Microsoft-recommended security settings, it is not the specific tool used for the distinct process of onboarding to Defender for Endpoint. D. an account protection policy: This policy type is used to configure identity-related security features like Windows Hello for Business or Credential Guard, not for EDR onboarding. E. an antivirus policy: Antivirus policies are used to configure the settings for Microsoft Defender Antivirus, which is distinct from onboarding the device to the broader Defender for Endpoint EDR service.

References:

1. Microsoft Learn. "Onboard devices and configure Microsoft Defender for Endpoint capabilities." This official documentation explicitly states that to onboard devices using Intune, you should create an Endpoint detection and response policy. It details the steps: "Sign in to the Microsoft Intune admin center... Select Endpoint security Endpoint

detection and response Create Policy."

URL: <https://learn.microsoft.com/en-us/microsoft-365/security/defenderendpoint/onboarding-endpoint-security-policy?view=o365-worldwide>

2. Microsoft Learn. "Endpoint detection and response policy for endpoint security in Intune."

This document describes the purpose of the EDR policy: "Use endpoint security policies for endpoint detection and response (EDR) to manage the EDR settings for your devices and to onboard devices to Microsoft Defender for Endpoint."

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

CertEmpire

Question: 26

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.

- 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.

Answer:

B, D

Explanation:

To ensure that only Android Enterprise work profile devices can enroll in Intune, you must configure two specific platform settings within an enrollment restriction policy. First, you must explicitly permit the desired enrollment method by setting Android Enterprise (work profile) to Allow. Second, you must prohibit the legacy enrollment method, Android device administrator, by setting it to Block. This combination ensures that the work profile is the only available path for Android device enrollment, fulfilling the requirement.

Why Incorrect Options are Wrong:

A: This is incorrect because blocking only personally owned devices under the Android device administrator is insufficient. It would still permit corporate-owned devices to enroll using this legacy, non-work profile method. C: This is incorrect because it allows enrollment via the legacy Android device administrator method, which directly contradicts the goal of restricting enrollment to only work profiles.

References:

1. Microsoft Learn Set enrollment restrictions in Microsoft Intune. This official documentation details the specific settings required. Under the "Create a device platform restriction" section for Android, it explicitly states: "To block Android device administrator and only allow Android Enterprise personally-owned work profiles, configure the platform settings as follows: ... Set Android device administrator to Block. Set Android Enterprise (work profile) to Allow."

URL: <https://learn.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictionsset#create-a-device-platform-restriction>

Question: 27

HOTSPOT - You have the device configuration profile shown in the following exhibit.

Kiosk ...

Windows 10 and later

✓ Basics
2 Configuration settings
③ Assignments

Configure your devices to run in kiosk mode. Before you select a kiosk mode, review your app assignments in the Mobile Apps blade. Apps that you want to run in kiosk mode should be assigned to a Windows device. [Learn more about Windows kiosk mode.](#)

Select a kiosk mode * ①

Single app, full-screen kiosk

User logon type * ①

Auto logon (Windows 10, version 1803+)

Application type * ①

Add Microsoft Edge browser

This kiosk profile requires Microsoft Edge version 87 and later with Windows 10 version 1909 and later. [Learn more about Microsoft Edge kiosk mode.](#)

Edge Kiosk URL * ①

https://contoso.com

Microsoft Edge kiosk mode type ①

Public Browsing (inPrivate)

Refresh browser after idle time ①

5

Specify Maintenance Window for App Restarts * ①

Require

Not configured

Maintenance Window Start Time

MM/DD/YYYY



h:mm:ss A

Maintenance Window Recurrence ①

Daily (recommended)

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

Answer Area

Users [answer choice]

▼

- can access any URL
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com

Windows 10 and later devices can have [answer choice]

▼

- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has multiple tabs
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

Answer:

Users can access any URL Windows 10 and later devices can have a single Microsoft Edge instance that has multiple tabs

Explanation:

The provided configuration sets up a single-app kiosk on Windows 10 devices using Microsoft Edge. The key settings determining the user experience are the Microsoft Edge kiosk mode type and the Select a kiosk mode option. User Access: The profile is set to Public Browse (InPrivate). This mode is specifically designed for public-use scenarios where users can browse the web freely. It starts at the specified URL (https://contoso.com) but, unlike the "Digital/Interactive Signage" option, it does not restrict navigation. Users can type any web address into the address bar or click any link to navigate to other sites. The session data is cleared when the browser is refreshed after the 5-minute idle time. Device State: The profile establishes a Single app, full-screen kiosk. This dedicates the device to running only one instance of the selected application, which is Microsoft Edge. The Public Browse (InPrivate) mode is explicitly documented to support multiple tabs, allowing users to open different websites simultaneously within that single browser instance.

References:

Source: Microsoft Learn Official Microsoft Documentation

Article: Configure Microsoft Edge kiosk mode

Section: In the "Configure a kiosk profile" section, under "Microsoft Edge kiosk mode type," the documentation states:

Public Browse (InPrivate): "Runs a multi-tab version of Microsoft Edge InPrivate for public Browse. Users can browse the web openly, but no Browse data is saved between sessions."

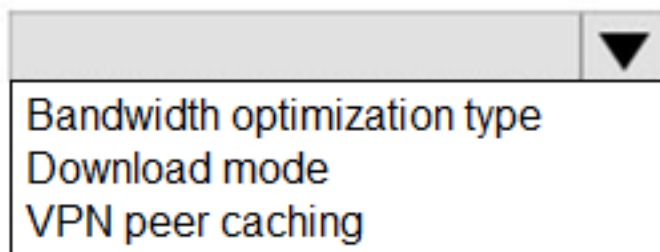
URL: <https://learn.microsoft.com/en-us/deployedge/microsoft-edge-kiosk-mode-configureintune>

Question: 28

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.

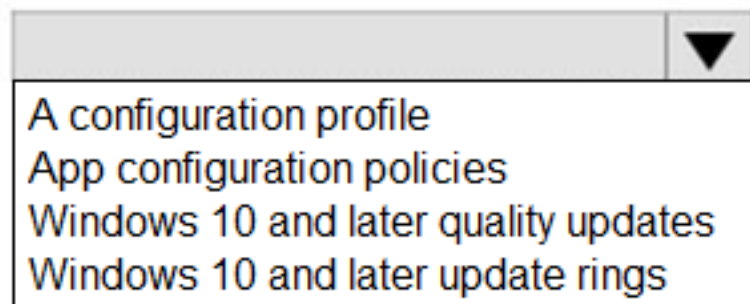
Answer Area

Delivery Optimization setting:



A dropdown menu with a grey header and a downward arrow. The menu is open, showing three options: "Bandwidth optimization type", "Download mode", and "VPN peer caching".

Intune object:



A dropdown menu with a grey header and a downward arrow. The menu is open, showing four options: "A configuration profile", "App configuration policies", "Windows 10 and later quality updates", and "Windows 10 and later update rings".

Answer:

Delivery Optimization setting: "HTTP blended with peering behind the same NAT" (Download Mode = 1)

Intune object: Windows "Device configuration profile" that uses the Delivery Optimization template

Explanation:

The requirement is to let devices obtain Windows updates both directly from Microsoft (internet) and from peers on the same local network. Delivery Optimization Download Mode = 1 (" HTTP blended with peering behind the same NAT") exactly enables downloads from Microsoft CDN plus peer-to-peer only with devices located behind the same NAT/local LAN. In Intune, Delivery Optimization settings are deployed through a Windows 10/11 Device configuration profile created with the " Delivery Optimization" template; compliance, update rings, or app policies cannot set this parameter.

References:

1. Microsoft Learn - "Configure Delivery Optimization for Windows devices in Intune", section "Download mode": value 1 = "HTTP blended with peering behind the same NAT".
<https://learn.microsoft.com/mem/intune/configuration/delivery-optimizationwindows#download-mode>
2. Microsoft Learn - same article, section "Create the policy": "In Intune, create a device configuration profile (Windows 10 and later Templates Delivery Optimization) to deploy these settings."

CertEmpire

Question: 29

HOTSPOT - You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

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

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

From Intune, you create and send a custom notification named Notification1 to Group1. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
User1 receives Notification1 on Device1.	<input type="radio"/>	<input type="radio"/>
User2 receives Notification1 on Device2.	<input type="radio"/>	<input type="radio"/>
User1 receives Notification1 on Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Statement 1: User1 receives Notification1 on Device1. Yes Statement 2: User2 receives Notification1 on Device2. No Statement 3: User1 receives Notification1 on Device3. No

Explanation:

Targeting: In Microsoft Intune, custom notifications are sent to user groups. The action specifies that Notification1 is sent to Group1. User Recipient: Based on the user table, User1 is the only user who is a member of Group1. Therefore, only User1 is targeted to receive the notification. User2 is in Group2 and will not receive the notification. Device Delivery: The notification is delivered as a push notification via the Company Portal app to the devices associated with the

targeted user. Statement 1: User1 is in the target group (Group1). The notification will be sent to User1's enrolled devices. As Device1 is also in Group1, it's implied this device is managed for User1. Thus, User1 receives the notification on Device1. Statement 2: User2 is not in the target group (Group1), so they will not receive the notification on any device. Statement 3: While User1 is the correct recipient, Device3 is a member of Group2, implying it is associated with User2. The notification follows the user to their devices. Since Device3 is not implied to be User1's device, User1 would not receive the notification on it.

References:

Microsoft Learn Microsoft Intune Documentation: "Send custom notifications in Microsoft Intune"

URL: <https://learn.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications>

Relevant Section: In the "Create a custom notification" section, Step 5 states, "On the Assignments page, select the groups you want to send this custom notification to... The notification is sent to the users of the groups you select." This confirms that the targeting is based on user membership in the selected groups.

Question: 30

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

Answer:

D

Explanation:

The Intune Data Warehouse exposes reporting data through an OData feed. Microsoft Power BI is the designated business analytics tool for connecting to this OData feed. It allows administrators to import the data warehouse model and create custom, interactive reports and dashboards, such as a detailed device inventory. This provides more advanced and customizable reporting capabilities than the built-in reports in the Microsoft Intune admin center.

CertEmpire

Why Incorrect Options are Wrong:

A. the Company Portal app: This is an end-user application for device enrollment and accessing corporate apps; it has no administrative reporting capabilities. B. Endpoint analytics: This is a specific feature within Intune for analyzing device performance and user experience, not a general-purpose tool for building custom reports from the Data Warehouse. C. the Azure portal app: This is a mobile application for managing Azure resources and does not have the business intelligence features required to connect to and visualize data from the Intune Data Warehouse.

References:

1. Microsoft Learn. (2023). Use the Microsoft Intune Data Warehouse. "With the Intune Data Warehouse, you can... Access your Intune data from your Power BI client." and "You can use the Power BI file to create reports." URL:
<https://learn.microsoft.com/enus/mem/intune/fundamentals/reports-data-warehouse>
2. Microsoft Learn. (2023). Connect to the Data Warehouse with Power BI. "You can use the Power BI App to load the data and create pre-built reports... You can also connect to the Intune Data Warehouse from the Power BI Desktop by using the OData feed URL." URL:
<https://learn.microsoft.com/en-us/mem/intune/fundamentals/reports-data-warehouseconnect-pow-erbi>

Question: 31

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 Apple 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.

Answer:

A

Explanation:

The Apple MDM Push certificate (APNs) is the foundational prerequisite for managing any Apple device (iOS, iPadOS, macOS) in Microsoft Intune. This certificate establishes a secure communication trust between Intune and the Apple Push Notification service, which is essential for sending management policies and commands to the devices. Before any enrollment profile can be created or any Apple device can be enrolled, the APNs certificate must be configured in the Intune tenant.

CertEmpire

Why Incorrect Options are Wrong:

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.

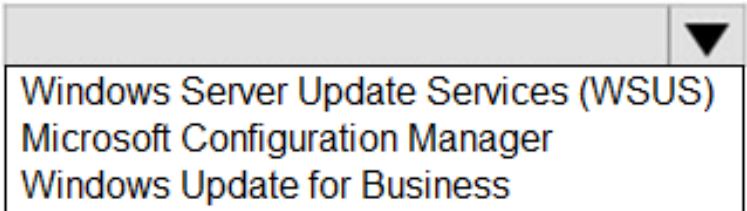
References:

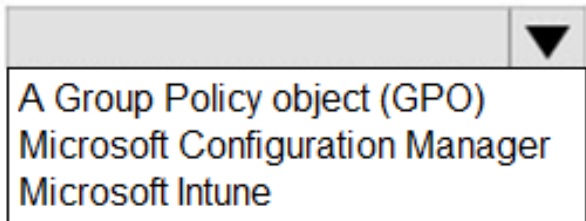
1. Microsoft Learn Get an Apple MDM push certificate for Intune: This document explicitly states, "Before you can manage iOS/iPadOS and macOS devices in Microsoft Intune, you must set up an Apple MDM Push certificate." This confirms it is the initial, required step.
URL: <https://learn.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificateget>
2. Microsoft Learn Enroll iOS/iPadOS devices by using Apple Configurator: The "Prerequisites" section of this guide lists "Apple MDM Push certificate" as the first requirement for this specific enrollment method.
URL: <https://learn.microsoft.com/en-us/mem/intune/enrollment/apple-configurator-enroll-ios>

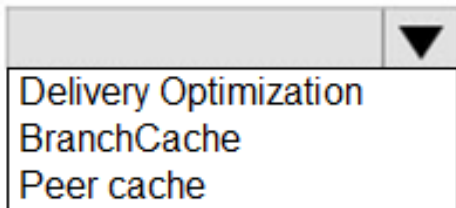
Question: 32

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.

Answer Area

Windows Update technology to use: 

Manage the configuration by using: 

Manage the traffic by using: 

Answer:

Windows Update technology to use: Windows Update for Business
Manage the configuration by using: Microsoft Intune
Manage the traffic by using: Delivery Optimization

Explanation:

Windows Update for Business (WUfB) is the appropriate technology because it's a cloud-based service that enables central management of Windows updates directly from Microsoft's servers. This approach eliminates the need for on-premises server infrastructure (like WSUS or Configuration Manager), thus minimizing costs as required by the scenario. Microsoft Intune is the correct management tool. Since all computers are joined to Azure AD, Intune (a cloud-based endpoint management solution) can be used to configure and enforce WUfB policies across all devices from a single, central console. This fulfills the central management requirement without

relying on traditional on-premises tools like Group Policy Objects (GPO), which are designed for Active Directory Domain Services. Delivery Optimization is a built-in Windows peer-to-peer technology designed specifically to reduce internet bandwidth consumption for updates. It allows computers on the same local network to share downloaded update files with each other. By enabling and configuring Delivery Optimization via Intune, only a few computers will download updates directly from the internet, and the rest will acquire them from their local peers, significantly minimizing internet traffic.

References:

Windows Update for Business & Intune: Microsoft's official documentation states, "You can use Microsoft Intune and Group Policy to configure the settings for Windows Update for Business." This confirms the use of Intune to manage WUfB policies for cloud-managed (Azure AD-joined) devices.

Source: Microsoft Learn, "Windows Update for Business deployment service"

Delivery Optimization: The documentation describes Delivery Optimization as the primary method for reducing update-related bandwidth consumption. "Delivery Optimization is a cloud-managed solution that allows clients to download source files from alternate sources (such as other peers on the network)... You can use Microsoft Intune to configure Delivery Optimization."

Source: Microsoft Learn, "What is Delivery Optimization?"

Source: Microsoft Learn, "Set up Delivery Optimization for Windows updates"

Question: 33

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

Answer:

A

Explanation:

In Microsoft Intune, a configuration profile is the correct tool for deploying detailed device settings. To meet the requirements, you would create a device configuration profile using either the "Delivery Optimization" template or the "Settings Catalog." This allows you to configure the "Download mode" to "LAN (1)" for peer-to-peer sharing on the local network and set specific bandwidth limitations, such as "Maximum download bandwidth percentage (on-battery)" and "Maximum download bandwidth percentage (plugged in)" to 50%. This approach provides the necessary granular control to satisfy all requirements directly through Intune.

Why Incorrect Options are Wrong:

B. a Windows Update for Business Group Policy setting: Group Policy is not the primary management tool for Intune-enrolled devices; using it can cause policy conflicts. Configuration profiles are the native Intune method. C. a Microsoft Peer-to-Peer Networking Services Group Policy setting: This is an incorrect and less specific Group Policy path. Delivery Optimization has its own dedicated policies, and GPOs are not the preferred method here. D. an Update ring for Windows 10 and later profile: While an update ring can set the Delivery Optimization download mode, it does not provide the granular settings needed to limit bandwidth by a specific percentage.

References:

1. Microsoft Intune Documentation - Delivery Optimization settings for Windows devices: This document explicitly details the settings available in an Intune configuration profile for Delivery Optimization, including "Download mode" and "Maximum download bandwidth percentage".

URL: <https://learn.microsoft.com/en-us/mem/intune/configuration/delivery-optimizationsettings>

2. Microsoft Intune Documentation - Create a device profile in Microsoft Intune: This guide outlines the process of creating configuration profiles, which is the mechanism used to deploy Delivery Optimization settings.

URL: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-profiles-create>

3. Microsoft Intune Documentation - Update rings for Windows 10 and later policy in Intune: This source shows the settings available in an update ring, confirming that while it includes a "Delivery optimization download mode," it lacks the specific bandwidth percentage controls required by the question.

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

CertEmpire

Question: 34

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. You have the groups shown in the following table.

Name	Type	Location
Group1	Universal distribution group	Contoso.com
Group2	Global security group	Contoso.com
Group3	Group	Computer1
Group4	Group	Computer1

Which groups can you add to Group4?

- A. Group2 only
- B. Group1 and Group2 only
- C. Group2 and Group3 only
- D. Group1, Group2, and Group3

Answer:

A

CertEmpire

Explanation:

Group4, located on Computer1, is a local group. The membership of local groups is governed by specific Active Directory and local security rules. Group2 is a Global security group from the contoso.com domain. According to standard Active Directory procedures (often summarized by the "AGLP" principle: Accounts go into Global groups, which go into Local groups, which get Permissions), global security groups can be added as members to local groups on workstations and member servers within the same domain.

Why Incorrect Options are Wrong:

Group1 (Universal distribution group): This group cannot be added to Group4. Local groups are security principals used to assign permissions. Distribution groups, like Group1, are used for email distribution lists and do not have security identifiers (SIDs) that can be used for granting permissions. Therefore, they cannot be members of local security groups. Group3 (Local group): This group also cannot be added to Group4. Windows security architecture prevents nesting one local group inside another local group on the same computer. This rule prevents circular membership and simplifies local permission management. Since Group1 and Group3 cannot be added, options B, C, and D are incorrect.

References:

Microsoft Learn Active Directory security groups:

URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understandsecurity-groups>

Reference: Under the "Group scope" section, it details what each group scope can contain.

For local groups (on workstations and member servers, not to be confused with Domain Local groups), it's stated they can contain global and universal groups. Under the "Group types" section, it clarifies that only security groups can be used to assign permissions.

Microsoft Learn Group types:

URL:

<https://learn.microsoft.com/en-us/windows/security/identity-protection/accesscontrol/group-types>

Reference: This document explicitly states, "Distribution groups are used for sending email notifications to a group of users. You can't use distribution groups to assign permissions."

This supports why Group1 is ineligible.

Microsoft Learn Default local groups:

URL: <https://learn.microsoft.com/en-us/windows/security/identity-protection/accesscontrol/default-local-groups>

Reference: This page discusses built-in local groups. The principles of local group membership apply to all local groups, including custom ones like Group4. It reinforces that local groups cannot contain other local groups.

CertEmpire

Question: 35

HOTSPOT - You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have the Windows 11 devices shown in the following table.

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

You deploy the device compliance policy shown in the exhibit. (Click the Exhibit tab.)

Basics [Edit](#)

Name	Policy1
Description	--
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

Compliance settings [Edit](#)

Device Health

Require BitLocker	Require
-------------------	---------

Actions for noncompliance [Edit](#)

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

Scope tags [Edit](#)

Default

Assignments [Edit](#)

Included groups

Group

Group1

Group3

◀ ▶

Excluded groups

Group

Group2

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

Answer Area

Statements	Yes	No
Device1 will have Policy assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 will have Policy assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 will have Policy assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Device1 will have Policy1 assigned and will be marked as compliant: Yes Device2 will have Policy1 assigned and will be marked as compliant: No Device3 will have Policy1 assigned and will be marked as compliant: No

Explanation:

Device1: Yes. The device is in Group1, which is an included group for the policy. Since Device1 has BitLocker enabled, it meets the policy's compliance requirement and will be marked as compliant. Device2: No. The device is in Group1 and Group3, both of which are included groups. The policy will be assigned to Device2. However, Device2 has BitLocker disabled, so it does not meet the compliance requirement and will be marked as noncompliant. Device3: No. The device is a member of both an included group (Group1) and an excluded group (Group2). In Microsoft Intune, exclude assignments always override include assignments. Therefore, Policy1 will not be assigned to Device3 at all, and it cannot be evaluated for compliance by this policy.

References:

Microsoft Intune Documentation - Assign user and device profiles: This document clarifies how assignments work, stating, "Exclude assignments override include assignments... If a device is in two groups, one group is in the included assignment, and the second group is in the excluded assignment, then the device is excluded and the policy isn't deployed."

Source: Microsoft Learn, "Assign user and device profiles in Microsoft Intune," section on "Include and exclude groups."

Microsoft Intune Documentation - Device compliance policies: This resource explains that for a device to be considered compliant, it must meet the rules and settings defined in the assigned policy.

Source: Microsoft Learn, "Device compliance policies in Microsoft Intune," section on "How Intune compliance policies work."