

Exam Questions MD-101

Managing Modern Desktops (beta)

<https://www.2passeasy.com/dumps/MD-101/>



NEW QUESTION 1

- (Exam Topic 1)

You need to meet the device management requirements for the developers. What should you implement?

- A. folder redirection
- B. Enterprise State Roaming
- C. home folders
- D. known folder redirection in Microsoft OneDrive

Answer: B

Explanation:

Litware identifies the following device management requirements:

➤ Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in. Enterprise State Roaming allows for the synchronization of Microsoft Edge browser setting, including favorites and reading list, across devices.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-refer>

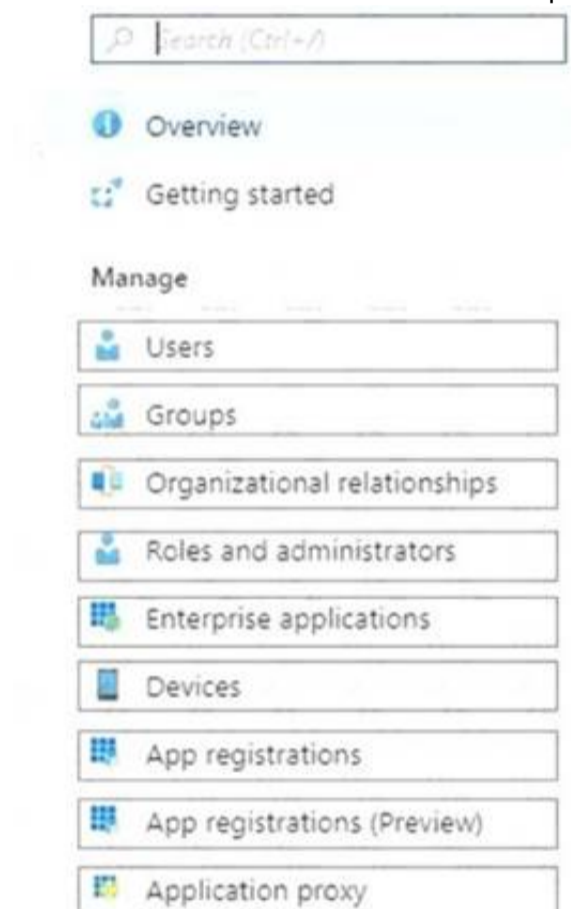
NEW QUESTION 2

- (Exam Topic 1)

You need to meet the technical requirements for Windows AutoPilot.

Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 3

- (Exam Topic 2)

You are evaluating which devices are compliant.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 is compliant	<input type="radio"/>	<input type="radio"/>
Device3 is compliant	<input type="radio"/>	<input type="radio"/>
Device4 is compliant	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device1 is compliant	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is compliant	<input checked="" type="radio"/>	<input type="radio"/>
Device4 is compliant	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 4

- (Exam Topic 2)

You need to meet the technical requirements for the IT department. What should you do first?

- A. From the Azure Active Directory blade in the Azure portal, enable Seamless single sign-on.
 B. From the Configuration Manager console, add an Intune subscription.
 C. From the Azure Active Directory blade in the Azure portal, configure the Mobility (MDM and MAM) settings.
 D. From the Microsoft Intune blade in the Azure portal, configure the Windows enrollment settings.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients>

NEW QUESTION 5

- (Exam Topic 2)

What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1 can enroll a maximum of:

<input checked="" type="checkbox"/>	5 devices
<input type="checkbox"/>	10 devices
<input type="checkbox"/>	15 devices
<input type="checkbox"/>	1,000 devices
<input type="checkbox"/>	An unlimited number of devices

User2 can enroll a maximum of:

<input checked="" type="checkbox"/>	5 devices
<input type="checkbox"/>	10 devices
<input type="checkbox"/>	15 devices
<input type="checkbox"/>	1,000 devices
<input type="checkbox"/>	An unlimited number of devices

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

User1 can enroll a maximum of:

5 devices
10 devices
15 devices
1,000 devices
An unlimited number of devices

User2 can enroll a maximum of:

5 devices
10 devices
15 devices
1,000 devices
An unlimited number of devices

NEW QUESTION 6

- (Exam Topic 2)

You need a new conditional access policy that has an assignment for Office 365 Exchange Online. You need to configure the policy to meet the technical requirements for Group4.

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

NOTE: Each correct selection is worth one point.

New

Conditions

Device state (preview)

Info

Name

PolicyA

Assignments

Users and groups

0 users and groups selected

Cloud apps

1 app included

Conditions

0 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Info

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps (preview)

Not configured

Device state (preview)

Not configured

Info

Configure

Yes No

Include

Exclude

Select the device state condition used to exclude devices from policy.

Device Hybrid Azure AD joined

Device marked as compliant

A. Mastered

B. Not Mastered

Answer: A

Explanation:

The policy needs to be applied to Group4 so we need to configure Users and Groups. The Access controls are set to Block access

Access controls
Grant
Block access

We therefore need to exclude compliant devices. From the scenario:

➤ Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Note: When a device enrolls in Intune, the device information is updated in Azure AD to include the device compliance status. This compliance status is used by conditional access policies to block or allow access to e-mail and other organization resources.

References:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions https://docs.microsoft.com/en-us/intune/device-compliance-get-started

NEW QUESTION 7

- (Exam Topic 3)

You implement the planned changes for Connection1 and Connection2

How many VPN connections will there be for User1 when the user signs in to Device 1 and Devke2? To answer select the appropriate options in the answer area.

NOTE; Each correct selection is worth one point.

Passing Certification Exams Made Easy

visit - https://www.2PassEasy.com

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Graphical user interface, table Description automatically generated

NEW QUESTION 8

- (Exam Topic 4)
You have computers that run Windows 10 and are joined to Azure Active Directory (Azure AD). All users sign in to the computers by using their Azure AD account. Enterprise State Roaming is enabled.
From the Settings app, a user named User1 adds a Microsoft account. Which account will be used for the Synchronizing Windows setting?

- A. the work account only
- B. the Microsoft account only
- C. both the Microsoft account and the work account

Answer: A

Explanation:
Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable>

NEW QUESTION 9

- (Exam Topic 4)
You have computers that run Windows 10 as shown in the following table.

Name	Configuration
Computer1	Active Directory domain-joined
Computer2	Microsoft Azure Active Directory (Azure AD) –joined
Computer3	Hybrid Microsoft Azure Active Directory (Azure AD)-joined

Computer2 and Computer3 are enrolled in Microsoft Intune.
In a Group Policy object (GPO) linked to the domain, you enable the Computer Configuration/Administrative Templates/Windows Components/Search/Allow Cortana setting.
In an Intune device configuration profile, you configure the following:

- > Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP to a value of 1
- > Experience/AllowCortana to a value of 0.

Each of the following statement, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
Computer1 can use Cortana for each.	<input type="radio"/>	<input type="radio"/>
Computer2 can use Cortana for search.	<input type="radio"/>	<input type="radio"/>
Computer3 can use Cortana for search.	<input type="radio"/>	<input type="radio"/>

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Reference:

<https://blogs.technet.microsoft.com/cbernier/2018/04/02/windows-10-group-policy-vs-intune-mdm-policy-who>

NEW QUESTION 10

- (Exam Topic 4)

Your network contains an Active Directory domain. Active Directory is synced with Microsoft Azure Active Directory (Azure AD).

There are 500 domain-joined computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune.

You plan to implement Windows Defender Exploit Guard.

You need to create a custom Windows Defender Exploit Guard policy, and then distribute the policy to all the computers.

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

NOTE: Each correct selection is worth one point.

Tool to use to configure the settings:

▼

Security & Compliance in Microsoft 365

Windows Configuration Designer

Windows Defender Security Center

Distribution method:

▼

An Azure policy

A Group Policy object (GPO)

An Intune device compliance policy

A. Mastered

B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/enable-ex>

NEW QUESTION 10

- (Exam Topic 4)

You have 500 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

You plan to distribute certificates to the computers by using Simple Certificate Enrollment Protocol (SCEP).

You have the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Root certification authority (CA)
Server3	Subordinate certification authority (CA)
Server4	Network Device Enrollment Service (NDES)

NDES issues certificates from the subordinate CA.

You are configuring a device profile as shown in the exhibit. (Click the Exhibit tab.)

You need to complete the SCEP profile.

Create profile

* Name
MD_101 ✓

Description
Enter a description... ✓

* Platform
Windows 10 and later

* Profile type
SCEP certificate

Settings
1 configured

Scope (Tags)
0 scope(s) selected

SCEP Certificate

Windows 10 and later

Certificate type
User

* Subject name format
Common name including email

Subject alternative name
2 selected

* Certificate validity period
Years 1

* Key storage provider (KSP)
Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP

* Key usage
2 selected

* Key size (bits)
2048

* Hash algorithm
SHA-2

* Root Certificate
Select a certificate

* Extended key usage

Name	Object Identifier	Predefined values	
Not configured	Not configured	Not configured	Add
Any Purpose	2.5.29.37.0		...
Client Authentication	1.3.6.1.5.5.7.3.2		...
Secure Email	1.3.6.1.5.5.7.3.4		...

- A. Server1
- B. Server2
- C. Server3
- D. Server4

Answer: D

NEW QUESTION 15

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Directory group named Group1 that contains Windows 10 Enterprise devices and Windows 10 Pro devices.

From Microsoft Intune, you create a device configuration profile named Profile1.

You need to ensure that Profile1 applies to only the Windows 10 Enterprise devices in Group1. Solution: You configure an applicability rule for Profile1. You assign Profile1 to Group1. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create>

NEW QUESTION 17

- (Exam Topic 4)

You have a Windows 10 device named Device1 that is joined to Active Directory and enrolled in Microsoft Intune.

Device 1 is managed by using Group Policy and Intune.

You need to ensure that the Intune settings override the Group Policy settings. What should you configure?

- A. a device configuration profile
- B. an MDM Security Baseline profile
- C. a device compliance policy
- D. a Group Policy Object (GPO)

Answer: A

Explanation:

Reference:

<https://uem4all.com/2018/04/02/windows-10-group-policy-vs-intune-mdm-policy-who-wins/>

NEW QUESTION 22

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains devices enrolled in Microsoft Intune. You need to create Endpoint security policies to enforce the following requirements:

- Computers that run macOS must have FileVault enabled.
- Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled.
- Computers that run Windows 10 must have Microsoft Defender Application Control enabled.

Which Endpoint security feature should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Features	Answer Area
Account protection	Computers that run macOS must have FileVault enabled: <input type="text"/>
Attack surface reduction (ASR)	Computers that run Windows 10 must have Microsoft Defender Application Control enabled: <input type="text"/>
Disk encryption	Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled: <input type="text"/>
Endpoint detection and response (EDR)	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Disk encryption

Computers that run macOS must have FileVault enabled.

Intune supports macOS FileVault disk encryption. FileVault is a whole-disk encryption program that is included with macOS. You can use Intune to configure FileVault on devices that run macOS 10.13 or later.

Box 2: Attack surface reduction (ASR)

Computers that run Windows 10 must have Microsoft Defender Application Control enabled. Attack surface reduction profiles include:

* Application control - Application control settings can help mitigate security threats by restricting the applications that users can run and the code that runs in the System Core (kernel). Manage settings that can block unsigned scripts and MSIs, and restrict Windows PowerShell to run in Constrained Language Mode.

Note: Attack surface reduction rules target certain software behaviors, such as: Launching executable files and scripts that attempt to download or run files

Running obfuscated or otherwise suspicious scripts

Performing behaviors that apps don't usually initiate during normal day-to-day work

Box 3: Account protection

Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled.

The account protection policy is focused on settings for Windows Hello and Credential Guard, which is part of Windows identity and access management.

Note: Microsoft Defender Credential Guard protects against credential theft attacks. It isolates secrets so that only privileged system software can access them.

Reference: <https://learn.microsoft.com/en-us/mem/intune/protect/encrypt-devices-filevault> <https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy> <https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

NEW QUESTION 27

- (Exam Topic 4)

You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

- MDM user scope: Group1
- MAM user scope: Group2

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference: <https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll> <https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/>

NEW QUESTION 29

- (Exam Topic 4)

You install a feature update on a computer that runs Windows 10. How many days do you have to roll back the update?

- A. 5
- B. 10
- C. 14
- D. 30

Answer: B

Explanation:

Microsoft has changed the time period associated with operating system rollbacks with Windows 10 version 1607, decreasing it to 10 days. Previously, Windows 10 had a 30-day rollback period.

References:

<https://redmondmag.com/articles/2016/08/04/microsoft-shortens-windows-10-rollback-period.aspx>

NEW QUESTION 32

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company uses Windows Autopilot to configure the computer settings of computers issued to users. A user named User1 has a computer named Computer1 that runs Windows 10.

User1 leaves the company.

You plan to transfer the computer to a user named User2.

You need to ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement.

Solution: You perform a local Windows Autopilot Reset. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 36

- (Exam Topic 4)

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains 50 Windows 10 devices.

All the devices are enrolled in Microsoft Endpoint Manager.

You discover that Group Policy settings override the settings configured in Microsoft Endpoint Manager policies.

You need to ensure that the settings configured in Microsoft Endpoint Manager override the Group Policy settings.

What should you do?

- A. From the Microsoft Endpoint Manager admin center, create an Administrative Templates device profile
- B. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy
- C. From the Microsoft Endpoint Manager admin center, create a custom device profile
- D. From Group Policy Management Editor, configure the User Configuration settings in the Default DomainPolicy

Answer: C

Explanation:

Reference:

<https://uem4all.com/2018/04/02/windows-10-group-policy-vs-intune-mdm-policy-who-wins/>

NEW QUESTION 38

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune to manage personal and corporate devices. The tenant contains three Windows 10 devices as shown in the following exhibit.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
LON-CL2	Yes	Windows	10.0.17763.615	Azure AD registered	User2	Microsoft Intune	Yes
LON-CL4	Yes	Windows	10.0.17763.107	Azure AD joined	User1	Microsoft Intune	Yes

How will Intune classify each device after the devices are enrolled in Intune automatically? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Identified by Intune as a personal device:

LON-CL2 only
 LON-CL4 only
 Both LON-CL2 and LON-CL4
 Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

LON-CL2 only
 LON-CL4 only
 Both LON-CL2 and LON-CL4
 Neither LON-CL2 or LON-CL4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Table Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join> <https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register>

NEW QUESTION 39

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to ensure that feature and quality updates install automatically during a maintenance window. Solution: From the Windows Update settings, you enable Configure Automatic Updates, select 4-Auto download and schedule the install, and then enter a time.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/sccm/sum/deploy-use/automatically-deploy-software-updates>

NEW QUESTION 40

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune to manage the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	Android Enterprise
Device4	iOS
Device5	iPadOS

You need to deploy a compliance solution that meets the following requirements:

- > Marks the devices as Not Compliant if they do not meet compliance policies
- > Remotely locks noncompliant devices

What is the minimum number of compliance policies required, and which devices support the remote lock action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Minimum number of compliance policies required:

1
2
3
4
5

Devices that support the remote lock action:

Device1 only
Device2 and Device3 only
Device4 and Device5 only
Device2, Device3, Device4, and Device5
Device1, Device2, Device3, Device4, and Device5

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application, table Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started> <https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance>

NEW QUESTION 43

- (Exam Topic 4)

Your network contains an Active Directory domain. The domain contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You have a server named Server that runs Windows Server 2019 and has the Windows Deployment Services role installed. Server1 contains an x86 boot image and three Windows 10 install images. The install images are shown in the following table.

Name	Architecture	User permission
Image1	x64	Full control: Administrators, WDSServer
Image2	x64	Full control: Administrators Read: Group1
Image3	x86	Full control: Administrators, WDSServer Read: Group2

You purchase a computer named Computer1 that is compatible with the 64-bit version of Windows 10. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can install Image1 on Computer1 by using Windows Deployment Services (WDS).	<input type="radio"/>	<input type="radio"/>
User1 can install Image2 on Computer1 by using Windows Deployment Services (WDS).	<input type="radio"/>	<input type="radio"/>
User2 can install Image3 on Computer1 by using Windows Deployment Services (WDS).	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Box 1: No

User1 is a member of Group1. User1 does not have any permission to Image1. Box 2: Yes

User1 has read permissions to Image2 through Group1. Box 3: Yes

User2 has read permissions to Image3 through Group2.

NEW QUESTION 47

- (Exam Topic 4)

You need to assign the same deployment profile to all the computers that are configured by using Windows Autopilot. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: each correct selection is worth one point.

- A. Join the computers to Microsoft Azure Active Directory (Azure AD)
- B. Assign a Windows AutoPilot deployment profile to a group
- C. Join the computers to an on-premises Active Directory domain
- D. Create a Microsoft Azure Active Directory (Azure AD) group that has dynamic membership rules and uses the operatingSystem tag
- E. Create a Group Policy object (GPO) that is linked to a domain
- F. Create a Microsoft Azure Active Directory (Azure AD) group that has dynamic membership rules and uses the ZTDID tag

Answer: BF

Explanation:

References:

<https://www.petervanderwoude.nl/post/automatically-assign-windows-autopilot-deployment-profile-to-windows>

NEW QUESTION 48

- (Exam Topic 4)

Your network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD).

You have a Microsoft 365 subscription.

You create a conditional access policy for Microsoft Exchange Online.

You need to configure the policy to prevent access to Exchange Online unless is connecting from a device that is hybrid Azure AD-joined.

Which settings should you configure?

- A. Locations
- B. Device platforms
- C. Sign-in risk
- D. Device state

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#device-state>

NEW QUESTION 53

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system builds can access network resources.

Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Settings

Require BitLocker.

Prevent jailbroken devices from having corporate access.

Prevent rooted devices from having corporate access.

Require Secure Boot to be enabled on the device.

Answer Area

Device1:

Setting

Device2:

Setting

Device3:

Setting

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1:

Device Compliance settings for Windows 10/11 in Intune

There are the different compliance settings you can configure on Windows devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating system, set a risk level using Microsoft Defender for Endpoint, and more.

Note: Windows Health Attestation Service evaluation rules Require BitLocker:

Windows BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted Platform Module (TPM) to help protect the Windows operating system and user data. It also helps confirm that a computer isn't tampered with, even if its left unattended, lost, or stolen. If the

computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can't be accessed until the TPM verifies the state of the computer.

Not configured (default) - This setting isn't evaluated for compliance or non-compliance.

Require - The device can protect data that's stored on the drive from unauthorized access when the system is off, or hibernates.

Box 2: Prevent jailbroken devices from having corporate access Device Compliance settings for iOS/iPadOS in Intune

There are different compliance settings you can configure on iOS/iPadOS devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require an email, mark rooted (jailbroken) devices as not compliant, set an allowed threat level, set passwords to expire, and more.

Device Health

Jailbroken devices

Supported for iOS 8.0 and later

Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted (jailbroken) devices as not compliant.

Box 3: Prevent rooted devices from having corporate access. Device compliance settings for Android Enterprise in Intune

There are different compliance settings you can configure on Android Enterprise devices in Intune. As part of your mobile device management (MDM) solution, use these settings to mark rooted devices as not compliant, set an allowed threat level, enable Google Play Protect, and more.

Device Health - for Personally-Owned Work Profile Rooted devices

Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted devices as not compliant.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows> <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work> <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios>

NEW QUESTION 58

- (Exam Topic 4)

Your company has a System Center Configuration Manager deployment that uses hybrid mobile device management (MDM). All Windows 10 devices are Active Directory domain-joined.

You plan to migrate from hybrid MDM to Microsoft Intune standalone. You successfully run the Intune Data Importer tool.

You need to complete the migration.

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

NOTE: Each correct selection is worth one point.

- A. In Intune, add a device enrollment manager (DEM).
- B. Change the tenant MDM authority to Intune.
- C. Assign all users Intune licenses.
- D. Create a new Intune tenant.

Answer: BC

Explanation:

References:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/migrate-hybridmdm-to-intunesa> <https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/migrate-prepare-intune> <https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/change-mdm-authority>

NEW QUESTION 63

- (Exam Topic 4)

You have computers that run Windows 10 and are managed by using Microsoft Intune. Users store their files in a folder named D:\Folder1.

You need to ensure that only a trusted list of applications is granted write access to D:\Folder1. What should you configure in the device configuration profile?

- A. Microsoft Defender SmartScreen
- B. Microsoft Defender Exploit Guard
- C. Microsoft Defender Application Guard
- D. Microsoft Defender Application Control

Answer: B

Explanation:

Reference:

<https://www.microsoft.com/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attacksurface-against-next-generation-malware/>

NEW QUESTION 67

- (Exam Topic 4)

You have 100 devices that run Windows 10 and are joined to Microsoft Azure Active Directory (Azure AD). You need to prevent users from joining their home computer to Azure AD.

What should you do?

- A. From the Device enrollment blade in the Intune admin center, modify the Enrollment restriction settings.
- B. From the Devices blade in the Azure Active Directory admin center, modify the Device settings.
- C. From the Device enrollment blade in the Intune admin center, modify the Device enrollment manages settings.
- D. From the Mobility (MDM and MAM) blade in the Azure Active Directory admin center, modify the Microsoft Intune enrollment settings.

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/intune/enrollment-restrictions-set>

NEW QUESTION 71

- (Exam Topic 4)

You have a Microsoft Intune subscription that has the following device compliance policy settings: Mark devices with no compliance policy assigned as: Compliant
Compliance status validity period (days): 14

On January 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group2

On January 4, you create the following two device compliance policies:

- > Name: Policy1
- > Platform: Windows 10 and later
- > Require BitLocker: Require
- > Mark device noncompliant: 5 days after noncompliance
- > Scope (Tags): Tag1
- > Name: Policy2
- > Platform: Windows 10 and later
- > Firewall: Require
- > Mark device noncompliant: Immediately
- > Scope (Tags): Tag2

On January 5, you assign Policy1 and Policy2 to Group1.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
On January 7, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No.

Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.

Box 2: No

For the same reason as Box1.

Box 3: Yes

Policy1 and Policy2 apply to Group1. Device2 is not a member of Group1 so the policies don't apply.

The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

NEW QUESTION 72

- (Exam Topic 4)

Your network contains an Active Directory domain named contoso.com. The domain contains 500 computers that run Windows 7. Some of the computers are used by multiple users.

You plan to refresh the operating system of the computers to Windows 10.

You need to retain the personalization settings to applications before you refresh the computers. The solution must minimize network bandwidth and network storage space.

Which command should you run on the computer? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

▼

/i MigApp.xml

dism.exe

scandisk.exe

scanstate.exe

usmtutils.exe

▼

/nocompress /ui :Contoso*

/encrypt

/genconfig.file1.xml

/hardlink

/localonly

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax#how-to-use-ui-and-ue>

NEW QUESTION 74

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune.

You use the Company Portal app to access and install published apps to enrolled devices. From the Microsoft Endpoint Manager admin center, you add a Microsoft Store app. Which two App information types are visible in the Company Portal?

Note: Each correct selection is worth one point.

- A. information URL
- B. Developer
- C. Privacy URL
- D. Owner

Answer: BC

NEW QUESTION 76

- (Exam Topic 4)

You have a Microsoft 365 tenant that contains the objects shown in the following table.

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group
Group4	Security group

In the Microsoft Endpoint Manager admin center, you are creating a Microsoft 365 Apps app named App1. To which objects can you assign App1?

- A. Admin1, Group3. and Group4 only
- B. Group1, Group2. Group3. and Group4 only
- C. Admin1, Group1, Group2. Group3, and Group4
- D. Group1, Group3, and Group4 only
- E. Group3 and Group4 only

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy>

<https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

NEW QUESTION 81

- (Exam Topic 4)

Your company has a Microsoft 365 subscription.

The company uses Microsoft Intune to manage all devices.

The company uses conditional access to restrict access to Microsoft 365 services for devices that do not comply with the company's security policies.

You need to identify which devices will be prevented from accessing Microsoft 365 services. What should you use?

- A. The Device Health solution in Windows Analytics.
- B. Windows Defender Security Center.
- C. The Device compliance blade in the Intune admin center.
- D. The Conditional access blade in the Azure Active Directory admin center.

Answer: C

NEW QUESTION 82

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company uses Windows AutoPilot to configure the computer settings of computers issued to users. A user named User1 has a computer named Computer1 that runs Windows 10. User1 leaves the company. You plan to transfer the computer to a user named User2.

You need to ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement.

Solution: You create a new Windows AutoPilot self-deploying deployment profile. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 85

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

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

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

From Intune, you create and send a custom notification named Notification1 to Group1.

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

NOTE: Each correct selection is worth one point.

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated with medium confidence

Reference:

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

NEW QUESTION 86

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD).

You have the Windows 10 devices shown in the following table.

Name	Active Directory	Endpoint Configuration Manager agent	Microsoft Intune	Azure AD
Device1	Joined	Not installed	Enrolled	Registered
Device2	Not joined	Installed	Enrolled	Registered
Device3	Not joined	Not installed	Enrolled	Joined
Device4	Joined	Installed	Not enrolled	Registered
Device5	Not joined	Installed	Not enrolled	Joined
Device6	Joined	Installed	Enrolled	Joined

You need to ensure that you can use co-management to manage all the Windows 10 devices. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Join Device 1, Device2, and Device4 to Azure AD.
- B. Unjoin Device3, Device5, and Device6 from Azure AD, and then register the devices in Azure AD.
- C. Enroll Device4 and Device5 in Intune.
- D. Join Device2, Device3, and Device5 to the domain.
- E. Install the Endpoint Configuration Manager agent on Device1 and Device3.

Answer: CE

Explanation:

Co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune.

Co-management requires Configuration Manager version 1710 or later and enrollment in Microsoft Intune. Windows 10 devices must be hybrid Azure AD joined.

Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview>

NEW QUESTION 88

- (Exam Topic 4)

Your network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The domain contains computers that run Windows 10. The computers are enrolled in Microsoft Intune and Windows Analytics.

Your company protects documents by using Windows Information Protection (WIP). You need to identify non-approved apps that attempt to open corporate

documents. What should you use?

- A. the Device Health solution in Windows Analytics
- B. Microsoft Cloud App Security
- C. Intune Data Warehouse
- D. the App protection status report in Intune

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/wip>

NEW QUESTION 89

- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune. You need to ensure that only applications that you explicitly allow can run on the computers. What should you use?

- A. Windows Defender Credential Guard
- B. Windows Defender Exploit Guard
- C. Windows Defender Application Guard
- D. Windows Defender Antivirus.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guardv based-security-and-windows-defender-application-control>

NEW QUESTION 93

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a group named Group1.

You create a Conditional Access policy named CAPolicy1 and assign CAPolicy1 to Group1.

You need to configure CAPolicy1 to require the members of Group1 to reauthenticate every eight hours when they connect to Microsoft Exchange Online. What should you configure?

- A. Session access controls
- B. an assignment that uses a User risk condition
- C. an assignment that uses a Sign-in risk condition
- D. Grant access controls

Answer: A

Explanation:

User sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.

Sign-in frequency control

- Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.
- Browse to Azure Active Directory > Security > Conditional Access.
- Select New policy.
- Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
- Choose all required conditions for customer's environment, including the target cloud apps.
- Under Access controls > Session.

Select Sign-in frequency.

Choose Periodic reauthentication and enter a value of hours or days or select Every time.

- Save your policy. Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-life>

NEW QUESTION 95

- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

You need to set a custom image as the wallpaper and sign-in screen.

Which two settings should you configure in Device restrictions? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Create profile

Name

MD_101

Description

Enter a description...

Platform

Windows 10 and later

Profile type

Device restrictions

Settings

Configure

Scope (Tags)

0 scope(s) selected

Device restrictions

Windows 10 and later

Select a category to configure settings.

App Store

13 settings available

Cellular and connectivity

15 settings available

Cloud and Storage

4 settings available

Cloud Printer

6 settings available

Control Panel and Settings

16 settings available

Display

2 settings available

General

24 settings available

Locked Screen Experience

6 settings available

Messaging

3 settings available

Microsoft Edge Browser

28 settings available

Network proxy

8 settings available

Password

13 settings available

Per-app privacy exceptions

1 setting available

Personalization

1 setting available

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Sign-in screen, or Locked screen, image is set under Locked screen experience Wallpaper image, or Desktop background picture, URL is set under Personalization. References:
<https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10>

NEW QUESTION 96

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft Intune subscription.

Contoso.com contains a user named user1@contoso.com.

You have a computer named Computer1 that runs Windows 8.1.

You need to perform an in-place upgrade of Computer1 to Windows 10.

Solution: From Windows 8.1, you run setup.exe from the Windows 10 installation media. Does this meet the goal?

- A. Yes
 B. No

Answer: A

Explanation:

Reference:

<https://www.kapilarya.com/how-to-upgrade-to-windows-10-using-iso-file>

NEW QUESTION 99

- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

You need to configure an Intune device configuration profile to meet the following requirements:

- Prevent Microsoft Office applications from launching child processes.
- Block users from transferring files over FTP.

Which two settings should you configure in Endpoint protection? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Create Profile

*Name

MD101

Description

Enter a description

*Platform

Windows 10 and later

*Profile type

Endpoint protection

Settings

Configure

Scope (Tags)

0 scope(s) selected

Endpoint protection

Windows 10 and later

Select a category to configure settings

Windows Defender Application Gu...
11 settings available

Windows Defender Firewall
40 settings available

Windows Defender SmartScreen
2 settings available

Windows Encryption
37 settings available

Windows Defender Exploit Guard
20 settings available

Windows Defender Application Co...
2 settings available

Windows Defender Application Gua...
1 setting available

Windows Defender Security Center
14 settings available

Local device security options
46 settings available

Xbox services
5 settings available

OK

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10>

NEW QUESTION 103

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

When computers start from the LiteTouchPE_x64.iso image and connect to MDT1. the welcome screen appears as shown In the following exhibit.



You need to prevent the welcome screen from appearing when the computers connect to MDT1. Which three actions should you perform in sequence? To answer move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Modify the CustomSettings.ini file.

Update the deployment share.

Modify the Bootstrap.ini file.

Replace the ISO image.

Modify the task sequence.

Answer Area

>

<

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Modify the Bootstrap.ini file.
Add this to your bootstrap.ini file and then update the deployment share and use the new boot media created in that process:
SkipBDDWelcome=YES
Box 2: Modify the CustomSettings.ini file. SkipBDDWelcome
Indicates whether the Welcome to Windows Deployment wizard page is skipped.
For this property to function properly it must be configured in both CustomSettings.ini and BootStrap.ini. BootStrap.ini is processed before a deployment share (which contains CustomSettings.ini) has been selected.
Box 3: Update the deployment share. Reference:
https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#table-6-deployment-wizard-pages

NEW QUESTION 105

- (Exam Topic 4)
You manage a Microsoft Deployment Toolkit (MDT) deployment share named DS1. OS! contains an Out-of-Box Drivers folder named Windows 10 x64 that has subfolders in the format of (make name)\ (model name).
You need to modify a deployment task sequence to ensure that all the drivers In the folder that match the make and model of the computers are installed without using PnP detection or selection profiles.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Phase that you must modify in the deployment task sequence:

Preinstall

Install

Preinstall

Validation

Task that you must use to specify which folder contains the drivers:

Inject Drivers

Gather

Inject Drivers

Set Task Sequence Variable

Validate

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Preinstall PREINSTALL

Completes any tasks that need to be done (such as creating new partitions) before the target operating system is deployed.

Box 2: Inject Drivers Inject Drivers

This task sequence step injects drivers that have been configured for deployment to the target computer.

The unique properties and settings for the Inject Drivers task sequence step type are:

* Property: TypeSet this read-only type to Inject Drivers.

* Settings

Install only matching drivers: Injects only the drivers that the target computer requires and that match what is available in Out-of-Box Drivers

Install all drivers: Installs all drivers

Selection profile: Installs all drivers in the selected profile

Reference: <https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference>

NEW QUESTION 106

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company uses Windows Update for Business.

The research department has several computers that have specialized hardware and software installed. You need to prevent the video drivers from being updated automatically by using Windows Update.

Solution: From the Device Installation and Restrictions settings in a Group Policy object (GPO), you enable Prevent installation of devices using drivers that match these device setup classes, and then you enter the device GUID.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

References:

https://www.stigviewer.com/stig/microsoft_windows_server_2012_member_server/2013-07-25/finding/WN12

NEW QUESTION 107

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company uses Windows Update for Business.

The research department has several computers that have specialized hardware and software installed. You need to prevent the video drivers from being updated automatically by using Windows Update.

Solution: From the Windows Update settings in a Group Policy object (GPO), you enable Do not include drivers with Windows Updates.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

References:

https://www.stigviewer.com/stig/microsoft_windows_server_2012_member_server/2013-07-25/finding/WN12

NEW QUESTION 109

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.

Computer1 has apps that are compatible with Windows 10.

You need to perform a Windows 10 in-place upgrade on Computer1.

Solution: You add Windows 10 startup and install images to a Windows Deployment Services (WDS) server. You start Computer1 by using WDS and PXE, and then you initiate the Windows 10 installation.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Reference: <https://docs.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios-and-tools>

NEW QUESTION 112

- (Exam Topic 4)

Your company has devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	iOS

In Microsoft Endpoint Manager, you define the company's network as a location named Location1. Which devices can use network location-based compliance policies?

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

Answer: E

Explanation:

Intune supported operating systems

Intune supports devices running the following operating systems (OS): iOS

Android Windows macOS

Note: View the device compliance settings for the different device platforms: Android device administrator

Android Enterprise iOS

macOS

Windows Holographic for Business

Windows 8.1 and later Windows 10/11

Reference: <https://docs.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers> <https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

NEW QUESTION 115

- (Exam Topic 4)

Your company has several Windows 10 devices that are enrolled in Microsoft Intune.

You deploy a new computer named Computer1 that runs Windows 10 and is in a workgroup. You need to enroll Computer1 in Intune.

Solution: From Computer1, you sign in to <https://portal.manage.microsoft.com> and use the Devices tab. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Use MDM enrolment.

MDM only enrollment lets users enroll an existing Workgroup, Active Directory, or Azure Active directory joined PC into Intune. Users enroll from Settings on the existing Windows PC.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods>

NEW QUESTION 117

- (Exam Topic 4)

You have a computer named Computer1 that runs Windows 10. Computer is used by a user named User1. You need to ensure that when User1 opens websites from untrusted locations by using Microsoft Edge,

Microsoft Edge runs in isolated container.

What should you do first?

- A. From Windows Features, turn on Windows Defender Application Guard.
- B. From Windows Security, configure the Device security settings.
- C. From Windows Security, configure the Virus & threat protection settings.
- D. From Windows Features, turn on Hyper-V Platform.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/wd-a> <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/install>

NEW QUESTION 119

- (Exam Topic 4)

You have a server named Server1 and computers that run Windows 8.1. Server1 has the Microsoft Deployment Toolkit (MDT) installed.

You plan to upgrade the Windows 8.1 computers to Windows 10 by using the MDT deployment wizard. You need to create a deployment share on Server1.

What should you do on Server1, and what are the minimum components you should add to the MDT deployment share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

On Server1:

Import the Deployment Image Servicing and Management (DISM) PowerShell module.
Import the WindowsAutopilotIntune Windows PowerShell module.
Install the Windows Assessment and Deployment Kit (Windows ADK).
Install the Windows Deployment Services server role.

Add to the MDT deployment share:

Windows 10 image and package only
Windows 10 image and task sequence only
Windows 10 image only
Windows 10 image, task sequence, and package

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Install the Windows Deployment Services role. Install and initialize Windows Deployment Services (WDS) On the server:
 Open an elevated Windows PowerShell prompt and enter the following command: Install-WindowsFeature -Name WDS -IncludeManagementTools
 WDSUTIL /Verbose /Progress /Initialize-Server /Server:MDT01 /RemInst:"D:\RemoteInstall" WDSUTIL /Set-Server /AnswerClients:All
 Box 2: Windows 10 image and task sequence only Create the reference image task sequence
 In order to build and capture your Windows 10 reference image for deployment using MDT, you will create a task sequence.
 Reference:
<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment>
<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference-im>

NEW QUESTION 123

- (Exam Topic 4)

Your company uses Microsoft Intune to manage devices. You need to ensure that only Android devices that use Android work profiles can enroll in Intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.
 NOTE: each correct selection is worth one point.

- A. From Select platforms, set Android work profile to Allow.
- B. From Configure platforms, set Android Personally Owned to Block.
- C. From Configure platforms, set Android Personally Owned to Allow.
- D. From Select platforms, set Android to Block.

Answer: AD

Explanation:

<https://docs.microsoft.com/en-us/Intune/enrollment-restrictions-set>

NEW QUESTION 125

- (Exam Topic 4)

You have a Microsoft 365 subscription.
 You have 20 computers that run Windows 10 and are joined to Microsoft Azure Active Directory (Azure AD)
 You plan to replace the computers with new computers that run Windows 10. The new computers will be joined to Azure AD.
 You need to ensure that the desktop background, the favorites, and the browsing history are available on the new computer.
 What should you use?

- A. Roaming user profiles
- B. Folder Redirection
- C. The Microsoft SharePoint Migration Tool
- D. Enterprise State Roaming

Answer: D

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs>

NEW QUESTION 128

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
 After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
 You have a computer that runs Windows 8.1.
 Two days ago, you upgraded the computer to Windows 10. You need to downgrade the computer to Windows 8.1. Solution: From the Settings app, you use the Recovery options. Does this meet the goal?

- A. Yes
 B. No

Answer: A

Explanation:

Reference:

https://answers.microsoft.com/en-us/windows/forum/windows_10-windows_install/how-to-recover-restore-your

NEW QUESTION 130

- (Exam Topic 4)

You use a Microsoft Intune subscription to manage iOS devices.

You configure a device compliance policy that blocks jailbroken iOS devices. You need to enable Enhanced jailbreak detection.

What should you configure?

- A. the device compliance policy
 B. the Compliance policy settings
 C. a network location
 D. a configuration profile

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

NEW QUESTION 133

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. User1 has the device shown in the following table.

Name	Operating system	Version	Join type	Mobile device management (MDM)
Device1	Windows	10.0.18362.0	Azure AD registered	None
Device2	Windows	10.0.18362.30	Azure AD registered	Microsoft Intune
Device3	Windows	10.0.18362.0	Azure AD joined	None
Device4	Windows	10.0.18362.30	Azure AD joined	Microsoft Intune

Enterprise State Roaming is configured for User1. User1 signs in to Device4 and changes the desktop.

You need to identify on which devices User1 will have a changed desktop. Which devices should you identify?

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

Answer: A

Explanation:

The requirements of Enterprise State Roaming are:

- Windows 10, with the latest updates, and a minimum Version 1511 (OS Build 10586 or later) is installed on the device.
- The device is Azure AD joined or hybrid Azure AD joined.
- Ensure that Enterprise State Roaming is enabled for the tenant in Azure AD.
- The user is assigned an Azure Active Directory Premium license.
- The device must be restarted and the user must sign in again to access Enterprise State Roaming features.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-troubleshooting>

NEW QUESTION 138

- (Exam Topic 4)

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

Name	Platform	Group
Device1	Windows 10	Group1, Group2
Device2	Android	Group2
Device3	iOS	Group2, Group3

You create device configuration profiles in Intune as shown in the following table.

Name	Platform	Minimum password length
Profile1	Windows 10 and later	4
Profile2	Android	5
Profile3	iOS	6
Profile4	Android	7
Profile5	iOS	8

You assign the device configuration profiles to groups as shown in the following table.

Group	Profile
Group1	Profile3
Group2	Profile1, Profile2, Profile4
Group3	Profile3, Profile5

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 must have a minimum password length of seven characters.	<input type="radio"/>	<input type="radio"/>
Device2 must have a minimum password length of seven characters.	<input type="radio"/>	<input type="radio"/>
Device3 must have a minimum password length of six characters.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot>

NEW QUESTION 143

- (Exam Topic 4)

Your company has computers that run Windows 8.1, Windows 10, or macOS. The company uses Microsoft Intune to manage the computers.

You need to create an Intune profile to configure Windows Hello for Business on the computers that support it.

Which platform type and profile type should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Platform type:

☐ macOS
☒ Windows 10 and later
☐ Windows 8.1 and later

Profile type:

☐ Device restrictions
☒ Device restrictions (Windows 10 Team)
☐ Endpoint protection

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/intune/endpoint-protection-configure>

NEW QUESTION 146

- (Exam Topic 4)

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains Windows 10 devices that are managed by using Microsoft Endpoint Configuration Manager.

You plan to deploy Microsoft 365 Apps for enterprise to the devices by using Configuration Manager. You create a Configuration.xml file as shown in the following exhibit.

```
<Configuration ID="67e*0d4f-814a-4466-9e3c-1388d66a527c">
  <Add OfficeClientEdition="64" Channel="Current" OfficeMgmtCOM="TRUE">>
    <Product ID="O365ProPlusRetail">
      <Language ID="MatchOS" />
      <ExcludeApp ID="Access" />
      <ExcludeApp ID="Groove" />
      <ExcludeApp ID="Lync" />
      <ExcludeApp ID="Publisher" />
    </Product>
  </Add>
  <Property Name="SharedComputerLicensing" Value="0"/>
  <Property Name="PinIconsToTaskbar" Value="TRUE"/>
  <Property Name="SCLCacheOverride" Value="0" />
  <Property Name="AUTOACTIVATE" Value="0" />
  <Property Name="FORCEAPPSHUTDOWN" Value="TRUE"/>
  <Property Name="DeviceBasedLicensing" Value="1" />
  <RemoveMSI />
  <AppSettings>
    <Setup Name="Company" Value="Contoso.com" />
  </AppSettings>
  <Display Level="None" AcceptEULA="TRUE" />
  <Logging Level="Standard" Path="\\Server1\Office" />
</Configuration>
```

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

NOTE: Each correct selection is worth one point.

Microsoft 365 Apps for enterprise will be installed from
[answer choice]

New Microsoft Office feature updates will be available
to devices [answer choice]

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options> <https://docs.microsoft.com/en-us/deployoffice/overview-update-channels#semi-annual-enterprise-channel-overv>

NEW QUESTION 148

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You plan to use Endpoint analytics. You need to create baseline metrics. What should you do first?

- A. Create an Azure Monitor workbook.
- B. Onboard 10 devices to Endpoint analytics.
- C. Create a Log Analytics workspace.
- D. Modify the Baseline regression threshold.

Answer: B

Explanation:

Onboarding from the Endpoint analytics portal is required for Intune managed devices. Reference: <https://docs.microsoft.com/en-us/mem/analytics/enroll-intune>

NEW QUESTION 153

- (Exam Topic 4)

You have a Microsoft Azure Active Directory (Azure AD) tenant. All corporate devices are enrolled in Microsoft Intune.

You have a web-based application named App1 that uses Azure AD to authenticate.

You need to prompt all users of App1 to agree to the protection of corporate data when they access App1 from both corporate and non-corporate devices. What should you configure?

- A. Notifications in Device compliance
- B. Terms and Conditions in Device enrollment
- C. Terms of use in Conditional access
- D. an Endpoint protection profile in Device configuration

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

NEW QUESTION 155

- (Exam Topic 4)

You have computers that run Windows 10 and are configured by using Windows AutoPilot. A user performs the following tasks on a computer named Computer1:

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

You perform a Windows AutoPilot Reset on Computer1.

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

NOTE: Each correct selection is worth one point.

The Wi-Fi connection will be:

<input type="checkbox"/>	Removed
<input type="checkbox"/>	Retained and the passphrase will be retained
<input type="checkbox"/>	Retained but the passphrase will be reset

App1 will be:

<input type="checkbox"/>	Reinstalled at sign-in
<input type="checkbox"/>	Removed
<input type="checkbox"/>	Retained

The VPN connection will be:

<input type="checkbox"/>	Removed
<input type="checkbox"/>	Retained and the credentials will be cached
<input type="checkbox"/>	Retained but the credentials will be reset

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 158

- (Exam Topic 4)

Your company has a Microsoft Azure Active Directory (Azure AD) tenant. All users in the company are licensed for Microsoft Intune.

You need to ensure that the users enroll their iOS device in Intune. What should you configure first?

- A. A Device Enrollment Program (DEP) token.
- B. An Intune device configuration profile.
- C. A Device enrollment manager (DEM) account.
- D. An Apple MDM Push certificate.

Answer: D

Explanation:

Reference:

https://www.manageengine.com/mobile-device-management/help/enrollment/mdm_creating_apns_certificate.ht

Prerequisites for iOS enrollment Before you can enable iOS devices, complete the following steps: Make sure your device is eligible for Apple device enrollment.

Set up Intune - These steps set up your Intune infrastructure. In particular, device enrollment requires that you set your MDM authority. Get an Apple MDM Push certificate - Apple requires a certificate to enable management of iOS and macOS devices.

<https://docs.microsoft.com/en-gb/intune/enrollment/apple-mdm-push-certificate-get>

NEW QUESTION 163

- (Exam Topic 4)

Your company has computers that run Windows 10. The employees at the company use the computers. You plan to monitor the computers by using the Update Compliance solution.

You create the required resources in Azure.

You need to configure the computers to send enhanced Update Compliance data.

Which two Group Policy settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Local Group Policy Editor	
File Action View Help	
Setting	State
Toggle user control over Insider builds	Not configured
Allow commercial data pipeline	Not configured
Allow device name to be sent in Windows diagnostic data	Not configured
Allow Telemetry	Not configured
Configure the Commercial ID	Not configured
Configure diagnostic data upload endpoint for Desktop Analytics	Not configured
Configure telemetry opt-in change notifications	Not configured
Configure telemetry opt-in setting user interface	Not configured
Disable deleting diagnostic data	Not configured
Disable diagnostic data viewer	Not configured
Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service	Not configured
Limit Enhanced diagnostic data to the minimum required by Windows Analytics	Not configured
Configure Connected User Experiences and Telemetry	Not configured
Do not show feedback notifications	Not configured
Configure collection of browsing data for Desktop Analytics	Not configured

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-configuration-manual>

NEW QUESTION 167

- (Exam Topic 4)

You create a Windows Autopilot deployment profile.

You need to configure the profile settings to meet the following requirements:

- Include the hardware serial number in the computer name.

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

NOTE: Each correct selection is worth one point.

Answer Area

Create profile ...

Windows PC

✓ Basics 2 Out-of-box experience (OOBE) 3 Assignments 4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode *	①	User-Driven	▼
Join to Azure AD as *	①	Azure AD joined	▼
Microsoft Software License Terms	①	Show	Hide
i important information about hiding license terms			
Privacy settings	①	Show	Hide
i The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. Learn more			
Hide change account options	①	Show	Hide
User account type	①	Administrator	Standard
Allow White Glove OOBE	①	No	Yes
Language (Region)	①	Operating system default	▼
Automatically configure keyboard	①	No	Yes
Apply device name template	①	No	Yes

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Graphical user interface Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/autopilot/profiles>

NEW QUESTION 171

- (Exam Topic 4)

You have a computer named Computer1 that runs Windows 10.

The Wi-Fi network profile for Computer1 is configured as shown in the following exhibit.

Connect automatically when in range

☒ On

Network profile

☒ Public

Your PC is hidden from other devices on the network and can't be used for printer and file sharing.

☐ Private

For a network you trust, such as at home or work. Your PC is discoverable and can be used for printer and file sharing if you set it up.

[Configure firewall and security settings](#)

The Delivery Optimization options for Computer1 are configured as shown in the following exhibit.

Allow downloads from other PCs

☒ On

☐ PC's on my local network

☒ PCs on my local network, and PCs on the Internet

From which computers will Computer1 will receive updates and to which computers will Computer1 provide updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Receive updates from:

Local computers only
Computers on the internet only
Local computers and computers on the internet

Provide updates to:

Local computers only
Computers on the internet only
Local computers and computers on the internet

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

NEW QUESTION 175

- (Exam Topic 4)

You are licensed for Microsoft Endpoint Manager.

You use Microsoft Endpoint Configuration Manager and Microsoft Intune.

You have devices enrolled in Configuration Manager as shown in the following table.

Name	Collection
Device1	Collection1
Device2	Collection2
Device3	Collection1, Collection2

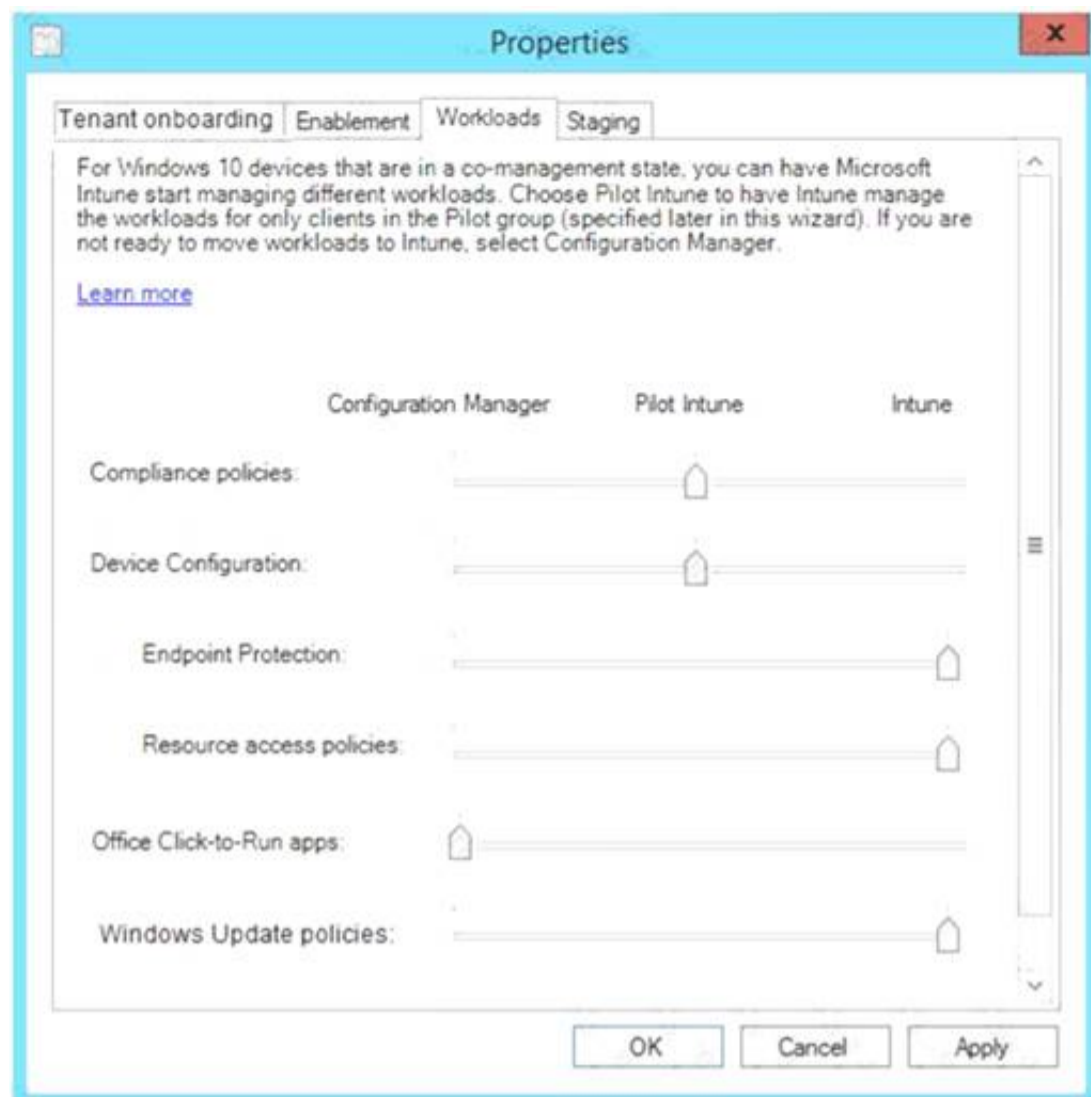
In Configuration Manager, you enable co-management and configure the following settings:

- > Automatic enrolment in Intune: Pilot
- > Intune Auto Enrollment: Collection1

In Configuration Manager, you configure co-management staging to have the following settings:

- > Compliance policies: Collection2
- > Device Configuration: Collection1

In Configuration Manager, you configure co-management workloads as shown in the following exhibit.



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

Statements	Yes	No
You can use the Microsoft Endpoint Manager admin center to monitor the compliance status of Device1.	<input type="radio"/>	<input type="radio"/>
You can use the Microsoft Endpoint Manager admin center to monitor the compliance status of Device2.	<input type="radio"/>	<input type="radio"/>
You can use the Microsoft Endpoint Manager admin center to monitor the compliance status of Device3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/comanage/workloads>

NEW QUESTION 177

- (Exam Topic 4)

Your company has a Microsoft 365 subscription.

A new user named Admin1 is responsible for deploying Windows 10 to computers and joining the computers to Microsoft Azure Active Directory (Azure AD).

Admin1 successfully joins computers to Azure AD.

Several days later, Admin1 receives the following error message: "This user is not authorized to enroll. You can try to do this again or contact your system administrator with the error code (0x801c0003)."

You need to ensure that Admin1 can join computers to Azure AD and follow the principle of least privilege.

- A. Assign the Global administrator role to Admin1.
- B. Modify the Device settings in Azure AD.
- C. Assign the Cloud device administrator role to Admin1.
- D. Modify the User settings in Azure AD.

Answer: B

Explanation:

References:

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

NEW QUESTION 178

- (Exam Topic 4)

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

Name	Platform	IP address
Device1	Windows	192.168.10.35
Device2	Android	10.10.10.40
Device3	Android	192.168.10.10

The devices are members of a group named Group1.

In Intune, you create a device compliance location that has the following configurations:

- Name: Network1
- IPv4 range: 192.168.0.0/16

In Intune, you create a device compliance policy for the Android platform. The policy has following configurations:

- Name: Policy1
- Device health: Rooted devices: Block
- Locations: Location: Network1
- Mark device noncompliant: Immediately
- Assigned: Group1

In Intune device compliance policy has the following configurations:

- Mark devices with no compliance policy assigned as: Compliant
- Enhanced jailbreak detection: Enabled
- Compliance status validity period (days): 20

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/intune/device-compliance-get-started>

NEW QUESTION 181

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have 20 computers that run Windows 10 and are joined to Microsoft Azure Active Directory (Azure AD). You plan to replace the computers with new computers that run Windows 10. The new computers will be joined to Azure AD.

You need to ensure that the desktop background, the favorites, and the browsing history are available on the new computers.

Solution: You configure Enterprise State Roaming. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settingsrefere>

NEW QUESTION 184

- (Exam Topic 4)

You use Windows Admin Center to remotely administer computers that run Windows 10.

When connecting to Windows Admin Center, you receive the message shown in the following exhibit.

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

 [Go to your Start page](#)

Details

Your PC doesn't trust this website's security certificate.

Error Code: DLG_FLAGS_INVALID_CA

[Go on to the webpage](#) (Not recommended)

You need to prevent the message from appearing when you connect to Windows Admin Center. To which certificate store should you import the certificate?

- A. Personal
- B. Trusted Root Certification Authorities
- C. Client Authentication Issuers

Answer: A

Explanation:

Reference:

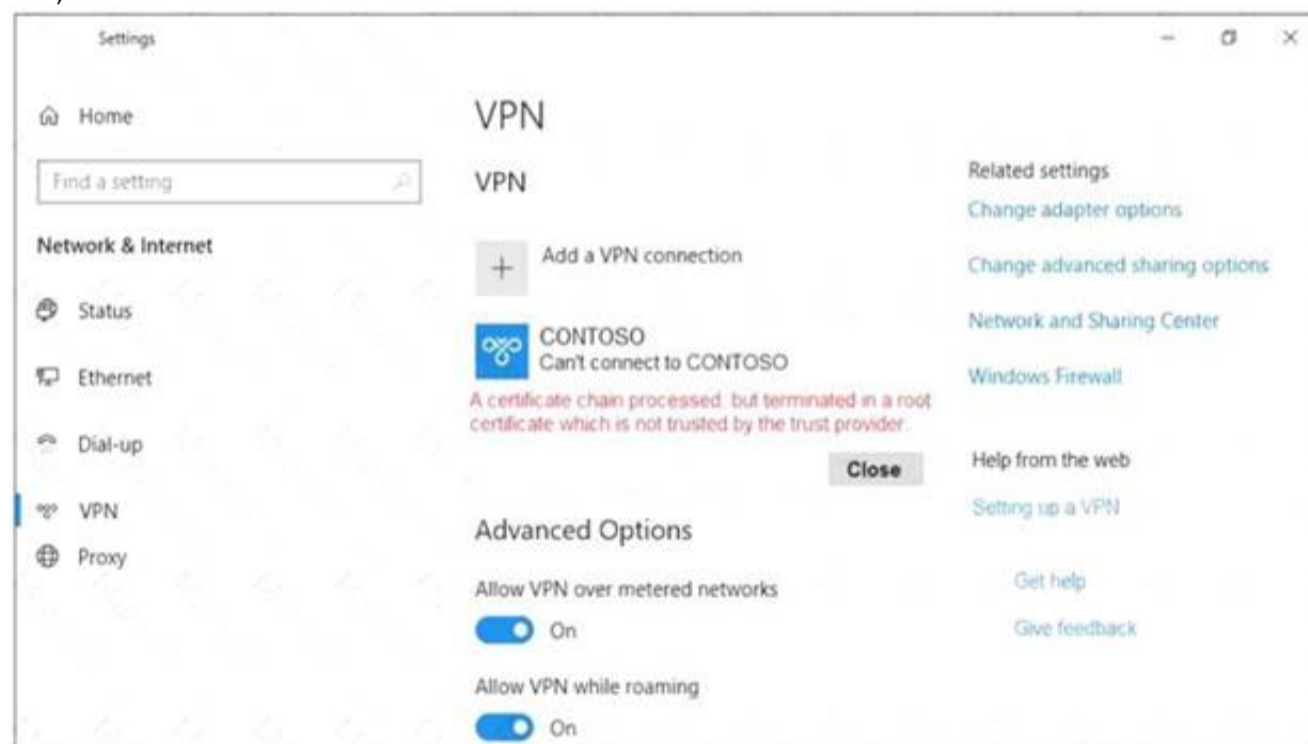
<https://social.technet.microsoft.com/Forums/en-US/6b3abb8e-007e-4047-bd30-2946b9c3aaba/windows-admin-c>

NEW QUESTION 187

- (Exam Topic 4)

You are configuring an SSTP VPN.

When you attempt to connect to the VPN, you receive the message shown in the exhibit. (Click the Exhibit tab.)



What should you do to ensure that you can connect to the VPN?

- A. Change the VPN type
- B. Generate a computer certificate from the root certification authority (CA)
- C. Install the root certificate

Answer: B

NEW QUESTION 190

- (Exam Topic 4)

You have the Microsoft Deployment Toolkit (MDT) installed in three sites as shown in the following table.

MDT instance name	Site	Default gateway
MDT1	New York	10.1.1.0/24
MDT2	London	10.5.5.0/24
MDT3	Dallas	10.4.4.0/24

You use Distributed File System (DFS) Replication to replicate images in a share named Production. You configure the following settings in the Bootstrap.ini file.

[Settings] Priority=DefaultGateway, Default [DefaultGateway] 10.1.1.1=NewYork 10.5.5.1=London

[NewYork] DeployRoot=\\MDT1\Production\$ [London] DeployRoot=\\MDT2\Production\$ KeyboardLocale=en-gb

[Default]

DeployRoot=\\MDT3\Production\$ KeyboardLocale=en-us

You plan to deploy Windows 10 to the computers shown in the following table.

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
TB1 will download the image from MDT3.	<input type="radio"/>	<input type="radio"/>
DT1 will have a KeyboardLocale of en-gb.	<input type="radio"/>	<input type="radio"/>
LT1 will download the image from MDT1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/build-a-distributed-environment-fo>

NEW QUESTION 193

- (Exam Topic 4)

You have computers that run Windows 8.1 or Windows 10. All the computers are enrolled in Microsoft Intune, Endpoint Configuration Manager, and Desktop Analytics. Co-management is enabled for your environment.

You plan to upgrade the Windows 8.1 computers to Windows 10.

You need to identify which Windows 8.1 computers do NOT have supported Windows 10 drivers.

What should you use?

- A. the General Hardware Inventory report in Configuration Manager
- B. the List of devices in a specific device category report in Configuration Manager
- C. Deployment plans in Desktop Analytics
- D. the Device compliance report in Intune

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans>

NEW QUESTION 198

- (Exam Topic 4)

You have a Microsoft 365 subscription. All devices run Windows 10.

You need to prevent users from enrolling the devices in the Windows Insider Program.

What should you configure from Microsoft 365 Device Management? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a Windows 10 security baseline
- B. an app configuration policy
- C. a custom device configuration profile
- D. a Windows 10 update ring
- E. a device restrictions device configuration profile

Answer: D

NEW QUESTION 202

- (Exam Topic 4)

You have Windows 10 devices that are managed by using Microsoft Intune. Intune and the Microsoft Store for Business are integrated.

You need to deploy the Remote Desktop modern app as an automatic install to the Windows 10 devices without user interaction.

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

NOTE: Each correct selection is worth one point.

- A. Create an Azure Active Directory group that contains all users.
- B. From the Intune portal, create a Microsoft Store app for the Remote Desktop modern app.
- C. From the Intune portal assign the app to the Azure Active Directory group.
- D. Create an Azure Active Directory group that contains the Windows 10 devices.
- E. From the Microsoft Store for Business portal, assign a license for the app to all the users in the Azure Active Directory group.
- F. For your organization, make the app available in the Microsoft Store for Business.

Answer: BCD

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-add> <https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy> <https://docs.microsoft.com/en-us/mem/intune/apps/windows-store-for-business>

NEW QUESTION 204

- (Exam Topic 4)

Your company uses Windows Defender Advanced Threat Protection (Windows Defender ATP). Windows Defender ATP includes the machine groups shown in the following table.

Rank	Name	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
5	Group5	Name starts with COMP
Last	Ungrouped machines (default)	Not applicable

You onboard a computer to Windows Defender ATP as shown in the following exhibit.



What is the effect of the Windows Defender ATP configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Computer1 will be a member of:

▼

Group3 only

Group4 only

Grou5 only

Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:

▼

Group1 only

Group2 only

Group1 and Group2 only

Group1, Group2, Group3, Group4, and Group5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Computer1 will be a member of:

Group3 only
Group4 only
Group5 only
Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:

Group1 only
Group2 only
Group1 and Group2 only
Group1, Group2, Group3, Group4, and Group5

NEW QUESTION 209

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a computer that runs Windows 8.1.

Two days ago, you upgraded the computer to Windows 10. You need to downgrade the computer to Windows 8.1.

Solution: You restart the computer to Windows Recovery Environment (Windows RE) and use the Advanced options.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 210

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You need provide a user the ability to disable Security defaults and create Conditional Access policies. The solution must use the principle of least privilege.

Which role should you assign to the user?

- A. Global Administrator
- B. Conditional Access Administrator
- C. Security Administrator
- D. Intune Administrator

Answer: B

Explanation:

To enable or disable security defaults in your directory, sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator.

Note: Conditional Access Administrator

Users with this role have the ability to manage Azure Active Directory Conditional Access settings. Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

NEW QUESTION 211

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain. The domain contains member computers that run Windows 8.1 and are enrolled in Microsoft Intune.

You need to identify which computers can be upgraded to Windows 10.

Solution: You install the Microsoft Assessment and Planning Toolkit. From the Microsoft Assessment and Planning Toolkit, you collect inventory data and run the Windows 10 Readiness scenario.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 213

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1 and the devices shown in the following table.

Name	Operating system	Azure AD status
Device1	Windows 11	Joined
Device2	Windows 10	Joined

User1 can access her Microsoft Exchange Online mailbox from both Device 1 and Device2.

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: Office 365 Exchange Online

* Access controls

* Grant: Block access

You need to configure CAPolicy1 to allow mailbox access from Device 1 but block mailbox access from Device2.

Solution: You add a condition that specifies a trusted locations. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead use solution: You add a condition to filter for devices. Note: Conditional Access: Filter for devices

When creating Conditional Access policies, administrators have asked for the ability to target or exclude specific devices in their environment. The condition filter for devices gives administrators this capability. Now you can target specific devices using supported operators and properties for device filters and the other available assignment conditions in your Conditional Access policies.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices>

NEW QUESTION 215

- (Exam Topic 4)

You use Microsoft Intune to manage client computers. The computers run one of the following operating systems:

> Windows 8.1

> Windows 10 Pro

> Windows 10 Enterprise

> Windows 10 Enterprise LTSC

You plan to manage Windows updates on the computers by using update rings. Which operating systems support update rings?

A. Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Enterprise LTSC only

B. Windows 8.1, Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Enterprise LTSC

C. Windows 10 Enterprise and Windows 10 Enterprise LTSC only

D. Windows 10 Pro and Windows 10 Enterprise only

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure>

NEW QUESTION 216

- (Exam Topic 4)

Your network contains an Active Directory domain. The domain contains 10 computers that run Windows 8.1 and use local user profiles.

You deploy 10 new computers that run Windows 10 and join the computers to the domain.

You need to migrate the user profiles from the Windows 8.1 computers to the Windows 10 computers. What should you do?

A. From the Windows 8.1 computer of each user, run imagex.exe/capture, and then from the Windows 10 computer of each user, run imagex.exe/apply.

B. Configure roaming user profiles for the user

C. Instruct the users to first sign in to and out of their Windows 8.1 computer and then to sign in to their Windows 10 computer.

D. From the Windows 8.1 computer of each user, run scanstate.exe, and then from the Windows 10 computer of each user, run loadstate.exe.

E. Configure Folder Redirection for the user

F. Instruct the users to first sign in to and out of their Windows 8.1 computer, and then to sign in to their Windows 10 computer.

Answer: C

Explanation:

The ScanState command is used with the User State Migration Tool (USMT) 10.0 to scan the source computer, collect the files and settings, and create a store.

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax> <https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-loadstate-syntax>

NEW QUESTION 221

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. The subscription contains the users shown in the following table.

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

Group2 and Group3 are members of Group1. All the users use Microsoft Excel.

From the Microsoft Endpoint Manager admin center, you create the policies shown in the following table.

Name	Type	Priority	Assigned to	Default file format for Excel
Policy1	Policies for Office apps	0	Group1	OpenDocument Spreadsheet (*.ods)
Policy2	Policies for Office apps	1	Group2	Excel Binary Workbook (*.xlsb)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
 NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
When User1 saves a new spreadsheet, the .ods format is used.	<input type="radio"/>	<input type="radio"/>
When User2 saves a new spreadsheet, the .xlsb format is used.	<input type="radio"/>	<input type="radio"/>
When User3 saves a new spreadsheet, the .xlsx format is used.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

User1 is member of Group1 and Group2.

Policy1 with priority 0 is assigned to Group1: default file format for Excel is.ods. Policy2 with priority 1 is assigned to Group2: default file format for Excel is.xlsb.

Note: Key points to remember about policy order

Policies are assigned an order of priority. Devices receive the first applied policy only. You can change the order of priority for policies.

Default policies are given the lowest order of priority.

Box 2: Yes

User2 is member of Group2.

Group2 and Group3 are members of Group1.

Box 3: No

User3 is member of Group3.

Group2 and Group3 are members of Group1.

Reference: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-policy-order>

NEW QUESTION 225

- (Exam Topic 4)

You have computers that run Windows 10, are joined to Azure Active Directory (Azure AD), and are enrolled in Microsoft Intune.

You have an Azure web app named App1. App1 only allows connections over HTTPS. App1 uses a certificate from an on-premises certification authority (CA).

You need to ensure that the computers can connect to App1 from Microsoft Edge.

Which type of device configuration profile should you create in Microsoft Endpoint Manager?

- A. trusted certificate
- B. Simple Certificate Enrollment Protocol (SCEP) certificate
- C. imported public key pair (PKCS) certificate
- D. public key pair (PKCS) certificate

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/certificates-scep-configure> <https://docs.microsoft.com/en-us/mem/intune/protect/certificates-configure>

NEW QUESTION 228

- (Exam Topic 4)

Your company has a Microsoft Azure Active Directory (Azure AD) tenant and computers that run Windows 10.

The company uses Microsoft Intune to manage the computers. The Azure AD tenant has the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

The device type restrictions in Intune are configured as shown in the following table:

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

User3 is a device enrollment manager (DEM) in Intune.

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

NOTE: Each correct selection is worth one point.

Statements

Yes

No

User1 can enroll a Windows device in Intune.

☐
☐

User2 can enroll a Windows device in Intune.

☐
☐

User3 can enroll an iOS device in Intune.

☐
☐

A. Mastered

B. Not Mastered

Answer: A

Explanation:

No, Yes, No

Policy 1 - Priority 1 (Android, iOS, Windows) Applied to None Policy 2 - Priority 2 (Windows) Applied to Group 2 Policy 3 - Priority 3 (Android) Applied to Group 1
 User 1 is in G1, so they cannot enroll Windows devices. User 2 is in both G1 & G2, G2 has P2 with a Pri.2 which means, even though they are in G1, G1 has a pri.3, so P3 will not apply User 3 is not a member of any group so the Default will apply. Policy 1 is assigned to NONE, default is assigned to All users, therefore they can NOT enroll iOS as default is only Android & Win.

References:

<https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-android>

NEW QUESTION 229

- (Exam Topic 4)

You have a shared computer that runs Windows 10. The computer is infected with a virus.

You discover that a malicious TTF font was used to compromise the computer.

You need to prevent this type of threat from affecting the computer in the future. What should you use?

A. Windows Defender Exploit Guard

B. Windows Defender Application Guard

C. Windows Defender Credential Guard

D. Windows Defender System Guard

E. Windows Defender SmartScreen

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/windowsd>

NEW QUESTION 232

- (Exam Topic 4)

You have a hybrid Microsoft Azure Active Directory (Azure AD) tenant, a Microsoft System Center Configuration Manager (Current Branch) environment, and a Microsoft 365 subscription.

You have computers that run Windows 10 as shown in the following table.

Name	Managed by Configuration Manager	Domain membership
Computer1	Yes	Active Directory-joined
Computer2	Yes	Hybrid Azure AD-joined
Computer3	Yes	Azure AD-joined

You plan to use Microsoft 365 Device Management.

Which computers support co-management by Configuration Manager and Device Management?

A. Computer1, Computer2, and Computer3

B. Computer3 only

C. Computer1 and Computer2 only

D. Computer2 only

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview>

NEW QUESTION 236

- (Exam Topic 4)

You have a Microsoft Intune subscription.

You create the Windows Autopilot deployment profile-shown in the following exhibit.

Create profile
 Windows Autopilot deployment profiles

* Name:

Description:

By default, this profile can only be applied to Autopilot devices synced from the Autopilot service. [Learn More.](#)
 Convert all targeted devices to Autopilot

* Deployment mode

* Join to Azure AD as

Out-of-box experience (OOBE)
 Create profile

Configure the out-of-box experience for your AutoPilot devices

The following options are automatically enabled for AutoPilot devices in self-deploying mode:

- Skip Work or Home usage selection
- Skip OEM registration and OneDrive configuration
- Skip user authentication in OOBE

End user license agreement (EULA)

What does it mean to skip the EULA?

Privacy Settings

Hide change account options

User account type

Apply computer name template (Windows Insider only)

Out-of-box experience (OOBE)
 Defaults configured >

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

NOTE: Each correct selection is worth one point.

Users who deploy by using Profile1
[answer choice]

are prevented from modifying any desktop settings
 can create additional local users on the device
 can modify the desktop settings for all device users
 can modify the desktop settings only for themselves

Users can configure the **[answer choice]** during the deployment

computer name
 Cortana settings
 keyboard layout

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/user-driven>

NEW QUESTION 237

- (Exam Topic 4)

You have a Microsoft 365 tenant.

You have a Windows 10 update ring named Policy1 as shown in the following exhibit.

Basics

Name	Policy1
Description	--

Update ring settings

Update settings

Servicing channel	Semi-Annual Channel
Microsoft product updates	Allow
Windows drivers	Block
Quality update deferral period (days)	0
Feature update deferral period (days)	0
Set feature update uninstall period (2–60 days)	14

A Windows 10 Feature update deployment named Policy2 is configured as shown in the following exhibit.

Deployment settings

Name	Policy2
Description	--
Feature deployment settings	
Name	Windows 10 2004

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

Name	Windows 10 edition	Policy applied
Device1	Windows 10 Enterprise, version 20H2	Policy1
Device2	Windows 10 Pro, version 2004	Policy2
Device3	Windows 10 Enterprise, version 20H2	Policy2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 will install feature updates twice a year.	<input type="radio"/>	<input type="radio"/>
Device2 will install feature update 20H2.	<input type="radio"/>	<input type="radio"/>
Device3 will be downgraded to feature update 2004.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings>

NEW QUESTION 238

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1 and the devices shown in the following table.

Name	Operating system	Azure AD status
Device1	Windows 11	Joined
Device2	Windows 10	Joined

User1 can access her Microsoft Exchange Online mailbox from both Device 1 and Device2.

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: Office 365 Exchange Online

- * Access controls
- * Grant: Block access

You need to configure CAPolicy1 to allow mailbox access from Device 1 but block mailbox access from Device2.

Solution: You add a condition that specifies device platforms. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use solution: You add a condition to filter for devices. Note: Conditional Access: Filter for devices

When creating Conditional Access policies, administrators have asked for the ability to target or exclude specific devices in their environment. The condition filter for devices gives administrators this capability. Now you can target specific devices using supported operators and properties for device filters and the other available assignment conditions in your Conditional Access policies.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices>

NEW QUESTION 240

- (Exam Topic 4)

You have a Microsoft Office 365 E1 subscription. You plan to create Conditional Access policies.

You need to ensure that users have the required licenses. The solution must minimize costs. Which type of license should you assign to each user?

- A. Microsoft Intune
- B. Azure Active Directory Premium Plan 1
- C. Office 365 E3
- D. Windows 365 Business

Answer: C

NEW QUESTION 243

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	macOS

In Endpoint security, you need to configure a disk encryption policy for each device.

Which encryption type should you use for each device, and which role-based access control (RBAC) role in Intune should you use to manage the encryption keys?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

FileVault
Cryptsetup
Encrypting File System (EFS)
BitLocker Drive Encryption (BitLocker)

Device2:

FileVault
Cryptsetup
Encrypting File System (EFS)
BitLocker Drive Encryption (BitLocker)

RBAC role:

Help Desk Operator
Application Manager
Intune Role Administrator
Policy and Profile Manager

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

NEW QUESTION 245

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) deployment share that has a path of D:\MDTShare. You need to add a feature pack to the boot image.

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

Actions

Answer Area

Modify the Windows PE properties of the deployment share.

Modify the General properties of the deployment share.

Copy the feature pack to D:\MDTShare\Packages.

Copy the feature pack to D:\MDTShare\Tools\x86.

Update the deployment share.



- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, chat or text message Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using>

NEW QUESTION 250

- (Exam Topic 4)

You have the devices shown in the following table.

Name	Operating system
Device1	Windows 10 Enterprise
Device2	Windows 8.1 Pro
Device3	Android 9.03
Device4	iOS

You plan to implement Desktop Analytics.

You need to identify which devices support the following:

- > Compatibility insights
- > App usage insights

Which devices should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Compatibility insights:

Device1 only
 Device1 and Device2 only
 Device3 and Device4 only
 Device1, Device2, Device3, and Device4

App usage insights:

Device1 only
 Device1 and Device2 only
 Device3 and Device4 only
 Device1, Device2, Device3, and Device4

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/compat-assessment><https://docs.microsoft.co> <https://azure.microsoft.com/en-us/updates/application-insights-adds-support-for-ios-and-android-apps-improved>

NEW QUESTION 255

- (Exam Topic 4)








You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You need to create Endpoint security policies to meet the following requirements:

- Hide the Firewall & network protection area in the Windows Security app.
- Disable the provisioning of Windows Hello for Business on the devices.

Which two policy types should you use? To answer, select the policies in the answer area.

NOTE: Each correct selection is worth one point.

Manage

 Antivirus
 Disk encryption
 Firewall
 Endpoint detection and response
 Attack surface reduction
 Account protection
 Device compliance
 Conditional access

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

In the Antivirus policy settings, you can hide the Firewall and network protection area in the Windows Security app.

Windows Hello for Business settings are configured in Identity protection. Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/antivirus-security-experience-windows-settings> <https://docs.microsoft.com/en-us/mem/intune/protect/identity-protection-windows-settings>

NEW QUESTION 257

- (Exam Topic 4)

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.

You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.

Which tool should you use?

- A. Microsoft Defender Security Center
- B. Desktop Analytics
- C. Microsoft Defender for Endpoint Power BI app
- D. Microsoft Secure Score

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwid>

NEW QUESTION 261

- (Exam Topic 4)

In Microsoft Intune, you have the device compliance policies shown in the following table.

Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8	Require	<i>Not applicable</i>	5 days	Group1
Policy2	Windows 10	Not configured	Require	7 days	Group2
Policy3	Windows 10	Required	Require	10 days	Group2

The Intune compliance policy settings are configured as shown in the following exhibit.

Save Discard

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

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

Enhanced jailbreak detection ☐ Enabled ☒ Disabled

Compliance status validity period (days) ☒

On June 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	Use BitLocker Drive Encryption (BitLocker)	Windows Defender	Member of
Device1	No	Enabled	Group1
Device2	No	Enabled	Group2

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
On June 4, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On June 6, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On June 9, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 264

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company uses Windows AutoPilot to configure the computer settings of computers issued to users. A user named User1 has a computer named Computer1 that runs Windows 10. User1 leaves the company. You plan to transfer the computer to a user named User2.

You need to ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement.

Solution: You create a new Windows AutoPilot user-driven deployment profile. Does this meet the goal?

- A. Yes
 B. No

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/user-driven>

Windows Autopilot user-driven mode lets you configure new Windows devices to automatically transform them from their factory state to a ready-to-use state. This process doesn't require that IT personnel touch the device.

The process is very simple. Devices can be shipped or distributed to the end user directly with the following instructions:

Unbox the device, plug it in, and turn it on.

Choose a language (only required when multiple languages are installed), locale, and keyboard.

Connect it to a wireless or wired network with internet access. If using wireless, the user must establish the Wi-Fi link.

Specify your e-mail address and password for your organization account. The rest of the process is automated. The device will:

Join the organization.

Enroll in Intune (or another MDM service) Get configured as defined by the organization. Reference:

<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/user-driven>

NEW QUESTION 265

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company uses Windows AutoPilot to configure the computer settings of computers issued to users. A user named User1 has a computer named Computer1 that runs Windows 10. User1 leaves the company. You plan to transfer the computer to a user named User2.

You need to ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement.

Solution: You perform a remote Windows AutoPilot Reset. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 270

- (Exam Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a computer that runs Windows 8.1.

Two days ago, you upgraded the computer to Windows 10. You need to downgrade the computer to Windows 8.1.

Solution: From Windows Update in the Settings app, you use the Advanced options. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 271

- (Exam Topic 4)

You have the MDM Security Baseline profile shown in the MDM exhibit. (Click the MDM tab.)

[Home](#) > [Endpoint security](#) > [MDM Security Baseline](#) >

Create profile

Block Office applications from injecting code into other processes ⓘ	Disable
Block Office applications from creating executable content ⓘ	Audit mode
Block all Office applications from creating child processes ⓘ	Audit mode
Block Win32 API calls from Office macro ⓘ	Disable
Block execution of potentially obfuscated scripts (js/vbs/ps) ⓘ	Disable

You have the ASR Endpoint Security profile shown in the ASR exhibit. (Click the ASR tab.)

[Home](#) > [Endpoint security](#) > [ASR Endpoint security](#) >

Edit profile

^ Attack Surface Reduction Rules

Block credential stealing from the Windows local security authority subsystem (lsass.exe) ⓘ	Audit mode
Block Adobe Reader from creating child processes ⓘ	Audit mode
Block Office applications from injecting code into other processes ⓘ	Audit mode
Block Office applications from creating executable content ⓘ	Audit mode
Block all Office applications from creating child processes ⓘ	Audit mode
Block Win32 API calls from Office macro ⓘ	Audit mode

You plan to deploy both profiles to devices enrolled in Microsoft Intune.

You need to identify how the following settings will be configured on the devices:

- > Block Office applications from creating executable content
- >

Block Win32 API calls from Office macro Currently, the settings are disabled locally on each device.
 What are the effective settings on the devices? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Answer Area

Block Office applications from creating executable content:

Audit mode
Block
Disable
Warn

Block Win32 API calls from Office macro:

Audit mode
Block
Disable
Warn

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Audit mode

According to the ASR Endpoint Security profile and to the MDM Security Baseline profile
 , Block Office applications from creating executable content is set to Audit mode. Box 2: Disable

Block Win32 API calls from Office macro: According to MDM Security Baseline profile it is set to disable. According to the ASR Endpoint Security profile it is set to Audit mode.

The profiles are merged. The Baseline profile overrides the Endpoint Security profile. Note:

When two or more policies have conflicting settings, the conflicting settings are not added to the combined policy, while settings that don't conflict are added to the superset policy that applies to a device.

Attack surface reduction rule merge behavior is as follows:

Endpoint security > Security baselines > Microsoft Defender for Endpoint Baseline > Attack Surface Reduction Rules.

MDM Security Baseline profile ASR Endpoint Security profile.

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

NEW QUESTION 273

- (Exam Topic 4)

Your company has computers that run Windows 10 and are Microsoft Azure Active Directory (Azure AD)-joined.

The company purchases an Azure subscription.

You need to collect Windows events from the Windows 10 computers in Azure. The solution must enable you to create alerts based on the collected events.

What should you create in Azure and what should you configure on the computers? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Resource to create in Azure:

An Azure event hub
An Azure Log Analytics workspace
An Azure SQL database
An Azure Storage account

Configuration to perform on the computers:

Configure the Event Collector service
Create an event subscription
Install the Microsoft Monitoring Agent

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent>

NEW QUESTION 277

- (Exam Topic 4)

You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 10.

You create a new task sequence by using the Standard Client Task Sequence template to deploy Windows 10 Enterprise to new computers. The computers have a single hard disk.

You need to modify the task sequence to create a system volume and a data volume. Which phase should you modify in the task sequence?

- A. Preinstall
- B. State Restore
- C. Initialization
- D. Postinstall

Answer: A

Explanation:

Reference:

<https://www.prajwaldesai.com/create-extra-partition-in-mdt/>

NEW QUESTION 282

- (Exam Topic 4)

You have a Microsoft Azure subscription that contains an Azure Log Analytics workspace.

You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup. You need to ensure that you can use Log Analytics to query events from Computer1.

What should you do on Computer1?

- A. Configure the commercial ID
- B. Join Azure Active Directory (Azure AD)
- C. Create an event subscription
- D. Install the Microsoft Monitoring Agent

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agent-windows>

NEW QUESTION 284

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MD-101 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MD-101 Product From:

<https://www.2passeasy.com/dumps/MD-101/>

Money Back Guarantee

MD-101 Practice Exam Features:

- * MD-101 Questions and Answers Updated Frequently
- * MD-101 Practice Questions Verified by Expert Senior Certified Staff
- * MD-101 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * MD-101 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year