Microsoft

Exam Questions MD-102

Endpoint Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

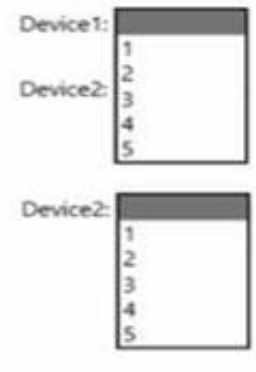
Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 1)
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.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, table Description automatically generated

NEW QUESTION 2
- (Exam Topic 1)
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

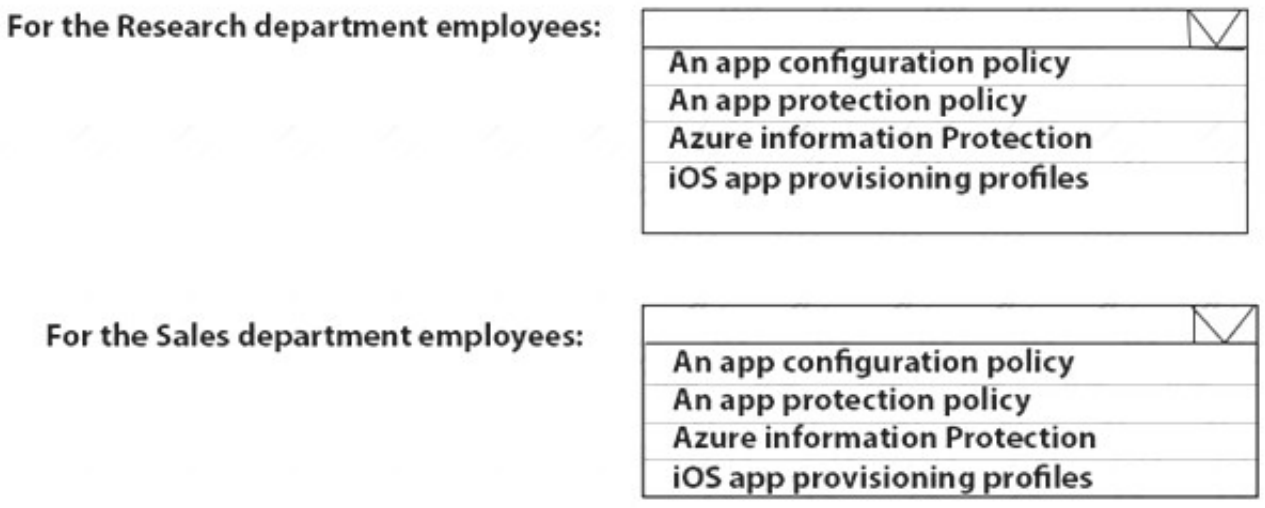
Statements	Yes	No
If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	○	○
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	○	○
If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, letter Description automatically generated

NEW QUESTION 3
- (Exam Topic 2)
You need to recommend a solution to meet the device management requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:

https://github.com/MicrosoftDocs/IntuneDocs/blob/master/intune/app-protection-policy.md
https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#do-not-forward-option-fo

NEW QUESTION 4
- (Exam Topic 2)
What should you use to meet the technical requirements for Azure DevOps?

A. An app protection policy
B. Windows Information Protection (WIP)
C. Conditional access
D. A device configuration profile

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/manage-conditional-access? view=azure-devops

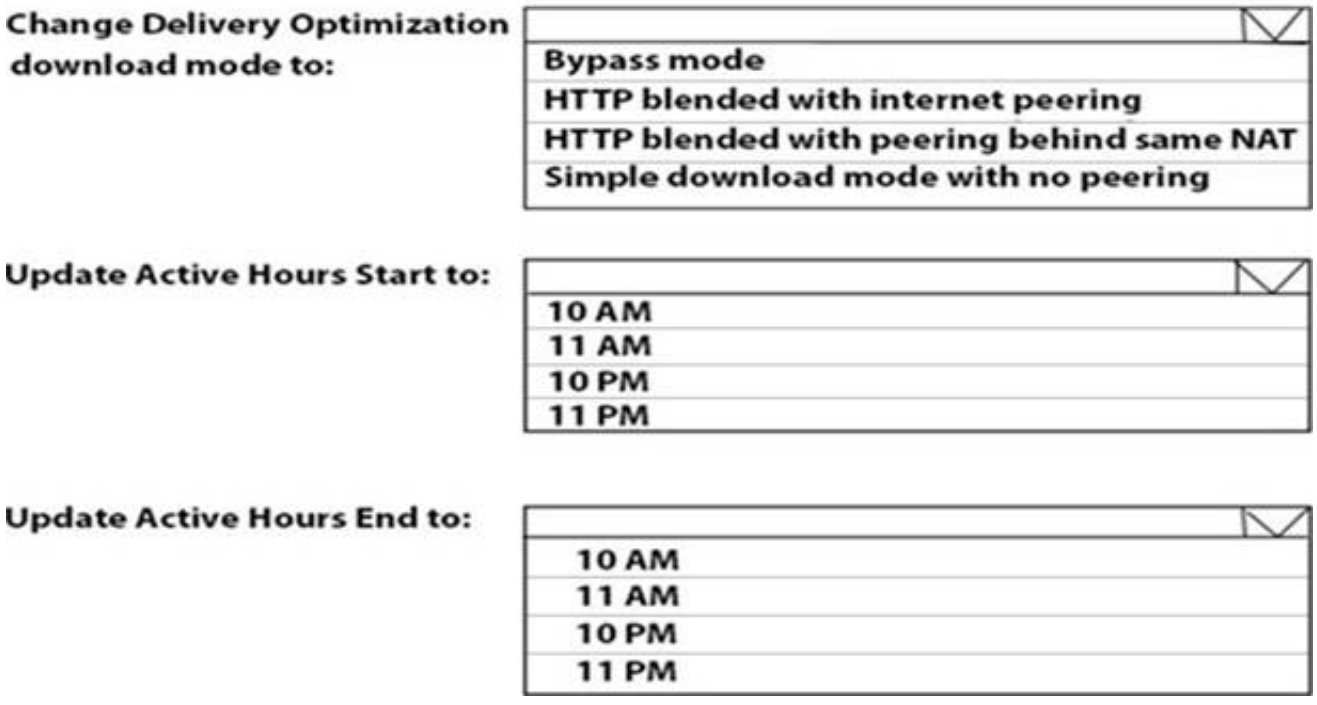
NEW QUESTION 5
- (Exam Topic 2)
What should you upgrade before you can configure the environment to support co-management?

A. the domain functional level
B. Configuration Manager
C. the domain controllers
D. Windows Server Update Services (WSUS)

Answer: B

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

NEW QUESTION 6
- (Exam Topic 2)
You need to resolve the performance issues in the Los Angeles office.
How should you configure the update settings? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated with low confidence
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization https://2pintsoftware.com/delivery-optimization-dl-mode/

NEW QUESTION 7
- (Exam Topic 3)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You have a Windows 11 device named Device1 that is enrolled in Intune. Device1 has been offline for 30
days.
You need to remove Device1 from Intune immediately. The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and

OEM-installed apps must be retained.
What should you use?

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

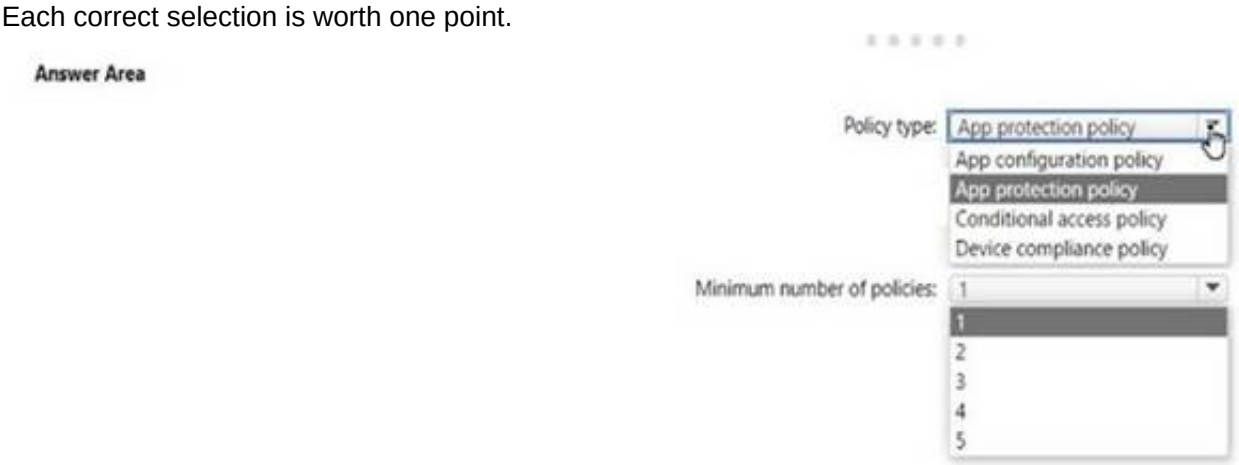
Answer: B

Explanation:
A retire action removes a device from Intune management and removes any apps and data provisioned by Intune. User-installed apps, personal data, and OEM-installed apps are retained. A retire action can be performed on devices that are offline for more than 30 days. References:
https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

NEW QUESTION 8
- (Exam Topic 3)
You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

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

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

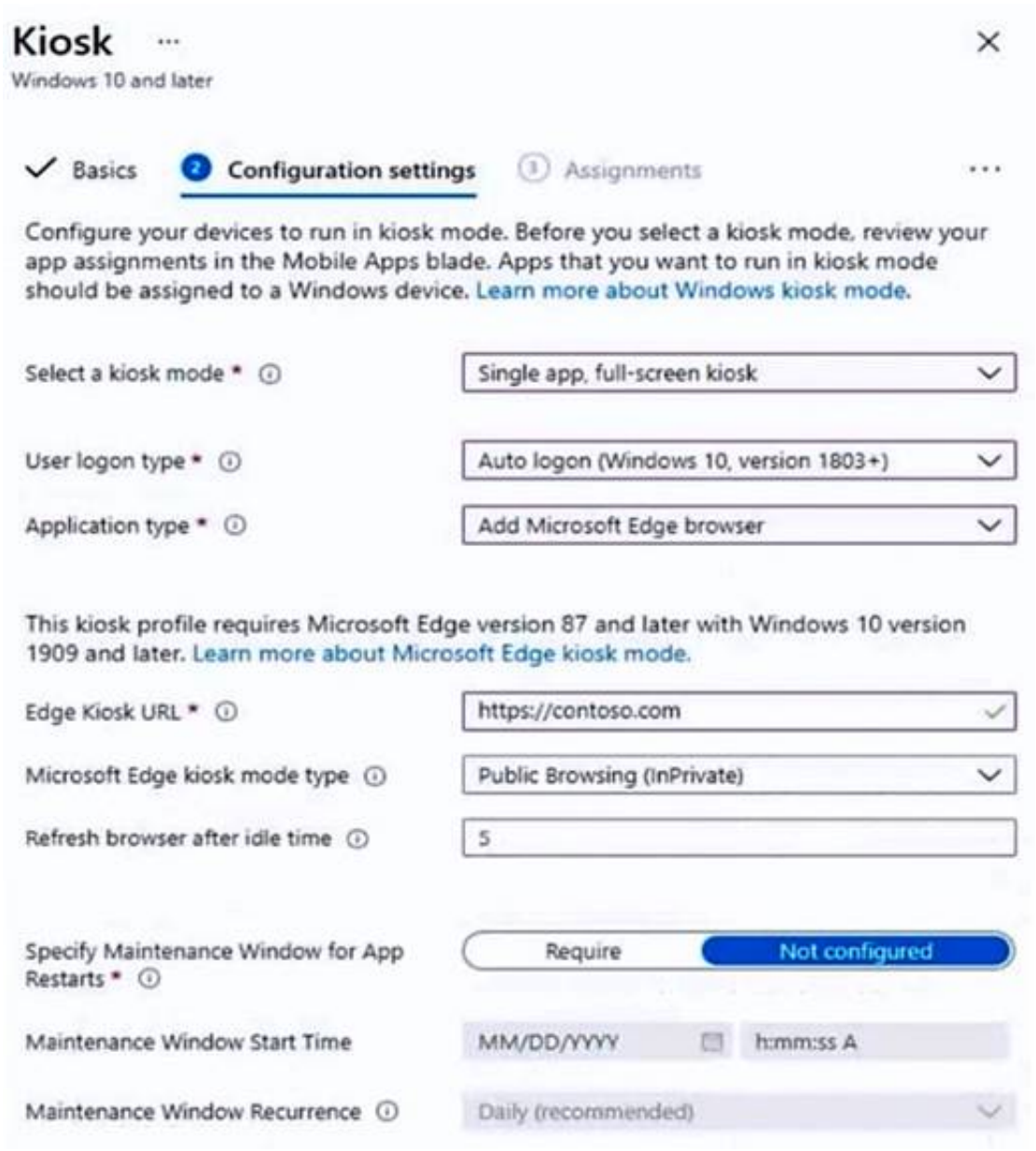


A. Mastered
B. Not Mastered

Answer: A

Explanation:
of Corre Answer Only: The correct answer is app protection policy because it allows you to customize the settings of apps for iOS/iPadOS or Android devices1. One of the settings you can configure is Restrict cut, copy, and paste between other apps, which lets you prevent users from copying data from App1 and pasting the data into other apps2. You only need one policy to apply this setting to all devices that have App1 installe1d.
References: 1: App configuration policies for Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview 2: Troubleshoot restricting cut, copy, and paste between applications - Intune | Microsoft Learn
https://learn.microsoft.com/en-us/troubleshoot/mem/intune/app-protection-policies/troubleshoot-cut-copy-paste

NEW QUESTION 9
- (Exam Topic 3)
You have the device configuration profile shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

Users	can access any URL. cannot view the address bar in Microsoft Edge. can only access URLs that include contoso.com. can only access URLs that start with https://contoso.com/ .
Windows 10 devices can have	a single Microsoft Edge instance that has a single tab. a single Microsoft Edge instance that has multiple tabs. multiple Microsoft Edge instances that have multiple tabs. multiple Microsoft Edge instances that each has a single tab.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Users can only access URLs that start with https://contoso.com/ Windows 10 and later devices can have multiple Microsoft Edge instances that each has a single tab
he device configuration profile shown in the exhibit is a kiosk browser profile that configures Microsoft Edge to run in kiosk mode. The profile has the following settings:
- Kiosk mode: Enabled
- Kiosk type: Multi-app
- Allowed URLs: https://contoso.com/*
- Address bar: Disabled

These settings mean that users can only access URLs that start with https://contoso.com/ and cannot view the address bar in Microsoft Edge. The kiosk type of Multi-app allows users to open multiple instances of Microsoft Edge, but each instance can only have a single tab. Therefore, users cannot access any URL, cannot view the address bar in Microsoft Edge, and can have multiple Microsoft Edge instances that each has a single tab. References: https://docs.microsoft.com/en-us/mem/intune/configuration/kiosk-settings#kiosk-browser-settings

NEW QUESTION 10
- (Exam Topic 3)
You have an on-premises server named Server! that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1. You need to ensure that MDT1 supports multicast deployments. What should you install on Server1?

A. Multipath I/O (MPIO)
B. Multipoint Connector
C. Windows Deployment Services (WDS)
D. Windows Server Update Services (WSUS)

Answer: C

NEW QUESTION 10
- (Exam Topic 3)
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you configure the Windows Hello for Business enrollment options.
Does this meet the goal?

A. Yes
B. No

Answer: B

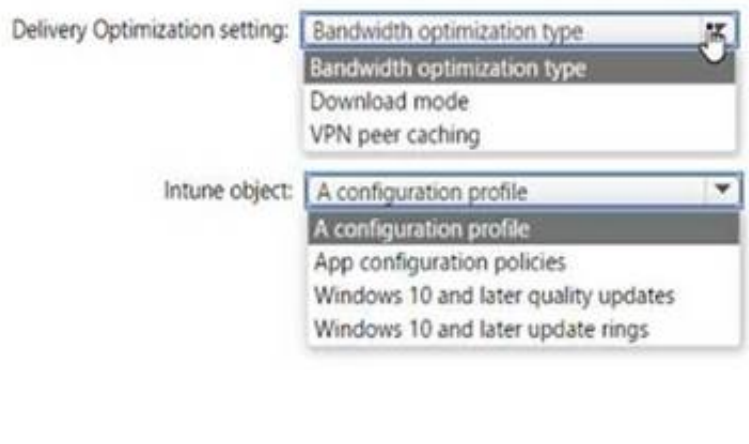
NEW QUESTION 15
- (Exam Topic 3)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You use Windows Autopilot to deploy Windows 11 to devices.
A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device.
You need to ensure that when a deployment fails, the deployment logs can be collected. What should you configure?

A. the automatic enrollment settings
B. the Windows Autopilot deployment profile
C. the enrollment status page (ESP) profile
D. the device configuration profile

Answer: B

NEW QUESTION 18
- (Exam Topic 3)
You have 100 Windows 10 devices enrolled in Microsoft Intune.
You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.
Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

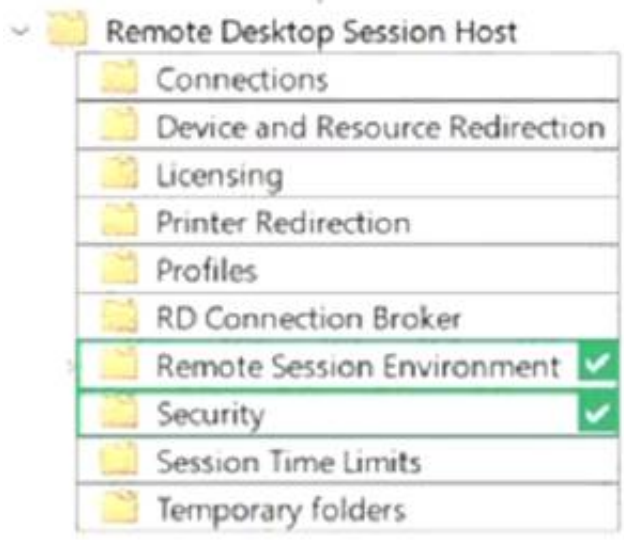
Explanation:
Delivery Optimization setting: B. Download mode Intune object: A configuration profile
To configure the devices to retrieve Windows updates from the internet and from other computers on a local network, you need to configure the Download mode setting in a Delivery Optimization device configuration profile. This setting specifies how the devices use Delivery Optimization to download updates. You can choose from several options, such as HTTP only, LAN only, or Group. For example, you can set the Download mode to Group and specify a group ID for the devices to share updates among themselves and with other devices that have the same group ID. You can also set the Download mode to Internet to allow the devices to download updates from Microsoft or other devices on the internet that use Delivery Optimization. References: https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-windows

NEW QUESTION 20
- (Exam Topic 3)
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a network share. You start Computer1 from Windows PE (WinPE), and then you run setup.exe from the network share.
Does this meet the goal?

A. Yes
B. No

Answer: B

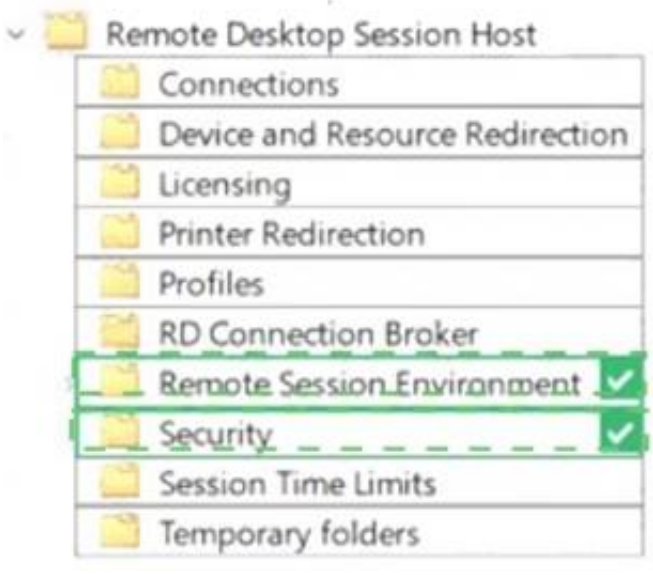
NEW QUESTION 21
- (Exam Topic 3)
Your network contains an Active Directory domain. The domain contains 1.000 computers that run Windows 11.
You need to configure the Remote Desktop settings of all the computers. The solution must meet the following requirements:
• Prevent the sharing of clipboard contents.
• Ensure that users authenticate by using Network Level Authentication (NLA).
Which two nodes of the Group Policy Management Editor should you use? To answer, select the appropriate nodes in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 22
- (Exam Topic 3)
You have a Microsoft 365 subscription.
You use Microsoft Intune Suite to manage devices.
You have the iOS app protection policy shown in the following exhibit.

Access requirements

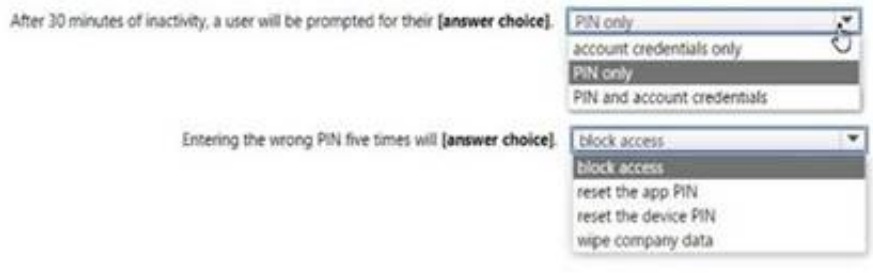
PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS 8+/iPadOS)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS 11+/iPadOS)	Block
PIN reset after number of days	No
Number of days	0
App PIN when device PIN is set	Require
Work or school account credentials for access	Require
Recheck the access requirements after (minutes of inactivity)	30

Conditional launch

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

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point,

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1 = PIN only
Box 2 = reset the PIN app
iOS/iPadOS app protection policy settings - Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios

NEW QUESTION 24
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune. You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS
devices. The solution must minimize administrative effort. What should you do?

A. From the Microsoft Endpoint Manager admin center, create a configuration profile.
B. From the Microsoft Endpoint Manager admin center, create a security baseline.
C. Onboard the macOS devices to the Microsoft 365 compliance center.
D. Install Defender for Endpoint on the macOS devices.

Answer: D

Explanation:
Just install, and use Defender for Endpoint on Mac. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac

NEW QUESTION 25
- (Exam Topic 3)
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.	○	○
User1 can enroll Device2 in Intune by using automatic enrollment.	○	○
User2 can enroll Device1 in Intune by using automatic enrollment.	○	○

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 30
- (Exam Topic 3)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You need to review the startup times and restart frequencies of the devices. What should you use?

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

Answer: D

Explanation:
Endpoint analytics is a feature of Microsoft Intune that provides insights into the performance and health of devices. You can use endpoint analytics to review the startup times and restart frequencies of the devices, as well as other metrics such as sign-in times, battery life, app reliability, and software inventory. References: https://docs.microsoft.com/en-us/mem/analytics/overview

NEW QUESTION 31
- (Exam Topic 3)
You use Microsoft Intune and Intune Data Warehouse.
You need to create a device inventory report that includes the data stored in the data warehouse. What should you use to create the report?

A. the Azure portal app
B. Endpoint analytics
C. the Company Portal app
D. Microsoft Power Bl

Answer: D

Explanation:
You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:
Devices Enrollment
App protection policy Compliance policy
Device configuration profiles Software updates
Device inventory logs
Note: Load the data in Power BI using the OData link
With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.

- Sign in to the Microsoft Endpoint Manager admin center.
- Select Reports > Intune Data warehouse > Data warehouse.
- Retrieve the custom feed URL from the reporting blade, for example:

- Open Power BI Desktop.
- Choose File > Get Data. Select OData feed.
- Choose Basic.
- Type or paste the OData URL into the URL box.
- Select OK.
- If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
- Select Organizational account.
- Type your username and password.
- Select Sign In.
- Select Connect.
- Select Load.

Reference: https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

NEW QUESTION 33
- (Exam Topic 3)
You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from Windows event logs.
The computers have the logged events shown in the following table.

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

Which events are collected in the Log Analytics workspace?

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

Answer: E

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

NEW QUESTION 34
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune. You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS
devices. The solution must minimize administrative effort.
What should you do?

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

Answer: C

Explanation:
To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices.
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/mac-install-with-int

NEW QUESTION 36
- (Exam Topic 3)
You have a Microsoft Deployment Toolkit (MDT) server named MDT1.
When computers start from the LiteTouchPE_x64.lso 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.

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 39
- (Exam Topic 3)
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 build 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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 44
- (Exam Topic 3)
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 48
- (Exam Topic 3)
Your company uses Microsoft Intune to manage devices.
You need to ensure that only Android devices that use Android work profiles can enroll in intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer
presents part of the solution.
NOTE Each correct selection is worth one point.

A. From Platform Settings, set Android device administrator Personally Owned to Block.
B. From Platform Settings, set Android Enterprise (work profile) to Allow.
C. From Platform Settings, set Android device administrator Personally Owned to Allow
D. From Platform Settings, set Android device administrator to Block.

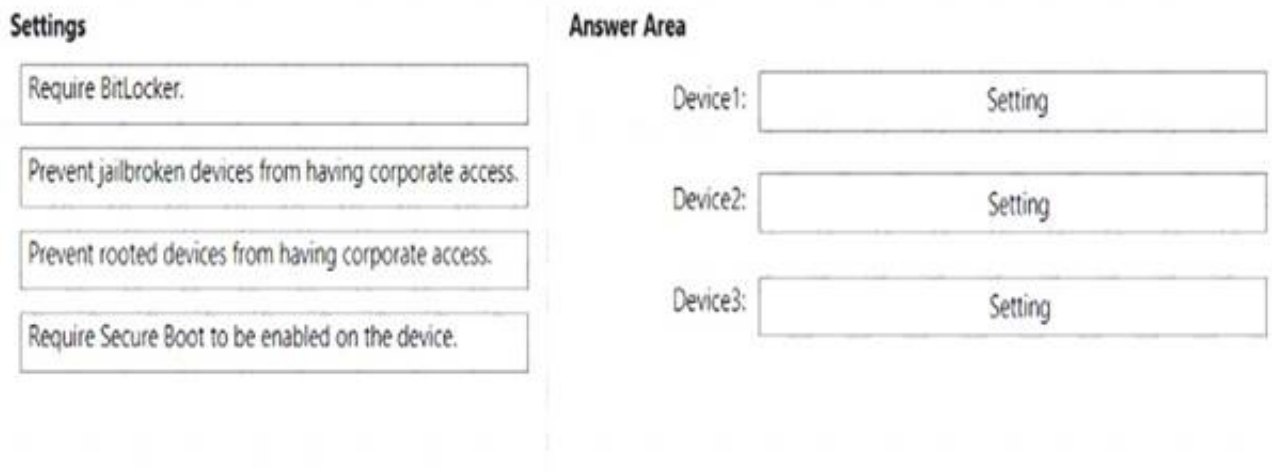
Answer: AB

Explanation:
To ensure that only Android devices that use Android work profiles can enroll in Intune, you need to perform two configurations in the device enrollment restrictions. First, you need to set Android device administrator Personally Owned to Block. This prevents users from enrolling personal Android devices that use device administrator mode. Second, you need to set Android Enterprise (work profile) to Allow. This allows users to enroll corporate-owned or personal Android devices that use work profiles. References: https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set

NEW QUESTION 52
- (Exam Topic 3)
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.



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 56
- (Exam Topic 3)
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 57
- (Exam Topic 3)
You have an Azure AD group named Group1. Group! contains two Windows 10 Enterprise devices named Device1 and Device2. You create a device configuration profile named Profile1. You assign Profile! to Group1. You need to ensure that Profile! applies to Device1 only. What should you modify in Profile 1?

A. Assignments
B. Settings
C. Scope (Tags)
D. Applicability Rules

Answer: D

Explanation:
To ensure that Profile1 applies to Device1 only, you need to modify the Applicability Rules in Profile1. You can use applicability rules to filter which devices receive a profile based on criteria such as device model, manufacturer, or operating system version. You can create an applicability rule that matches Device1's properties and excludes Device2's properties. References:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#applicability-rules

NEW QUESTION 62
- (Exam Topic 3)
Your company standardizes on Windows 10 Enterprise for all users.
Some users purchase their own computer from a retail store. The computers run Windows 10 Pro.
You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Azure AD, and install several Microsoft Store apps.
The solution must meet the following
requirements:
• Ensure that any applications installed by the users are retained.
• Minimize user intervention.
What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. Windows Autopilot
B. Microsoft Deployment Toolkit (MDT)
C. a Windows Configuration Designer provisioning package
D. Windows Deployment Services (WDS)

Answer: A

NEW QUESTION 67
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You have a device named Device1 that is enrolled in Intune.
You need to ensure that User1 can use Remote Help from the Intune admin center for Device1. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Deploy the Remote Help app to Device1.
B. Assign the Help Desk Operator role to User1.
C. Assign the Intune Administrator role to User1.
D. Assign a Microsoft 365 E5 license to User1.
E. Rerun device onboarding on Device1.
F. Assign the Remote Help add-on license to User1.

Answer: ABF

NEW QUESTION 68
- (Exam Topic 3)
Your company uses Microsoft Defender for Endpoint Microsoft Defender for Endpoint includes the device 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 Microsoft Defender for Endpoint as shown in the following exhibit.

What is the effect of the Microsoft Defender for Endpoint configuration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Computer1 will be a member of:
- Group3 only
- Group4 only
- Grou5 only
- Group3, Group4, and Group5 only

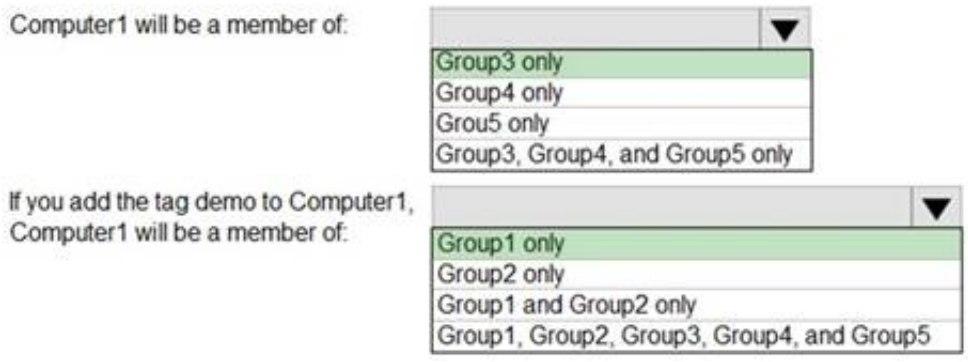
If you add the tag demo to Computer1, Computer1 will be a member of:
- Group1 only
- Group2 only
- Group1 and Group2 only
- Group1, Group2, Group3, Group4, and Group5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 69
- (Exam Topic 3)
You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models.
You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models.
What should you do first?

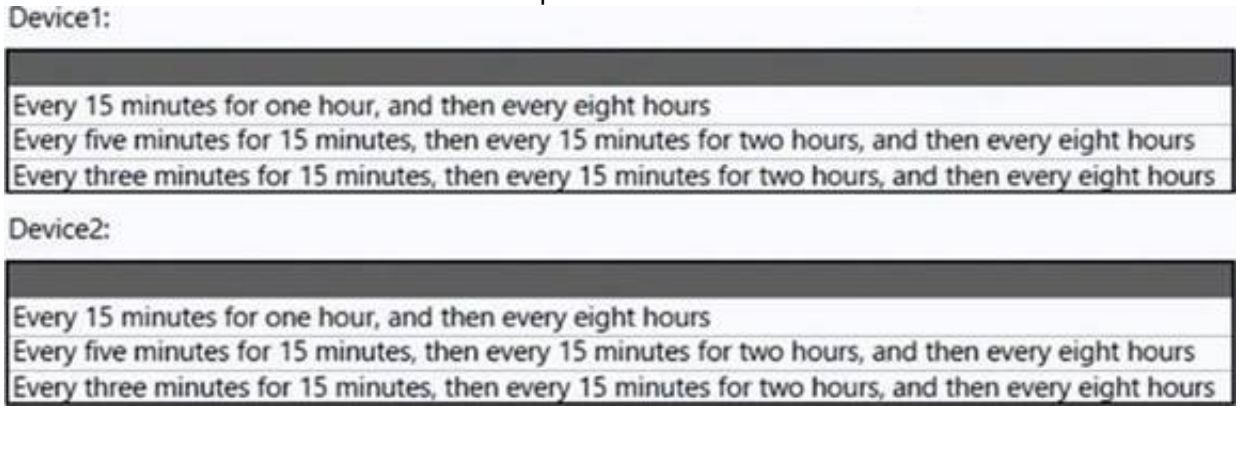
A. Import an OS package.
B. Create a selection profile.
C. Add a Gather task to the task sequence.
D. Add a Validate task to the task sequence.

Answer: B

NEW QUESTION 74
- (Exam Topic 3)
You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	iOS

You plan to enroll the devices in Microsoft Intune.
How often will the compliance policy check-ins run after each device is enrolled in Intune? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Every three minutes for 15 minutes, then every 15 minutes for two hours, and then around every eight hours
If devices recently enroll, then the compliance, non-compliance, and configuration check-in runs more frequently. The check-ins are estimated at:
Windows 10: Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Graphical user interface, text, application, email Description automatically generated

Platform	Frequency
iOS/iPadOS	Every 15 minutes for 1 hour, and then around every 8 hours
macOS	Every 15 minutes for 1 hour, and then around every 8 hours
Android	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 10/11 PCs enrolled as devices	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 8.1	Every 5 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Box 2: Every 15 minutes for one hour, and then every eight hours iOS/iPadOS: Every 15 minutes for 1 hour, and then around every 8 hours
Reference: https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot

NEW QUESTION 77
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription.
You create a new update rings policy named Policy1 as shown in the following exhibit.

Update ring settings Edit

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

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point,

Answer Area

Updates that contain fixes and improvements to existing Windows functionality **[answer choice]**.
- can be deferred for 30 days
- can be deferred indefinitely
- can be deferred for 30 days
- will be installed immediately

Updates that contain new Windows functionality will be installed within **[answer choice]** of release.
- 1 day
- 1 day
- 30 days
- 60 days

A. Mastered
B. Not Mastered

Answer: A

Explanation:
*Updates that contain fixes and improvements to existing Windows functionality can be deferred for 30 days. This is because the update rings policy named Policy1 has the “Quality updates deferral period (days)” setting set to 30. This means that quality updates, which include fixes and improvements to existing Windows functionality, can be deferred for up to 30 days from the date they are released by Microsoft. After 30 days, the devices will automatically install the quality updates. References:

https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure
*Updates that contain new Windows functionality will be installed within 60 days of release.
This is because the update rings policy named Policy1 has the “Feature updates deferral period (days)” setting set to 60. This means that feature updates, which include new Windows functionality, can be deferred for up to 60 days from the date they are released by Microsoft. After 60 days, the devices will automatically install the feature updates. References:
https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure

NEW QUESTION 82
- (Exam Topic 3)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a Microsoft Deployment Toolkit (MDT) deployment share. You create a task sequence, and then you run the MDT deployment wizard on Computer1.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 84
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to perform the following tasks for User1:
- Set the Usage location to Canada.
- Configure the Phone and Email authentication contact info for self-service password reset (SSPR). Which two settings should you configure in the Azure Active Directory admin center? 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:
Graphical user interface, application Description automatically generated

NEW QUESTION 89
.....

Relate Links

100% Pass Your MD-102 Exam with Exambible Prep Materials

https://www.exambible.com/MD-102-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/