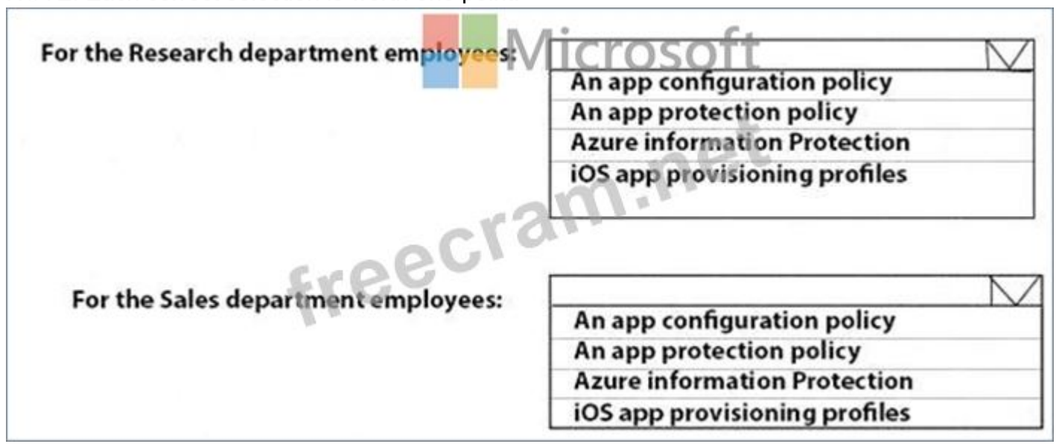
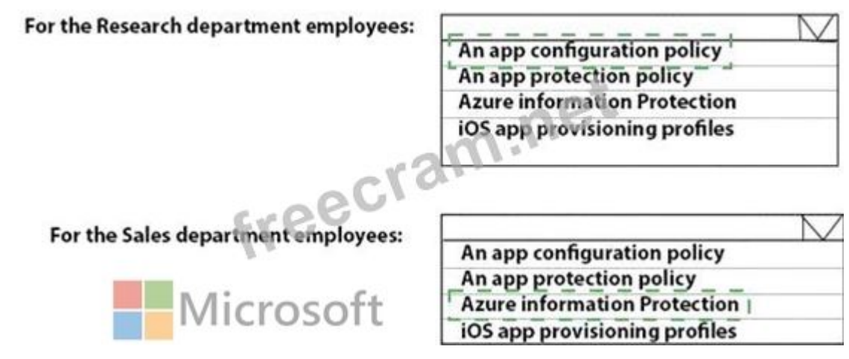
Microsoft.MD-102.v2026-11-06.q183

Exam Code:	MD-102
Exam Name:	Managing and Securing Microsoft 365 Endpoints by using Intune
Certification Provider:	Microsoft
Free Question Number:	183
Version:	v2026-11-06
# of views:	108
# of Questions views:	2001
https://www.freecram.net/torrent/Microsoft.MD-102.v2026-11-06.q183.html	

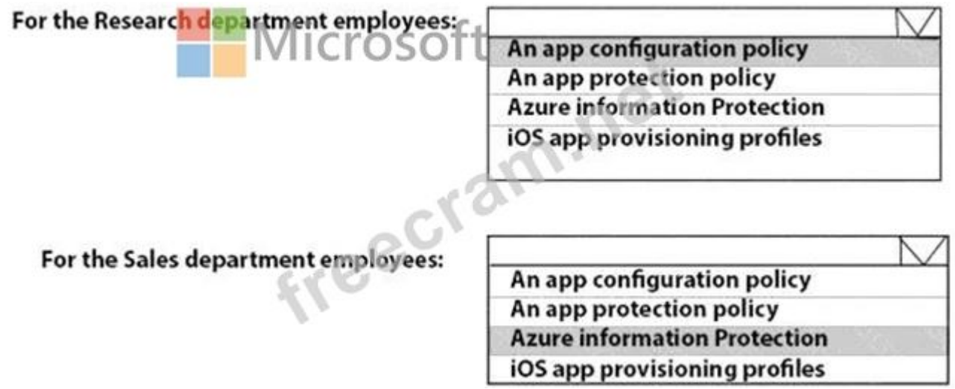
NEW QUESTION: 1
You need to recommend a solution to meet the device management requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



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-for-emails

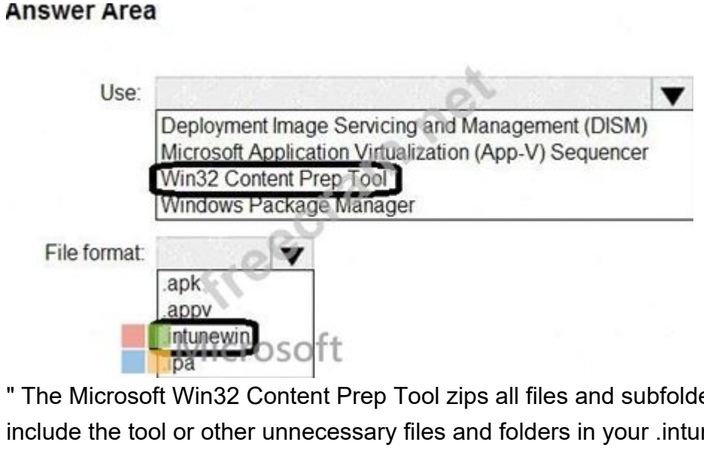
NEW QUESTION: 2
You have a Microsoft 365 E5 subscription that contains a computer named Computer1 that runs Windows 11.
Computer1 is enrolled in Microsoft Intune.
You need to deploy an app named App1 to Computer1. The App1 installation will use multiple files.
What should you use to package App1, and which file format will be used? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



" The Microsoft Win32 Content Prep Tool zips all files and subfolders when it creates the .intunewin file. Be sure to keep the Microsoft Win32 Content Prep Tool separate from the installer files and folders, so that you don ' t include the tool or other unnecessary files and folders in your .intunewin file. "

NEW QUESTION: 3

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:

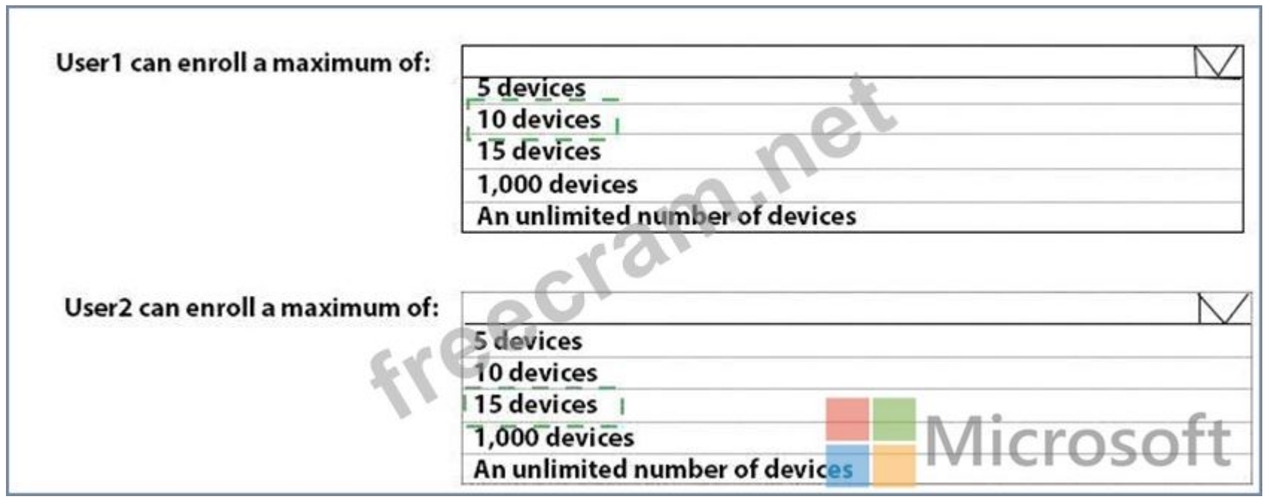
- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

User2 can enroll a maximum of:

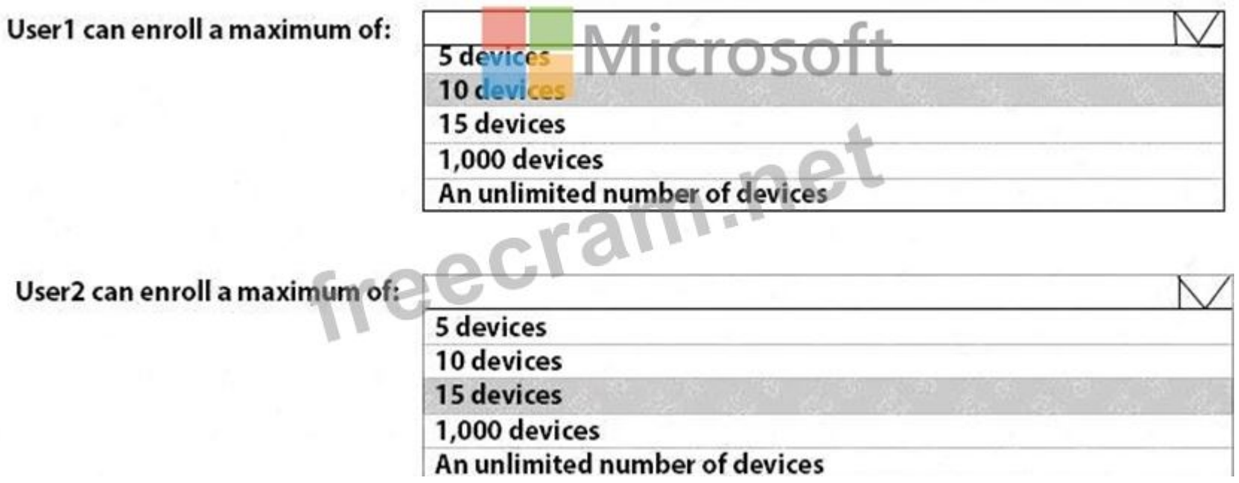
- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

freecram.net
Microsoft

Answer:



Explanation:



NEW QUESTION: 4

You have a Microsoft 365 subscription that uses Microsoft Intune Endpoint Privilege Management (EPM).

The subscription contains a group named Group1.

You have a trusted third-party app named App1 that is updated monthly. Users require elevated privileges to run App1.

You need to configure an EPM elevation rule that enables the members of Group1 to run App1. The solution must meet the following requirements:

* Allow elevation without administrator review.

* Require users to acknowledge each elevation event



Answer:



Explanation:



NEW QUESTION: 5

You have a Microsoft 365 E5 subscription and use the Microsoft Intune Suite. The subscription contains a Microsoft Sharepoint Online site named Site! and 500 Windows devices enrolled in Intune You have the apps shown in the following table.

Name	Type	Source location
App1	Win32	Site1
App2	Web app	Site1
App3	Microsoft Store app	Microsoft Store
App4	Win32	Enterprise App Catalog

You need to deploy the apps to the devices by using Intune.

For which apps must you upload app package files before you can deploy them?

A. App1 and App2 only

B. App1, App2, and App4 only

C. App1 and App4 only

D. App1. App2, App3, and App4

E. App1 only

Answer: (SHOW ANSWER)

NEW QUESTION: 6
You have a Microsoft 365 E5 subscription and use Microsoft Intune Suite.
You plan to use Intune to run remediation script packages.
What should you do first in the Microsoft Intune admin center?
A. Configure the Derived Credential settings.
B. Upload a Windows enterprise certificate.
C. Enable Windows license verification.
D. Enable Windows diagnostic data in processor configuration.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1 @contoso.com.
You join a Windows 10 device named Client1 to contoso.com.
You need to add User1 to the local Administrators group of Client1.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

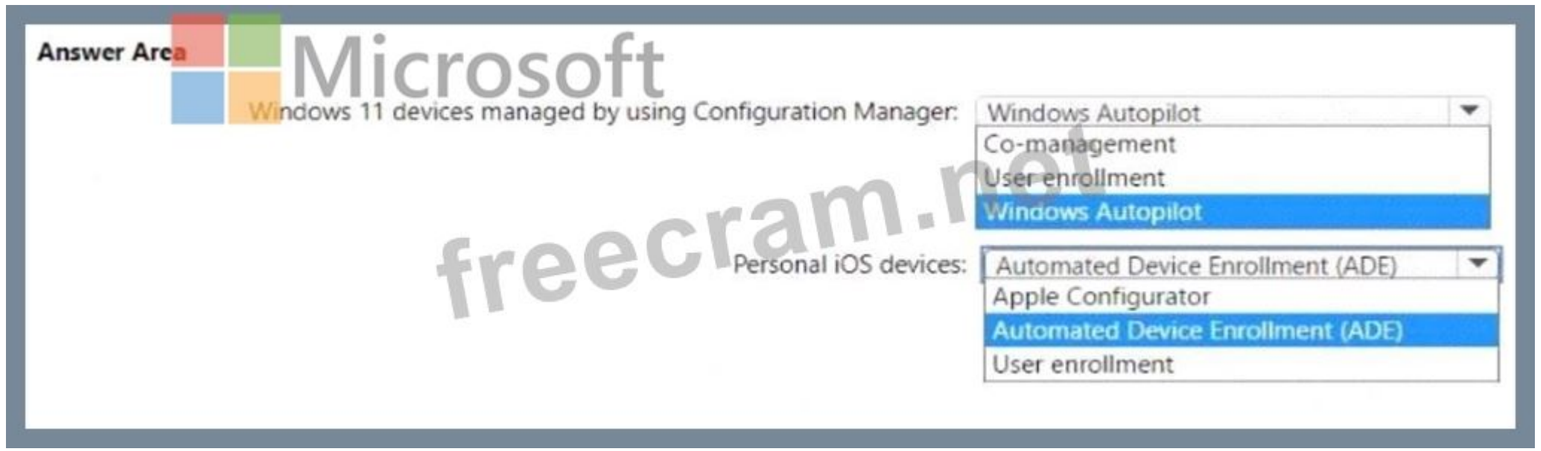


NEW QUESTION: 8
You have an Azure AD tenant that contains the devices shown in the following table.

Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered

You purchase Windows 11 Enterprise E5 licenses.
Which devices can use Subscription Activation to upgrade to Windows 11 Enterprise?
A. Device1, Device2, Device3, and Device4
B. Device1 only
C. Device1 and Device2 only
D. Device1 and Device3 only
Answer: (SHOW ANSWER)

NEW QUESTION: 9
You have a Microsoft 365 subscription.
You plan to enable Microsoft Intune enrollment for the following types of devices:
* Existing Windows 11 devices managed by using Configuration Manager
* Personal iOS devices
The solution must minimize user disruption.
Which enrollment method should you use for each device type? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



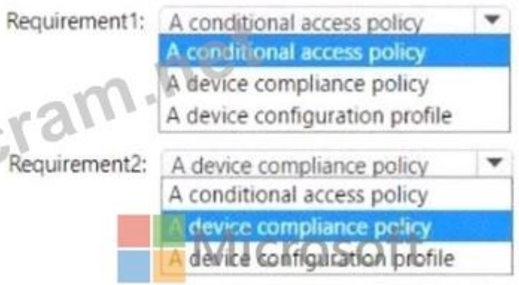
Explanation:
https://learn.microsoft.com/en-us/mem/configmgr/comanage/overview
for co-management
https://learn.microsoft.com/en-us/mem/intune/enrollment/ios-user-enrollment-supported-actions iOS user enrollment for BYOD

NEW QUESTION: 10
You have a Microsoft 365 subscription.
All computers are enrolled in Microsoft Intune.
You have business requirements for securing your Windows 11 environment as shown in the following table.

Requirement	Detail
Requirement1	Ensure that Microsoft Exchange Online can be accessed from known locations only.
Requirement2	Lock a device that has a high Microsoft Defender for Endpoint risk score.

What should you implement to meet each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



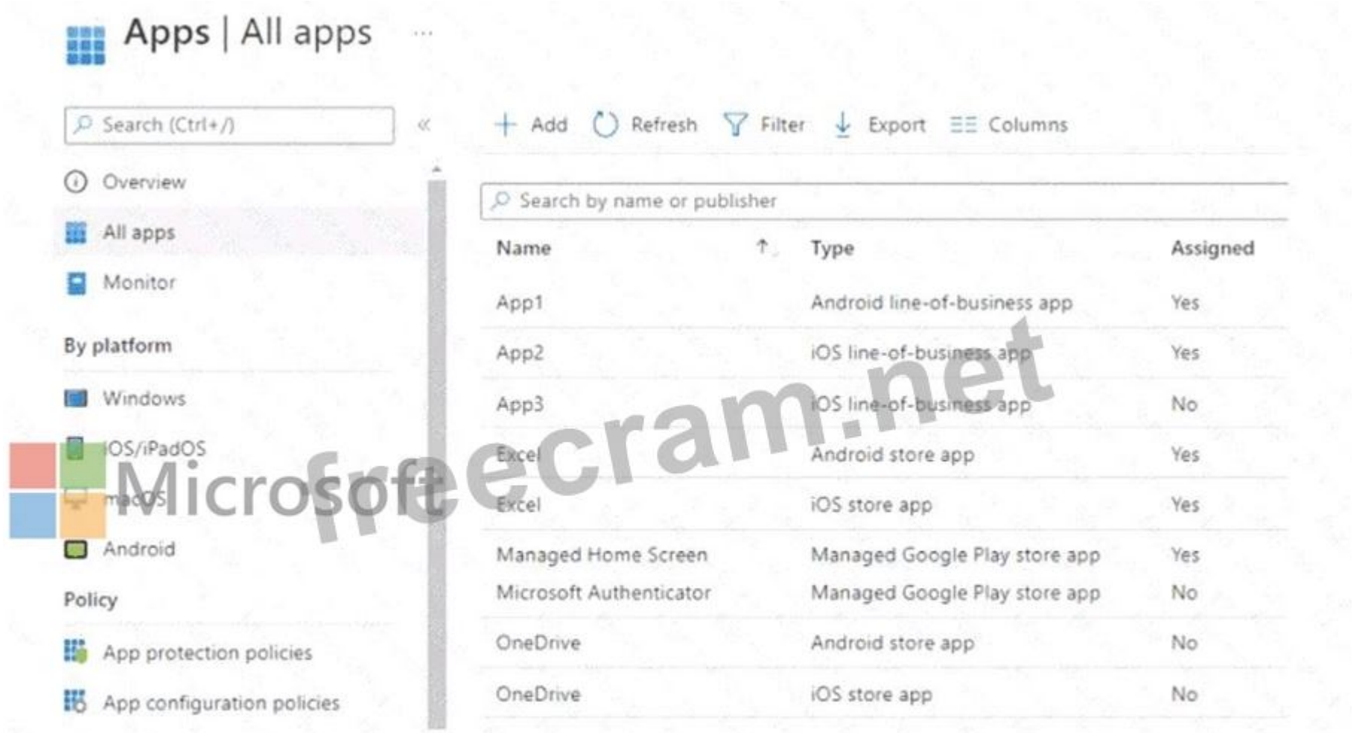
Explanation:



NEW QUESTION: 11

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

You have the apps shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.



Answer:

Microsoft
freecram.net



Explanation:



NEW QUESTION: 12

You have a Microsoft Deployment Toolkit (MDT) deployment shore.

You plan to deploy Windows 11 by using the Standard Client Task Sequence template.

You need to modify the task sequence to perform the following actions:

* Format disks to support Unified Extensible Firmware Interface (UEFI).
* Create a recovery partition.

Which phase of the Task sequence should you modify?

A. Preinstall

B. Initialization

C. Install

D. Post Install

Answer: (SHOW ANSWER)

NEW QUESTION: 13

You have a Microsoft 365 subscription and use Microsoft Intune Suite.

The subscription contains devices enrolled in Intune as shown in the following table.

Name	Platform	Join type
Device1	Windows 10	Microsoft Entra joined
Device2	Windows 11	Microsoft Entra registered
Device3	iOS	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

Which devices support Device query?

A. Device1 and Device2 only

B. Device1, Device2, Device3, and Device4
C. Device2 only
D. Device1 only
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.
When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.
You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you configure the Authentication methods.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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 BI
Answer: (SHOW ANSWER)
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:
https://fef.{yourtenant}.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?api- version=v1.0 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: 16
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. a configuration profile
B. the device compliance policy
C. the Compliance policy settings
D. a network location
Answer: (SHOW ANSWER)

Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 17
You have a Microsoft Entra tenant named contoso.com.
You have the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	iOS
Device3	Ubuntu Linux

Which devices can be Microsoft Entra Joined, and which devices can be registered in contoso.com? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Microsoft freecram.net

Answer:

Answer Area



freecram.net Microsoft

Explanation:



freecram.net

NEW QUESTION: 18

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. Create a selection profile.

B. Add a Gather task to the task sequence.

C. Import an OS package.

D. Add a Validate task to the task sequence.

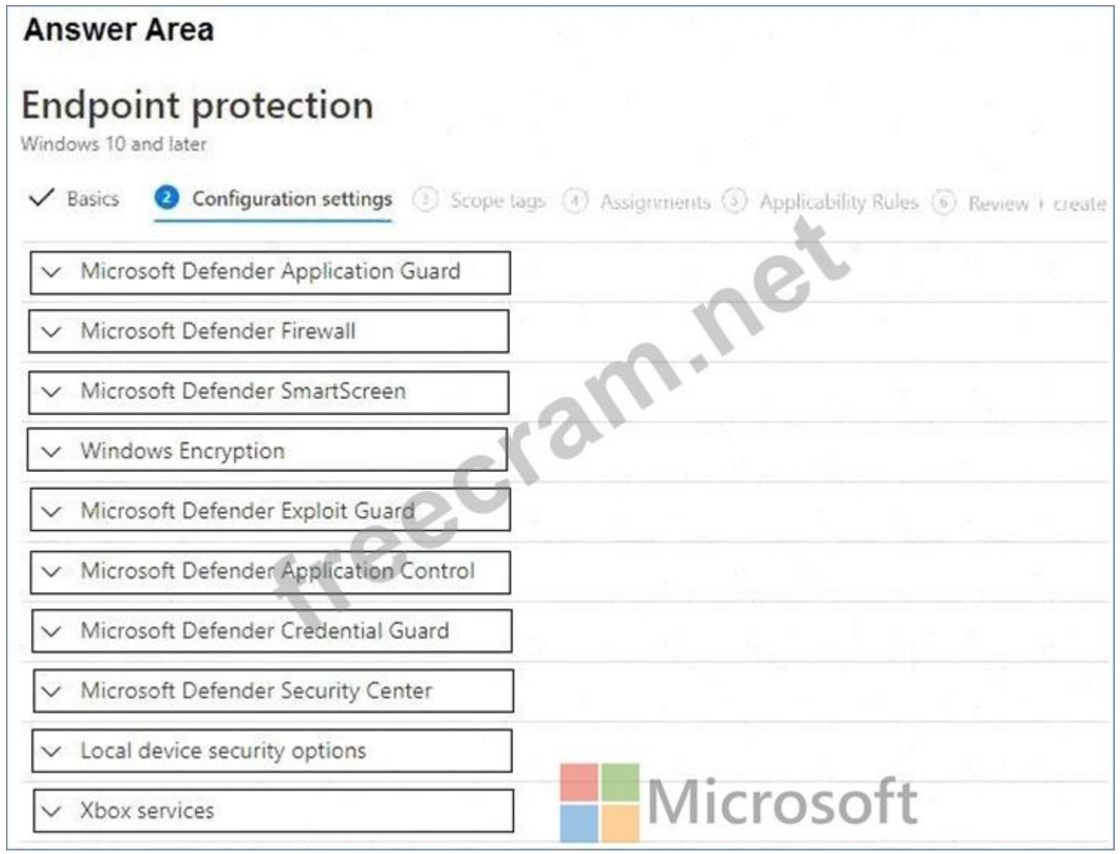
Answer: (SHOW ANSWER)

NEW QUESTION: 19
You have a Microsoft 365 subscription that uses Microsoft Intune to manage Windows devices and iOS devices.
Users report that Intune app deployments and remote device actions are delayed on both platforms.
You need to identify whether the issue relates to an active Intune service incident. The solution must minimize administrative effort.
What should you review in the Microsoft Intune admin center?
A. Audit logs
B. Diagnostic settings
C. Tenant status
D. Device diagnostics
Answer: C (LEAVE A REPLY)

NEW QUESTION: 20
You have a Microsoft 365 subscription.
You have devices enrolled in Microsoft Intune as shown in the following table.
To which devices can you deploy apps by using Intune?
Freecram.net
A. Device1, Device2, Device3, and Device4
B. Device1 and Device2 only
C. Device1 and Device3 only
D. Device1, Device2, and Device3 only
E. Device1 only
Answer: (SHOW ANSWER)

NEW QUESTION: 21
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



freecram.net

Answer:

Answer Area



Microsoft
freecram.net

Explanation:

Answer Area



freecram.net

References:
https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10#global-settings
https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10#microsoft-defender-exploit-guard

NEW QUESTION: 22
You have a Microsoft Entra tenant named contoso.com that contains a Windows 11 device named Device1 and a user named User1 User! registers Device1 in contoso.com.
Which capability is available to Device1 after registering in contoso.com.
A. authenticating to cloud resources by using single sign-on (SSO)
B. enforcing hard drive encryption
C. enforcing software updates
D. enforcing compliance policies
Answer: (SHOW ANSWER)

NEW QUESTION: 23
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.

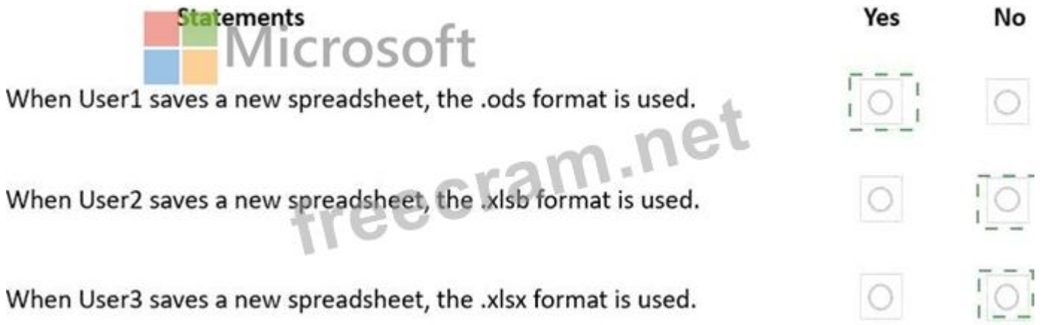
Name	Type	Priority	Assigned to	Default file format for Excel
Policy1	Policies for Office apps	0	Group1	OpenDocument Spreadsheet (*.ods)
Policy2	Policies for Office apps	1	Group2	Excel Binary Workbook (*.xlsb)

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
When User1 saves a new spreadsheet, the .ods format is used.	○	○
When User2 saves a new spreadsheet, the .xlsb format is used.	○	○
When User3 saves a new spreadsheet, the .xlsx format is used.	○	○

Answer:



Microsoft
freecram.net

Explanation:
Box 1: Yes
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: No
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: 24
You have a Microsoft 365 subscription.
You use Microsoft Intune to manage all devices.
Users have iOS devices with Microsoft apps installed.
You need to prevent users from cutting, copying, and pasting data between Microsoft Excel and other apps installed on the devices.
What should you configure'
A. policies for Microsoft Office apps
B. an app protection policy
C. an iOS app provisioning profile
D. an app configuration policy
Answer: (SHOW ANSWER)

NEW QUESTION: 25

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.

Answer Area

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.	○	○

Answer:

Answer Area

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.	○	○

Explanation:

Answer Area

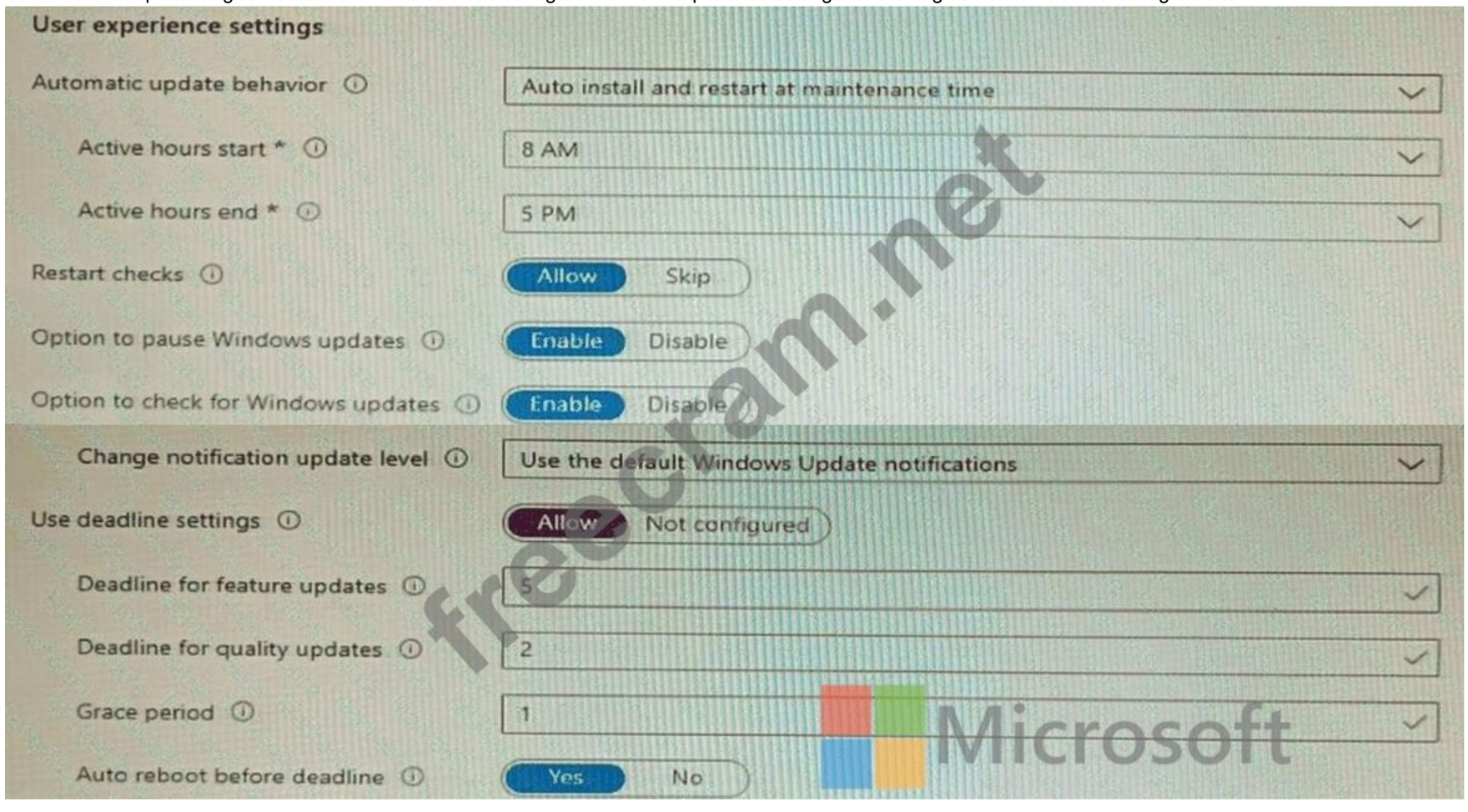
Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	●	○
User1 can enroll Device2 in Intune by using automatic enrollment.	○	●
User2 can enroll Device1 in Intune by using automatic enrollment.	○	●

NEW QUESTION: 26

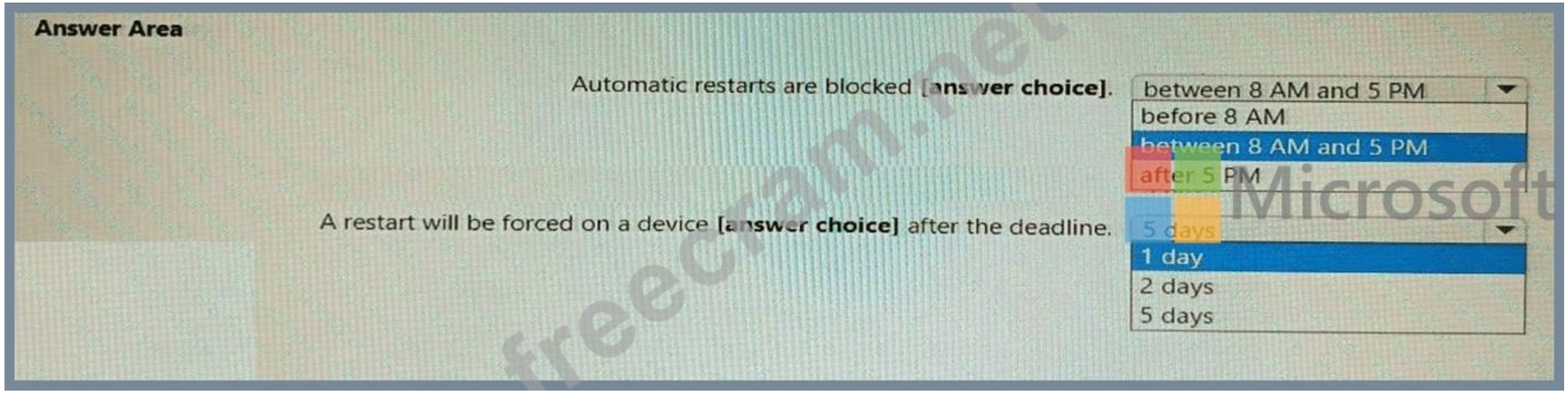
You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to manage Windows updates by using Intune.

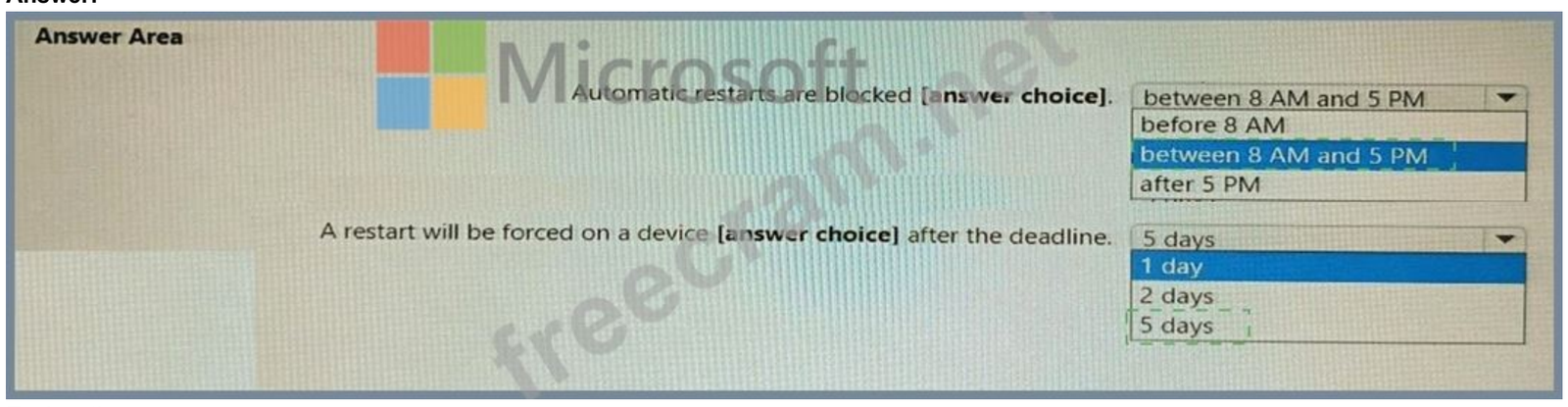
You create an update ring for Windows 10 and later and configure the User experience settings for the ring as shown in the following exhibit.



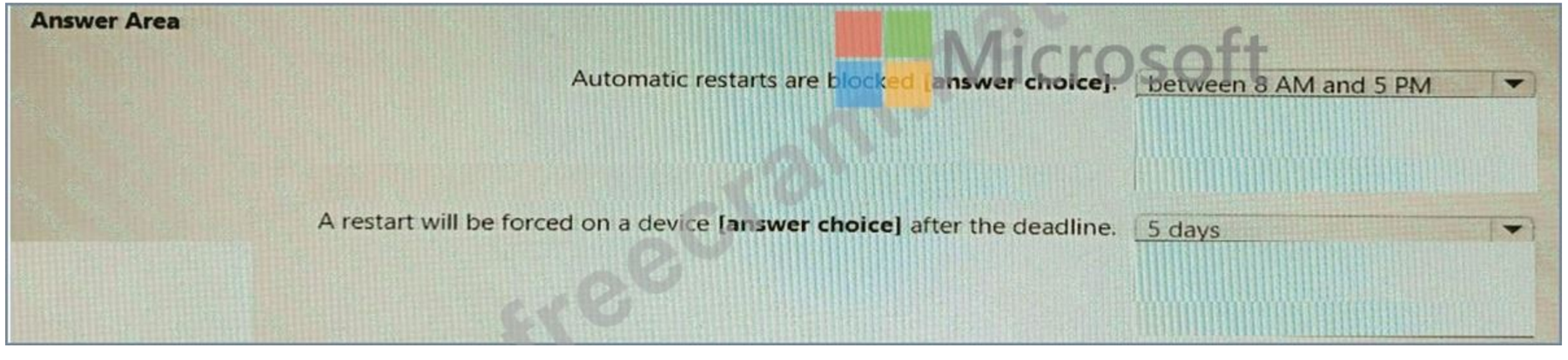
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 27
You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:
* Ensure that you can manage the personal devices by using Microsoft Intune.
* Ensure that users can access company data seamlessly from their personal devices.
* Ensure that users can only sign in to their personal devices by using their personal account What should you use to add the devices to Azure AD?
A. hybrid Microsoft Entra join
B. Microsoft Entra joined
C. Microsoft Entra registered
Answer: (SHOW ANSWER)
To implement MDM for personal devices that run Windows 11, you should use Azure AD registered. Azure AD registered devices are devices that are connected to your organization's resources using a personal device and a personal account. You can manage these devices by using Microsoft Intune and enable seamless access to company data. Users can only sign in to their personal devices by using their personal account, not their organizational account. Azure AD registered devices support Windows 10 or newer, iOS, Android, macOS, and Ubuntu 20.04/22.04 LTS1.
The other options are not suitable for this scenario because:
* Hybrid Azure AD join is for corporate-owned and managed devices that are joined to both on-premises Active Directory and Azure AD. Users can sign in to these devices by using their organizational account that exists in both directories2.
* AD joined is for devices that are joined only to on-premises Active Directory. These devices are not managed by Microsoft Intune and do not have access to cloud resources3.
References: What are Azure AD registered devices?, What are hybrid Azure AD joined devices?, What is an Active Directory domain join?

NEW QUESTION: 28
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.	O	O
On January 8, Device1 is marked as compliant.	O	O
On January 8, Device2 is marked as compliant.	O	O

Answer:

Statements	Yes	No
On January 7, Device1 is marked as compliant.	O	O
On January 8, Device1 is marked as compliant.	O	O
On January 8, Device2 is marked as compliant.	O	O

Explanation:

Statements	Yes	No
On January 7, Device1 is marked as compliant.	O	O
On January 8, Device1 is marked as compliant.	O	O
On January 8, Device2 is marked as compliant.	O	O

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: 29
You have a Microsoft 365 subscription that contains devices enrolled Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows
Device2	iOS
Device3	macOS

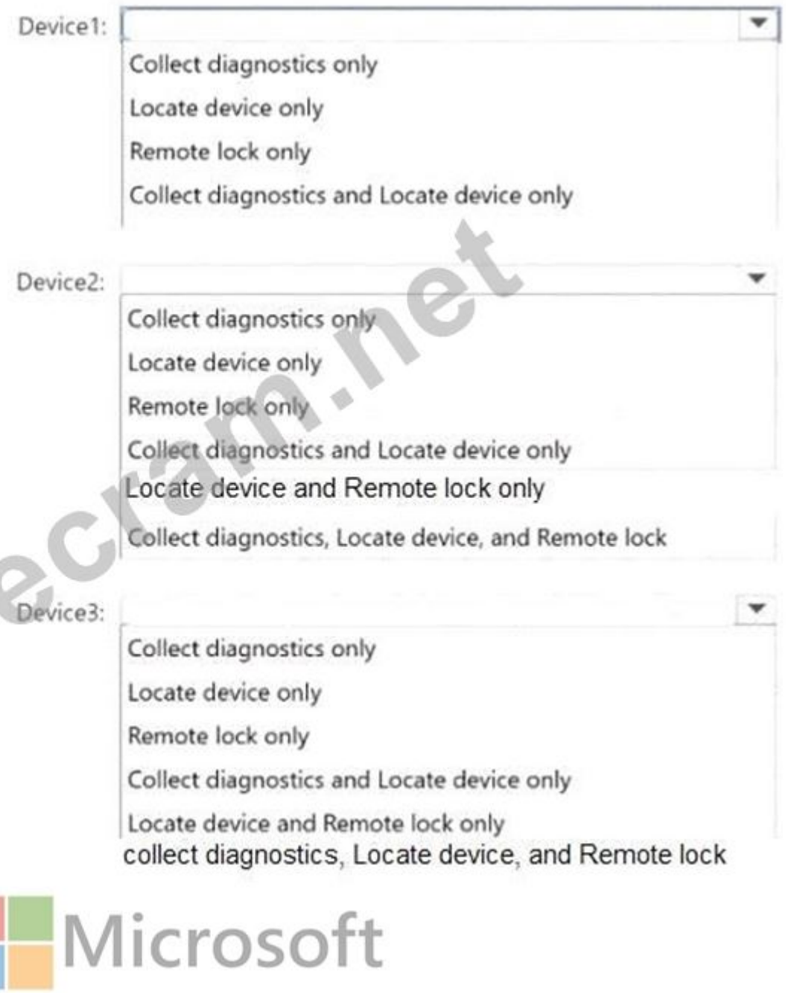
You plan to use the following remote actions on the devices:

* Collect diagnostics
* Locate device
* Remote lock

Which remote actions does each device support? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



freecram.net

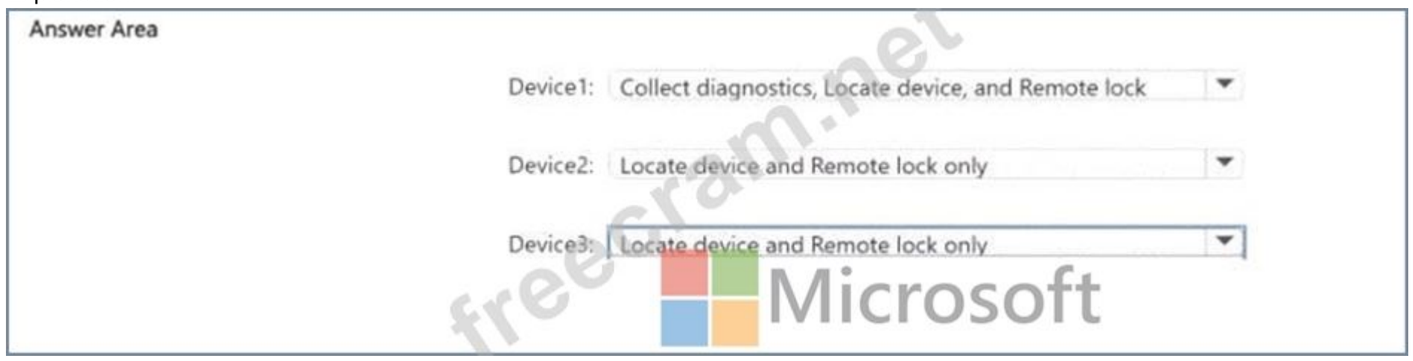
collect diagnostics, Locate device, and Remote lock

Microsoft

Answer:

Answer Area

Explanation:



NEW QUESTION: 30

-

You have a Microsoft 365 subscription that contains devices enrolled in Microsoft Intune.

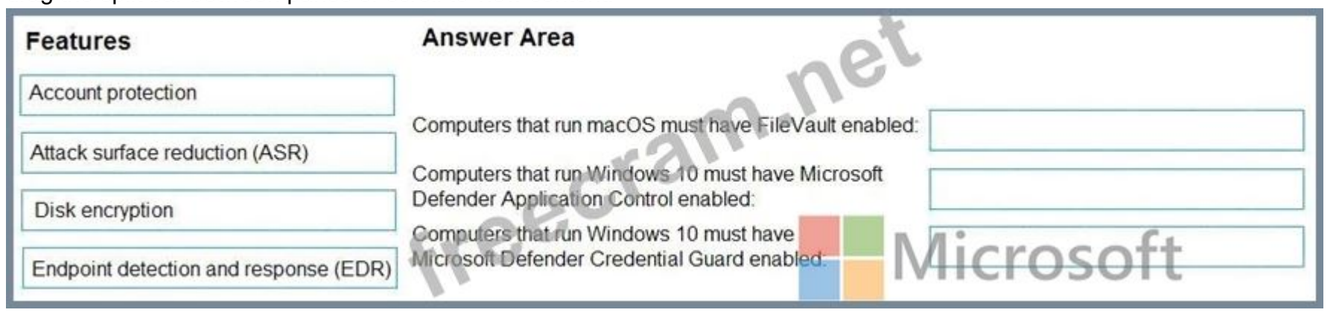
You need to create Endpoint security policies to enforce the following requirements:

* Computers that run macOS must have FileVault enabled.

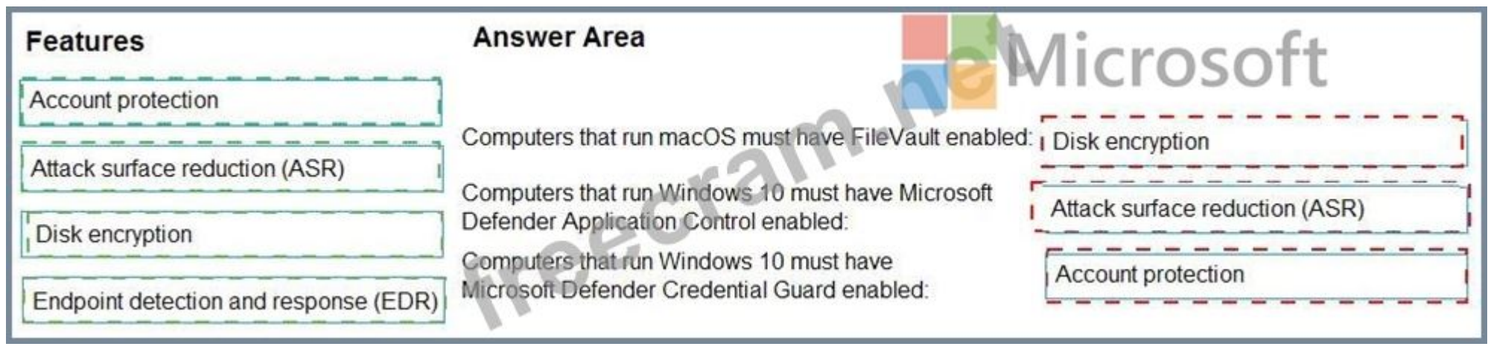
* Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled.

* Computers that run Windows 10 must have Microsoft Defender Application Control enabled.

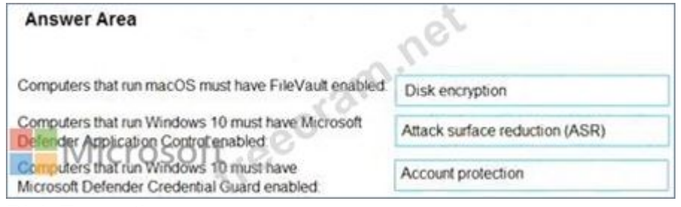
Which Endpoint security feature should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:



Explanation:



Disk Encryption

ASR - Ref https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy#:~:text=Application%20control%20%2D%20Application,Constrained%20Language%20Mode.

Account Protection - Ref https://learn.microsoft.com/en-us/windows/security/identity-protection/credential- guard/configure?tabs=intune#:~:text=You%20can%20also%20configure%20Credential%20Guard%20by%20using%20an%20account%20protection%20profile%20in%20endpoint%20security.

NEW QUESTION: 31

Your company has 200 computers that run Windows 10. The computers are managed by using Microsoft Intune. Currently, Windows updates are downloaded without using Delivery Optimization. You need to configure the computers to use Delivery Optimization. What should you create in Intune?

A. a device compliance policy

B. a device configuration profile

C. a Windows 10 update ring

D. an app protection policy
Answer: (SHOW ANSWER)

Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 32
Which user can enroll Device6 in Intune?
A. User4 and User 1 only
B. User1, User2, User3, and User4
C. User4. User Land User2 only
D. User4 and User2 only
Answer: (SHOW ANSWER)

NEW QUESTION: 33
In Microsoft Intune, you have the device compliance policies shown in the following table.

Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8.1 and later	Require	*Not applicable*	5 days	Group1
Policy2	Windows 10 and later	Not configured	Require	7 days	Group2
Policy3	Windows 10 and later	Require	Require	10 days	Group2

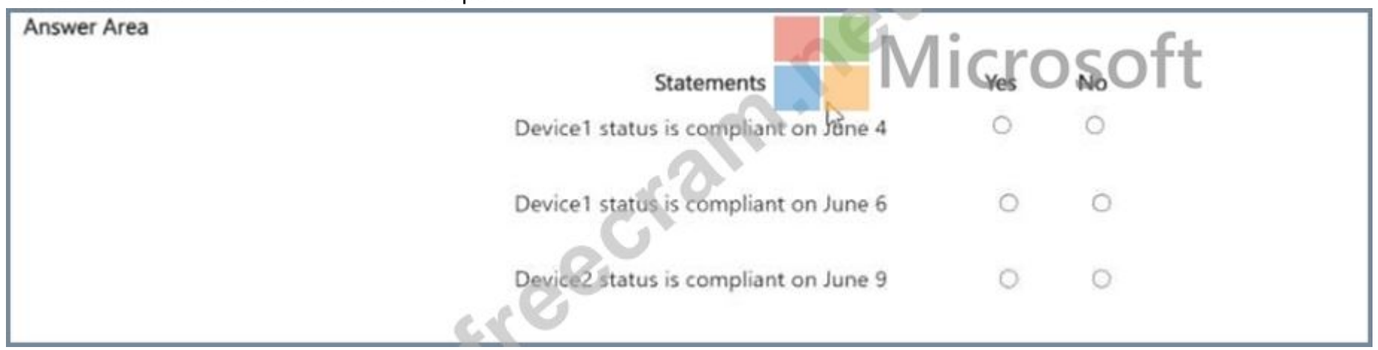
The Intune compliance policy settings are configured as shown in the following exhibit.



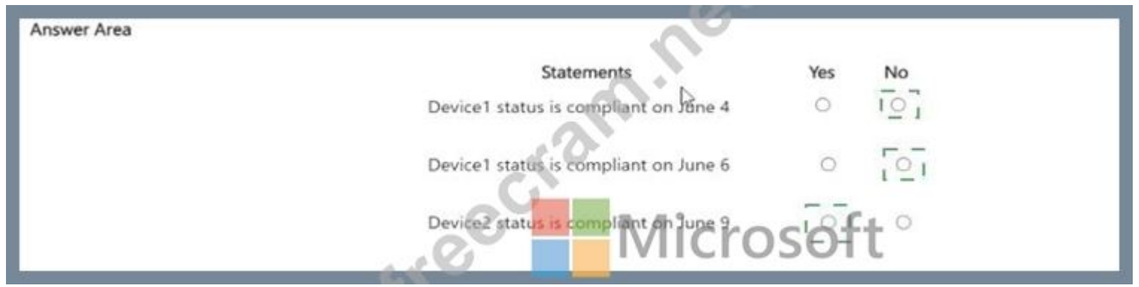
On June 1, you enroll Windows 11 devices in Intune as shown in the following table.

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

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



Answer:



Explanation:



NEW QUESTION: 34
You have an Azure AD tenant named contoso.com.
You plan to purchase 25 computers that run Windows 11. You plan to deliver the computers directly to users.
You need to ensure that during the out-of-box experience (OBE), users are prompted to sign in, and then the computers are configured to use Microsoft Intune.
Which two components should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a provisioning package
B. automatic enrollment
C. an unattend.xml answer file
D. a Windows Autopilot deployment profile for self-deploying mode
E. a Windows Autopilot deployment profile for user-driven mode
Answer: (SHOW ANSWER)
Self-deploying mode doesn ' t presently associate a user with the device (since no user ID or password is specified as part of the process).
Ref: https://learn.microsoft.com/en-us/autopilot/self-deploying#:~:text=Self%2Ddeploying%20mode%
20doesn%27t%20presently%20associate%20a%20user%20with%20the%20device%20(since%20no%
20user%20ID%20or%20password%20is%20specified%20as%20part%20of%20the%20process).
Windows Autopilot user-driven mode
Ref: https://learn.microsoft.com/en-us/autopilot/user-driven#:~:text=Specify%20your%20e%2Dmail%
20address%20and%20password%20for%20your%20organization%20account.

NEW QUESTION: 35
You have a Microsoft 365 subscription.
You need provide a user the ability to disable Security defaults and 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: (SHOW ANSWER)
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: 36
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the devices shown in the following table.

Name	Operating system	Azure AD status	Mobile device management (MDM)
Device1	Windows 8.1	Registered	*None*
Device2	Windows 10	Joined	*None*
Device3	Windows 10	Joined	Microsoft Intune

Contoso.com contains the Azure Active Directory groups shown in the following table.

Name	Members
Group1	Group2, Device1, Device3
Group2	Device2

You add a Windows Autopilot deployment profile. The profile is configured as shown in the following exhibit.

Create profile ...

Windows PC

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

Summary

Basics

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

Out-of-box experience (OOBE)

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

Assignments

Included groups	Group1
Excluded groups	--

freecram.net
Microsoft

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
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using	○	○

Answer:

Statements	Yes	No
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using	○	○

Explanation:
Box 1: No
Device1 has no Mobile device Management (MDM) configured.
Note: Device1 is running Windows 8.1, and is registered, but not joined.
Device1 is in Group1.
Profile1 is assigned to Group1.
Box 2: No
Device2 has no Mobile device Management (MDM) configured.
Note: Device2 is running Windows 10, and is joined.
Device2 is in Group2.
Group2 is in Group1.
Profile1 is assigned to Group1.
Box 3: Yes

Device3 has Mobile device Management (MDM) configured.
Device3 is running Windows 10, and is joined
Device1 is in Group1.
Profile1 is assigned to Group1.
Mobile device management (MDM) enrollment: Once your Windows 10 device joins Azure AD, Autopilot ensures your device is automatically enrolled with MDMs such as Microsoft Intune. This program can automatically push configurations, policies and settings to the device, and install Office 365 and other business apps without you having to get IT admins to manually sort the device. Intune can also apply the latest updates from Windows Update for Business.
Reference: https://xo.xello.com.au/blog/windows-autopilot

NEW QUESTION: 37
-
You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	RAM	Storage	TPM version
Device1	14 GB	256 GB	1.2
Device2	4 GB	64 GB	2.0
Device3	8 GB	128 GB	2.0

All the devices will be reimaged and licensed by using subscription activation.
The devices are assigned to the users shown in the following table.

Name	Device	License
User1	Device1	Microsoft 365 E5
User2	Device2	Microsoft 365 E3
User3	Device3	Office 365 E5, Enterprise Mobility + Security E5

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

Answer Area

Statements	Yes	No
Device1 can be upgraded to Windows 11 and activated.	○	○
Device2 requires additional hardware before it can be upgraded to Windows 11.	○	○
User3 requires an additional license to activate Windows 11 on Device3.	○	○

Answer:



Explanation:



NEW QUESTION: 38

You need to prepare for the deployment of the Phoenix office computers.

What should you do first?

A. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Azure Active Directory admin center.

B. Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

C. Extract the hardware ID information of each computer to an XML file and upload the file from the Devices settings in Microsoft Store for Business.

D. Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices

NEW QUESTION: 39

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

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

What two configurations should you perform from the Microsoft Intune admin center? Each correct answer is a complete solution.

NOTE: Each correct selection is worth one point.

A. a Windows 10 and later update ring

B. a Windows 10 and later security baseline

C. a device restrictions device configuration profile

D. a custom device configuration profile

E. an app configuration policy

Answer: (SHOW ANSWER)

NEW QUESTION: 40

You have a hybrid environment that contains a Microsoft Entra tenant and an on-premises Active Directory Domain Services (AD DS) domain. The environment contains the devices shown in the following table.

Name	Platform	Domain status
Device1	Windows 11	Workgroup
Device2	iOS	*Not applicable*

Which Microsoft Entra join type can each device use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 41

You have a Microsoft 365 E5 subscription that contains a group named Group1. You need to ensure that only the members of Group1 can join devices to the Microsoft Entra tenant. What should you configure in the Microsoft Entra admin center?

A. Enterprise State Roaming

B. Device settings

C. Mobility

D. User settings

Answer: (SHOW ANSWER)

NEW QUESTION: 42

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

You use Microsoft Intune to manage devices.

You have the devices shown in the following table.

Name	Operating system	Activation type
Device1	Windows 10 Pro for Workstation	Key
Device2	Windows 11 Pro	Key
Device3	Windows 11 Pro	Subscription

Which devices can be changed to Windows 11 Enterprise by using subscription activation?

A. Device3 only

B. Device2 and Device3 only

C. Device 1 and Device2 only

D. Device1, Device2, and Device3

Answer: (SHOW ANSWER)

https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation#subscription- activation-for-enterprise:~:text=For%20versions%20of%20Windows%20newer%20than%20Windows%2010%2C%20an%20upgrade%20to%20Windows%2010%20would%20first%20be%20required%2C%20followed%20by%20upgrading%20to%20the%20version%20of%20Windows%20Enterprise%20newer%20than%20Windows%2010

NEW QUESTION: 43

You have a Microsoft 365 subscription that uses Microsoft Intune and contains I.GOD Windows 11 devices The operational baseline for the subscription shows that fewer than one percent of Windows endpoints ate unhealthy You need to compare the current conditions with the established operational baseline. The solution must meet the following requirements

* Show timely endpoint health data for the devices

* Show current Intune incidents and advisories that affect the Intune tenant Which two resources should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Service health and message center

B. Device diagnostics in Tenant admin

C. the Windows 10/11 unhealthy endpoints report

D. a device compliance trends report

E. the Antivirus agent status report

Answer: (SHOW ANSWER)

NEW QUESTION: 44
You have a Microsoft 365 subscription that uses Microsoft Intune and contains a group named Group1.
You have a line-of-business (LOB) app named App1 that supports in-app notifications. App1 is assigned to all the users in subscription.
You need to ensure that the users in Group1 receive a custom notification when they launch App1.
What should you do?
A. Create an app configuration policy and assign the policy to Group1.
B. Create a device configuration profile and assign the profile to Group1.
C. Edit the assignment for App1.
D. Create an app protection policy and assign the policy to Group1.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
You have a Microsoft 365 E5 subscription that contains a group named Group! and 500 mobile devices that run Android or iOS.
You need to create app protection policies and Conditional Access policies for the subscription. The solution must meet the following requirements:
* Encrypt corporate data stored on the mobile devices.
* Automatically remove corporate data stored on a mobile device if the device is offline for 45 days.
* Ensure that only users assigned app protection policies can use mobile devices to access the subscription
* On the mobile devices used only by Group1, automatically remove corporate data stored on the devices if the devices are offline for 30 days.
What is the minimum number of policies you should create? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



freecram.net Microsoft
Answer:



Explanation:

Answer Area



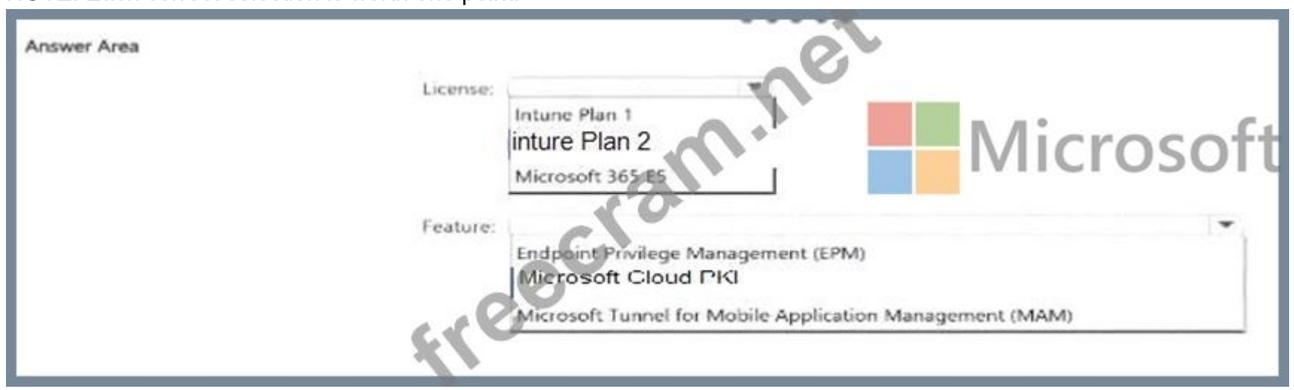
NEW QUESTION: 46

You have a Microsoft 365 E3 subscription

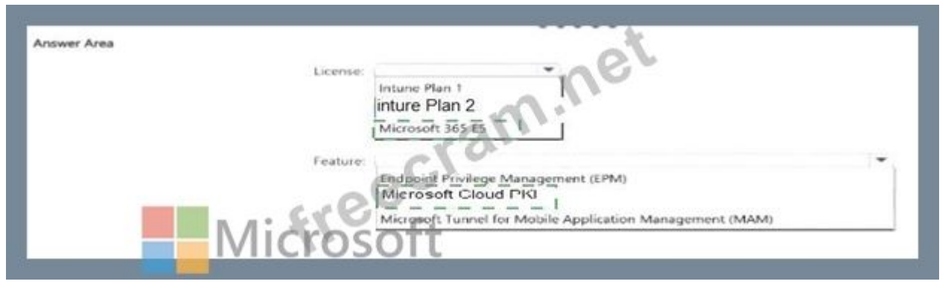
You need to recommend a Microsoft Intune solution to manage certificate based authentication for Wi Fi and VPN connections The solution must support certificate lifecycle management.

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.



Answer:



Explanation:



Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47
You have a Microsoft 365 E5 subscription.
You need to manage operating system updates for corporate-owned Android Enterprise devices enrolled in Microsoft Intune. What should you use?
A. a configuration profile
B. a compliance policy
C. an Endpoint security policy
D. an Android FOTA deployment
Answer: (SHOW ANSWER)

NEW QUESTION: 48
You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.
You create a user named User1.
You need to ensure that User1 can rotate Bitlocker recovery keys by using Intune.
Solution: From the Microsoft Intune admin center, you assign the Help Desk Operator role to User1.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 49

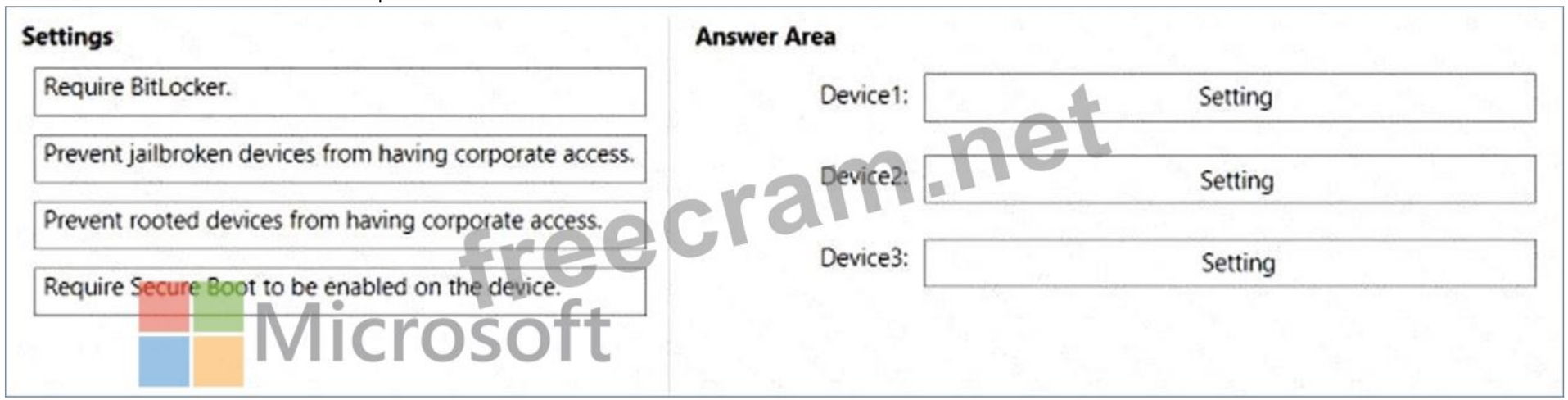
You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

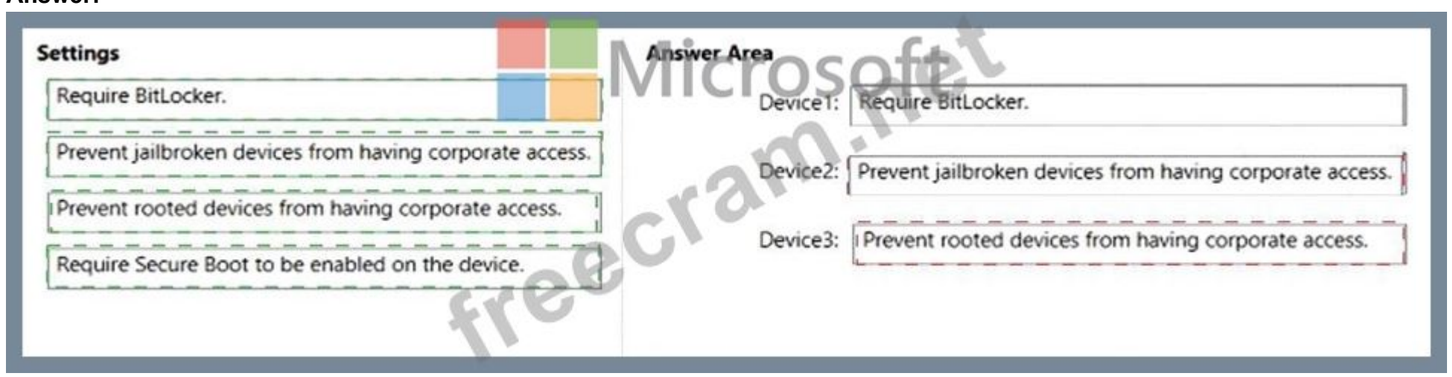
You need to ensure that only devices running trusted firmware or operating system builds can access network resources.

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.



Answer:



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: 50

You have an Azure AD tenant named contoso.com.
You have a workgroup computer named Computer1 that runs Windows 11.
You need to add Computer1 to contoso.com.
What should you use?

Freecram.net

A. dsreecmd.exe
B. the Settings app
C. netdom.exe
D. Computer Management
Answer: (SHOW ANSWER)

NEW QUESTION: 51

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: (SHOW ANSWER)

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: 52

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: (SHOW ANSWER)

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-lifetime

NEW QUESTION: 53

You have a Microsoft 365 subscription that contains 1.000 Windows 11 devices enrolled in Microsoft Intune.

You plan to use Intune to deploy an application named App1 that contains multiple installation files.

What should you do first?

A. Create an Android application package (APK).

B. Upload the contents of App1 to Intune.
C. Install the Microsoft Deployment Toolkit (MDT).
D. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
You have a Microsoft 365 subscription.
You need to enable passwordless authentication for all users. The solution must meet the following requirements:
* Users in the research department cannot use mobile devices and must authenticate from unmanaged Linux devices by using an alternative method.
* To access services, users in the sales department must authenticate by using their mobile phone.
* Administrative effort must be minimized.
Which authentication method should you use for each department? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Explanation:



NEW QUESTION: 55

You have a Microsoft 365 subscription that uses Microsoft Intune and contains a Microsoft Tunnel for Mobile Application Management (MAM) instance.

You have the devices shown in the following table.

Name	Operating system
Device1	Android
Device2	iOS

You need to ensure that you can use Tunnel for MAM on each device. The solution must minimize the number of apps required on each device.

Which apps should you install on each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 56

You have a Microsoft 365 subscription that includes Microsoft Intune.

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

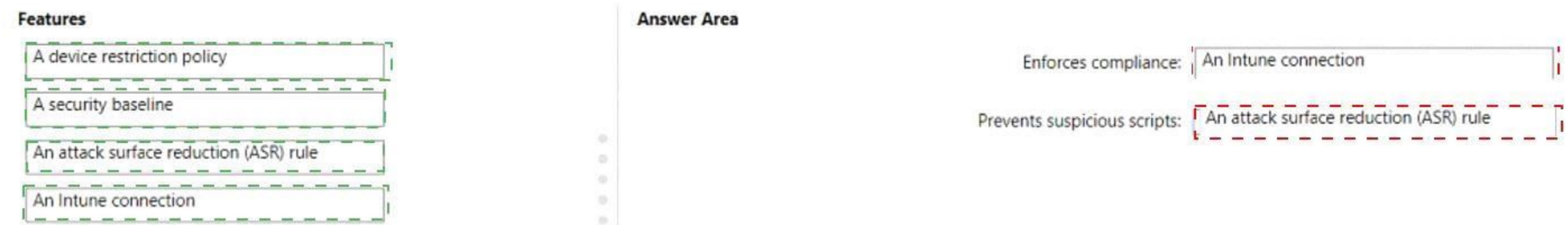
* Enforces compliance for Defender for Endpoint by using Conditional Access
* Prevents suspicious scripts from running on devices

What should you configure? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:



To enforce compliance for Defender for Endpoint by using Conditional Access, you need to configure an Intune connection in the Defender for Endpoint portal. This allows you to use Intune device compliance policies to evaluate the health and compliance status of devices that are enrolled in Defender for Endpoint.

You can then use Conditional Access policies to block or allow access to cloud apps based on the device compliance status. References: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/conditional-access To prevent suspicious scripts from running on devices, you need to configure an attack surface reduction (ASR) rule in Intune. ASR rules are part of the endpoint protection settings that you can apply to devices by using device configuration profiles. You can use the ASR rule "Block Office applications from creating child processes" to prevent Office applications from launching child processes such as scripts or executables.

References: https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10#attack- surface-reduction-asr-rules

NEW QUESTION: 57

You have a Microsoft Entra tenant that contains the following:

* Windows 11 devices that are joined to Microsoft Entra

* A user that has a display name of User1 and a UPN of user1@contoso.com You enable Remote Desktop on the Windows 11 devices.
You need to ensure that User1 can use Remote Desktop to connect to the devices.
How should you complete the command that must be run on each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 58
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra registered
Device2	Windows 11	Microsoft Entra joined
Device3	Android	Microsoft Entra registered
Device4	iOS	Microsoft Entra registered

All the devices are enrolled in Microsoft Intune and have Microsoft 365 Apps for enterprise installed On which devices can you use the Cloud Policy service for Microsoft 365 to manage Microsoft 365 Apps for enterprise?
A. Device1 only
B. Device1, Device2. Device3. and Device4
C. Device1, Device2, and Device3 only
D. Device1, Device2, and Device4 only
E. Device1 and Device2 only
Answer: (SHOW ANSWER)

NEW QUESTION: 59
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: (SHOW ANSWER)
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: 60
You have an Azure AD tenant named contoso.com.
You need to ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com.
What should you configure?
Freecram.net
A. Windows Autopilot
B. provisioning packages for Windows
C. Security defaults in Azure AD
D. Device settings in Azure AD
Answer: A (LEAVE A REPLY)
To ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com, you should configure theDevice settings in Azure AD. The Device settings allow you to manage which users can join devices to Azure AD and whether they are added as local administrators or standard users. By default, users who join devices to Azure AD are added to the local Administrators group, but you can change this setting to None or Selected1.
The other options are not relevant for this scenario because:
* Windows Autopilot is a service that allows you to pre-configure new devices and enroll them automatically to Azure AD and Microsoft Intune. It does not control the local administrator role of the users who join the devices2.
* Provisioning packages for Windows are files that contain custom settings and policies that can be applied to Windows devices during the setup process. They do not affect the Azure AD join process or the local administrator role of the users3.
* Security defaults in Azure AD are a set of basic identity security mechanisms that are enabled by default to protect your organization from common attacks. They do not include any settings related to device management or local administrator role4.
References: Manage device identities using the Microsoft Entra admin center, Windows Autopilot, Provisioning packages for Windows 10, What are security defaults?

NEW QUESTION: 61
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage Windows 11 devices.
You create a new policy set named Set and add five device configuration profiles for Windows 10 and later.
You create a device compliance policy named Policy1.
You need to ensure that when users are assigned the device configuration profiles in Set1, they are always assigned Policy1 also.
What should you configure?
A. the assignments of Policy1
B. the Policy1 configurations
C. the assignments of Set1

D. the Set1 configurations
Answer: C (LEAVE A REPLY)
You can include the following management objects in a policy set:
Apps
App configuration policies
App protection policies
Device configuration profiles
Device compliance policies
Windows autopilot deployment profiles
Enrollment status page
Settings catalog policies

Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 62
You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows
Device2	Android
Device3	iOS
Device4	macOS

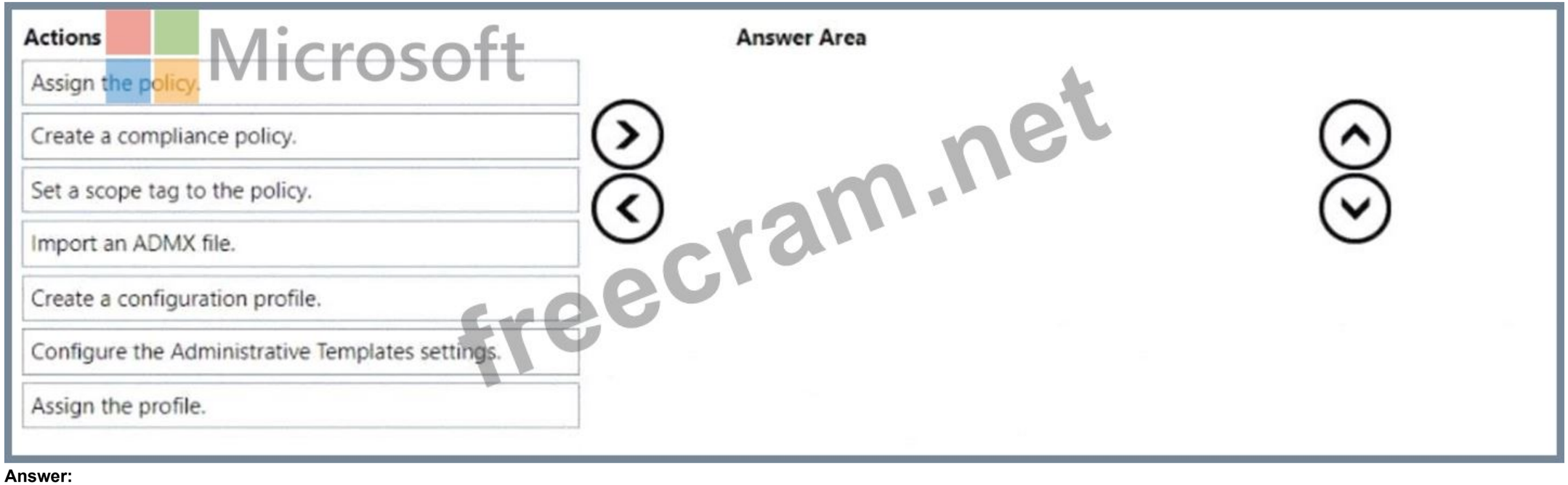
For which devices can you manage updates by using intune?
A. Devic1l only
B. Device1 and Oevice2 only
C. Device 1 and Device3 only
D. Device 1. Device3, and Device4 only
E. Device 1. Device2, Device3, and Device4
Answer: (SHOW ANSWER)

NEW QUESTION: 63
You have a Microsoft 365 subscription that uses Microsoft Intune and has the following advanced analytics reports enabled:
* Endpoint analytics
* Application reliability
* Work from anywhere
You purchase a new device named Device1 that is enrolled in Intune. You need to ensure that advanced analytics reports can be generated for Device1. Which telemetry should you enable for Device1?
A. hardware specifications
B. remote wipe status

C. device cloud-only identity information
D. endpoint performance and user experience data
Answer: (SHOW ANSWER)

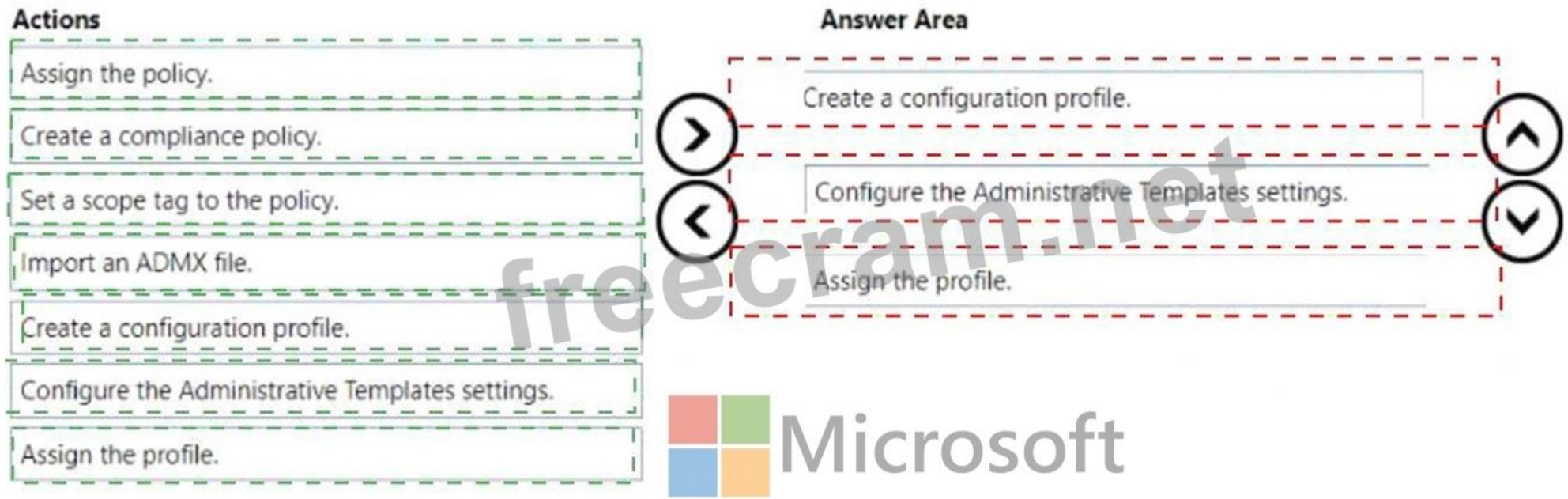
NEW QUESTION: 64
You have a Microsoft 365 E5 subscription.
All devices are enrolled in Microsoft Intune.
You need to ensure that devices that have NOT checked in for 30 days are deleted from intune.
What should you configure from the Microsoft Intune admin center?
A. a device limit restriction
B. a device clean-up rule
C. a configuration profile
D. automatic enrollment
Answer: (SHOW ANSWER)

NEW QUESTION: 65
You have an on-premises Active Directory domain that syncs to Azure AD tenant.
The tenant contains computers that run Windows 10. The computers are hybrid Azure AD joined and enrolled in Microsoft Intune. The Microsoft Office settings on the computers are configured by using an Group Policy Object (GPO).
You need to migrate the GPO to Intune.
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.



Microsoft
freecram.net

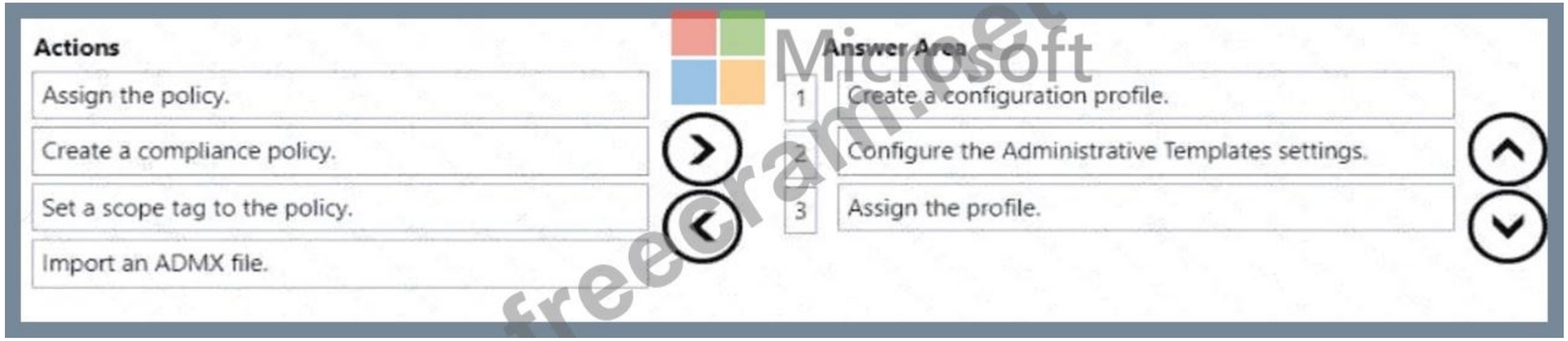
Answer:



freecram.net

Microsoft

Explanation:



freecram.net

Microsoft

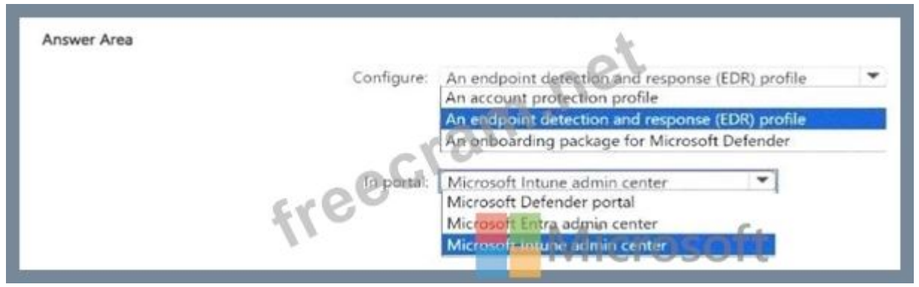
NEW QUESTION: 66

You have a Microsoft 365 subscription that includes Microsoft Intune and Microsoft Defender for Endpoint.

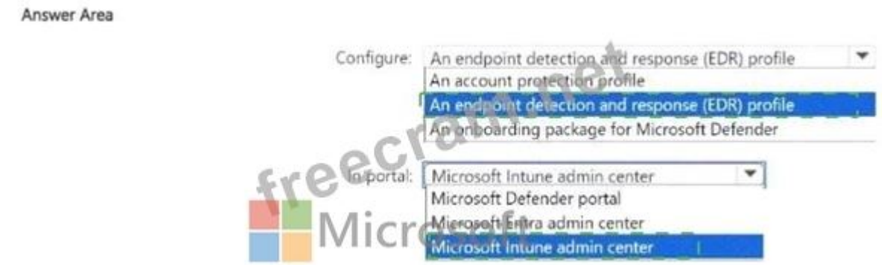
Users have devices that run Windows 11.

You deploy a connection from Defender for Endpoint to Intune.

You need to ensure that when a device is enrolled in Intune, the device is onboarded automatically to Defender for Endpoint What should you configure, and which portal should you use? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 67

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. No

B. Yes

Answer: (SHOW ANSWER)

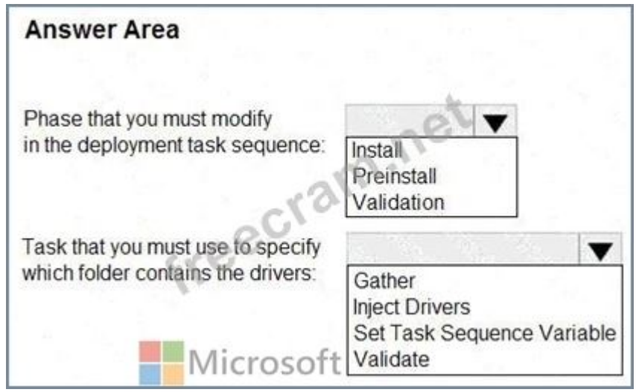
NEW QUESTION: 68

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

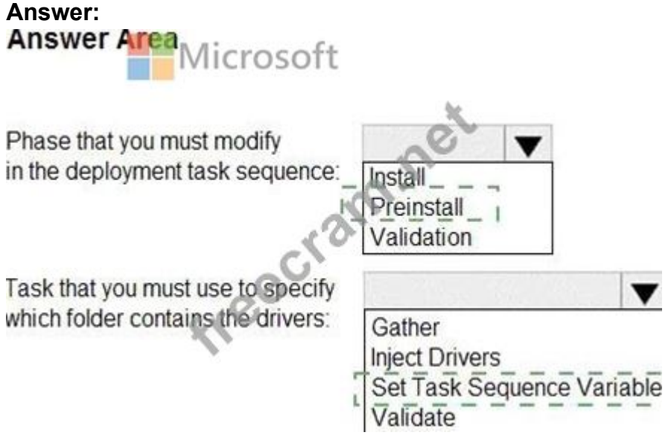
Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	iOS

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: (SHOW ANSWER)
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: 69
-
You manage a Microsoft Deployment Toolkit (MDT) deployment share named DS1. DS1 contains an Out-of- Box Drivers folder named Windows 11 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.

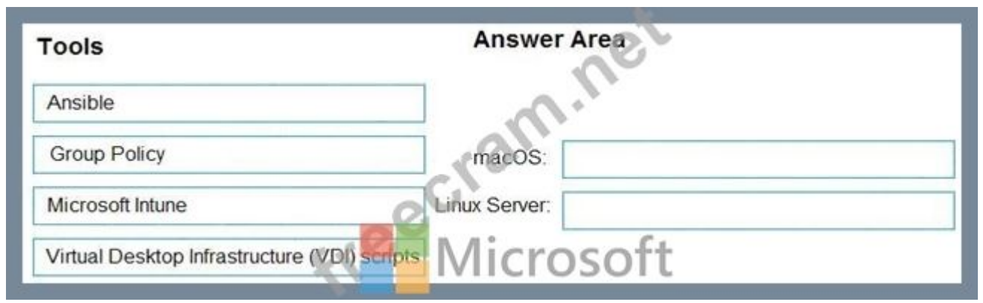


Answer:

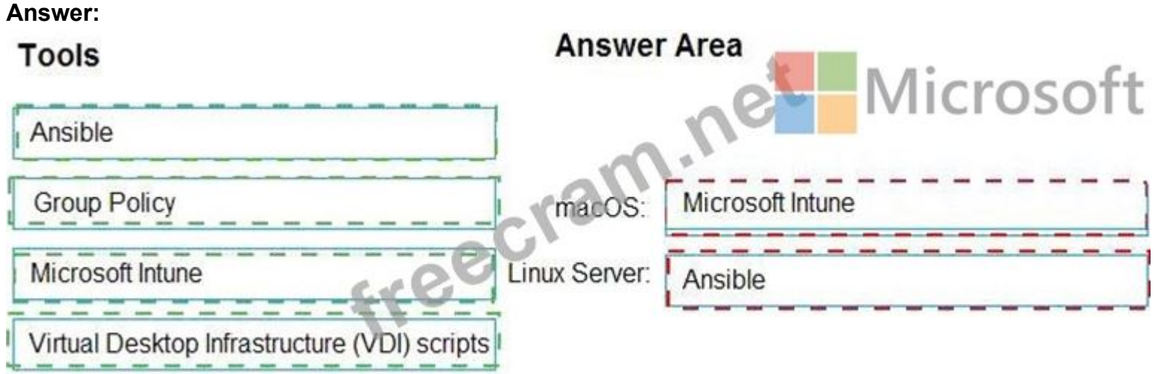


Explanation:
Preinstall
Set Task Sequence Variable

NEW QUESTION: 70
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.
You plan to onboard the following types of devices to Defender for Endpoint:
* macOS
* Linux Server
What should you use to onboard each device? To answer, drag the appropriate tools to the correct device types. Each tool 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.



Answer:



Explanation:



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

NEW QUESTION: 71

You have a Microsoft 365 E5 subscription. All Windows devices are enrolled in Microsoft Intune.

You need to create an app protection policy named Policy1 and apply Policy1 to the devices. What can you protect by using Policy1?

A. Microsoft OneDrive

B. Microsoft Teams

C. Microsoft Outlook

D. Microsoft Edge

Answer: (SHOW ANSWER)

NEW QUESTION: 72

Your company has a Microsoft 365 subscription.

All the users in the finance department own personal devices that run iOS or Android. All the devices are enrolled in Microsoft Intune.

The finance department adds new users each month.
The company develops a mobile application named App1 for the finance department users.
You need to ensure that only the finance department users can download Appl.
What should you do first?
A. Register App1 in Microsoft Entra.
B. Add App1 to a Microsoft Deployment Toolkit (MDT) deployment share.
C. Add App1 to Intune.
D. Add App1 to the vendor stores for iOS and Android applications.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 73
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: (SHOW ANSWER)
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: 74
You have a Microsoft 365 tenant and an internal certification authority (CA).
You need to use Microsoft Intune to deploy the root CA certificate to managed devices.
Which type of Intune policy and profile should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Policy type:

App configuration policy
App protection policy
Compliance policy
Configuration profile

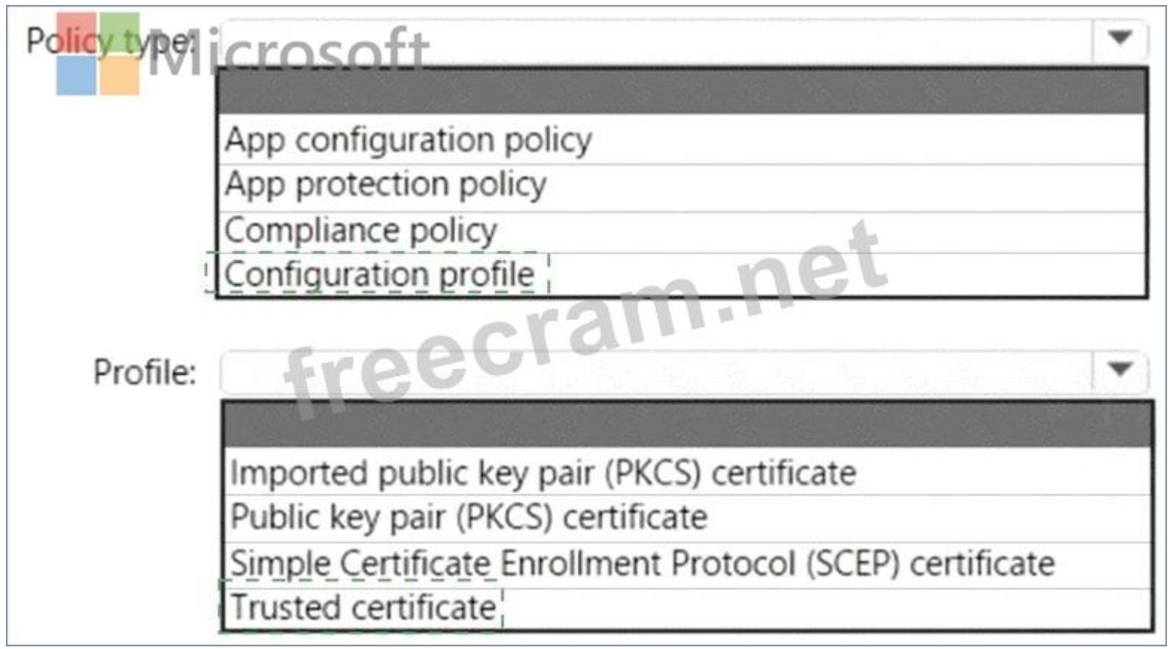
freecram.net

Microsoft

Profile:

Imported public key pair (PKCS) certificate
Public key pair (PKCS) certificate
Simple Certificate Enrollment Protocol (SCEP) certificate
Trusted certificate

Answer:



Explanation:

Box 1: Configuration profile

Create a trusted certificate profile.

Box 2: Trusted certificate

When using Intune to provision devices with certificates to access your corporate resources and network, use a trusted certificate profile to deploy the trusted root certificate to those devices. Trusted root certificates establish a trust from the device to your root or intermediate (issuing) CA from which the other certificates are issued.

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root

NEW QUESTION: 75

You have a Windows 11 capable device named Device1 that runs the 64-bit version of Windows 10 Enterprise and has Microsoft Office 2019 installed. You have the Windows 11 Enterprise images shown in the following table.

Name	Platform	Description
Image1	x64	Custom Windows 11 image that has Office 2021 installed
Image2	x64	Default Windows 11 image created by Microsoft

Which images can be used to perform an in-place upgrade of Device1?

A. image1 only

B. Image1 and Image2

C. Image2only

Answer: C (LEAVE A REPLY)

NEW QUESTION: 76

You have a Microsoft 365 E5 subscription.
You use Microsoft Intune to manage all devices.
You need to prepare a Win32 app named App1.exe for deployment.
What should you do first?
A. Package App1.exe in the INTUNEWIN format.
B. Upload App1 exe to Azure Blob Storage.
C. From the Microsoft 365 Apps admin center, create a deployment configuration.
D. From the Microsoft Intune admin center, create an app configuration policy.
Answer: (SHOW ANSWER)

Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 77
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: (SHOW ANSWER)
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-reference

NEW QUESTION: 78
You have a Microsoft 365 subscription that uses Microsoft Intune.
You need to ensure that you can deploy apps to Android Enterprise devices.
What should you do first?
A. Link your managed Google Play account to Intune.
B. Add a certificate connector.
C. Configure the Partner device management settings.
D. Create a configuration profile.
Answer: (SHOW ANSWER)

NEW QUESTION: 79

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

A. Group3 and Group4 only

B. Admin1, Group3, and Group4 only

C. Group1, Group3, and Group4 only

D. Group1, Group2, Group3, and Group4 only

E. Admin1, Group1. Group2, Group3, andGroup4

Answer: C (LEAVE A REPLY)

In the Microsoft Intune admin center, you can assign apps to users or devices. Users can be assigned to apps by using user groups or individual user accounts. Devices can be assigned to apps by using device groups. In this scenario, the objects shown in the table are as follows:

Admin1 is an individual user account that belongs to the Global administrators role group.

Group1 is a user group that contains 100 users.

Group2 is a device group that contains 50 devices.

Group3 is a user group that contains 200 users.

Group4 is a device group that contains 150 devices.

Since App1 is a Microsoft 365 Apps app, it can only be assigned to users, not devices. Therefore, Group2 and Group4 are not valid objects for app assignment. Admin1 is also not a valid object for app assignment, because individual user accounts can only be used for testing purposes, not for production deployment.

Therefore, the only valid objects for app assignment are Group1 and Group3, which are user groups.

NEW QUESTION: 80

What should you configure to meet the technical requirements for the Azure AD-joined computers?

A. Windows Hello for Business from the Microsoft Intune blade in the Azure portal.

B. The Accounts options in an endpoint protection profile.

C. The Password Policy settings in a Group Policy object (GPO).

D. A password policy from the Microsoft Office 365 portal.

Answer: (SHOW ANSWER)

References:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-manage- inorganization

NEW QUESTION: 81

Your company has a Remote Desktop Gateway (RD Gateway).

You have a server named Server1 that is accessible by using Remote Desktop Services (RDS) through the RD Gateway.

You need to configure a Remote Desktop connection to connect through the gateway.

Which setting should you configure?

A. Connect from anywhere

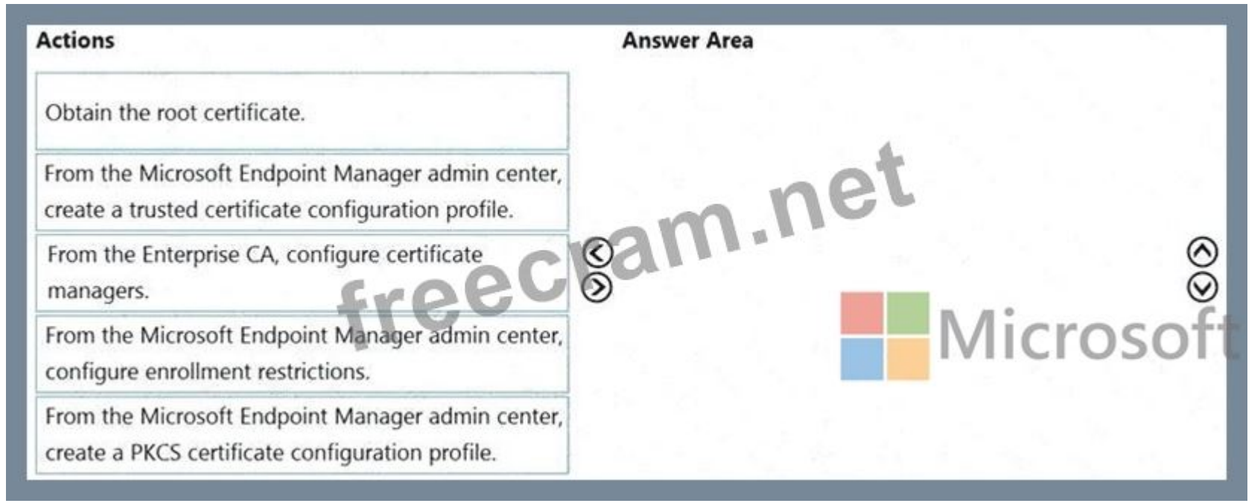
B. Server authentication

C. Connection settings
D. Local devices and resources
Answer: (SHOW ANSWER)
To connect to a remote server through the RD Gateway, you need to configure the Connect from anywhere setting in the Remote Desktop Connection client. This setting allows you to specify the domain name and port of the RD Gateway server, as well as the authentication method. The other settings are not related to the RD Gateway connection. References: Configure Remote Desktop Connection Settings for Remote Desktop Gateway

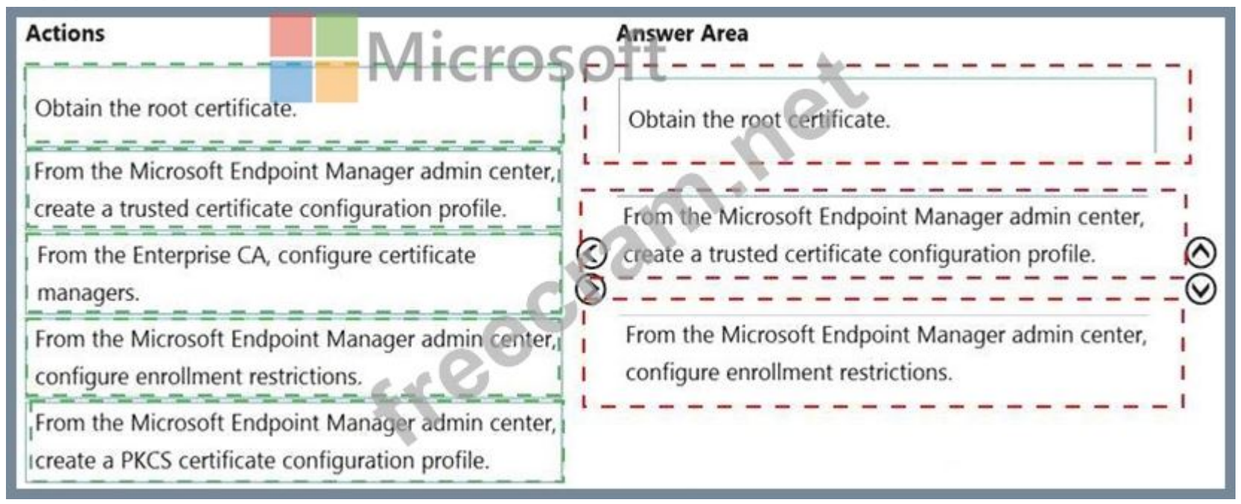
NEW QUESTION: 82
You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.
You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.
B. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.
C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.
D. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.
E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.
F. To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.
Answer: (SHOW ANSWER)
To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on Azure AD joined devices that are managed by Intune, you need to create a device configuration profile and configure the Endpoint protection settings. You can use this profile to configure various settings for firewall and antivirus protection on the devices.References:https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10

NEW QUESTION: 83
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: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients

NEW QUESTION: 84
You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on- premises Enterprise certification authority (CA).
You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure

NEW QUESTION: 85
You have a computer named Computer! that runs Windows 11.
A user named User1 plans to use Remote Desktop to connect to Computer1.
You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.
What should you do on Computer1?
A. Turn on Reputation-based protection.
B. Turn on Network Discovery.
C. Enable Network Level Authentication (NLA).
D. Configure the Remote Desktop Configuration service.
Answer: (SHOW ANSWER)

NEW QUESTION: 86
You have a Microsoft Entra tenant that contains the devices shown in the following table.

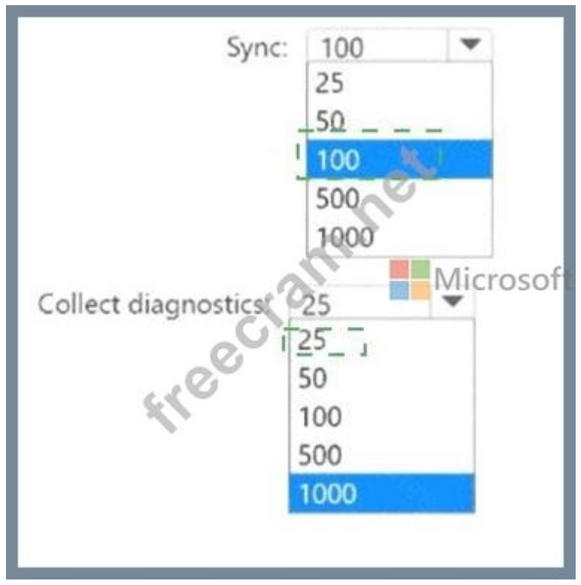
Name	Platform	Join type	Microsoft Intune
Device1	Windows 11	Microsoft Entra joined	Enrolled
Device2	Windows 11	Microsoft Entra joined	Not enrolled
Device3	Windows 11	Microsoft Entra registered	Enrolled
Device4	Android	Microsoft Entra registered	Enrolled

On which devices can you implement Endpoint Privilege Management (EPM)?
A. Device1, Device3, and Device4 only
B. Device1 and Device3 only
C. Device1 only
D. Device1, Device2. Device3, and Device4
E. Device1 and Device2 only
Answer: (SHOW ANSWER)

NEW QUESTION: 87
You have a Microsoft 365 subscription that contains 5,000 Windows devices enrolled in Microsoft Intune.
You plan to use the Sync and Collect diagnostics bulk device actions.
What is the maximum number of devices you can include in each action? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



freecram.net
Microsoft

NEW QUESTION: 88
Your network contains an Active Directory domain.
You deploy a Microsoft Entra tenant.
Another administrator configures the domain to synchronize to the Microsoft Entra tenant.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.
You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.
Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 89
You have a Microsoft 365 subscription that contains the following devices enrolled in Microsoft Intune:
* A corporate-owned Windows device named Device1
* A personally-owned Android device named Device2
You need to use a remote action on each device.
The solution must meet the following requirements:
* Repurpose Device1 by returning the device to the factory default settings.
* Remove only corporate data from Device2 and remove the device from Intune when the device checks in.
Which remote action should you use on each device? To answer, drag the appropriate remote actions to the correct devices. Each remote action 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.



Answer:



Explanation:



NEW QUESTION: 90

You are replacing 100 company-owned Windows devices.
You need to use the Microsoft Deployment Toolkit (MDT) to securely wipe and decommission the devices.
The solution must meet the following requirements:
* Back up the user state.
* Minimize administrative effort.
Which task sequence template should you use?

A. Sysprep and Capture

B. Standard Client Task Sequence

C. Standard Client Replace Task Sequence
D. Litetouch OEM Task Sequence
Answer: (SHOW ANSWER)

NEW QUESTION: 91
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.	○	○
User2 receives Notification1 on Device2.	○	○
User1 receives Notification1 on Device3.	○	○

Answer:

Statements	Yes	No
User1 receives Notification1 on Device1.	○	○
User2 receives Notification1 on Device2.	○	○
User1 receives Notification1 on Device3.	○	○

Explanation:

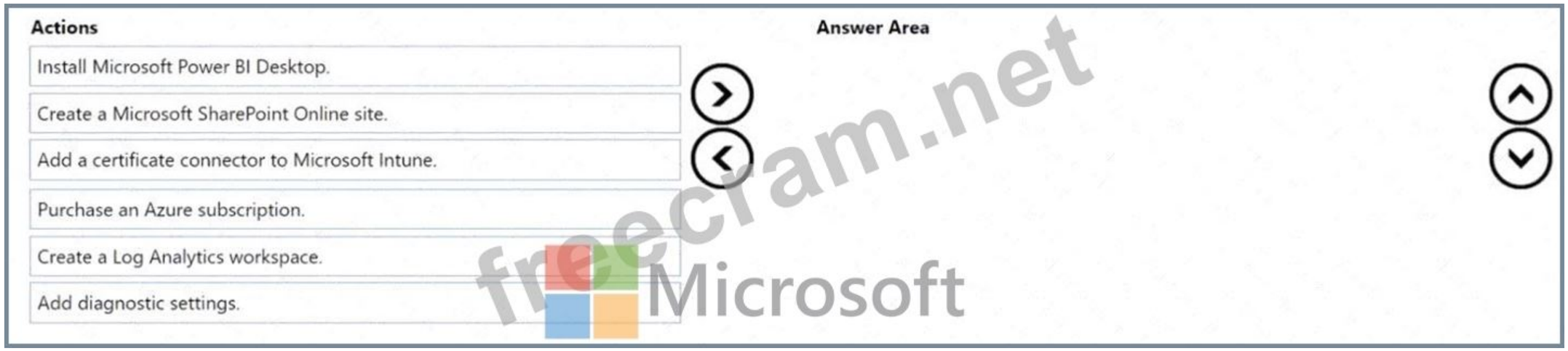


Reference:
https://docs.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications

Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

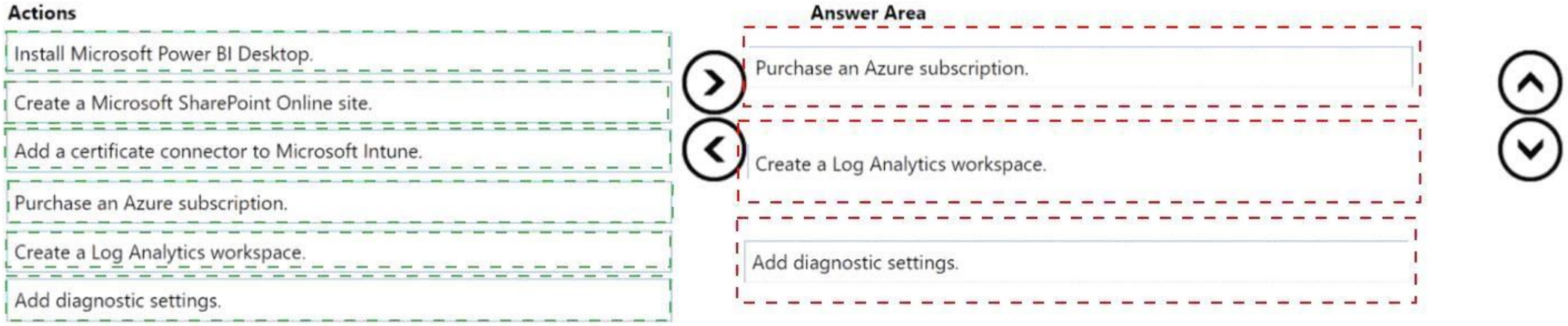
NEW QUESTION: 92
You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune.
You need to ensure that notifications of iOS updates are deferred for 30 days after the updates are released.
What should you create?
A. a device configuration profile based on the Device features template
B. a device configuration profile based on the Device restrictions template
C. an update policy for iOS/iPadOS
D. an iOS app provisioning profile
Answer: (SHOW ANSWER)
Manage iOS/iPadOS software update policies in Intune, delay visibility of software updates.
When you use update policies for iOS, you might have need to delay visibility of an iOS software update.
Reasons to delay visibility include:
Prevent users from updating the OS manually
To deploy an older update while preventing users from installing a more recent one To delay visibility, deploy a device restriction template that configures the following settings:
Defer software updates = Yes
This doesn't affect any scheduled updates. It represents days before software updates are visible to end users after release.
Delay default visibility of software updates = 1 to 90
90 days is the maximum delay that Apple supports.
Reference: https://docs.microsoft.com/en-us/mem/intune/protect/software-updates-ios

NEW QUESTION: 93
Your company has a Microsoft 365 E5 tenant.
All the devices of the company are enrolled in Microsoft Intune.
You need to create advanced reports by using custom queries and visualizations from raw Microsoft Intune data.
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.

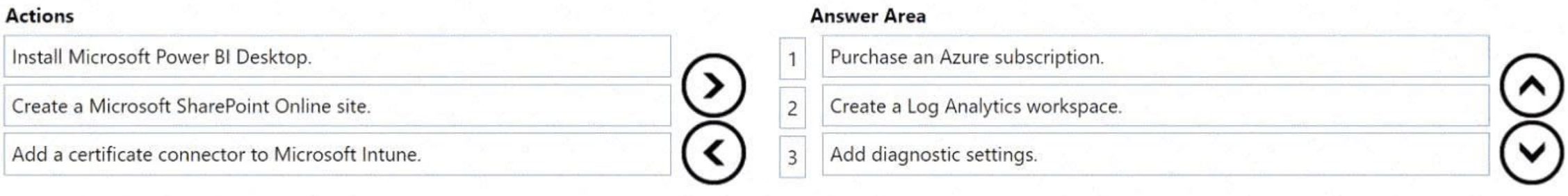


freecram.net

Answer:



Explanation:



Step 1: Purchase an Azure subscription.
Complex reporting functionality require an Azure subscription.
Step 2: Create a Log Analytics workspace.

Each Azure resource requires its own diagnostic setting. The diagnostic setting defines the following for a resource:
* One or more destinations to send the logs. Current destinations include Log Analytics workspace, Event Hubs, and Azure Storage.
* Categories of logs and metric data sent to the destinations defined in the setting. The available categories will vary for different resource types.
* Retention policy for data stored in Azure Storage.
Step 3: Add diagnostic settings.
You can create and view custom reports using the following steps:
1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Reports > Diagnostic settings add a diagnostic setting.
3. Etc.
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/reports

NEW QUESTION: 94
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 (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients

NEW QUESTION: 95
You have a Microsoft 365 E5 subscription.
You use Microsoft Intune to manage Windows 365 Cloud PC devices.
You need to deploy a Windows 365 Security Baseline to the Cloud PC devices. The solution must meet the following requirements:
* Block data execution prevention.
* Enable virtualization-based security (V8S) and Secure Boot.
What should you configure for the Windows 365 Security Baseline profile? To answer, select the appropriate options in the answer area.



Microsoft
freecram.net

Answer:



Explanation:



NEW QUESTION: 96

You have a Microsoft 365 E5 subscription that contains 100 Windows 11 devices and uses Microsoft Intune.

The devices are enrolled in Intune.

You discover that some devices take longer than others to start

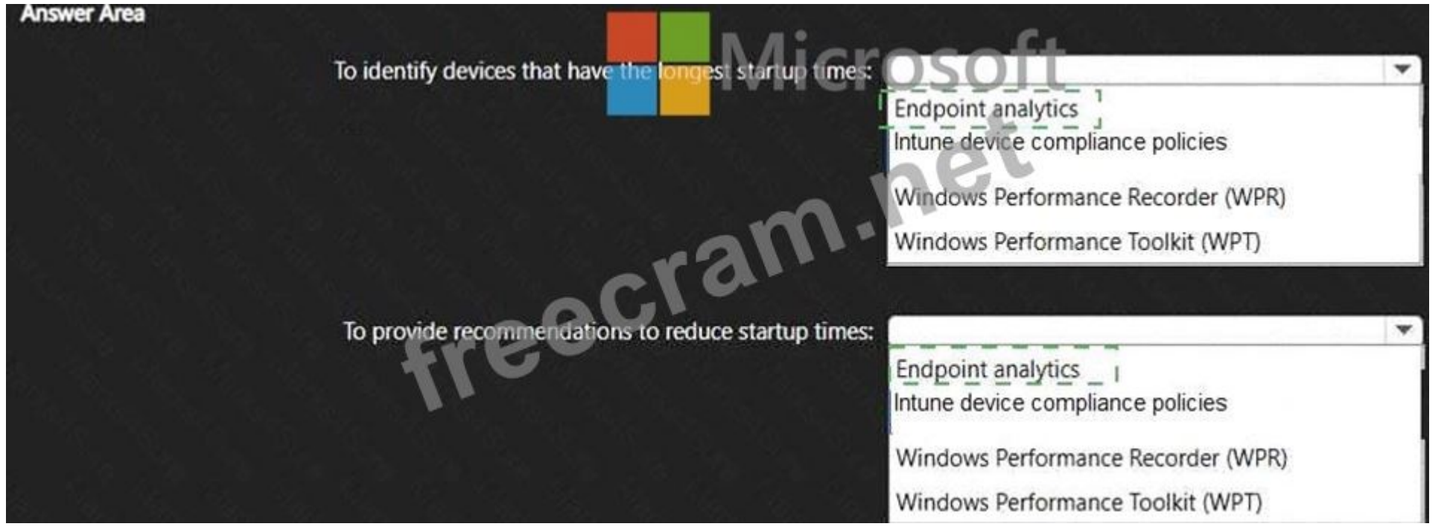
You need to identify which devices have the longest startup times. The solution must meet the following requirements:

* Track the startup times for all the devices.
* Provide recommendations to reduce startup times.
* Minimize administrative effort.

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



Answer:



Explanation:

Identify devices with the longest startup times: Endpoint analytics

* Provide recommendations to reduce startup times: Endpoint analytics

NEW QUESTION: 97

You have a Microsoft 365 subscription that contains a user named User1. The subscription contains devices enrolled in Microsoft intune as shown in the following table.

Name	Platform	Member of	Description
Device1	Windows 11	Group1	Disk encryption is not configured.
Device2	Windows 10	Group2	Disk encryption is configured.
Device3	Android	Group3	Device local storage is not encrypted.

Microsoft Edge is available on all the devices.

Intune has the device compliance policies shown in the following table.

Name	Platform	Setting	Applied to
Compliance1	Windows 10 and later	Require encryption of data storage on device	Group2
Compliance2	Android Enterprise	Require encryption of data storage on device	Group3

The Compliance policy settings are configured as shown in the exhibit. (Click the Exhibit tab.) You create the following Conditional Access policy:



* Name: Policy1
* Assignments
o Users and groups: User1
o Cloud apps or actions: Office 365 SharePoint Online
* Access controls
o Grant Require device to be marked as compliant
* Enable policy: On

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

Answer Area

Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	○	○
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	○	○
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	○	○

Answer:



Explanation:



NEW QUESTION: 98

You have a Microsoft Intune subscription.

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

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

An app named App1 is installed on each device.

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

A. 1

B. 2

C. 3

D. 4

E. 5

Answer: (SHOW ANSWER)

The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices1. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices1. The settings are assigned to user groups and applied when the app runs1. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune1. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings2. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration- policies-overview 2: Add app configuration policies for managed iOS/iPadOS devices | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-ios

NEW QUESTION: 99
You have a Microsoft 365 subscription that contains 1,000 Windows devices enrolled in Microsoft Intune.
You have the apps shown in the following table.

Name	Source size
App1	1 GB
App2	7 GB
App3	20 GB
App4	25 GB

You need to deploy App1 to the devices. Which apps can you deploy by using Intune?
A. App1, App2, and App3 only
B. App1 and App2 only
C. App1 only
D. App1, App2 App3, and App4
Answer: (SHOW ANSWER)

NEW QUESTION: 100
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform	Member of
Device1	Windows 11	Group1
Device2	Android	Group1
Device3	iOS	Group1, Group2

All the devices are enrolled in Microsoft Intune.
The devices have apps installed as shown in the following table.
Answer Area

Statements	Yes	No
Policy1 will apply to Teams on Device1.	○	○
Policy1 will apply to OneDrive on Device2.	○	○
Policy1 will apply to Microsoft Edge on Device3.	○	○

Answer:



Explanation:



NEW QUESTION: 101

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

You use Microsoft Intune to manage devices.

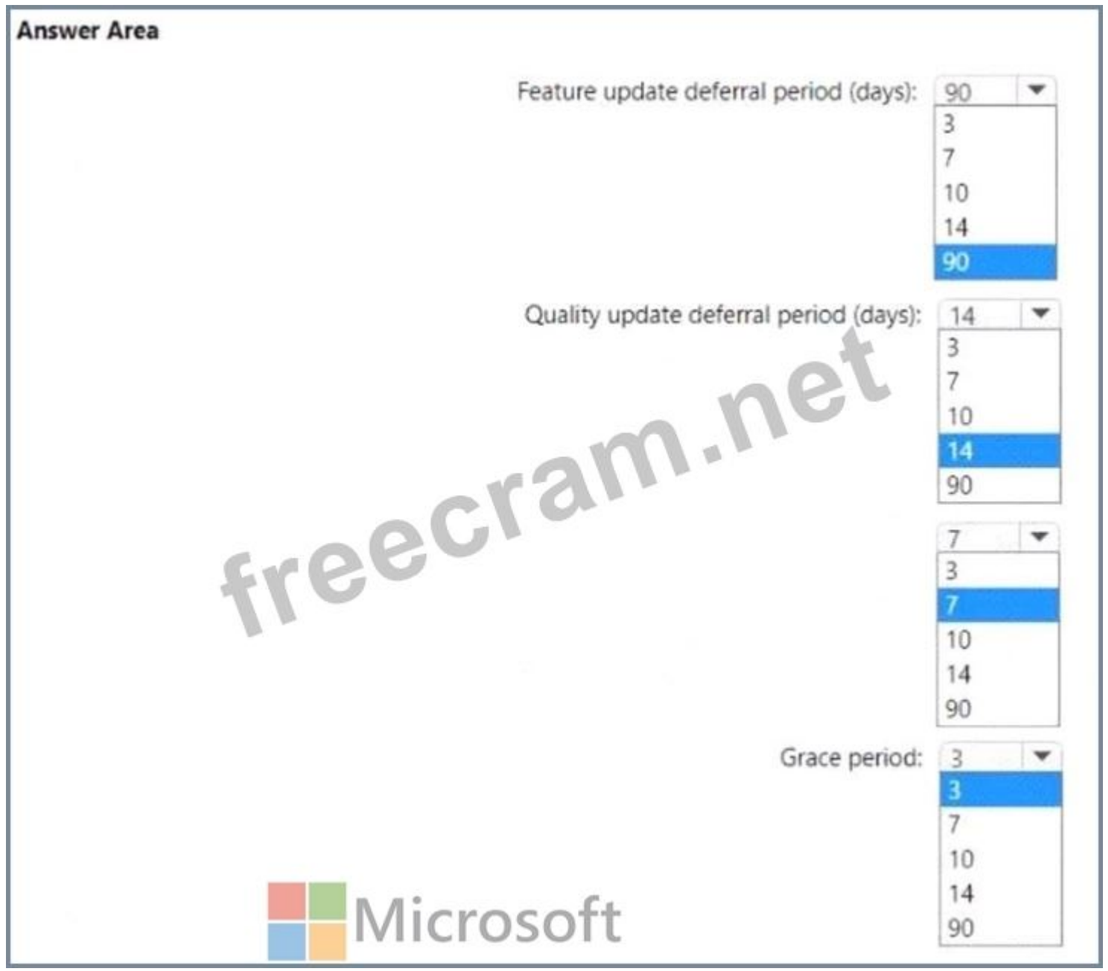
You need to configure an update ring that meets the following requirements:

* Fixes and improvements to existing Windows functionality can be deferred for 14 days but will install automatically seven days after that date.
* The installation of new Windows features can be deferred for 90 days but will install automatically 10 days after that date.
* Devices must restart automatically three days after an update is installed.

How should you configure the update ring? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

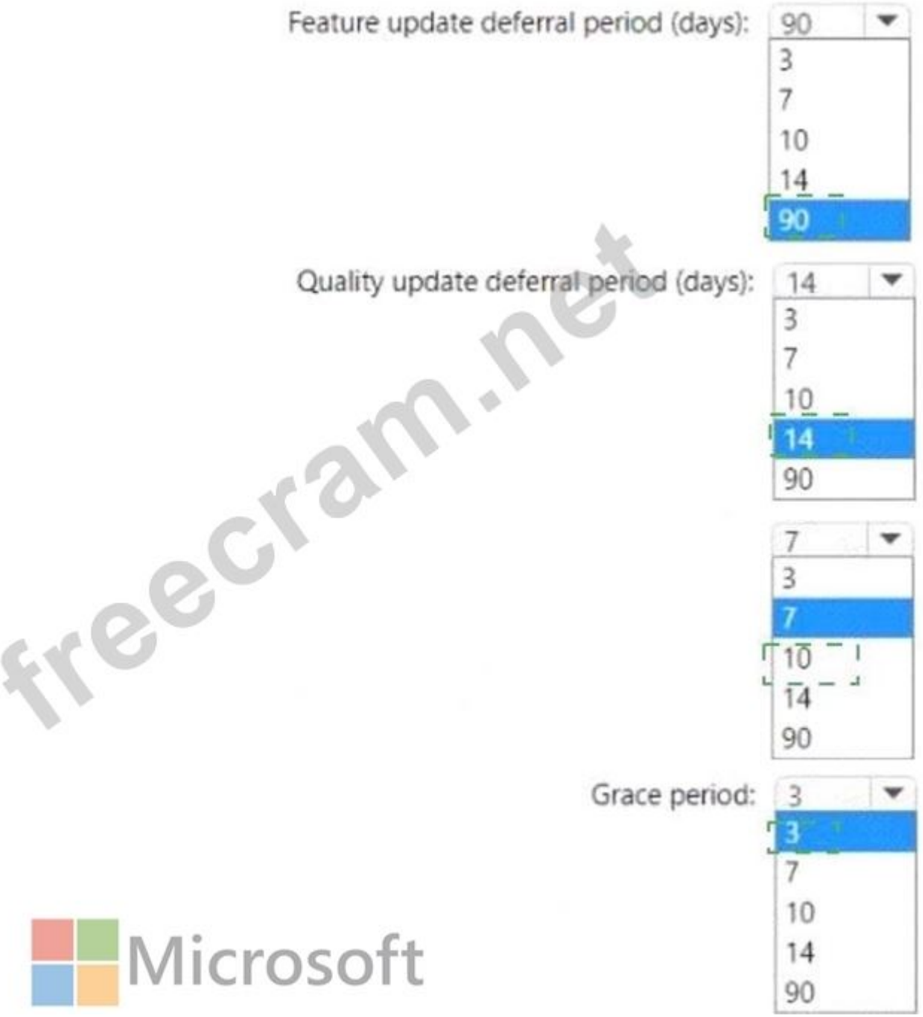


freecram.net

Microsoft

Answer:

Answer Area



Explanation:
90
14
10
3

NEW QUESTION: 102
You have a Microsoft 365 subscription that uses Microsoft Intune. The subscription contains 1,000 Windows
11 Enterprise devices that are Microsoft Entra joined.
The subscription has a Conditional Access policy that requires the devices be marked as compliant before users can access Microsoft 365 apps.
You have a custom line-of-business (LOB) app named App1 deployed to the devices. The installed version of App1 is unavailable in the built-in compliance policies and settings for Windows devices.

freecram.net

You need to extend compliance evaluation to ensure that Intune marks the devices as compliant based on the detected App1 version.
What should you do in the compliance policy?

A. Create an endpoint security policy and add a reusable settings group for the App1 version.

B. Create a PowerShell discovery script and add a JSON file that defines the compliant App1 version.

C. Create a PowerShell remediation and add a detection rule that evaluates the App1 version.

D. Create a device configuration profile for Windows and add a custom OMA-URI for the App1 version.

Answer: (SHOW ANSWER)

NEW QUESTION: 103

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

Name	Operating system	Edition
Device1	64-bit version of Windows 10	Home
Device2	32-bit version of Windows 10	Pro
Device3	64-bit version of Windows 10	Enterprise
Device4	64-bit version of Windows 10	Pro

You plan to upgrade the devices to Windows 11 Enterprise.
On which devices can you perform a direct in-place upgrade to Windows 11 Enterprise?

A. Device3 only

B. Device 3 and Device 4 only

C. Device2. Device3. and Devtce4 only

D. Device1. Device3, and Devtce4 only

E. Device1, Device2. Device3. and Devke4 only

Answer: (SHOW ANSWER)

https://learn.microsoft.com/en-us/windows/deployment/upgrade/windows-upgrade-paths https://learn.
microsoft.com/en-us/windows/deployment/upgrade/windows-edition-upgrades

NEW QUESTION: 104

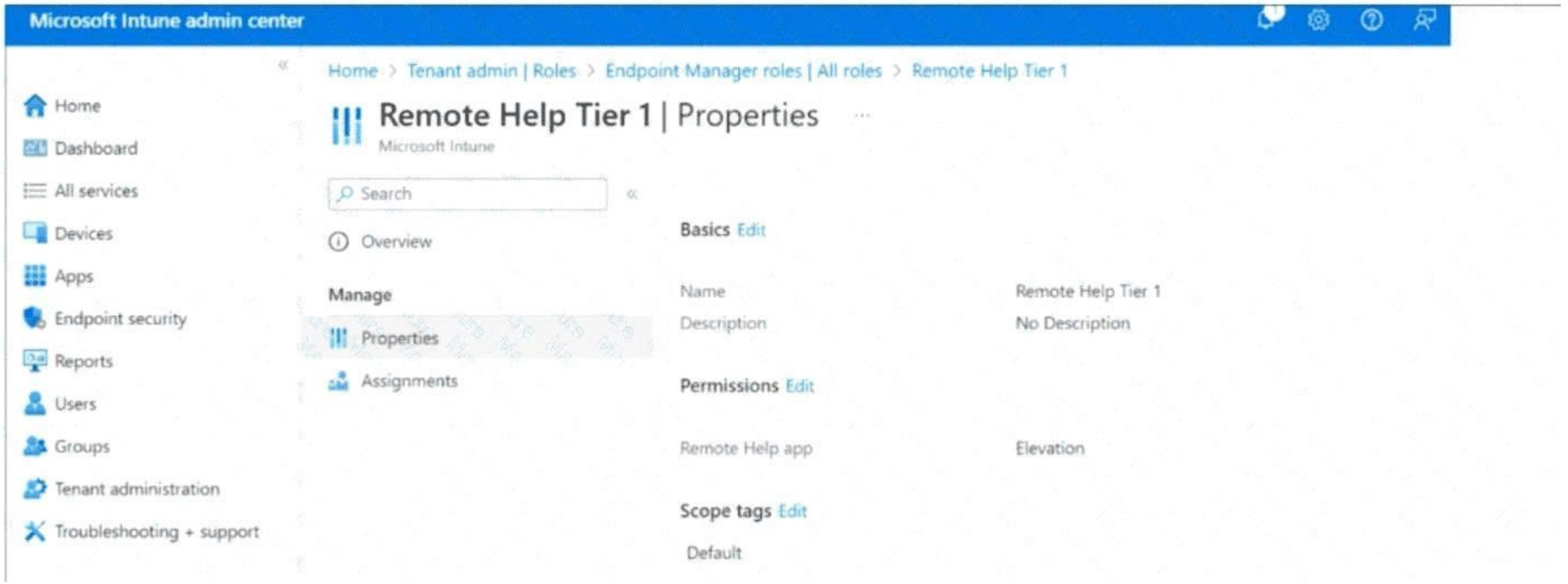
You have a Microsoft 365 E5 subscription that contains devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 11
Device2	iOS
Device3	Android

The subscription contains the users shown in the following table.

Name	Role	Role type
Admin1	Help Desk Operator	Built-in role
Admin2	Remote Help Tier1	Custom Intune role

The Remote Help Tier1 role is configured as shown in the following exhibit.



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

Statements	Yes	No
Admin1 can take full control of Device2.	○	○
Admin2 can take full control of Device1.	○	○
Admin2 can take unattended control of Device3.	○	○

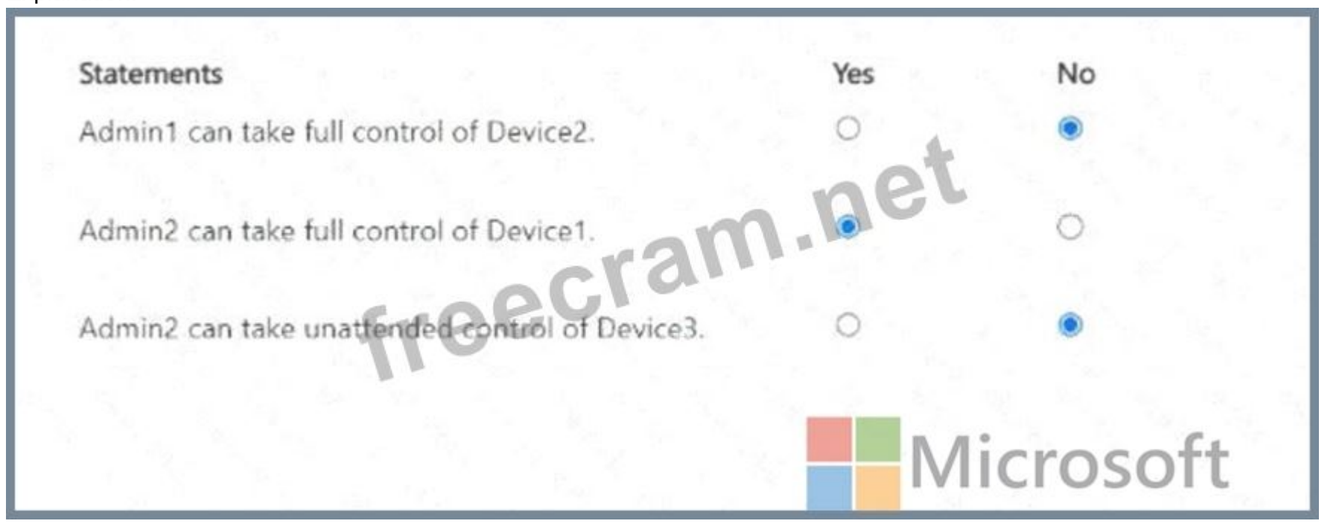
freecram.net
Microsoft

Answer:

Statements	Yes	No
Admin1 can take full control of Device2.	○	○
Admin2 can take full control of Device1.	○	○
Admin2 can take unattended control of Device3.	○	○

freecram.net
Microsoft

Explanation:



freecram.net

NEW QUESTION: 105
You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 11.
You create a new task sequence by using the Standard Client Task Sequence template to deploy Windows 11 Enterprise to new computers. The computers have a single hard disk.
You need to modify the task sequence to create a system volume and a data volume.
Which phase should you modify in the task sequence?
A. Preinstall
B. Initialization
C. Postinstall
D. State Restore
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Your company implements Azure AD, Microsoft 365, Microsoft Intune, and Azure Information Protection.
The company's security policy states the following:
* Personal devices do not need to be enrolled in Intune.
* Users must authenticate by using a PIN before they can access corporate email data.
* Users can use their personal iOS and Android devices to access corporate cloud services.
* Users must be prevented from copying corporate email data to a cloud storage service other than Microsoft OneDrive for Business.
You need to configure a solution to enforce the security policy.
What should you create?
A. an app protection policy from the Microsoft Intune admin center
B. a device configuration profile from the Microsoft Intune admin center
C. a data loss prevention (DIP) policy from the Microsoft Purview compliance portal
D. an insider risk management policy from the Microsoft Purview compliance portal

Answer: (SHOW ANSWER)

Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 107
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 Windows Autopilot deployment profile
B. the device configuration profile
C. the automatic enrollment settings
D. the enrollment status page (ESP) profile
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have a Microsoft Entra tenant named contoso.com.
You purchase an Android device named Devtce1.
You need to register Devtce1 in contoso.com.
Solution; You use the Google Chrome app.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

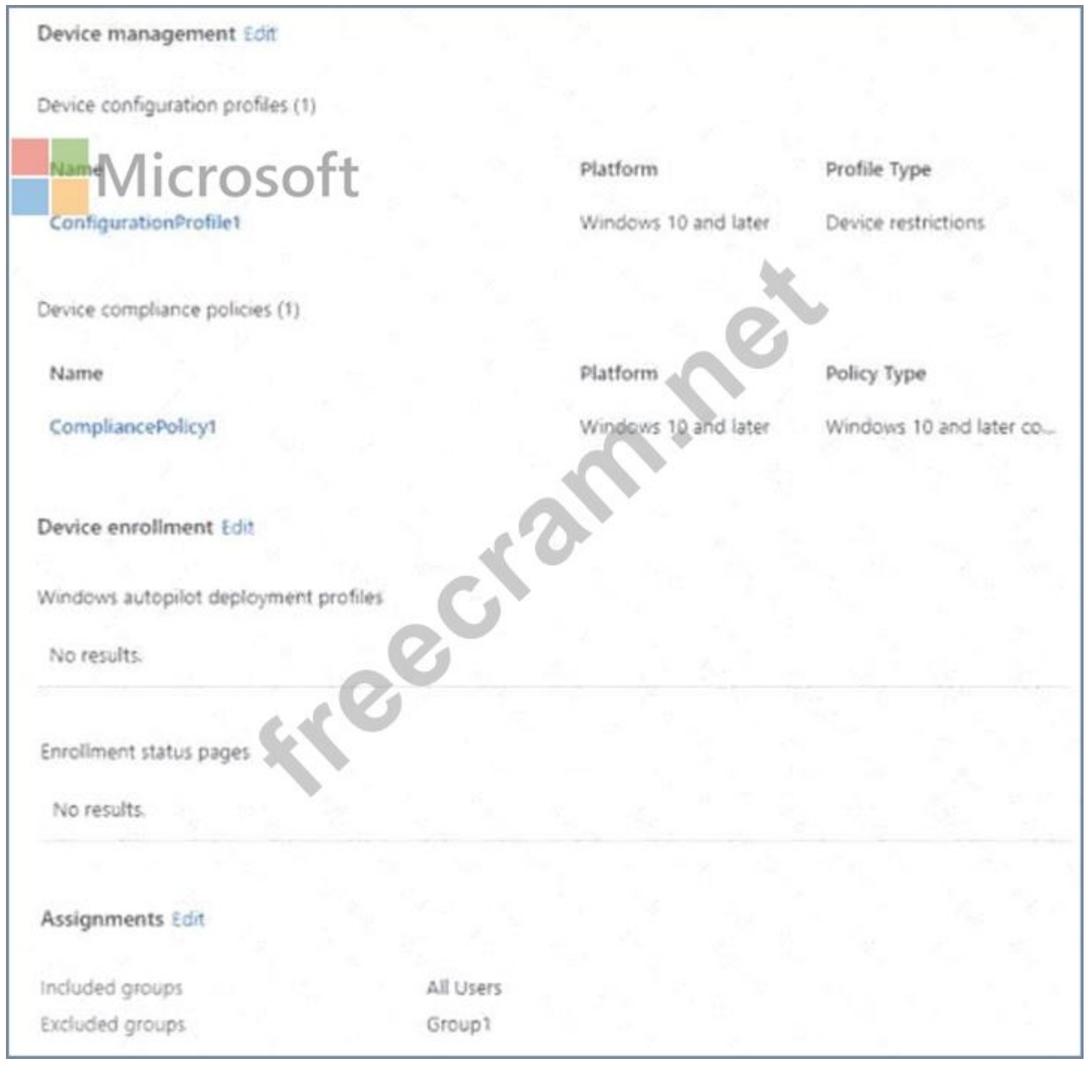
NEW QUESTION: 109
You have a Microsoft Intune subscription associated to an Azure AD tenant named contoso.com.
Users use one of the following three suffixes when they sign in to the tenant: us.contoso.com, eu.contoso.
com, or contoso.com.
You need to ensure that the users are NOT required to specify the mobile device management (MDM) enrollment URL as part of the enrollment process. The solution must minimize the number of changes.
Which DNS records do you need?
A. three CNAME records

B. one CNAME record only
C. three TXT records
D. one TXT record only
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-create-cname#:~:text=If%20your%20organization%20uses%20more%20than%20one%20UPN%20suffix%2C%20create%20one%20CNAME%20for%20each%20domain%20name

NEW QUESTION: 110
You have a Microsoft 36S subscription, use Microsoft Intune. and have the users shown in the following table.

Name	Member of
User1	Group1
User2	None
User3	None

You create a policy set named Set1 as shown in the exhibit. (Click the Exhibit tab.)



Microsoft
freecram.net

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

Name	Operating system	User
Device1	Windows 10	User1
Device2	Windows 11	User2
Device3	Android	User3

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

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○

Answer:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○

Explanation:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	●
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	●	○
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	●

NEW QUESTION: 111

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

Name	Operating system	Enrolled in Microsoft Intune
Device1	Windows 11	Yes
Device2	Windows 10	Yes
Device3	Android	Yes
Device4	iOS	Yes

All devices have Microsoft Edge installed.

From the Microsoft Intune admin center, you create a Microsoft

You need to apply Edge1 to all the supported devices.

To which devices should you apply Edge1?

A. Device1 only

B. Device1 and Device2 only

C. Device1, Device2, and Device3 only

D. Device1, Device2, and Device4 only
E. Device1, Device2, Device3, and Device4
Answer: (SHOW ANSWER)
This feature applies to:
* Windows 10 version 1809 and later
* Windows 11
https://learn.microsoft.com/en-us/mem/intune/protect/security-baselines-configure

NEW QUESTION: 112
You have a Microsoft Entra 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 11	Group1
Device2	Android	Group1
Device3	iOS	Group2

From Intune, you create and send a custom notification named Notification! to Group1. For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 113
Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer! and Computer2 that run Windows 10. On Computer1, you need to run the Invoke-Command cmdlet to execute several PowerShell commands on Computed. What should you do first?
A. From Active Directory, configure the Trusted for Delegation setting for the computer account of Computed.
B. On Computer1, run the HcK-PSSession cmdlet.
C. On Computed, run the Enable-PSRemoting cmdlet.
D. On Computed, add Computer! to the Remote Management Users group.
Answer: (SHOW ANSWER)

NEW QUESTION: 114
You have a Microsoft 365 E5 subscription. All devices are enrolled in Microsoft Intune.
You create a Conditional Access policy named Policy! that requires multifactor authentication (MFA).
You need to ensure that Policy1 only applies to devices marked as noncompliant. Which settings of Policy1 should you configure?
A. Device platforms under Conditions
B. Grant
C. Filter for devices under Conditions
D. Target resources
E. Session
Answer: (SHOW ANSWER)

NEW QUESTION: 115
You need to prepare for the deployment of the Phoenix office computers.
What should you do first?
A. Extract the hardware ID information of each computer to a CSV file and upload the file from the Devices settings in Microsoft Store for Business.
B. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Azure Active Directory blade in the Azure portal.
C. Generalize the computers and configure the Device settings from the Azure Active Directory blade in the Azure portal.
D. Extract the hardware ID information of each computer to an XLSX file and upload the file from the Devices settings in Microsoft Store for Business.
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices#manage-autopilot-deployment-profiles

NEW QUESTION: 116

You have two computers that run Windows 10. The computers are enrolled in Microsoft Intune as shown in the following table.

Name	Member of
Computer1	Group1
Computer2	Group1, Group2

Windows 10 update rings are defined in Intune as shown in the following table.

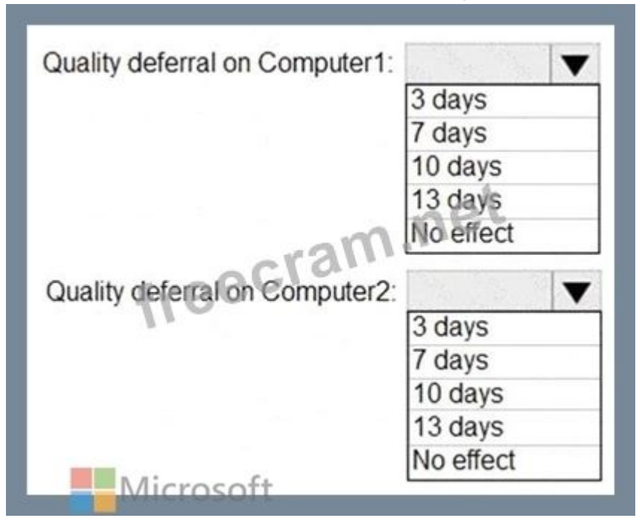
Name	Quality deferral (days)	Assigned
Ring1	3	Yes
Ring2	10	Yes

You assign the update rings as shown in the following table.

Name	Include	Exclude
Ring1	Group1	Group2
Ring2	Group2	Group1

What is the effect of the configurations on Computer1 and Computer2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Quality deferral on Computer1:

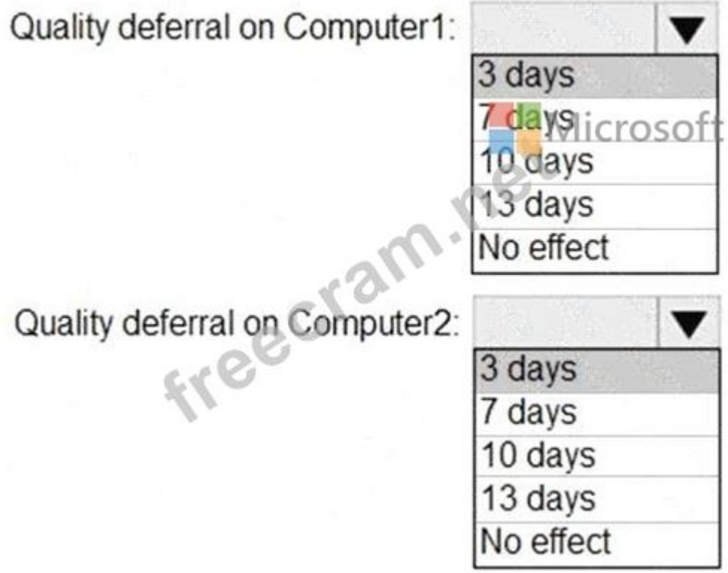
- 3 days
- 7 days
- 10 days
- 13 days
- No effect

Quality deferral on Computer2:

- 3 days
- 7 days
- 10 days
- 13 days
- No effect

freecram.net Microsoft

Explanation:



Computer1 and Computer2 are members of Group1. Ring1 is applied to Group1.

Note: The term " Exclude " is misleading. It means that the ring is not applied to that group, rather than that group being blocked.

References:

https://docs.microsoft.com/en-us/windows/deployment/update/waas-wufb-intune

https://allthingscloud.blog/configure-windows-update-business-using-microsoft-intune/

NEW QUESTION: 117
You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?
A. an attack surface reduction (ASR) policy
B. a security baseline
C. an endpoint detection and response (EDR) policy
D. an account protection policy
E. an antivirus policy
Answer: (SHOW ANSWER)
To onboard the devices to Microsoft Defender for Endpoint, you need to create an endpoint detection and response (EDR) policy in the Microsoft Intune admin center. This policy enables EDR capabilities on devices that are enrolled in Intune and allows you to configure various settings for EDR functionality. You can then assign the policy to groups of users or devices. References: https://docs.microsoft.com/en-us/mem/intune/protect/edr-windows

NEW QUESTION: 118
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

You are creating a compliance policy named Compliance1.
Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?
A. Group3 and Group4 only
B. Group3, Group4, and Admin1 only
C. Group1, Group2, and Group3 only
D. Group1, Group2, Group3, and Group4 only
E. Group1, Group2, Group3, Group4, and Admin1
Answer: (SHOW ANSWER)
Reference:
https://www.ravenswoodtechnology.com/microsoft-intune-compliance-notifications/
https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

NEW QUESTION: 119
You have a Microsoft 365 subscription that uses Microsoft Security Copilot in Intune.
In the Microsoft Intune admin center, a Security Copilot finding is generated from Microsoft Defender Vulnerability Management data. The finding includes associated Common Vulnerabilities and Exposure (CVE) information and an analysis of affected Windows devices.
Which agent generated the finding?

A. Change Review Agent
B. Vulnerability Remediation Agent
C. Device Offboarding Agent
D. Policy Configuration Agent
Answer: (SHOW ANSWER)

NEW QUESTION: 120
You have a Microsoft 365 E5 subscription.
You need to enroll Android Enterprise devices in Microsoft Intune by using zero-touch enrollment.
What should you do first?
Freecram.net
A. From the Microsoft Intune admin center, create a zero-touch configuration.
B. From the Microsoft Intune admin center, configure enrollment restrictions.
C. From the Microsoft Intune admin center, link a Managed Google Play account.
D. From the zero-touch enrollment portal, create a zero-touch configuration.
Answer: (SHOW ANSWER)

NEW QUESTION: 121
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.

Settings

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area

Device1:
Device2:
Device3:

Answer:



Explanation:



Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 122

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to a Microsoft Entra tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



freecram.net

User2 fails to authenticate to the Microsoft Entra tenant when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Microsoft Entra ID.
Solution: From the on-premises Active Directory domain, you set the UPN suffix for User2 to @contosoxom.
You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Your network contains an Active Directory domain.
The domain contains four computer named Computer 1. Computet2. Computed, and Computer4 that run Windows 10. Vou perform the following actions:
* On Computer1, you install Windows Admin Center and configure Windows Defender Firewall to allow incoming communication over TCP pons 80.443. and 6516.
* On Computed, you run the Enable-PS Remoting cmdlet.
* On Computer 3, you configure Windows Defender firewall to allow Windows Remote Management (WinRM) traffic
* On Computer4, you run the winrm quickconfig command.
You need to manage the computers remotely by using Windows Admin Center.
From which computers can you connect to Windows Admin Center, and which computers can you manage by using Windows Admin Center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 124

Your network contains an Active Directory domain.

You deploy a Microsoft Entra tenant.

Another administrator configures the domain to synchronize to the Microsoft Entra tenant.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.

You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.

Solution: From Microsoft Entra Connect Sync, you modify the Microsoft Entra credentials. Does this meet the goal?

A. No

B. Yes

Answer: A (LEAVE A REPLY)

NEW QUESTION: 125

You have a hybrid deployment of Azure AD that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Intune.

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

You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings.
What should you do?
A. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy.
B. From the Microsoft Intune admin center, create a custom device profile.
C. From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy.
D. From the Microsoft Intune admin center, create an Administrative Templates device profile.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126
You have a Microsoft 365 subscription.
You use Microsoft Intune to manage Windows 11 devices.
You need to implement Windows Local Administrator Password Solution (Windows LAPS).
What should you configure?
A. a configuration profile
B. an app protection policy
C. a device compliance policy
D. an account protection policy
Answer: (SHOW ANSWER)

NEW QUESTION: 127
You have a Microsoft intune subscription.
You have devices enrolled in intune as shown in the following table.

Name	Operating system
Device1	Android 14
Device2	Android 15
Device3	iOS 15.8.4
Device4	iOS 16.7.11
Device5	iOS 18.5

An app named App1 is installed on each device
What is the minimum number of app confirmation policies required to manage App1?
A. 5
B. 2
C. 1
D. i
E. 4
Answer: B (LEAVE A REPLY)

NEW QUESTION: 128
You have a Microsoft 365 subscription that includes Microsoft Intune.
You create a new Android app protection policy named Policy1 that prevents screen captures in all Microsoft apps. You discover that an unmanaged email client installed on Android devices can still capture screens You need to ensure that users can only use Microsoft apps to access email. What should you do?
A. Create a compliance policy.
B. Create a Conditional Access policy.

C. Modify the Data protection settings of Policy1.
D. Modify the assignments of Policy1.
Answer: (SHOW ANSWER)

NEW QUESTION: 129
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.
You create a user named User1.
You need to ensure that User1 can rotate BitLocker recovery keys by using Intune.
Solution: From the Microsoft Entra admin center, you assign the Cloud Device Administrator role to User1.
Does this meet the goal?
A. No
B. Yes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 130
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You plan to create Windows 11 device builds for the marketing and research departments The solution must meet the following requirements:
* Marketing department devices must support Windows Update for Business.
* Research department devices must have support for feature update versions for up to 36 months from release.
What is the minimum Windows 11 edition required for each department? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point



freecram.net Microsoft
Answer:

Answer Area



Explanation:



Marketing Department:

Windows 11 Pro: Supports Windows Update for Business and offers basic management features.

Research Department:

Windows 11 Enterprise: Extends feature updates to 36 months, crucial for their needs

NEW QUESTION: 131

You have a Microsoft 365 subscription. You plan to enroll 25 new devices in Microsoft Intune. You need to configure an enrollment notification for the new devices.

Following three which two types of notifications can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. SMS

B. Microsoft Teams message

C. push

D. email

E. phone call

Answer: (SHOW ANSWER)

NEW QUESTION: 132

To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Policy1:

- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

Policy2:

- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

Answer:

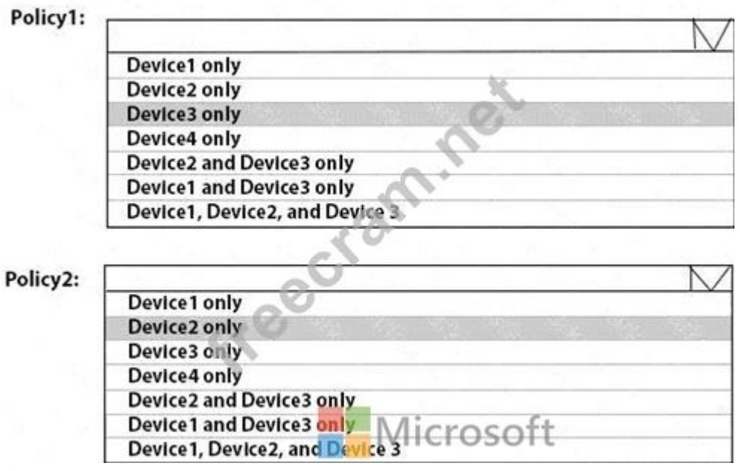
Policy1:

- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

Policy2:

- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

Explanation:



freecram.net
Microsoft

Reference:
https://docs.microsoft.com/en-us/intune/device-profile-assign

NEW QUESTION: 133
You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune.
You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.
Which extension should you select for the app package file?
A. .intunemac
B. apk
C. jpa
D. .appx
Answer: (SHOW ANSWER)
iOS/iPadOS LOB apps: Select Line-of-business app as the app type, select the App package file, and then enter an iOS/iPadOS installation file with the extension .ipa.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

NEW QUESTION: 134
You have a Microsoft 365 subscription. The subscription contains 500 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to manage the deployment of monthly security updates. The solution must meet the following requirements:
* Updates must be deployed to a group of test computers for quality assurance.
* Updates must be deployed automatically 15 days after the quality assurance testing.
What should you create in the Microsoft Intune admin center?
A. an update ring
B. a feature update policy
C. a device Configuration profile
D. a security baseline
Answer: (SHOW ANSWER)

NEW QUESTION: 135
You have a Microsoft 365 subscription that contains 500 Android devices. The devices are managed by using Microsoft Intune. You need to ensure that you can manage software updates for the devices by using Android FOTA. What should you do first?
A. Configure a connector, i
B. Add derived credentials.
C. Create a compliance policy.
D. Add a compliance partner.
Answer: (SHOW ANSWER)

NEW QUESTION: 136
You have a Microsoft 365 subscription that includes Microsoft Intune.
You have an update ring named UpdateRing1 that contains the following settings:
* Automatic update behavior: Auto install and restart at a scheduled time
* Automatic behavior frequency: First week of the month
* Scheduled install day: Tuesday
* Scheduled install time: 3 AM
From the Microsoft Intone admin center, you select Uninstall for the feature updates of UpdateRing1. When will devices start to remove the feature updates?
A. next Tuesday
B. when a user approves the uninstall
C. the first Tuesday of the next month
D. as soon as the policy is received
Answer: (SHOW ANSWER)

Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 137
You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace.
Which three types of data can you collect from the computers by using Log Analytics? Each correct answer a complete solution.
NOTE:Each correct selection is worth one point.
A. error events from the System log
B. failure events from the Security log
C. third-party application logs stored as text files
D. the list of processes and their execution times
E. the average processor utilization
Answer: (SHOW ANSWER)

You can collect error events from the System log, third-party application logs stored as text files, and the average processor utilization from the computers by using Log Analytics. These are some of the types of data that you can collect by using data sources such as Windows event logs, custom logs, and performance counters. You cannot collect failure events from the Security log or the list of processes and their execution times by using Log Analytics.References:https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-overview

NEW QUESTION: 138
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 BI
Answer: (SHOW ANSWER)
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:
https://fef.{yourtenant}.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?api- version=v1.0 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: 139
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: (SHOW ANSWER)
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-intune

NEW QUESTION: 140
You have a Microsoft 365 E5 subscription and 25 Apple iPads.
You need to enroll the iPads in Microsoft Intune by using the Apple Configurator enrollment method.
What should you do first?
Freedram.net
A. Upload a file that has the device identifiers for each iPad.
B. Modify the enrollment restrictions.
C. Configure an Apple MDM push certificate.
D. Add your user account as a device enrollment manager (DEM).
Answer: (SHOW ANSWER)
Reference:
https://www.manageengine.com/mobile-device-management/help/enrollment/mdm_creating_apns_certificate.
html
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: 141
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The tenant contains the users shown in the following table.

Name	Member of	On-premises sync
User1	Group1	Disabled
User2	Group2	Enabled

You assign Windows 10/11 Enterprise E5 licenses to Gtoup1 and Uset2.
You deploy the devices shown in the following table.

Name	Operating system	Joined to
Device1	Windows 11 Pro	Azure AD
Device2	Windows 11 Pro	AD DS
Device3	Windows 10 Pro	Azure AD

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

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.		
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.		
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.		

Answer:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.	○	☐
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	☐	○
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.	○	☐

Explanation:



NEW QUESTION: 142
You have a Microsoft 365 subscription that uses Microsoft Intune. You need to recommend which portals to use for the following actions:
* Administrators must be able to view the BitLocker recovery key for devices.
* Users must be able to recover the BitLocker recovery key for their device.
The solution must follow the principle of least privilege.

What should you recommend for each action? To answer, select the appropriate options in the answer area.



Answer:



Explanation:

To view the BitLocker recovery key for devices, administrators use: The Microsoft Intune admin center

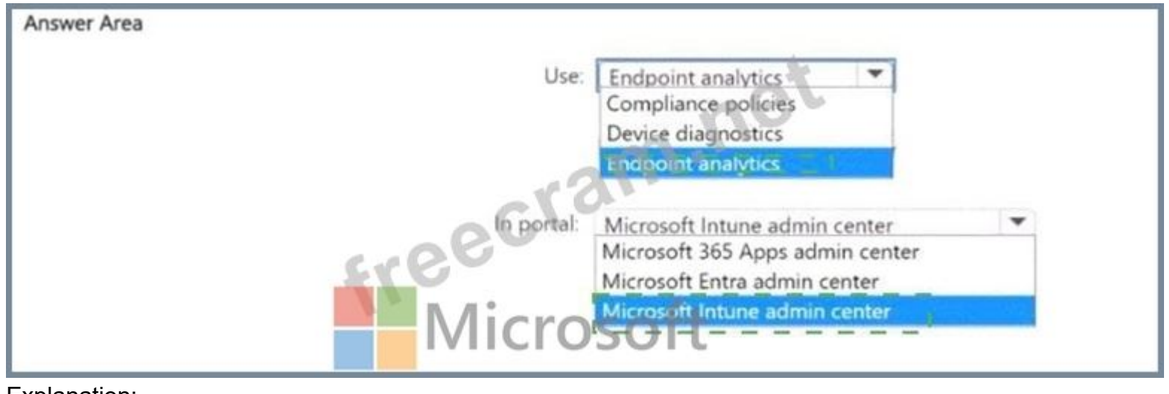
* To recover the BitLocker recovery key for devices, users use: Intune Company Portal Administrators with the appropriate Intune RBAC permissions can access BitLocker recovery information for managed Windows devices through the Microsoft Intune admin center. End users should not be granted administrative portal access merely to retrieve their own recovery key.

For self-service recovery, Microsoft Intune supports retrieving the BitLocker recovery key from the Company Portal. Users sign in with their organizational account, select their enrolled Windows device, and choose Get recovery key. This satisfies the principle of least privilege because users can recover the key for their own device without receiving elevated administrative permissions

NEW QUESTION: 143
You have a Microsoft 365 subscription.
You use Microsoft Intune to manage devices.
You need to assess device performance during startup and identify any device models that take longer than average to start.
What should you use to assess the device performance, and which portal should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



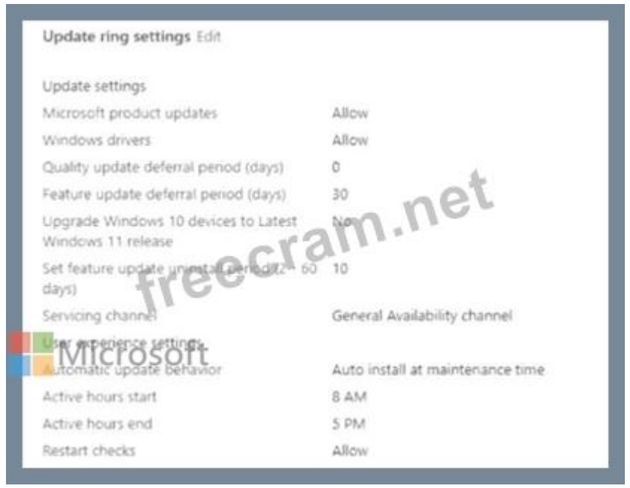
Answer:



Explanation:



NEW QUESTION: 144
You have a Microsoft 365 E5 subscription.
You create a new update ring policy named Policy1 as shown in the following exhibit

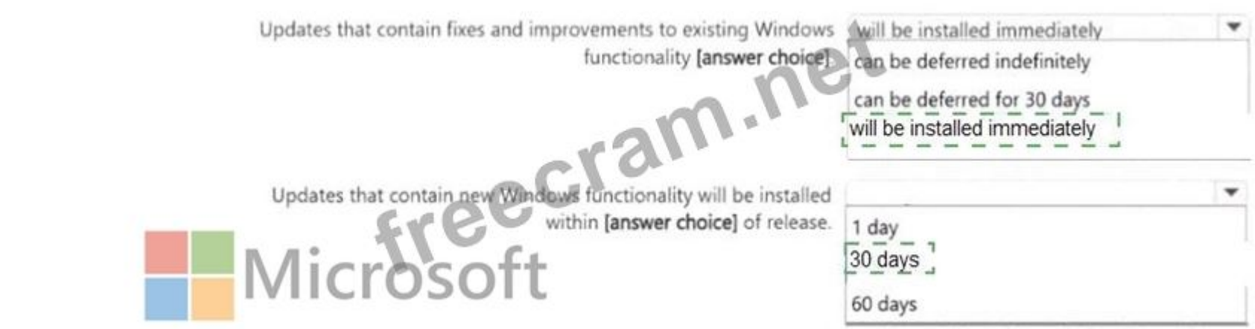


Use the drop down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Answer Area



Microsoft
freecram.net

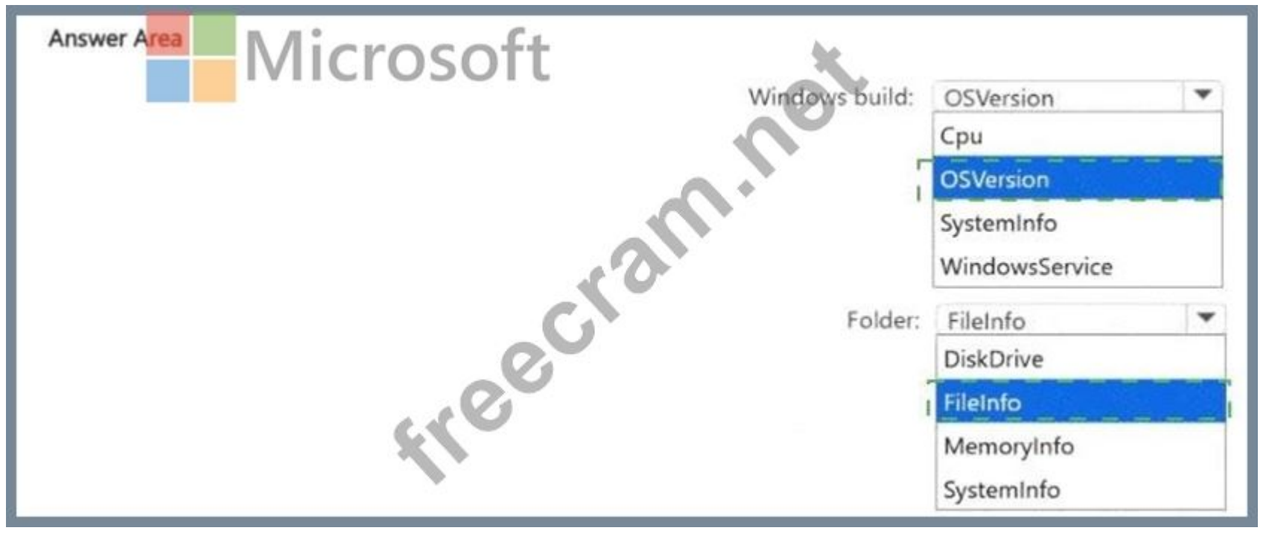
NEW QUESTION: 145
You have a Microsoft 365 subscription that includes Microsoft Intune.
You have 500 corporate-owned Android devices enrolled as fully managed devices.
You need to prepare an app named App1 for deployment to the devices.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point,
A. From the Intune Company Portal, download Appl.
B. Create an OEMConfig profile.
C. From the Managed Google Play Store, approve App1.
D. Sync App1 with Intune.
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work

NEW QUESTION: 146
You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.
You create a user named User1.
You need to ensure that User1 can rotate Bitlocker recovery keys by using Intune.
Solution: From the Microsoft Intune admin center, you assign the Endpoint Security Manager role to User1.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 147
You have a Microsoft 365 E5 subscription that contains two devices named Device1 and Device2.
You manage the devices by using Microsoft Intune.
You need to use Device query to meet the following requirements:
* Identify the Windows build on a device.
* Validate whether a folder exists on the C drive of a device.
Which table should you target for each requirement? To answer, select theappropriateoptions in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 148

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune.

You plan to manage Microsoft Defender Antivirus on the computers.

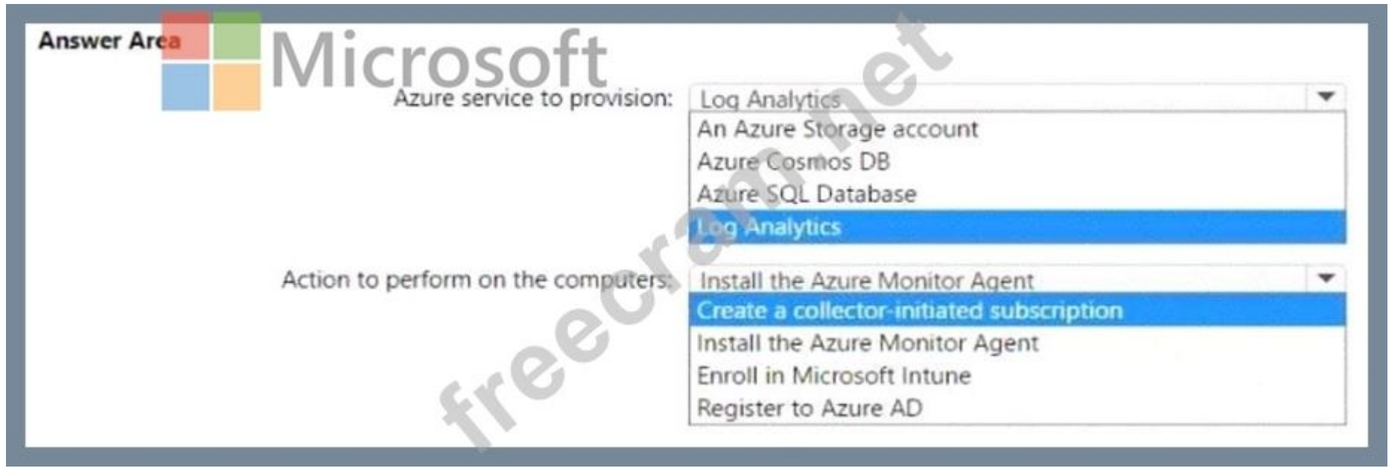
You need to prevent users from disabling Microsoft Defender Antivirus,

What should you do?
A. From the Microsoft Intune admin center, create a security baseline.
B. From the Microsoft 365 Defender portal, enable tamper protection.
C. From the Microsoft Intune admin center, create an account protection policy.
D. From the Microsoft Intune admin center, create an endpoint detection and response (EDR) policy.
Answer: (SHOW ANSWER)
Tamper protection is a feature of Microsoft Defender Antivirus that prevents users or malicious software from disabling or modifying the antivirus settings. Tamper protection can be enabled from the Microsoft 365 Defender portal for devices that are Azure AD joined and enrolled in Microsoft Intune. This will prevent users from turning off Microsoft Defender Antivirus or changing its configuration through Windows Security, PowerShell, Registry, or Group Policy. References: [Enable tamper protection]

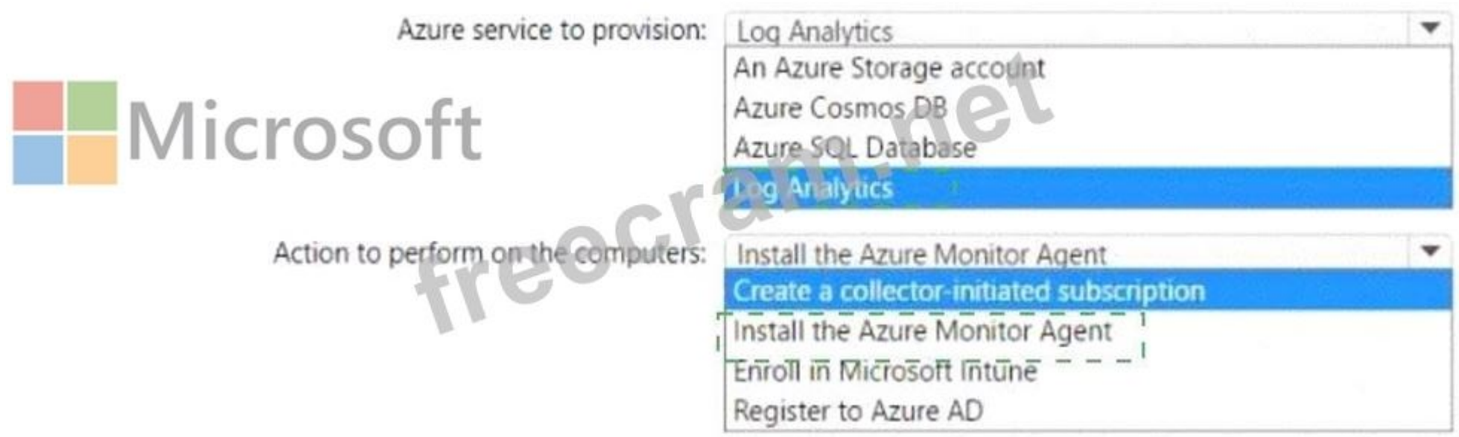
NEW QUESTION: 149
You install a feature update on a computer that runs Windows 10.
How many days do you have to roll back the update?
A. 30
B. 5
C. 14
D. 10
Answer: (SHOW ANSWER)

NEW QUESTION: 150
You have 25 computers that run Windows 10 Pro.
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You need to upgrade the computers to Windows 11 Enterprise by using an in-place upgrade. The solution must minimize administrative effort.
What should you use?
Freecram.net
A. Subscription Activation
B. Windows Autopilot
C. Microsoft Deployment Toolkit (MDT) and a default image of Windows 11 Enterprise
D. Microsoft Configuration Manager and a custom image of Windows 11 Enterprise
Answer: (SHOW ANSWER)

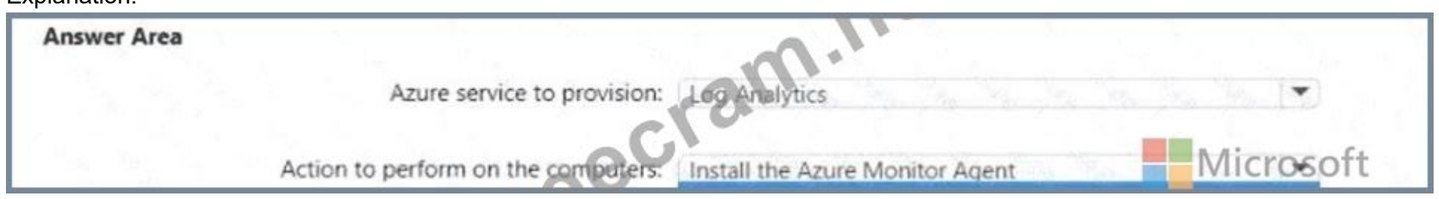
NEW QUESTION: 151
You have 1,000 computers that run Windows 10 and are members of an Active Directory domain.
You need to capture the event togs from the computers to Azure.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 152

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$
```

```
[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.	○	○
DT1 will have a KeyboardLocale of en-gb.	○	○
LT1 will download the image from MDT1.	○	○

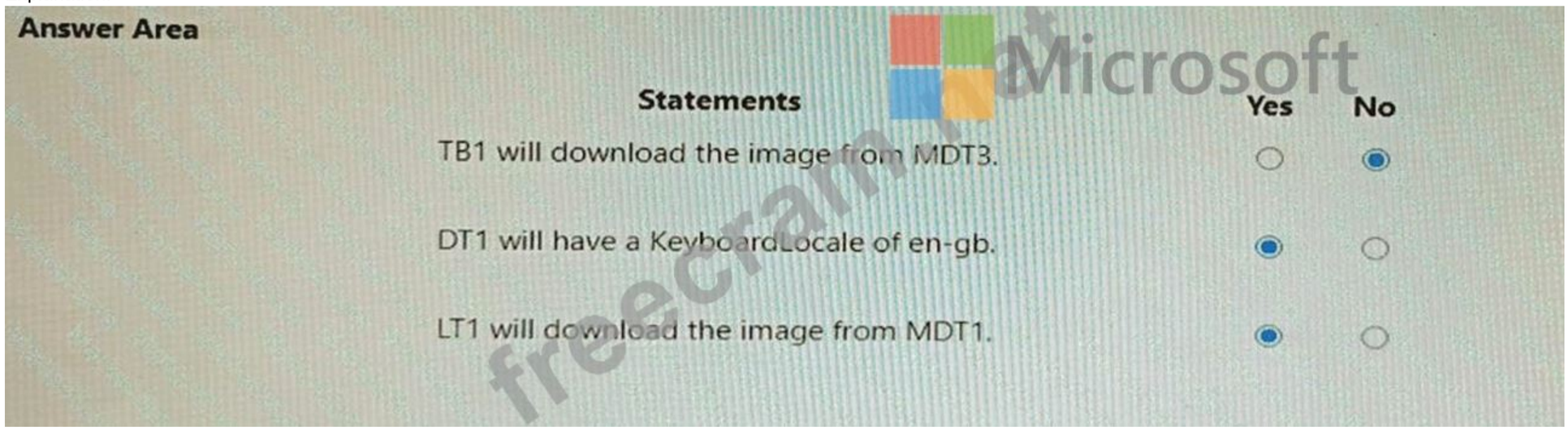
freecram.net Microsoft

Answer:

Statements	Yes	No
TB1 will download the image from MDT3.	○	◉
DT1 will have a KeyboardLocale of en-gb.	◉	○
LT1 will download the image from MDT1.	◉	○

freecram.net Microsoft

Explanation:



freecram.net Microsoft

NEW QUESTION: 153

You have a Microsoft 365 subscription that uses Microsoft Intune.

You have five new Windows 11 Pro devices.

You need to prepare the devices for corporate use. The solution must meet the following requirements:

* Install Windows 11 Enterprise on each device.

* Install a Windows Installer (MSI) package named App1 on each device.
* Add a certificate named Certificate1 that is required by App1.
* Join each device to Azure AD.
Which three provisioning options can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. subscription activation
B. a custom Windows image
C. an in-place upgrade
D. Windows Autopilot
E. provisioning packages
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages

NEW QUESTION: 154
You have a Microsoft 365 subscription that contains a user named User1 and 500 Windows devices enrolled in Microsoft Intune.
You configure an attack surface reduction {ASR) rule and enable the rule in Warn mode.
User1 downloads a file named file1.exe. When User1 attempts to run file1.exe he receives a prompt that the content has been blocked. The user unblocks the content.
How much time will pass until the user is prompted next to unblock the content?
A. 10 minutes
B. one week
C. 24 hours
D. one hour
Answer: (SHOW ANSWER)

NEW QUESTION: 155
You have a Microsoft 365 E5 subscription. You are implementing Microsoft Defender for Cloud Apps. You need to ensure that you can create OAuth app policies.
Solution: You configure Cloud Discovery. Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 156
You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Cloud Device Administrator
User1	*None*

You purchase the devices shown in the following table.

Name	Operating system
Device1	Windows 11
Device2	Android

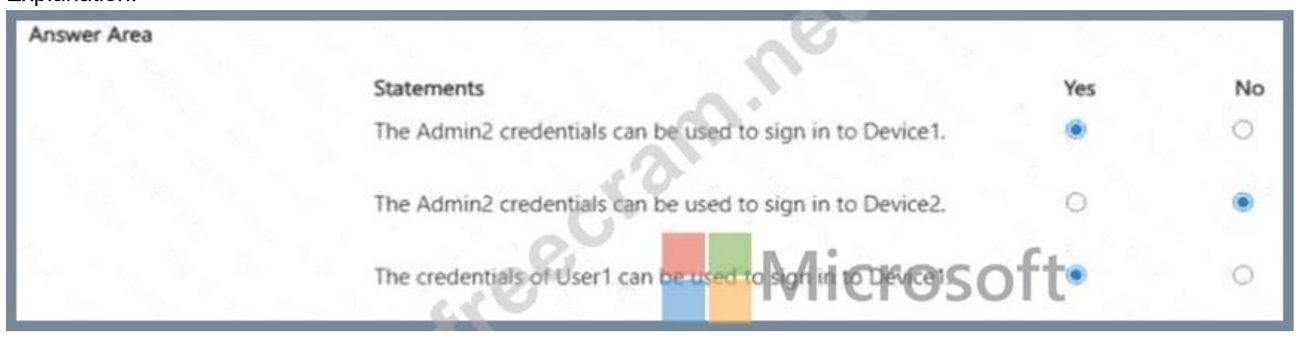
Administrators perform the following actions:
* Join Device1 to contoso.com by using the credentials of Admin1.
* Register Device2 in contoso.com by using the credentials of Admin2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

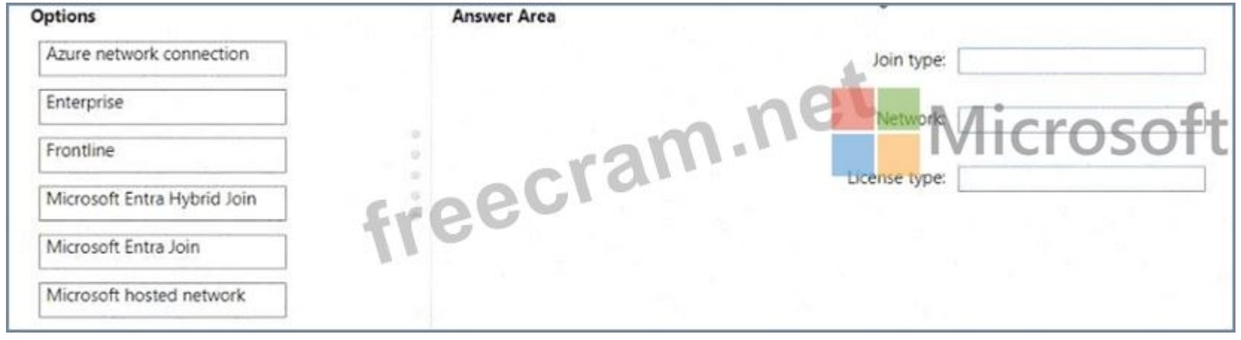


NEW QUESTION: 157
Your network contains an Active Directory domain named contoso.com. The domain contains 25 computers that run Windows 11- You have a Microsoft 365 subscription You have an Azure AD tenant that syncs with contoso.com.
You configure hybrid Azure AD join and discover that some of the computers have a registered state of Pending.
You need to ensure that the computers complete the join successfully.
What should you ensure?
A. that Windows is activated on all the computers

B. that the users of the computers are assigned Microsoft 365 licenses
C. that each computer has a line of sight to a domain controller
D. that the computers contain the latest quality updates
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/entra/identity/devices/hybrid-join-plan

NEW QUESTION: 158
Your network contains an Active Directory domain. The domain contains a computer named Computer! that runs Windows 11. You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:
* For the WinRM service, set Startup type to Automatic.
* Create a listener that accepts requests from any IP address.
* Enable a firewall exception for WS-Management communications.
Which PowerShell cmdlet should you use?
A. Enable-PSSessionConfiguration
B. Connect-WSMan
C. Enable-PSRemoting
D. Invoke-WSManAction
Answer: (SHOW ANSWER)

NEW QUESTION: 159
Your on-premises network contains an Active Directory Domain Services (AD DS) domain.
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains five virtual machines and is NOT connected to the on-premises network.
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You purchase Windows 365 Enterprise licenses.
You need to deploy Cloud PC. The solution must meet the following requirements:
* All users must be able to access their Cloud PC at any time without any restrictions.
* The users must be able to connect to the virtual machines on VNet1.
How should you configure the provisioning policy for Windows 365? To answer, drag the appropriate options to the correct settings. Each option 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.



freecram.net
Microsoft

Answer:



Explanation:



freecram.net
Microsoft

NEW QUESTION: 160

You have a Microsoft 365 subscription that includes Microsoft Intune.
You need to deploy a custom app to Android devices. The app uses the APK file format.
Which type of app should you select for the deployment?

A. Managed Google Play
B. web link
C. line-of-business (LOB)
D. Android store
E. built-in

Answer: (SHOW ANSWER)

NEW QUESTION: 161

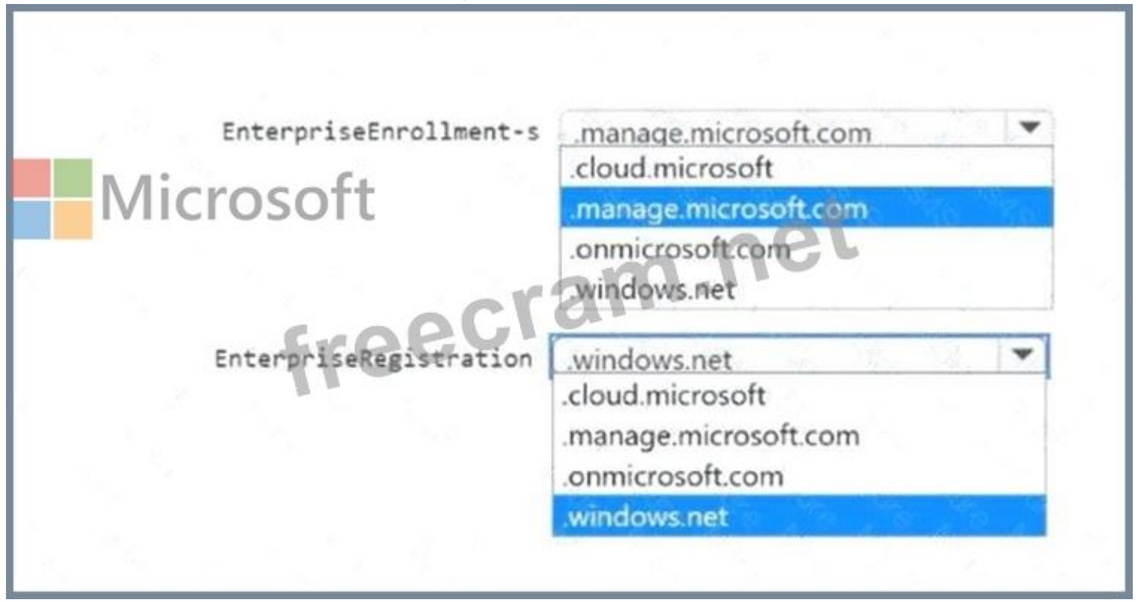
You have a Microsoft Entra tenant named contoso.com.
You manage devices by using Microsoft Intune. Automatic Intune enrollment is disabled.
Users report that they must enter the mobile device management (MDM) server address during device enrollment.
To reduce user interaction during device enrollment, you plan to create the following CNAME DNS hostname records:
* EnterpriseEnrollment.contoso.com

* EnterpriseRegistration.contoso.com

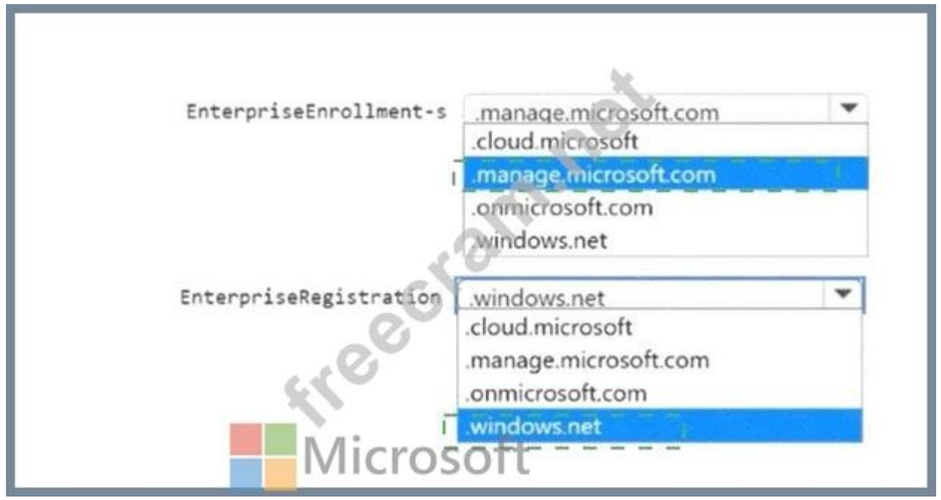
You need to configure a fully qualified domain name (FQDN) for each CNAME record to redirect enrollment requests to the Intune servers.

How should you configure each FQDN? To answer, select the appropriate options in the answer area.

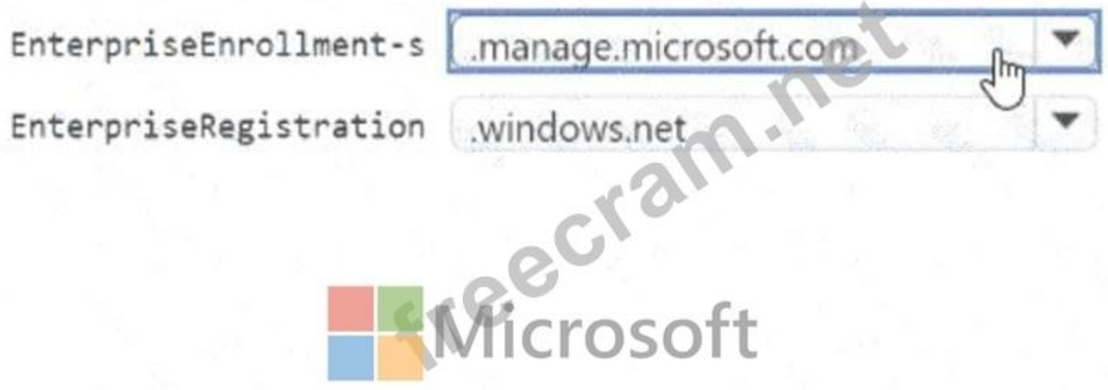
NOTE: Each correct selection is worth one point.



Answer:



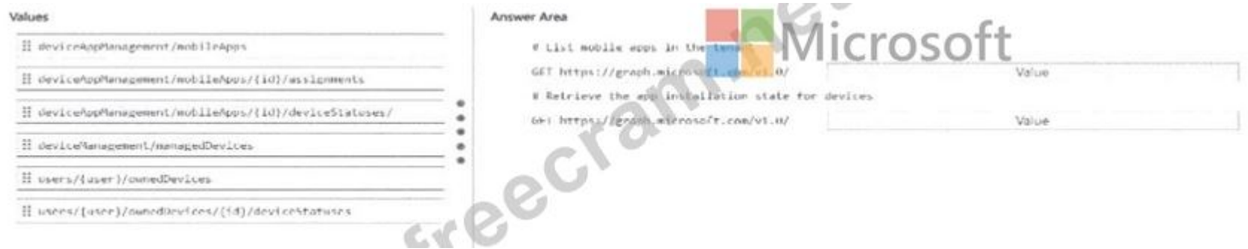
Explanation:



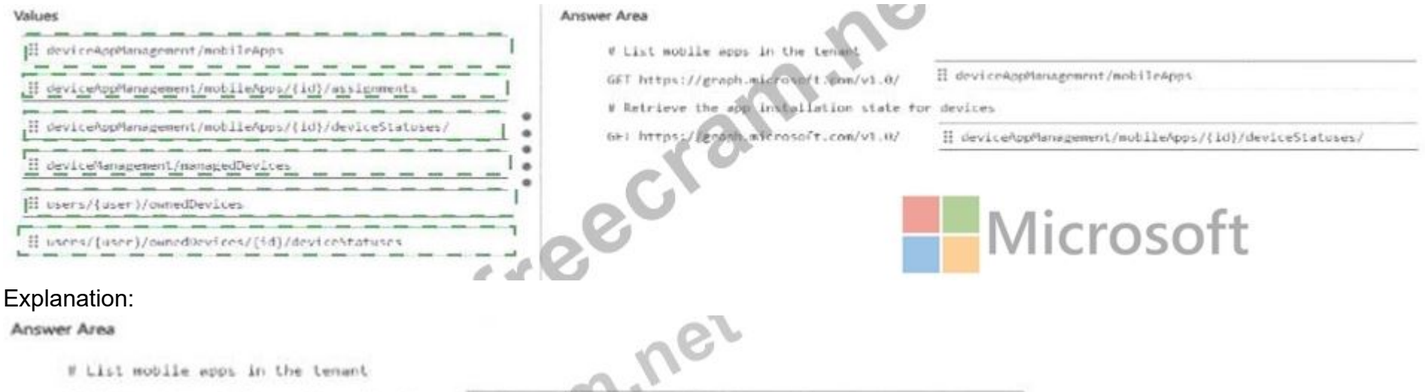
freecram.net

NEW QUESTION: 162
Which devices are registered by using the Windows Autopilot deployment service?
A. Device1 only
B. Device3 only
C. Device1 and Device3 only
D. Device1, Device2, and Device3
Answer: (SHOW ANSWER)
Scenario: Windows Autopilot Configuration
Assignments
Included groups: Group1
Excluded groups: Group2
Device1 is member of Group1.
Device2 is member of Group1 and member of Group2.
Device3 is member of Group1.
Group1 and Group2 have a Membership type of Assigned.
Exclusion takes precedence over inclusion in the following same group type scenarios.
Reference: https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

NEW QUESTION: 163
You have a Microsoft 365 subscription that uses Microsoft Intune.
You need to build Microsoft Graph requests that return the following information:
The available mobile apps in the subscription
The app installation state of each device in the Intune tenant
How should you complete the requests? To answer, drag the appropriate values to the correct targets. Each value 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.



Answer:



Explanation:



NEW QUESTION: 164

You have a Microsoft 365 E5 subscription that includes Microsoft Intune. The subscription contains a group named Group! Group1 contains devices enrolled in Intune.

You deploy Remote Help in Intune.

You need to configure Remote Help to only allow support administrators to join Remote Help sessions from the devices in Group1.

Which type of Microsoft Entra object should you create, and which type of policy should you configure7 To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

devices



Answer:



Explanation:



NEW QUESTION: 165

You have a Microsoft 365 subscription.

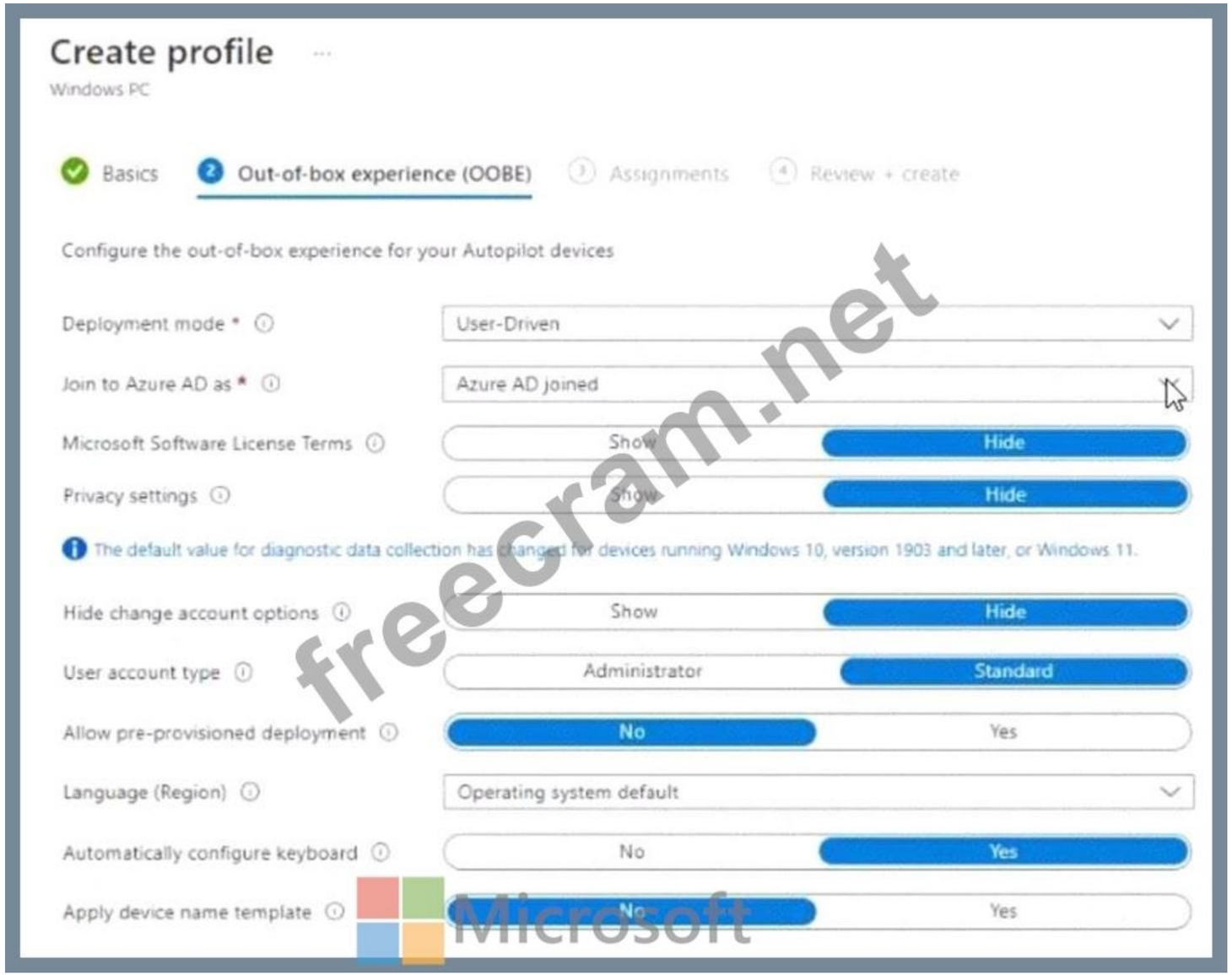
You create a retention label named Retention1 as shown in the following exhibit.



freecram.net

You apply Retention1 to all the Microsoft OneDrive content.
On January 1, 2020, a user stores a file named File1 in OneDrive.
On January 10, 2020, the user modifies File1.
On February 1, 2020, the user deletes File1.
When will File1 be removed permanently and unrecoverable from OneDrive?
A. August 1, 2020
B. July 1, 2020
C. July 10, 2020
D. February 1, 2020
Answer: (SHOW ANSWER)

NEW QUESTION: 166
You have a hybrid Azure AD tenant.
You configure a Windows Autopilot deployment profile as shown in the following exhibit.



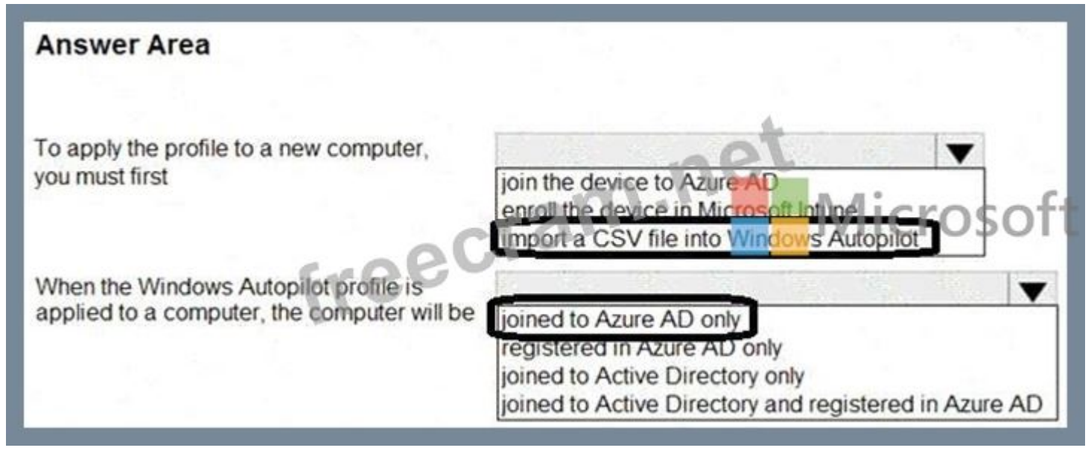
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



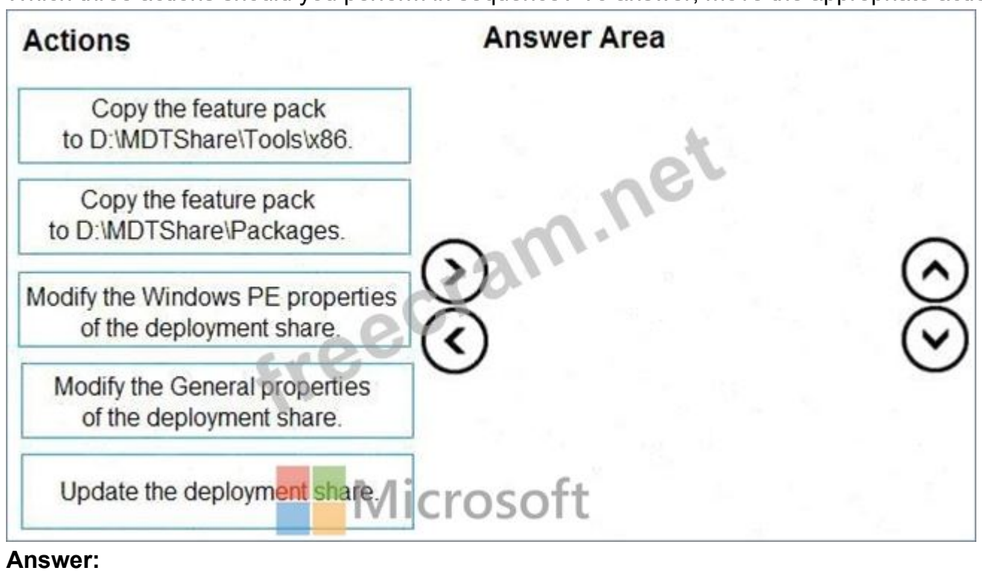
Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 167

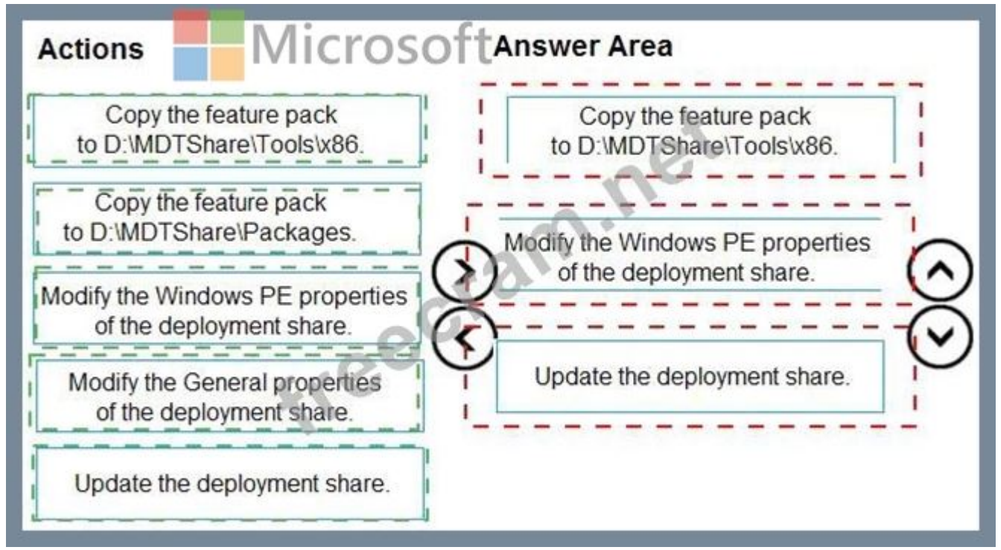
You have a Microsoft Deployment Toolkit (MDT) deployment share that has a path of D:\MDTShare.

You need to add a feature pack to the boot image.

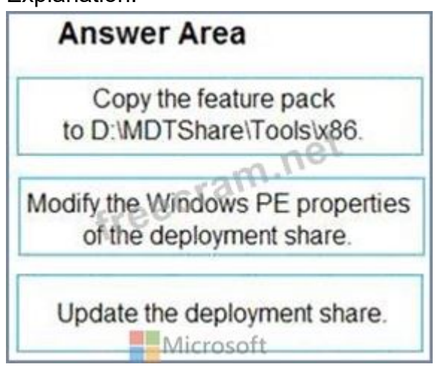
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:



Step 1: Copy the feature pack to D:\MDTShare\Tools\x86

Add a feature pack, DaRT 10 (part of MDOP 2015), to the boot images.

1. Copy the CAB files to the deployment share: MDTShare\Tools\x86
2. In the Deployment Workbench, right-click the MDTShare deployment share and select Properties.

Step 2: Modify the Windows PE properties of the deployment share

3. On the Windows PE tab, in the Platform drop-down list, make sure x86 is selected.
4. On the Features sub tab, select the Microsoft Diagnostics and Recovery Toolkit (DaRT) checkbox.

Step 3: Update the deployment share

Like the MDT Build Lab deployment share, the MDT Production deployment share needs to be updated after it has been configured. This is the process during which the Windows PE boot images are created.

NEW QUESTION: 168

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft Entra tenant named contoso.com.

You purchase an Android device named Device1.
You need to register Device1 in contoso.com.
Solution; You use the Microsoft Intune Company Portal app.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)

NEW QUESTION: 169
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 create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	○	○
User2 can remove D:\Folder1 from the list of protected folders on Device2.	○	○
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	○	○

Answer:

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

Explanation:

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

NEW QUESTION: 170

You have a Microsoft 365 E5 subscription.
You have a Microsoft Intune enrollment profile for Android Enterprise devices that has the following settings:
* Name: Profile1
* Token type: Corporate-owned, fully managed
You need to enroll a new Android device in Intune by using Profile1. What should you use to enroll the device?

A. aQRcode
B. the Intune app
C. the Company Portal app
D. the Microsoft Authenticate app
Answer: (SHOW ANSWER)

NEW QUESTION: 171
You have a Microsoft Entra tenant named contoso.com that contains the dynamic membership groups shown in the following table.

Name	Dynamic membership rule
Group1	(device.displayName -startsWith "Dev") or (device.deviceOSType -eq "Android")
Group2	(device.deviceTrustType -eq "Workplace")
Group3	(device.deviceTrustType -eq "AzureAD") and (device.deviceOSType -eq "Android")

You add devices to contoso.com as shown in the following table.

Name	Platform	Join type
Device1	Windows	Microsoft Entra joined
Device2	Windows	Microsoft Entra registered
Phone1	Android	Microsoft Entra registered

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

Answer Area

Statements	Yes	No
Device1 is a member of Group1 only.	○	○
Device2 is a member of Group1 and Group2.	○	○
Phone1 is a member of Group1 and Group3.	○	○

Answer:

Answer Area

Statements	Yes	No
Device1 is a member of Group1 only.	○	○
Device2 is a member of Group1 and Group2.	○	○
Phone1 is a member of Group1 and Group3.	○	○

Explanation:

Answer Area

Statements	Yes	No
Device1 is a member of Group1 only.	●	○
Device2 is a member of Group1 and Group2.	●	○
Phone1 is a member of Group1 and Group3.	○	●

NEW QUESTION: 172

Your network contains an on-premises Active Directory Domain Services (AD DS) domain.

You have a Microsoft 365 E5 subscription that includes Microsoft Intune and syncs with the AD DS domain.

Windows Local Administrator Password Solution (Windows LAPS) is enabled in Microsoft Entra ID.

The subscription has the custom roles shown in the following table.

Name	Permission
Role1	microsoft.directory/deviceLocalCredentials/password/read
Role2	microsoft.directory/deviceLocalCredentials/standard/read
Role3	microsoft.directory/deviceLocalCredentials/standard/read microsoft.directory/deviceLocalCredentials/password/read

Microsoft Entra contains the users shown in the following table.

Name	Built-in role	Assigned custom roles
User1	Helpdesk Administrator	Role1
User2	Security Reader	Role2
User3	*None*	Role3

You have the devices shown in the following table.

Name	Domain Join Type
Device1	Joined to AD DS
Device2	Microsoft Entra hybrid joined
Device3	Microsoft Entra joined

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

Answer Area

Statements	Yes	No
User1 can use Microsoft Entra to read the local administrator password of Device1.	○	○
User2 can use Microsoft Entra to read the local administrator password of Device2.	○	○
User3 can use Microsoft Entra to read the local administrator password of Device3.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can use Microsoft Entra to read the local administrator password of Device1.	○	○
User2 can use Microsoft Entra to read the local administrator password of Device2.	○	○
User3 can use Microsoft Entra to read the local administrator password of Device3.	○	○

Explanation:

Answer Area

Statements	Yes	No
User1 can use Microsoft Entra to read the local administrator password of Device1.	○	●
User2 can use Microsoft Entra to read the local administrator password of Device2.	○	●
User3 can use Microsoft Entra to read the local administrator password of Device3.	●	○

NEW QUESTION: 173

You have a Microsoft 365 E5 subscription that contains a user named User! and a web app named Appl.
App1 must only accept modern authentication requests.
You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:
* Assignments
° Users or workload identities: User1
° Cloud apps or actions: App1
* Access controls
° Grant: Block access
You need to block only legacy authentication requests to Appl. Which condition should you add to CAPolicy1?
A. Filter for devices
B. Device platforms
C. User risk
D. Sign-in risk
E. Client apps
Answer: (SHOW ANSWER)
you can use the client apps condition to block legacy authentication requests to App11. Legacy authentication is a term that refers to authentication protocols that do not support modern authentication features such as multi-factor authentication or conditional access2. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos2. To block legacy authentication requests, you need to configure the client apps condition to include Other clients, which covers any client that uses legacy authentication protocols13. References: 1: Conditional Access: Block legacy authentication | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/block-legacy-authentication 2:
What is legacy authentication? | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection
/conditional-access/legacy-authentication 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/client- apps-condition

NEW QUESTION: 174
You have the devices shown in the following table.

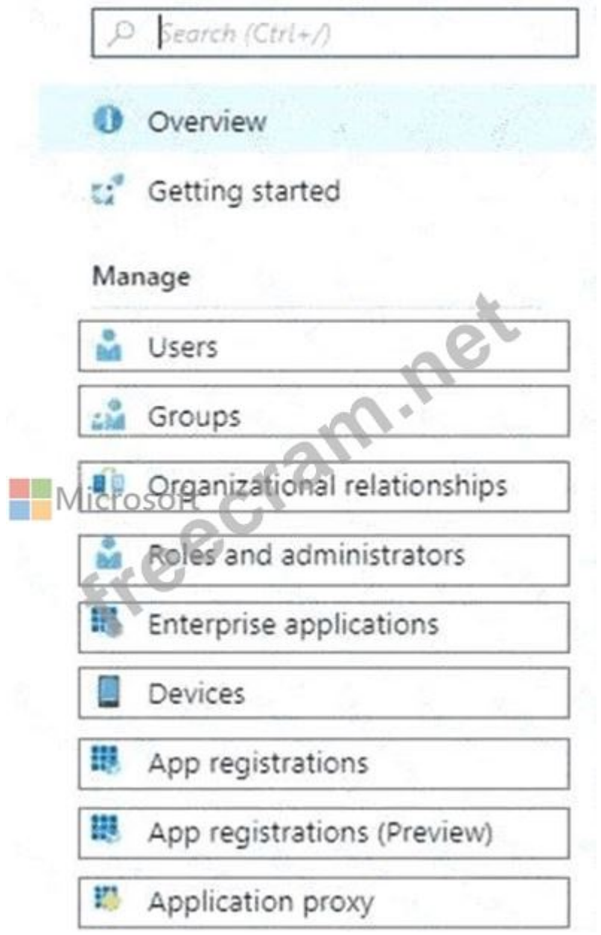
Name	Operating system	Domain member
Device1	Windows 11 Enterprise	No
Device2	Windows 10 Pro	Yes
Device3	Android	No
Device4	Mac OS X	No

You plan to implement Microsoft Defender for Endpoint.
You need to identify which devices can be onboarded to Microsoft Defender for Endpoint.
What should you identify?
A. Device1 only
B. Device2 only
C. Device1, Device2 only
D. Device1, Device2, and Device3 only
E. Device1, Device2, Device3, and Device4
Answer: (SHOW ANSWER)
Here is the list of Windows versions. Win10 and Win11 supported. The sentence " (standalone or as part of other Microsoft 365 plans) " excludes the domain needs.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?

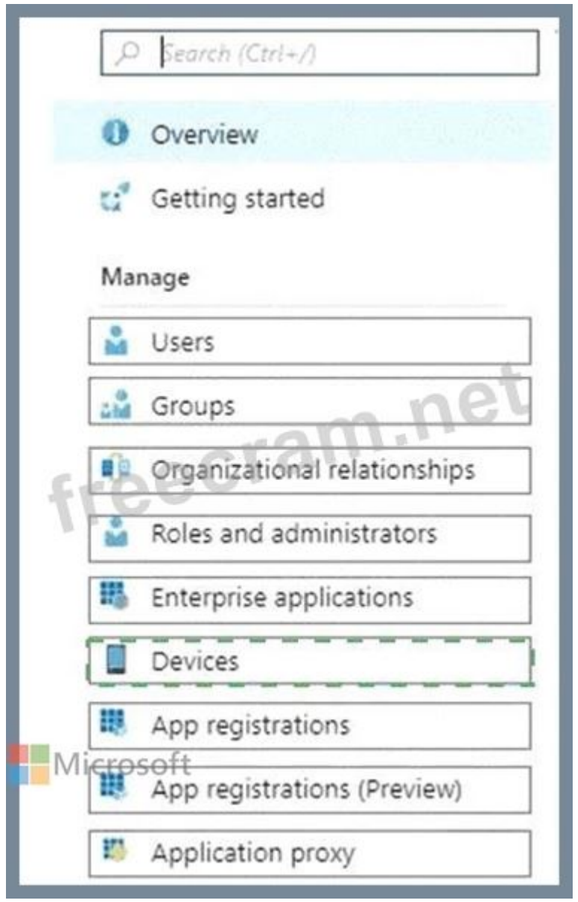
view=o365-worldwide
Here is the link for Android. No information about the specific version therefore it is supported.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-android?view=o365-worldwide Here is the link for MacOS System requirements: 14 (Sonoma), 13 (Ventura), 12 (Monterey). MAC OS X is older therefore unsupported.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac?view=o365-worldwide

NEW QUESTION: 175
You have a workgroup computer named Client1 that runs Windows 11 and connects to a public network.
You need to enable PowerShell remoting on Client1. The solution must ensure that PowerShell remoting connections are accepted from the local subnet only.
Which PowerShell command should you run?
A. Set-PSSessionConfiguration -AccessMode Local
B. Enable-PSRemoting -SkipNetworkProfileCheck
C. Enable-PSRemoting -Force
D. Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any
Answer: B (LEAVE A REPLY)

NEW QUESTION: 176
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.

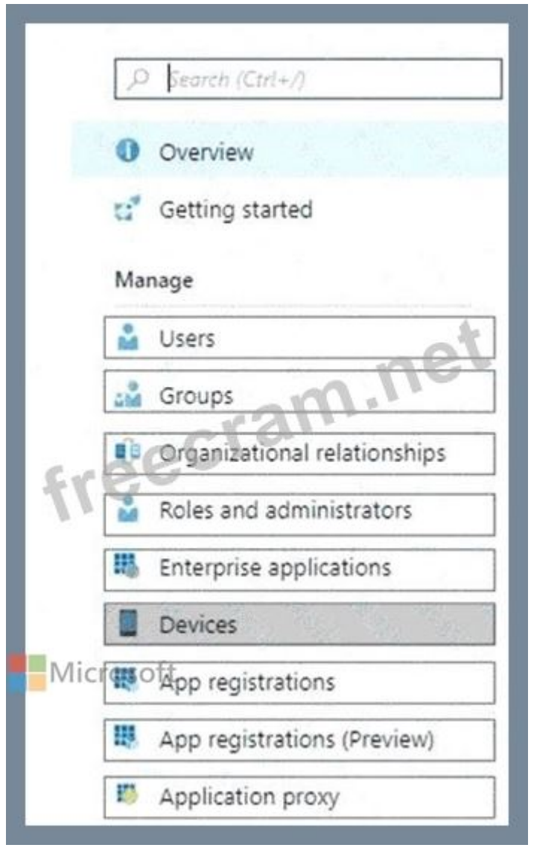

Search (Ctrl+/)
Overview
Getting started
Manage
Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy

Answer:



freecram.net
Microsoft

Explanation:



freecram.net
Microsoft

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

Topic 1, Litware inc

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Existing Environment

Current Business Model

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11:00 to 22:00.

Litware has a Microsoft System Center 2012 R2 Configuration Manager deployment. During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Configuration Manager	Hybrid Azure AD-joined
Research	10	Configuration Manager	Hybrid Azure AD-joined
HR	8.1	Configuration Manager	Hybrid Azure AD-joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

freecram.net

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed.

The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.) Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements

Business Goals

Litware plans to transition to co-management for all the company-owned Windows 10 computers. Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements

Litware identifies the following device management requirements:

Prevent the sales department employees from forwarding email that contains bank account information.

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.

Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements

Litware identifies the following technical requirements for the planned deployment:

Re-provision the sales department computers by using Windows AutoPilot.

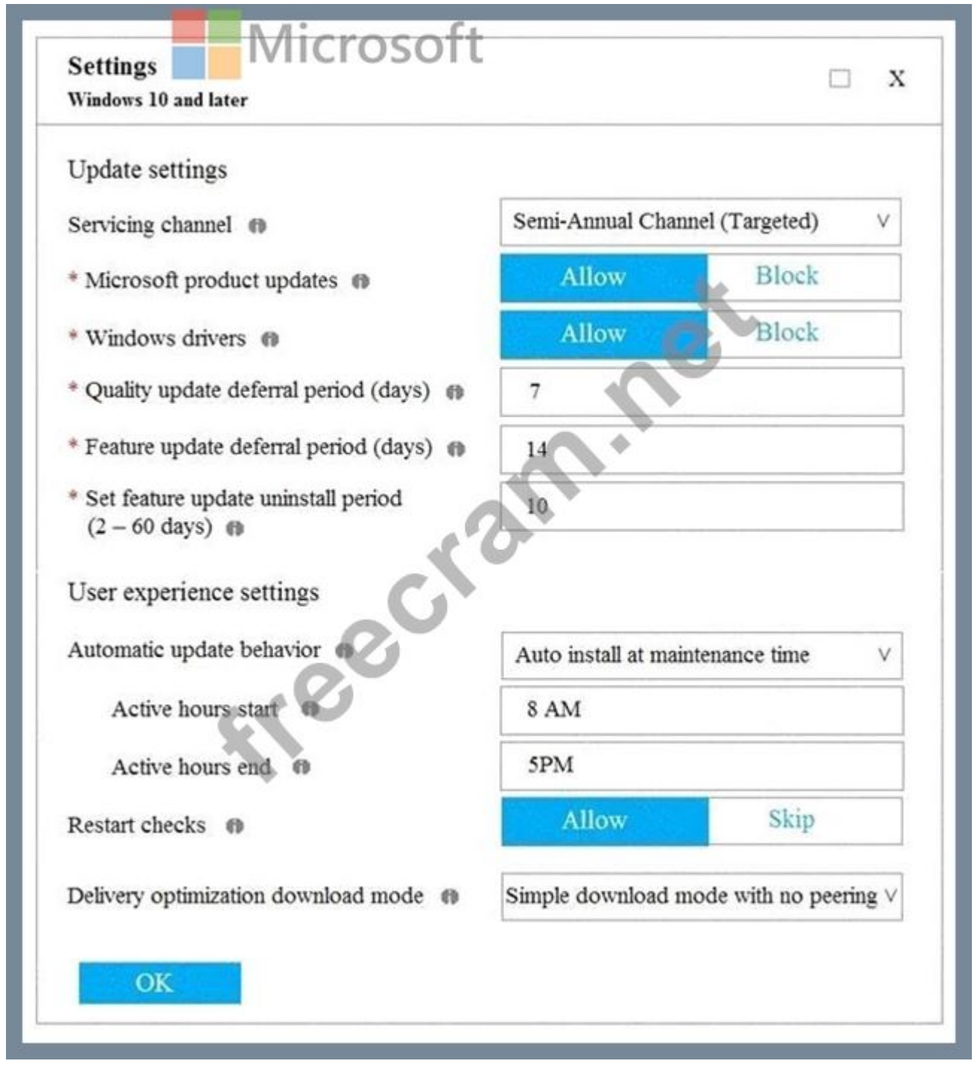
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.

Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every

30 days.

Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits



Microsoft
freecram.net

NEW QUESTION: 177

You have a Microsoft 365 subscription that contains a Windows 11 device named Device! and two users named User1 and User2. Device1 is enrolled in Microsoft Intune. User1 is assigned the Help Desk Operator role.

User2 signs in to Device1.

You have the following support requirements:

Requirement1: Review organization-wide failed Intune enrollment attempts by all users, including failure details and recommended remediation.

Requirement2: Investigate policy delivery issues for User2-

Requirement3: Investigate a configuration issue when an expected VPN profile is missing from the device configuration policy for Device1.



Answer:



Explanation:



NEW QUESTION: 178

You have a Microsoft 365 subscription that uses Microsoft Intune. Intune has automatic enrollment enabled.

You purchase 20 Windows 11 devices and join the devices to the Microsoft Entra tenant You need to enforce a lock screen timeout on the devices. The solution must minimize administrative effort. What must you create?

A. a configuration profile

B. a remediation script

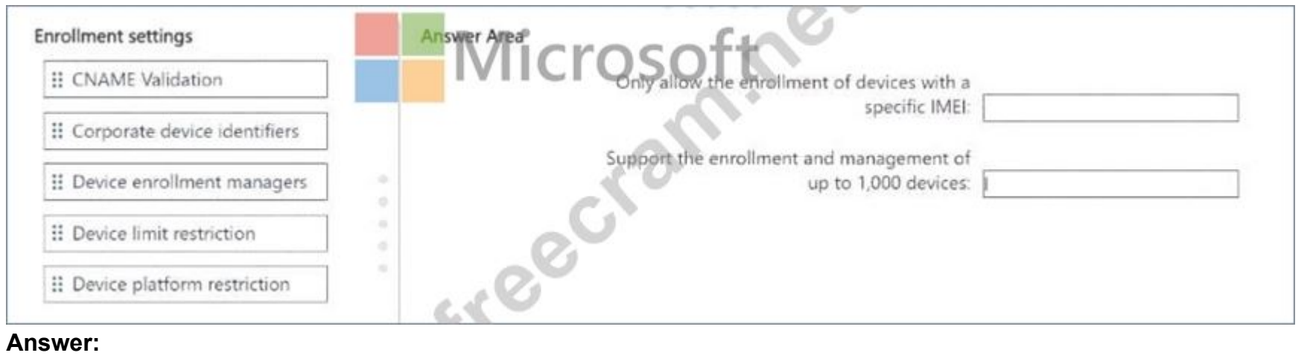
C. a compliance policy

D. a Conditional Access policy

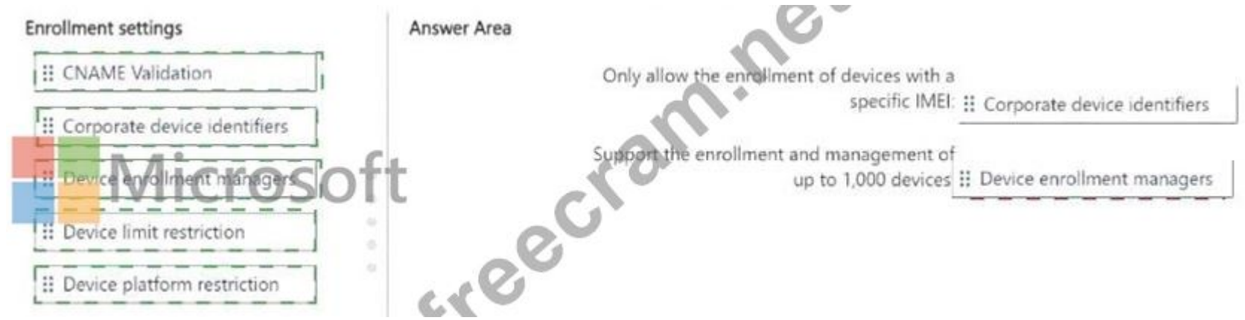
Answer: (SHOW ANSWER)

NEW QUESTION: 179
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: (SHOW ANSWER)
https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe#delete-devices-from-the-intune- admin-center

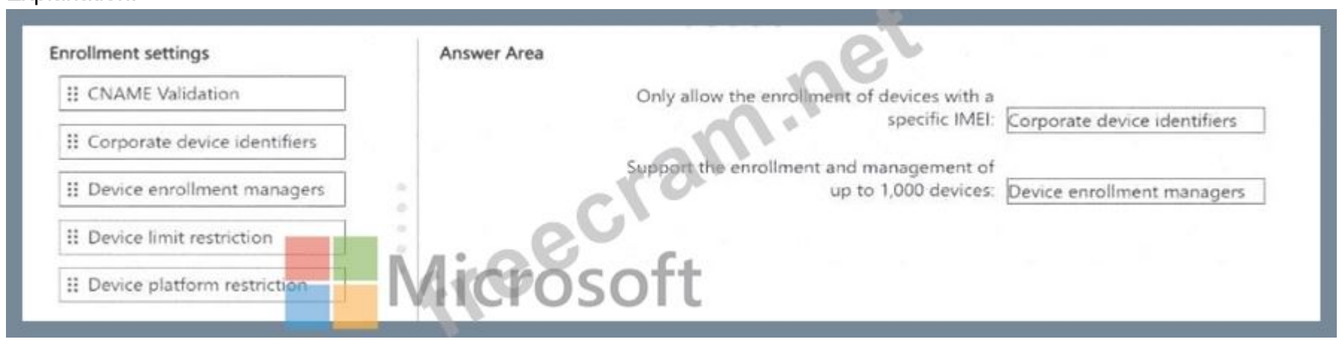
NEW QUESTION: 180
You have a Microsoft 365 subscription.
You plan to enroll devices in Microsoft Intune. You need to meet the following requirements:
* Only allow the enrollment of devices that have a specific international mobile equipment identifier (IMEI).
* Support the enrollment and management of up to 1,000 devices
Which enrollment setting should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.
devices



Answer:



Explanation:



NEW QUESTION: 181

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

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Enabled

You have the devices shown in the following table.

Name	Platform
Device1	Android
Device2	iOS

You have a Conditional Access policy named CAPolicy1 that has the following settings:

* Assignments

o Users or workload identities: User 1. User1

o Cloud apps or actions: Office 365 Exchange Online

o Conditions: Device platforms: Windows, iOS

* Access controls

o Grant Require multi-factor authentication

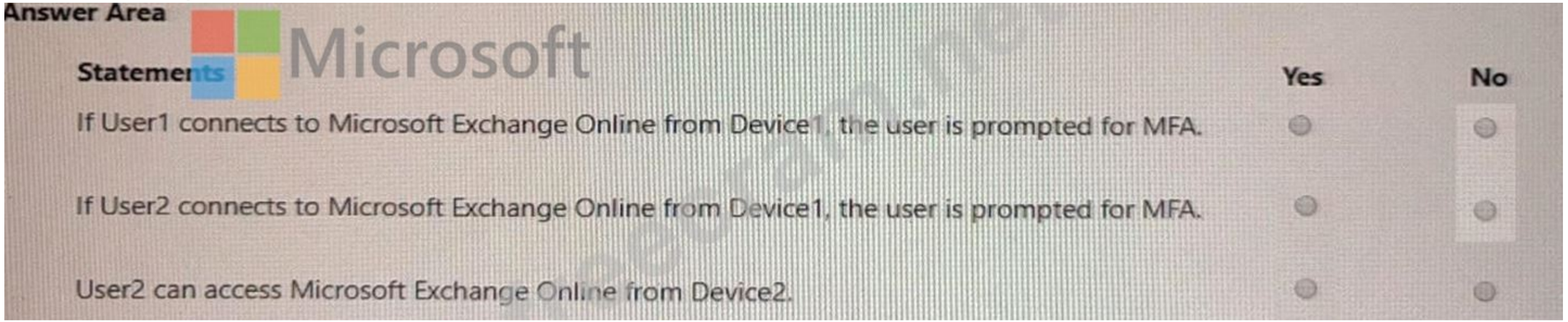
You have a Conditional Access policy named CAPolicy2 that has the following settings:

Assignments

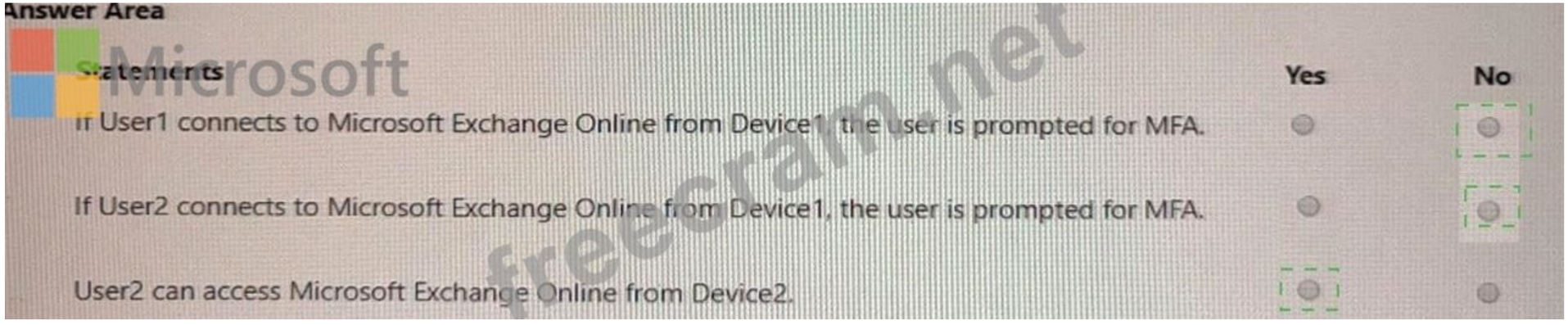
o Users or workload identities: Used, User2

o Cloud apps or actions: Office 365 Exch
o Conditions
Device platforms: Android, iOS
Filter for devices
Device matching the rule: Exclude filtered devices from policy
Rule syntax: device. displayName- contains " 1 "
Access controls
Grant Block access
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

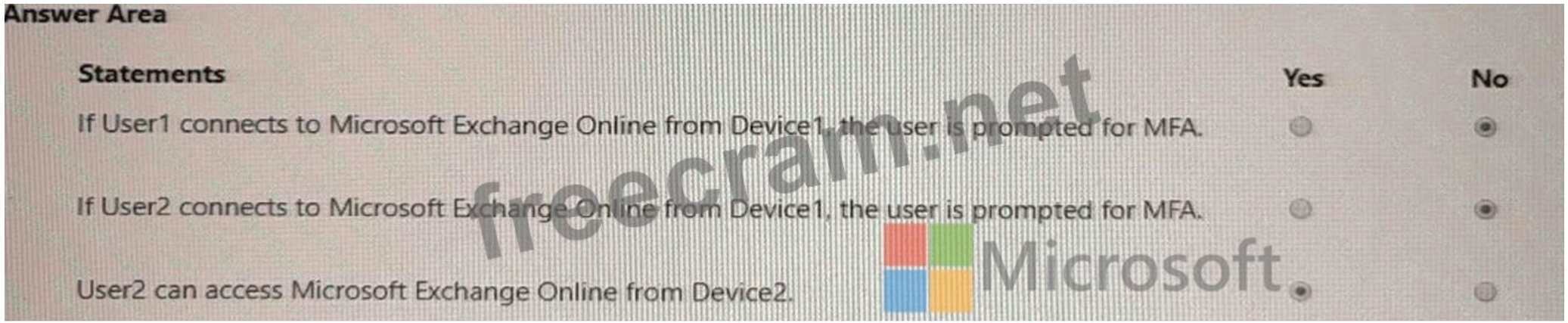
Answer Area



Answer:



Explanation:



Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 182
You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft Intune. You create an app configuration policy that contains the following settings:
* Device enrollment type: Managed devices
* Profile Type: All Profile Types
* Platform: Android Enterprise
Which two types of apps can be associated with the policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. Managed Google Play store app
B. Android store app
C. Web link
D. Android Enterprise system app
E. Built-in Android app
Answer: (SHOW ANSWER)

NEW QUESTION: 183
You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices.
You purchase a Microsoft 365 E5 subscription.
You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.
Which upgrade method should you use?
A. Windows Autopilot
B. a Microsoft Deployment Toolkit (MDT) lite-touch deployment
C. Subscription Activation

D. an in-place upgrade by using Windows installation media

Answer: (SHOW ANSWER)

Subscription Activation is a feature that allows you to upgrade from Windows 10 Pro or Windows 11 Pro to Windows 10 Enterprise or Windows 11 Enterprise without needing a product key or reinstallation. You just need to assign a subscription license (such as Microsoft 365 E5) to the user in Azure AD, and then sign in to the device with that user account. The device will automatically activate Windows Enterprise edition using the firmware-embedded activation key for Windows Pro edition. This method minimizes administrative effort and simplifies the upgrade process. References: Windows subscription activation, Deploy Windows Enterprise licenses

Valid MD-102 Dumps shared by ExamDiscuss.com for Helping Passing MD-102 Exam! ExamDiscuss.com now offer the **newest MD-102 exam dumps**, the ExamDiscuss.com MD-102 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com MD-102 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/MD-102/premium/ (**457** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)