Exam Questions MD-102

Endpoint Administrator

https://www.2passeasy.com/dumps/MD-102/

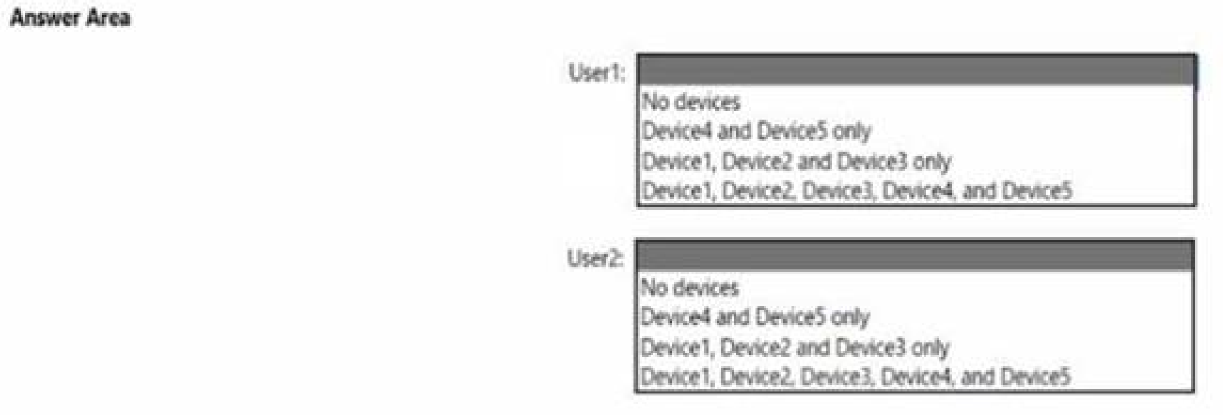
NEW QUESTION 1
- (Exam Topic 1)
Which devices are registered by using the Windows Autopilot deployment service?

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

Answer: C

Explanation:
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 2
- (Exam Topic 1)
User1 and User2 plan to use Sync your settings.
On which devices can the users use Sync your settings? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

User1:
No devices
Device4 and Device5 only
Device1, Device2 and Device3 only
Device1, Device2, Device3, Device4, and Device5

User2:
No devices
Device4 and Device5 only
Device1, Device2 and Device3 only
Device1, Device2, Device3, Device4, and Device5

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://www.jeffgilb.com/managing-local-administrators-with-azure-ad-and-intune/

NEW QUESTION 3
- (Exam Topic 1)
You implement Boundary1 based on the planned changes.
Which devices have a network boundary of 192.168.1.0/24 applied?

A. Device2 only
B. Device3 only
C. Device 1. Device2. and Device5 only
D. Device 1, Device2, Device3, and Device4 only

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/network-boundary-windows

NEW QUESTION 4
- (Exam Topic 2)
You need to meet the device management requirements for the developers. What should you implement?

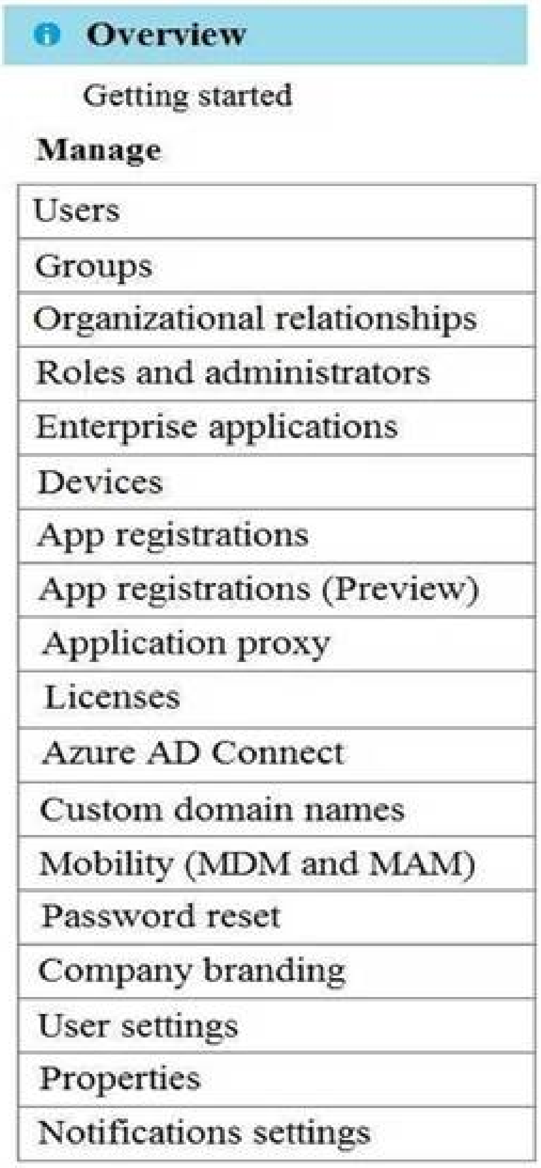
A. folder redirection
B. Enterprise State Roaming
C. home folders
D. known folder redirection in Microsoft OneDrive

Answer: B

Explanation:
Litware identifies the following device management requirements:
➢

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in. Enterprise State Roaming allows for the synchronization of Microsoft Edge browser setting, including
favorites and reading list, across devices.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-refer

NEW QUESTION 5
- (Exam Topic 2)
You need to meet the OOBE requirements for Windows AutoPilot.
Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://blogs.msdn.microsoft.com/sgern/2018/10/11/intune-intune-and-autopilot-part-3-preparing-your-environm
https://blogs.msdn.microsoft.com/sgern/2018/11/27/intune-intune-and-autopilot-part-4-enroll-your-first-device/

NEW QUESTION 6
- (Exam Topic 3)
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: C

Explanation:
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 7
- (Exam Topic 3)
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:

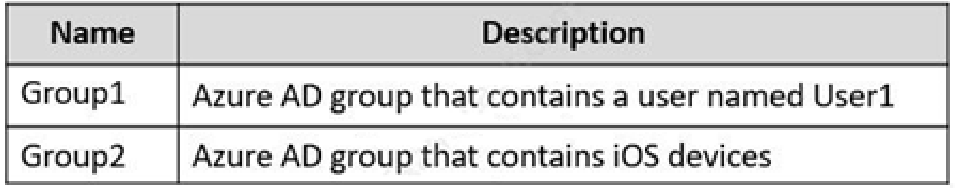
• Assignments
° Users or workload identities: User1
° Cloud apps or actions: App1
• Access controls
° Grant: Block access
You need to block only legacy authentication requests to Appl. Which condition should you add to CAPolicy1?

A. Filter for devices
B. Device platforms
C. User risk
D. Sign-in risk
E. Client apps

Answer: E

Explanation:
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 8
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.



Name	Description
Group1	Azure AD group that contains a user named User1
Group2	Azure AD group that contains iOS devices

You create a Conditional Access policy named CAPolicy1 that will block access to Microsoft Exchange Online from iOS devices. You assign CAPolicy1 to Group1.
You discover that User1 can still connect to Exchange Online from an iOS device. You need to ensure that CAPolicy1 is enforced.
What should you do?

A. Configure a new terms of use (TOU).
B. Assign CAPolicy1 to Group2.
C. Enable CAPolicy1
D. Add a condition in CAPolicy1 to filter for devices.

Answer: B

Explanation:
Common signals that Conditional Access can take in to account when making a policy decision include the following signals:
* User or group membership
Policies can be targeted to specific users and groups giving administrators fine-grained control over access.
* Device
Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.
Use filters for devices to target policies to specific devices like privileged access workstations.
* Etc.
Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

NEW QUESTION 9
- (Exam Topic 3)
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a network share. You start Computer1 from Windows PE (WinPE), and then you run setup.exe from the network share.
Does this meet the goal?

A. Yes
B. No

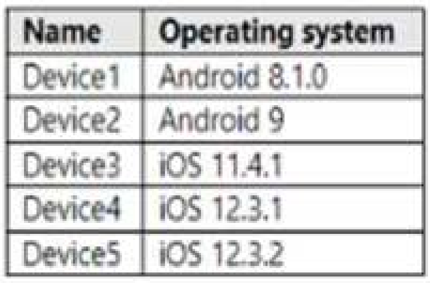
Answer: B

NEW QUESTION 10
- (Exam Topic 3)
Your network contains an Active Directory domain. The domain contains a user named Admin1. All computers run Windows 10.
You enable Windows PowerShell remoting on the computers.
You need to ensure that Admin1 can establish remote PowerShell connections to the computers. The solution must use the principle of least privilege.
To which group should you add Admin1?

A. Access Control Assistance Operators
B. Remote Desktop Users
C. Power Users
D. Remote Management Users

Answer: B

NEW QUESTION 10
- (Exam Topic 3)
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

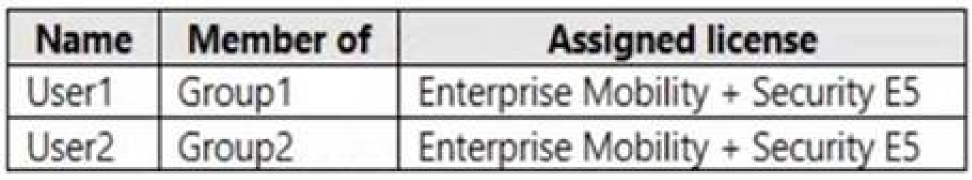
An app named App1 is installed on each device.
What is the minimum number of app configuration policies required to manage Appl ?

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

Answer: B

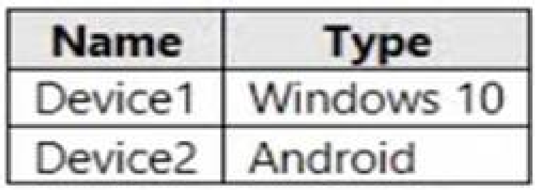
Explanation:
The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices1. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices1. The settings are assigned 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 13
- (Exam Topic 3)
You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.



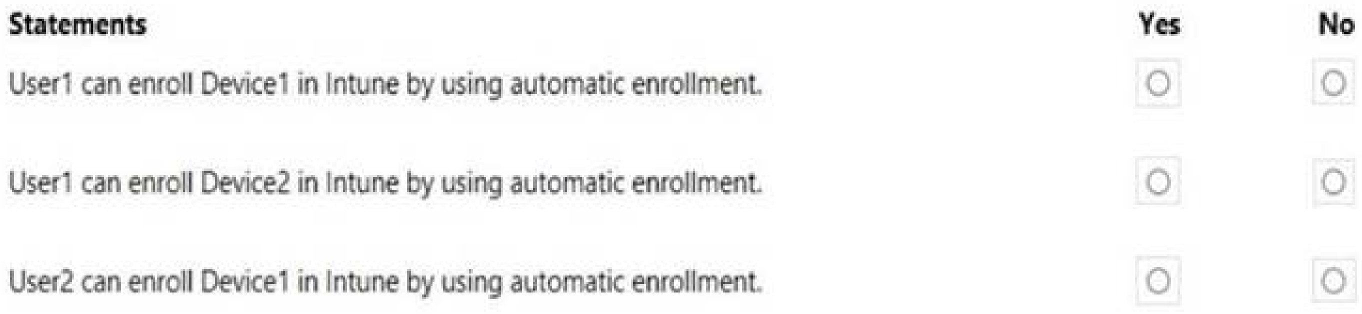
Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.



Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:
> MDM user scope: Group1
> MAM user scope: Group2
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



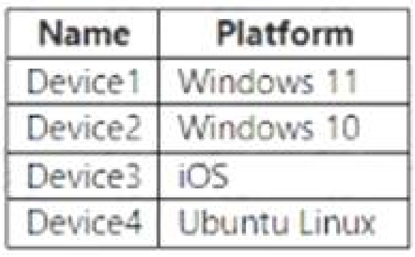
Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	○	○
User1 can enroll Device2 in Intune by using automatic enrollment.	○	○
User2 can enroll Device1 in Intune by using automatic enrollment.	○	○

A. Mastered
B. Not Mastered

Answer: A

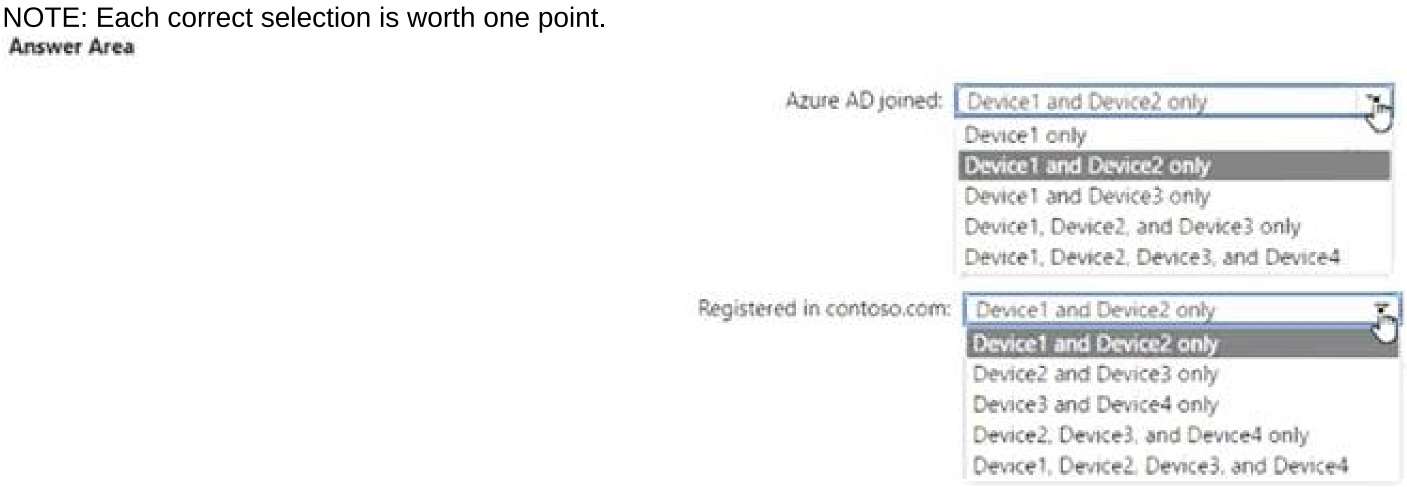
Explanation:
Graphical user interface, text, application Description automatically generated
Reference: https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/

NEW QUESTION 14
- (Exam Topic 3)
You have an Azure AD tenant named contoso.com. You have the devices shown in the following table.



Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	Ubuntu Linux

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



Answer Area

Azure AD joined: Device1 and Device2 only

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

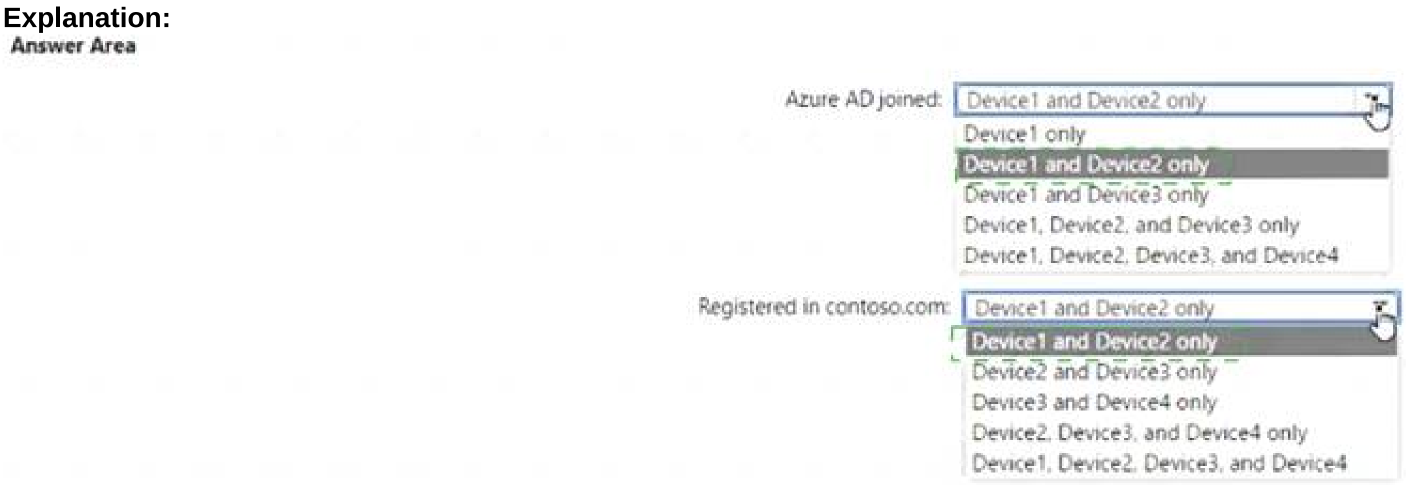
Registered in contoso.com: Device1 and Device2 only

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Azure AD joined: Device1 and Device2 only

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

Registered in contoso.com: Device1 and Device2 only

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

NEW QUESTION 15
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices. All the devices are enrolled in Microsoft Intune. You need to configure Delivery Optimization on the devices to meet the following requirements:
• Allow downloads from the internet and from other computers on the local network.
• Limit the percentage of used bandwidth to 50. What should you use?

A. a configuration profile
B. a Windows Update for Business Group Policy setting
C. a Microsoft Peer-to-Peer Networking Services Group Policy setting
D. an Update ring for Windows 10 and later profile

Answer: A

Explanation:
A configuration profile is the correct answer because it allows you to configure Delivery Optimization settings for Windows devices in Intune. You can specify the download mode, bandwidth limit, caching options, and more. A configuration profile is a template that contains one or more settings that you can apply to groups of devices. References:
> Windows 10 Delivery Optimization settings for Intune - Microsoft Intune | Microsoft Learn
> Delivery Optimization settings in Microsoft Intune

NEW QUESTION 16
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

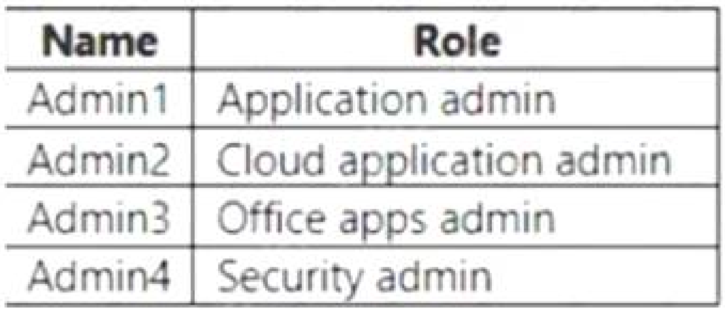
A. an attack surface reduction (ASR) policy
B. a security baseline
C. an endpoint detection and response (EDR) policy
D. an account protection policy
E. an antivirus policy

Answer: C

Explanation:

To onboard 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 17
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



Name	Role
Admin1	Application admin
Admin2	Cloud application admin
Admin3	Office apps admin
Admin4	Security admin

In the Microsoft 365 Apps admin center, you create a Microsoft Office customization. Which users can download the Office customization file from the admin center?

A. Admin1, Admin2, Admin3. and Admin4
B. Admin1, Admin2, and Admin3 only
C. Admin3 only
D. Admin3 and Admin4 only
E. Admin1 and Admin3 only

Answer: B

Explanation:
* Admin1
An application admin has full access to enterprise applications, applications registrations, and application proxy settings.
* Admin2
Mark your app as publisher verified.
In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.
* Admin3
Office Apps admin - Assign the Office Apps admin role to users who need to do the following:
- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health
Reference:
Office Apps admin - Assign the Office Apps admin role to users who need to do the following https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified

NEW QUESTION 20
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains a group named Group1.
You create a Conditional Access policy named CAPolicy1 and assign CAPolicy1 to Group1.
You need to configure CAPolicy1 to require the members of Group1 to reauthenticate every eight hours when they connect to Microsoft Exchange Online.
What should you configure?

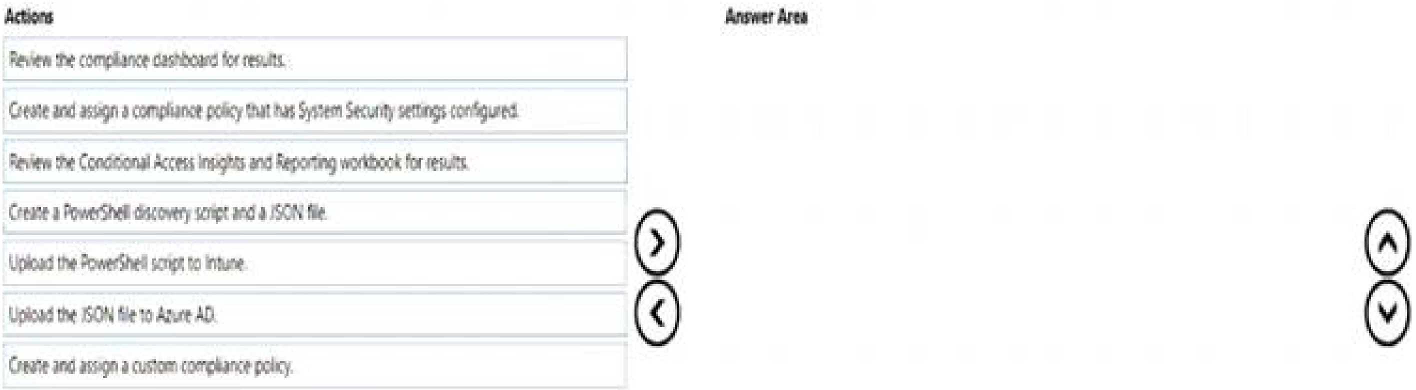
A. Session access controls
B. an assignment that uses a User risk condition
C. an assignment that uses a Sign-in risk condition
D. Grant access controls

Answer: A

Explanation:
User sign-in frequency
Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.
The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.
Sign-in frequency control
➢ Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.
➢ Browse to Azure Active Directory > Security > Conditional Access.
➢ Select New policy.
➢ Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
➢ Choose all required conditions for customer's environment, including the target cloud apps.
➢ Under Access controls > Session.
Select Sign-in frequency.
Choose Periodic reauthentication and enter a value of hours or days or select Every time.
➢ Save your policy. Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-life

NEW QUESTION 24
- (Exam Topic 3)
You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.
You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the

correct order.



Actions

Review the compliance dashboard for results.

Create and assign a compliance policy that has System Security settings configured.

Review the Conditional Access Insights and Reporting workbook for results.

Create a PowerShell discovery script and a JSON file.

Upload the PowerShell script to Intune.

Upload the JSON file to Azure AD.

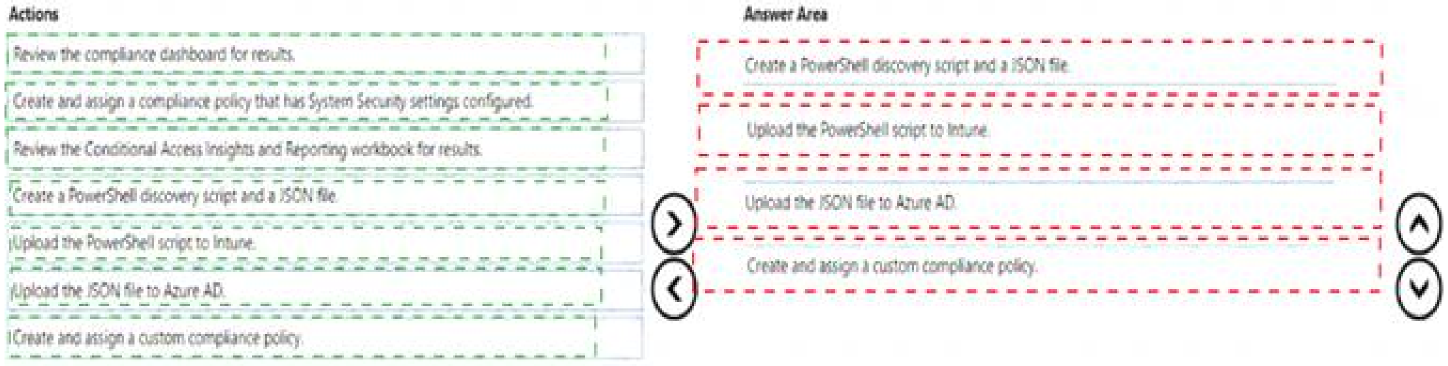
Create and assign a custom compliance policy.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

Review the compliance dashboard for results.

Create and assign a compliance policy that has System Security settings configured.

Review the Conditional Access Insights and Reporting workbook for results.

Create a PowerShell discovery script and a JSON file.

Upload the PowerShell script to Intune.

Upload the JSON file to Azure AD.

Create and assign a custom compliance policy.

Answer Area

Create a PowerShell discovery script and a JSON file.

Upload the PowerShell script to Intune.

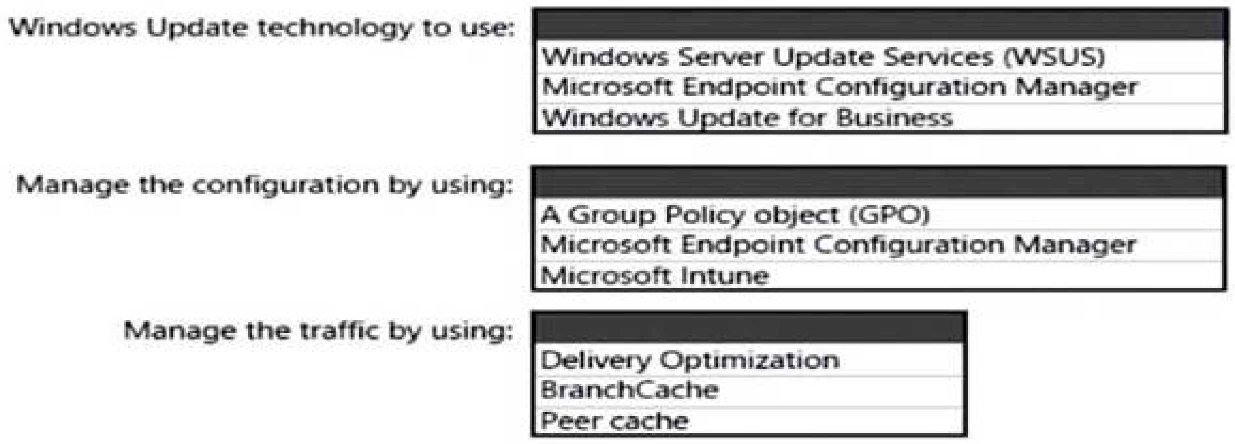
Upload the JSON file to Azure AD.

Create and assign a custom compliance policy.

NEW QUESTION 29
- (Exam Topic 3)
You have 100 computers that run Windows 10. You have no servers. All the computers are joined to Microsoft Azure Active Directory (Azure AD).
The computers have different update settings, and some computers are configured for manual updates. You need to configure Windows Update. The solution must meet the following requirements:

- The configuration must be managed from a central location.
- Internet traffic must be minimized.
- Costs must be minimized.

How should you configure Windows Update? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Windows Update technology to use:
- Windows Server Update Services (WSUS)
- Microsoft Endpoint Configuration Manager
- Windows Update for Business

Manage the configuration by using:
- A Group Policy object (GPO)
- Microsoft Endpoint Configuration Manager
- Microsoft Intune

Manage the traffic by using:
- Delivery Optimization
- BranchCache
- Peer cache

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Windows Server Update Services (WSUS)
Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.
Windows Server Update Services is a built-in server role that includes the following enhancements: Can be added and removed by using the Server Manager Includes Windows PowerShell cmdlets to manage the most important administrative tasks in WSUS Etc.
Box 2: A Group Policy object
In an Active Directory environment, you can use Group Policy to define how computers and users can interact with Windows Update to obtain automatic updates from Windows Server Update Services (WSUS).
Box 3: BranchCache
BranchCache is a bandwidth-optimization feature that has been available since the Windows Server 2008 R2 and Windows 7 operating systems. Each client has a cache and acts as an alternate source for content that devices on its own network request. Windows Server Update Services (WSUS) and Microsoft Endpoint Manager can use BranchCache to optimize network bandwidth during update deployment, and it's easy to configure for either of them. BranchCache has two operating modes: Distributed Cache mode and Hosted Cache mode.
Reference: https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-conf

NEW QUESTION 31

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

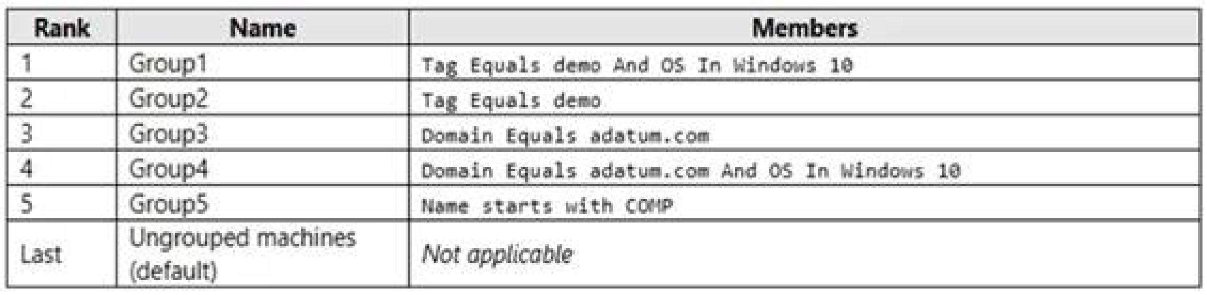
A. Assignments
B. Settings
C. Scope (Tags)
D. Applicability Rules

Answer: D

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

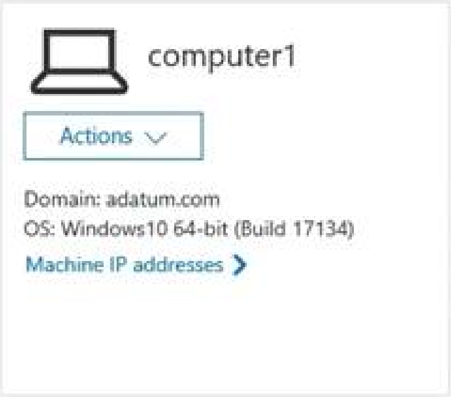
NEW QUESTION 32

- (Exam Topic 3)
Your company uses Microsoft Defender for Endpoint Microsoft Defender for Endpoint includes the device groups shown in the following table.



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

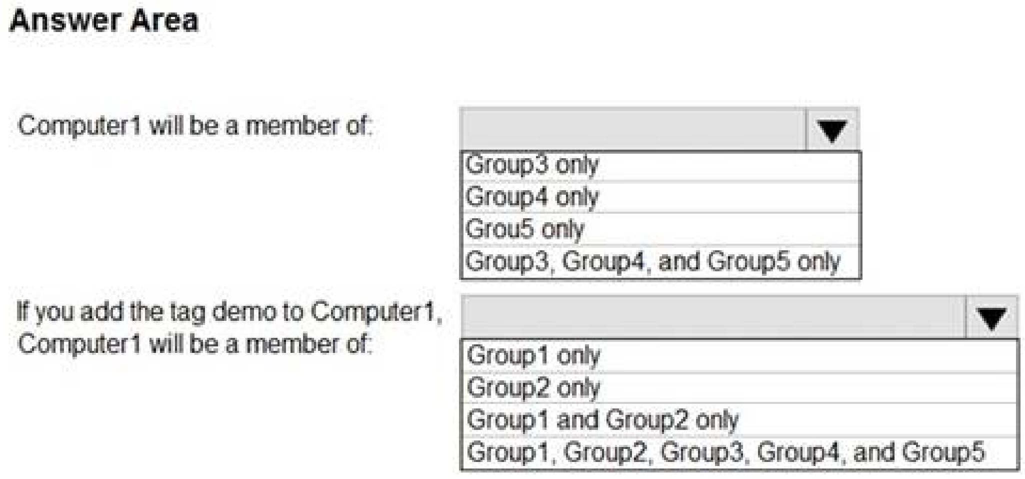
You onboard a computer to Microsoft Defender for Endpoint as shown in the following exhibit.



computer1

Domain: adatum.com
OS: Windows10 64-bit (Build 17134)

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



Answer Area

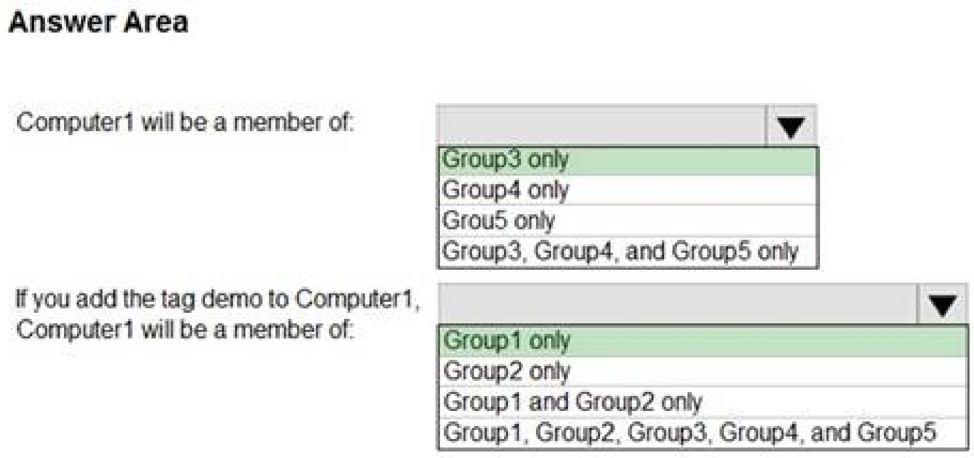
Computer1 will be a member of:
- Group3 only
- Group4 only
- Grou5 only
- Group3, Group4, and Group5 only

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

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

NEW QUESTION 33
- (Exam Topic 3)
You use Microsoft Intune and Intune Data Warehouse.
You need to create a device inventory report that includes the data stored in the data warehouse. What should you use to create the report?

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

Answer: D

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

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

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

NEW QUESTION 38
- (Exam Topic 3)
You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models.
You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models.
What should you do first?

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

Answer: B

NEW QUESTION 39
- (Exam Topic 3)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a Microsoft Deployment Toolkit (MDT) deployment share. You create a task sequence, and then you run the MDT deployment wizard on Computer1.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 44
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune.
You plan to integrate Intune with Microsoft Defender for Endpoint.
You need to establish a service-to-service connection between Intune and Defender for Endpoint. Which settings should you configure in the Microsoft Endpoint Manager admin center?

A. Connectors and tokens
B. Premium add-ons
C. Microsoft Tunnel Gateway
D. Tenant enrollment

Answer: A

Explanation:
Microsoft Defender for Endpoint – Important Service and Endpoint Settings You Should Configure Right Now.
As a prerequisite, however, head to tenant administration > connectors and tokens > Microsoft Defender for Endpoint and confirm the connection is enabled. You previously set this up in the advanced settings of Microsoft 365 Defender.
Reference: https://petri.com/microsoft-defender-for-endpoint-which-settings-configure-right-now/

NEW QUESTION 49
......