

Exam Questions MD-102

Endpoint Administrator

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



NEW QUESTION 1

- (Exam Topic 4)

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 2

- (Exam Topic 4)

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 3

- (Exam Topic 4)

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.

Actions

- Assign the policy.
- Create a compliance policy.
- Set a scope tag to the policy.
- Import an ADMX file.
- Create a configuration profile.
- Configure the Administrative Templates settings.
- Assign the profile.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- Assign the policy.
- Create a compliance policy.
- Set a scope tag to the policy.
- Import an ADMX file.
- Create a configuration profile.
- Configure the Administrative Templates settings.
- Assign the profile.

Answer Area

- Create a configuration profile.
- Configure the Administrative Templates settings.
- Assign the profile.

NEW QUESTION 4

- (Exam Topic 4)

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.

Actions

Answer Area

- Obtain the root certificate.
- From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.
- From the Enterprise CA, configure certificate managers.
- From the Microsoft Endpoint Manager admin center, configure enrollment restrictions.
- From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, email Description automatically generated

Reference:

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

NEW QUESTION 5

- (Exam Topic 4)

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 6

- (Exam Topic 4)

You have the devices shown in the following table.

Name	Operating system	Description
Device1	32-bit version of Windows 10	Retired device
Device2	64-bit version of Windows 11	New device
Server1	Windows Server 2019	File server

You need to migrate app data from Device1 to Device2. The data must be encrypted and stored on Seryer1 during the migration.

Which command should you run on each device? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

```

Device1:
LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Device2:
LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"
    
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

```

Device1:
LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Device2:
LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"
    
```

NEW QUESTION 7

- (Exam Topic 4)

You have an Azure AD group named Group1. Group1 contains two Windows 10 Enterprise devices named Device1 and Device2. You create a device configuration profile named Profile1. You assign Profile1 to Group1. You need to ensure that Profile1 applies to Device1 only. What should you modify in Profile1?

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

Answer: 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 8

- (Exam Topic 4)

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you configure the Windows Hello for Business enrollment options.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 9

- (Exam Topic 4)

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

NEW QUESTION 10

- (Exam Topic 4)

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	Answer Area
Review the compliance dashboard for results.	1
Create and assign a compliance policy that has System Security settings configured.	2
Review the Conditional Access Insights and Reporting workbook for results.	3
Create a PowerShell discovery script and a JSON file.	4
Upload the PowerShell script to Intune.	
Upload the JSON file to Azure AD.	
Create and assign a custom compliance policy.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
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 10

- (Exam Topic 4)

You have following types of devices enrolled in Microsoft Intune:

- Windows 10
- Android
- iOS

For which types of devices can you create VPN profiles in Microsoft Intune admin center?

- A. Windows 10 only
- B. Windows 10 and Android only
- C. Windows 10 and iOS only
- D. Android and iOS only
- E. Windows 10, Android, and iOS

Answer: E

NEW QUESTION 12

- (Exam Topic 4)

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 Windows 10 update ring
- C. a device configuration profile

D. an app protection policy

Answer: C

NEW QUESTION 15

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains two users named User1 and User2. You need to ensure that the users can perform the following tasks:

- User1 must be able to create groups and manage users.
- User2 must be able to reset passwords for non-administrative users. The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Microsoft 365 or Office 365 subscription comes with a set of admin roles that you can assign to users in your organization using the Microsoft 365 admin center. Each admin role maps to common business functions and gives people in your organization permissions to do specific tasks in the admin centers. To ensure that User1 can create groups and manage users, you should assign the User Administrator role to User1. This role allows User1 to create and manage all aspects of users and groups, including resetting passwords for non-administrative users. To ensure that User2 can reset passwords for non-administrative users, you should assign the Helpdesk Administrator role to User2. This role allows User2 to reset passwords, manage service requests, and monitor service health for non-administrative users.

NEW QUESTION 20

- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune. You need to configure an Intune device configuration profile to meet the following requirements:

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Create Profile

***Name**

MD101

Description

Enter a description

***Platform**

Windows 10 and later

***Profile type**

Endpoint protection

Settings >

Configure >

Scope (Tags)
0 scope(s) selected >

Endpoint protection

Windows 10 and later

Select a category to configure settings

Windows Defender Application Gu...
11 settings available >

Windows Defender Firewall
40 settings available >

Windows Defender SmartScreen
2 settings available >

Windows Encryption
37 settings available >

Windows Defender Exploit Guard
20 settings available >

Windows Defender Application Co...
2 settings available >

Windows Defender Application Gua...
1 setting available >

Windows Defender Security Center
14 settings available >

Local device security options
46 settings available >

Xbox services
5 settings available >

OK

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated

References:

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

NEW QUESTION 23

- (Exam Topic 4)

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

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

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

Computer1 has apps that are compatible with Windows 10.

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

Solution: You 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 26

- (Exam Topic 4)

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

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system 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:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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:

NEW QUESTION 28

- (Exam Topic 4)

You have a Microsoft Intune deployment that contains the resources shown in the following table.

Name	Type	Platform
Comply1	Device compliance policy	Windows 10 and later
Comply2	Device compliance policy	iOS/iPadOS
CA1	Conditional Access policy	Not applicable
Conf1	Device configuration profile	Windows 10 and later
Office1	Office app policy	Not applicable

You create a policy set named Set1 and add Comply1 to Set1. Which additional resources can you add to Set1?

- A. Conf1 only
- B. Comply2 only
- C. Comply2 and Conf1 only
- D. CA1, Conf1, and Office 1 only
- E. Comply2, CA1, Conf1, and Office1

Answer: B

NEW QUESTION 32

- (Exam Topic 4)

You have a Microsoft Intune subscription.

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

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

An app named App1 is installed on each device.

What is the minimum number of app configuration policies required to manage App1?

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

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 devices. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices. 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 33

- (Exam Topic 3)

You need to meet the technical requirements for the LEG department computers.

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

Actions

Answer Area

- Configure the commercial ID on the LEG department computers.
- Create an Azure Machine Learning service workspace.
- Create an Azure Log Analytics workspace.
- Install the Microsoft Monitoring Agent on the LEG department computers.
- Add a solution to a workspace.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a white box Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-azure-portal>

NEW QUESTION 34

- (Exam Topic 3)

You need to meet the requirements for the MKG department users. What should you do?

- A. Assign the MKG department users the Purchaser role in Microsoft Store for Business
- B. Download the APPX file for App1 from Microsoft Store for Business
- C. Add App1 to the private store
- D. Assign the MKG department users the Basic Purchaser role in Microsoft Store for Business
- E. Acquire App1 from Microsoft Store for Business

Answer: E

Explanation:

References:

<https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store> Enable the users in the MKG department to use App1.

The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. When admins add apps to the private store, all employees in the organization can view and download the apps. Your private store is available as a tab in Microsoft Store app, and is usually named for your company or organization. Only apps with online licenses can be added to the private store.

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store>

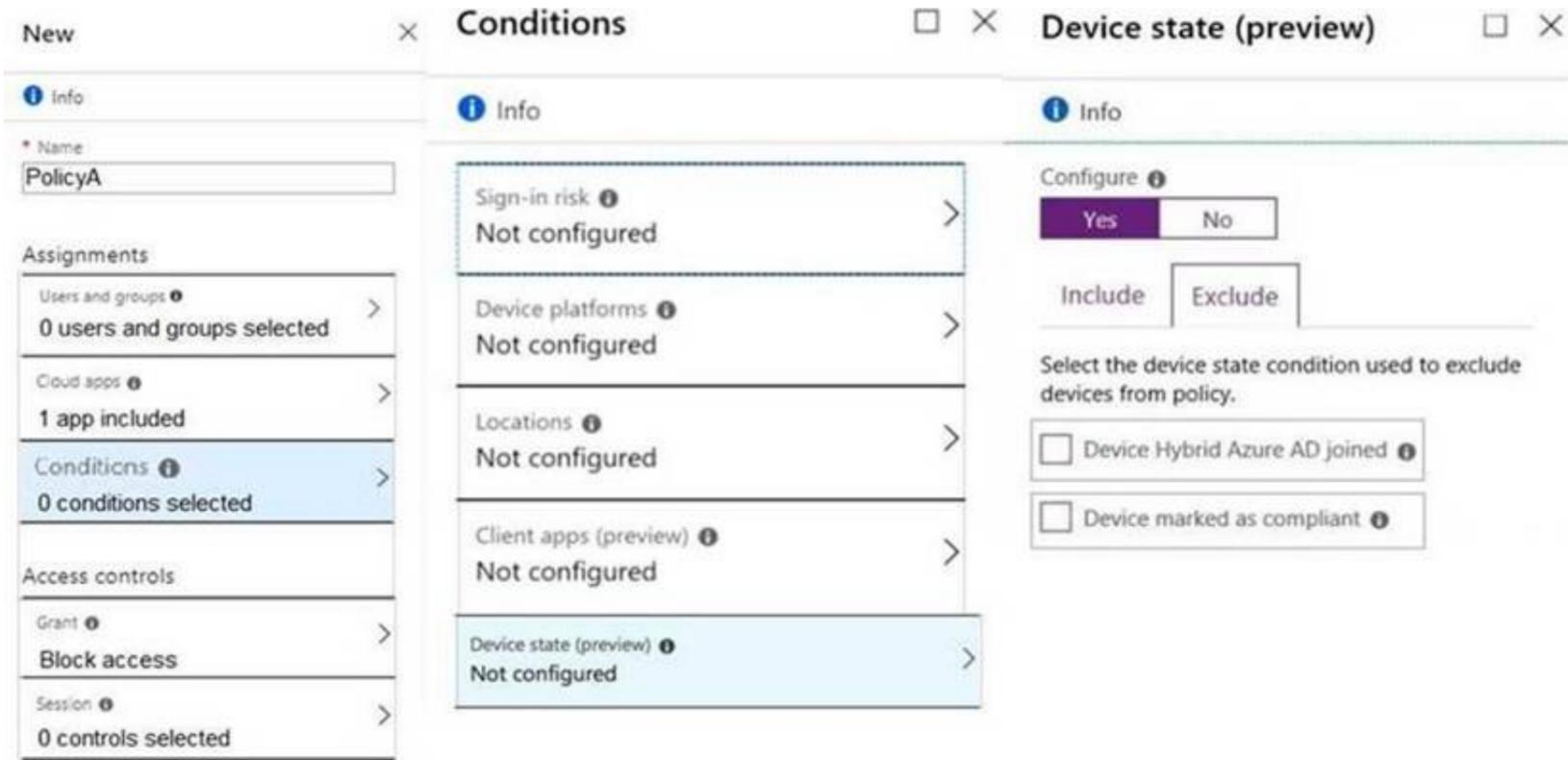
NEW QUESTION 38

- (Exam Topic 3)

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

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

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

A screenshot of a computer Description automatically generated

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

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

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

References:

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

NEW QUESTION 41

- (Exam Topic 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:

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

User2 can enroll a maximum of:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1 can enroll a maximum of:

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

User2 can enroll a maximum of:

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

NEW QUESTION 42

- (Exam Topic 3)

You need to meet the technical requirements for the new HR department computers.

How should you configure the provisioning package? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Specify ComputerName as:

"HR"+ RAND(4)
"HumanResources-" + RAND(????)
HR-%RAND:4%
HR-????
HumanResources-%RAND:4%

Specify AccountOU as:

CN=Computers, CN=HR, DC=Contoso, DC=com
Computers/HumanResources/Contoso.com
Contoso.com/HR/Computers
OU=Computers, OU=HR, DC=Contoso, DC=com

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-accounts>

NEW QUESTION 45

- (Exam Topic 2)

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: A

Explanation:

References:

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

NEW QUESTION 48

- (Exam Topic 2)

What should you upgrade before you can configure the environment to support co-management?

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

Answer: B

Explanation:

References:

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

NEW QUESTION 50

- (Exam Topic 2)

You need to recommend a solution to meet the device management requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

For the Research department employees:

<input type="checkbox"/>	An app configuration policy
<input type="checkbox"/>	An app protection policy
<input type="checkbox"/>	Azure information Protection
<input type="checkbox"/>	iOS app provisioning profiles

For the Sales department employees:

<input type="checkbox"/>	An app configuration policy
<input type="checkbox"/>	An app protection policy
<input type="checkbox"/>	Azure information Protection
<input type="checkbox"/>	iOS app provisioning profiles

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://github.com/MicrosoftDocs/IntuneDocs/blob/master/intune/app-protection-policy.md>

<https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#do-not-forward-option-fo>

NEW QUESTION 53

- (Exam Topic 2)

What should you use to meet the technical requirements for Azure DevOps?

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

Answer: C

Explanation:

References:

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

NEW QUESTION 55

- (Exam Topic 1)

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

NOTE: Each correct selection is worth one point.

Statements

Yes No

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

<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------

User2 can remove D:\Folder1 from the list of protected folders on Device2.

<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------

User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.

<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated with medium confidence

NEW QUESTION 57

- (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 60

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.

You need to configure the devices to run a single app in kiosk mode.

Which Configuration settings should you modify in the device restrictions profile?

- A. General
- B. Users and Accounts
- C. System security
- D. Device experience

Answer: D

Explanation:

To configure the devices to run a single app in kiosk mode, you need to modify the Device experience settings in the device restrictions profile. You can specify the app package name and activity name for the app that you want to run in kiosk mode. References:

<https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work#device-experie>

NEW QUESTION 61

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You have a Windows 11 device named Device1 that is enrolled in Intune. Device1 has been offline for 30 days.

You need to remove Device1 from Intune immediately. The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and OEM-installed apps must be retained.

What should you use?

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

Answer: B

Explanation:

A retire action removes a device from Intune management and removes any apps and data provisioned by Intune. User-installed apps, personal data, and OEM-installed apps are retained. A retire action can be performed on devices that are offline for more than 30 days. References:

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

NEW QUESTION 65

- (Exam Topic 4)

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 70

- (Exam Topic 4)
 You have a Microsoft 365 E5 subscription.
 You create an app protection policy for Android devices named Policy1 as shown in the following exhibit.

Home > Apps >

Create policy ×

- ✔ Basics
- 2 Apps
- 1 Data protection
- 4 Access requirements
- ⋮

Choose how you want to apply this policy to apps on different devices. Then add at least one app.

Target to apps on all device types ⓘ Yes No

Device types * ⓘ Unmanaged ▼

Target policy to All Apps ▼

i We'll continue to add managed apps to your policy as they become available in Intune. [View a list of apps that will be targeted](#)

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.

To apply Policy1 to an Android device, you must **[answer choice]**.

[answer choice]
install the Company Portal app on the device
install the Microsoft Authenticator app on the device
onboard the device to Microsoft Defender for Endpoint
onboard the device to the Microsoft 365 compliance center

When Policy1 is assigned, the policy will apply to **[answer choice]**.

[answer choice]
users only
devices only
users and devices

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Install the Intune Company Portal app on the device
 On Android, Android devices will prompt to install the Intune Company Portal app regardless of which Device type is chosen.
 Box 2: Devices only
 For Android devices, unmanaged devices are devices where Intune MDM management has not been detected. This includes devices managed by third-party MDM vendors.
 Reference:
<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#app-protection-policies-for-iosipado>

NEW QUESTION 74

- (Exam Topic 4)
 You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1@contoso.com	Security Administrator
Admin2@contoso.com	Cloud Device Administrator
User1@contoso.com	None

You have a computer named Computer1 that runs Windows 10. Computer1 is in a workgroup and has the local users shown in the following table.

Name	Member of
Administrator1	Network Configuration Operators
Administrator2	Power Users
UserA	Administrators

UserA joins Computer1 to Azure AD by using user1@contoso.com.

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@contoso.com is a member of the local Administrators group on Computer1.	<input type="radio"/>	<input type="radio"/>
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	<input type="radio"/>	<input type="radio"/>
Admin2@contoso.com can install software on Computer1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2@contoso.com can install software on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 76

- (Exam Topic 4)

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

Feature update deferral period (days): 90

Quality update deferral period (days): 14

Grace period: 3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Feature update deferral period (days): 90

Quality update deferral period (days): 14

Grace period: 3

NEW QUESTION 77

- (Exam Topic 4)

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. Standard Client Task Sequence
- B. Standard Client Replace Task Sequence
- C. Litetouch OEM Task Sequence
- D. Sysprep and Capture

Answer: B

NEW QUESTION 81

- (Exam Topic 4)

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

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

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

What should you configure?

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

Answer: A

Explanation:

User sign-in frequency

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

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

Sign-in frequency control

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

Select Sign-in frequency.

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

- > Save your policy. Reference:

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

NEW QUESTION 83

- (Exam Topic 4)

You use a Microsoft Intune subscription to manage iOS devices.

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

What should you configure?

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

Answer: D

NEW QUESTION 88

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You need to review the startup times and restart frequencies of the devices. What should you use?

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

Answer: D

Explanation:

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

NEW QUESTION 89

- (Exam Topic 4)

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

Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8.1 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.

Save Discard

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

Mark devices with no compliance policy assigned as Compliant Not Compliant

Enhanced jailbreak detection Enabled Disabled

Compliance status validity period (days) ✓

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

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO. Then the third device has 2 policies, the first one is compliant and the second policy is not compliant but the device is not marked as non-compliant due to the fact that mark device as non-compliant is set to 10 days. This means that the machine will be compliant until June 10th.

Source:

Mark device non-compliant: By default, this action is set for each compliance policy and has a schedule of zero (0) days, marking devices as noncompliant immediately.

When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant.

This action is supported on all platforms supported by Intune. <https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance>

NEW QUESTION 94

- (Exam Topic 4)

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 Area

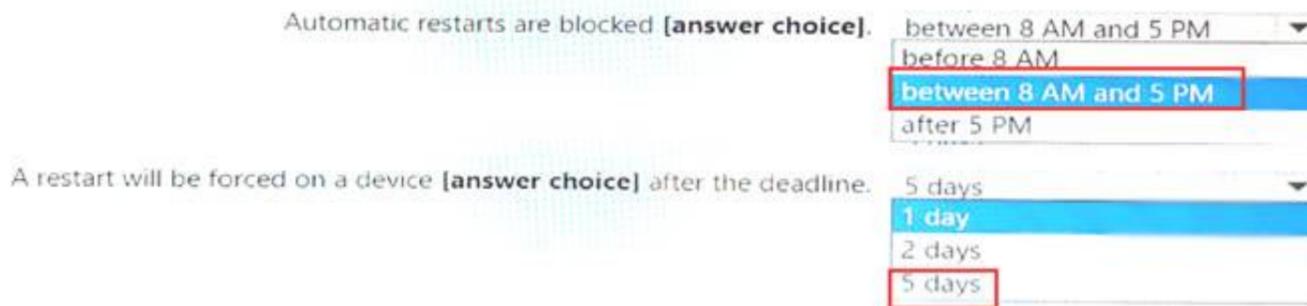
Automatic restarts are blocked [answer choice].

A restart will be forced on a device [answer choice] after the deadline.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Answer Area

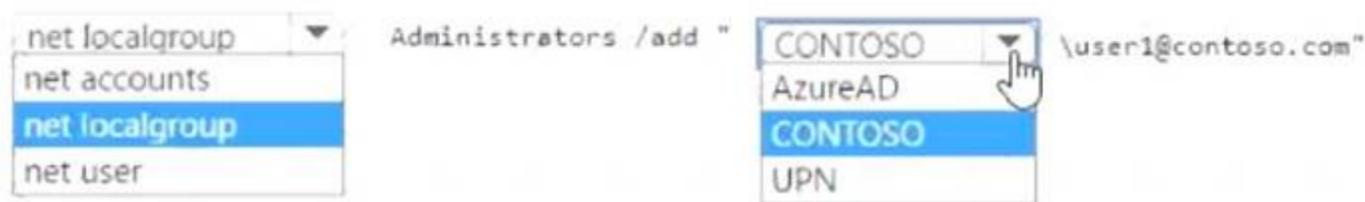


NEW QUESTION 98

- (Exam Topic 4)

You have an 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 11 device named Client 1 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 Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

net localgroup Administrators /add "AzureAD\user1@contoso.com"

This command will add the Azure AD user with the UPN of user1@contoso.com to the local Administrators group of the device1. You need to use the AzureAD prefix and double backslashes to specify the user's domain2. You also need to enclose the user's name in quotation marks if it contains special characters like @1.

You can run this command from an elevated command prompt on Client1, or remotely by using PowerShell or other tools1. You can also use the Intune Role Administrator role or the Additional local administrators on all Azure AD joined devices setting to manage the local administrators group on Azure AD joined devices34.

NEW QUESTION 99

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. Auto-enrollment in Intune is configured.

You have 100 Windows 11 devices in a workgroup.

You need to connect the devices to the corporate wireless network and enroll 100 new Windows devices in Intune.

What should you use?

- A. a provisioning package
- B. a Group Policy Object (GPO)
- C. mobile device management (MDM) automatic enrollment
- D. a device configuration policy

Answer: C

NEW QUESTION 102

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

You create a new update rings policy named Policy1 as shown in the following exhibit.

Update ring settings [Edit](#)

Update settings

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

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

Answer Area

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

*Updates that contain new Windows functionality will be installed within 60 days of release.

This is because the update rings policy named Policy1 has the “Feature updates deferral period (days)” setting set to 60. This means that feature updates, which include new Windows functionality, can be deferred for up to 60 days from the date they are released by Microsoft. After 60 days, the devices will automatically install the feature updates. References:

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

NEW QUESTION 106

- (Exam Topic 4)

You have a Microsoft 365 ES subscription that uses Microsoft Intune. You have the apps shown in the following exhibit.

Apps | All apps

Search (Ctrl+/)

+ Add Refresh Filter Export Columns

- Overview
- All apps
- Monitor
- By platform
 - Windows
 - iOS/iPadOS
 - macOS
 - Android
- Policy
 - App protection policies
 - App configuration policies

Name	Type	Assigned
App1	Android line-of-business app	Yes
App2	iOS line-of-business app	Yes
App3	iOS line-of-business app	No
Excel	Android store app	Yes
Excel	iOS store app	Yes
Managed Home Screen	Managed Google Play store app	Yes
Microsoft Authenticator	Managed Google Play store app	No
OneDrive	Android store app	No
OneDrive	iOS store app	No

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.

You can create configuration policies for [answer choice] iOS-supported apps.

- 1
- 2
- 3
- 4
- 5

You can create configuration policies for [answer choice] Android-supported apps.

- 1
- 2
- 3
- 4
- 5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

You can create configuration policies for [answer choice] iOS-supported apps.

- 1
- 2
- 3
- 4
- 5

You can create configuration policies for [answer choice] Android-supported apps.

- 1
- 2
- 3
- 4
- 5

NEW QUESTION 111

- (Exam Topic 4)

You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a compliance policy that meets the following requirements:

- Requires BitLocker Drive Encryption (BitLocker) on each device
- Requires a minimum operating system version

Which setting of the compliance policy 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,

Settings

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Answer Area

Requires BitLocker:

Requires a minimum operating system version:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Settings

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Answer Area

Requires BitLocker: System Security

Requires a minimum operating system version: Device Properties

NEW QUESTION 112

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD. A user named User1 uses the domain-joined devices shown in the following table.

Name	Operating system
Device1	Windows 10 Pro
Device2	Windows 11 Pro

In the Microsoft Entra admin center, you assign a Windows 11 Enterprise E5 license to User1. You need to identify what will occur when User1 next signs in to the devices.

What should you identify for each device? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Device1: Will activate as Windows 11 Enterprise

Device2: Will not upgrade to Windows 11 Enterprise

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Device 1:

> Will activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windows 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 1 has Windows 11 Pro, so it meets the requirement. When User1 signs in to Device 1 with their Azure AD account, the device will automatically activate as Windows 11 Enterprise without changing the edition.

> Will not activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windows 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 2 has Windows 10 Home, so it does not meet the requirement. When User1 signs in to Device 2 with their Azure AD account, the device will not activate as Windows 11 Enterprise by subscription.

NEW QUESTION 115

- (Exam Topic 4)

You use the Microsoft Deployment Toolkit (MDT) to manage Windows 11 deployments. From Deployment Workbench, you modify the WinPE settings and add PowerShell support. You need to generate a new set of WinPE boot image files that contain the updated settings. What should you do?

- A. From the Deployment Shares node, update the deployment share.
- B. From the Advanced Configuration node, create new media.
- C. From the Packages node, import a new operating system package
- D. From the Operating Systems node, import a new operating system.

Answer: A

NEW QUESTION 116

- (Exam Topic 4)

Your company has a computer named Computer1 that runs Windows 10. Computer1 was used by a user who left the company.

You plan to repurpose Computer1 and assign the computer to a new user. You need to redeploy Computer1 by using Windows Autopilot.

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

Actions

- Upload the file by using Microsoft Intune.
- Generate a CSV file that contains the computer information.
- Reset the computer.
- Generate a JSON file that contains the computer information.
- Upload the file by running azcopy.exe.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To redeploy Computer1 by using Windows Autopilot, you need to perform the following three actions in sequence:

- > Generate a JSON file that contains the computer information. This file specifies the Autopilot profile to be applied during the deployment. You can use the Get-AutopilotProfilesForExistingDevices PowerShell script to generate this file1.
- > Reset the computer. You can use the Windows Automatic Redeployment feature to trigger a reset from the login screen by pressing Ctrl + R and providing an administrator account2. Alternatively, you can use the Windows Autopilot Reset feature to remotely reset the device from Intune1.
- > Upload the file by running azcopy.exe. This step copies the JSON file to a blob storage account in Azure, where it can be accessed by the device during the deployment. You need to specify the storage account name, access key, and container name as parameters for azcopy.exe1.

NEW QUESTION 118

- (Exam Topic 4)

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

Name	Member of
User1	Group1
User2	Group2

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

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

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

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

NOTE: Each correct selection is worth one point.

Statements

Yes No

User1 receives Notification1 on Device1.

Yes No

User2 receives Notification1 on Device2.

Yes No

User1 receives Notification1 on Device3.

Yes No

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated with medium confidence

Reference:

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

NEW QUESTION 122

- (Exam Topic 4)

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 Intune admin center, you select Uninstall for the feature updates of UpdateRing1. When will devices start to remove the feature updates?

- A. when a user approves the uninstall
- B. as soon as the policy is received
- C. next Tuesday
- D. the first Tuesday of the next month

Answer: C

NEW QUESTION 123

- (Exam Topic 4)

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

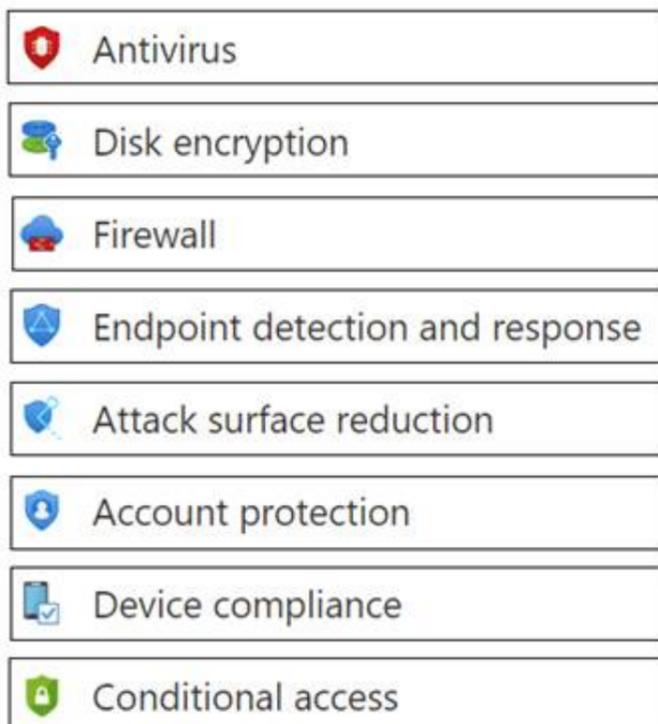
- > Hide the Firewall & network protection area in the Windows Security app.
- > Disable the provisioning of Windows Hello for Business on the devices.

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

NOTE: Each correct selection is worth one point.

Answer Area

Manage



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

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

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

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

NEW QUESTION 127

- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to set a custom image as the wallpaper and sign-in screen.

Which two settings should you configure in the Device restrictions configuration profile? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Device restrictions

Windows 10 and later

- ✓ Basics
- 2 Configuration settings**
- 3 Assignments
- 4 Applicability Rules
- 5 Review + create

- App Store
- Cellular and connectivity
- Cloud and Storage
- Cloud Printer
- Control Panel and Settings
- Display
- General
- Locked Screen Experience ✓**
- Messaging
- Microsoft Edge Browser
- Network proxy
- Password
- Per-app privacy exceptions
- Personalization ✓**
- Printer
- Privacy
- Projection

Previous

Next

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Device restrictions

Windows 10 and later

Basics
 2 Configuration settings
 3 Assignments
 4 Applicability Rules
 5 Review + create

- App Store
- Cellular and connectivity
- Cloud and Storage
- Cloud Printer
- Control Panel and Settings
- Display
- General
- Locked Screen Experience** ✓
- Messaging
- Microsoft Edge Browser
- Network proxy
- Password
- Per-app privacy exceptions
- Personalization** ✓
- Printer
- Privacy
- Projection

NEW QUESTION 130

- (Exam Topic 4)

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

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No.

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

Box 2: No

For the same reason as Box1. Box 3: Yes

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

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

NEW QUESTION 134

- (Exam Topic 4)

Your network contains an Active Directory domain. The domain contains a computer named Computer1 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. Connect-WSMan
- B. Enable-PSRemoting
- C. Invoke-WSManAction
- D. Enable-PSSessionConfiguration

Answer: B

NEW QUESTION 135

- (Exam Topic 4)

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

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

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

Answer: A

NEW QUESTION 140

- (Exam Topic 4)

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

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

Which tool should you use?

- A. Microsoft Defender for Endpoint Power 81 app
- B. Microsoft Secure Score
- C. Endpoint Analytics
- D. Microsoft 365 Defender portal

Answer: B

NEW QUESTION 144

- (Exam Topic 4)

Your company standardizes on Windows 10 Enterprise for all users.

Some users purchase their own computer from a retail store. The computers run Windows 10 Pro.

You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Azure AD, and install several Microsoft Store apps.

The solution must meet the following

requirements:

- Ensure that any applications installed by the users are retained.
- Minimize user intervention.

What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

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

Answer: A

NEW QUESTION 148

- (Exam Topic 4)

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

Answer Area

Marketing:

Research:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Marketing:

Research:

NEW QUESTION 149

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MD-102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MD-102 Product From:

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

Money Back Guarantee

MD-102 Practice Exam Features:

- * MD-102 Questions and Answers Updated Frequently
- * MD-102 Practice Questions Verified by Expert Senior Certified Staff
- * MD-102 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * MD-102 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year