Free Questions for MD-102

Shared by Craft on 30-05-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: Hotspot

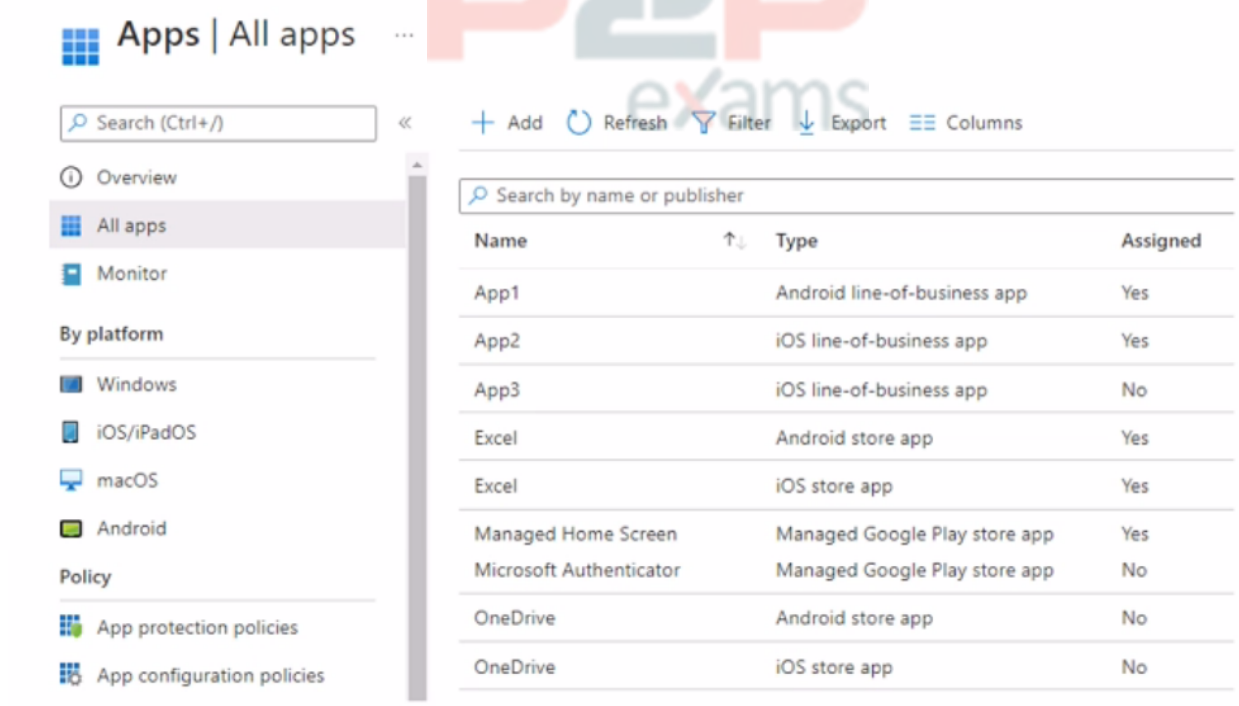
Case Study: Mix Questions

Mix Questions

MD-102 Mix Questions IN THIS CASE STUDY

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

You have the apps shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

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

Answer:

See the Answer in the Premium Version!

Question 2

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

MD-102 Mix Questions IN THIS CASE STUDY

Your network contains an on-premises Active Directory domain. The domain contains two computers named Computer1 and Computer? that run Windows 10.

You install Windows Admin Center on Computer1.

You need to manage Computer2 from Computer1 by using Windows Admin Center.

What should you do on Computed?

Options:

A- Update the TrustedHosts list
B- Run the Enable-PSRemoting cmdlet
C- Allow Windows Remote Management (WinRM) through the Microsoft Defender firewall.
D- Add an inbound Microsoft Defender Firewall rule.

Answer:

B

Explanation:

To manage a remote computer from Windows Admin Center, you need to enable PowerShell remoting on the remote computer. You can do this by running the Enable-PSRemoting cmdlet, which configures the WinRM service, creates a listener, and allows inbound firewall rules for PowerShell remoting. The other options are not sufficient or necessary for this task.Reference:Installation and configuration for Windows Remote Management

Question 3

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

MD-102 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune. You need to prevent the printing of corporate data from managed apps on the devices, should you configure?

Options:

A- an app configuration policy
B- a security baseline
C- an app protection policy
D- an iOS app provisioning profile

Answer:

C

Explanation:

An app protection policy is a set of rules that controls how data is accessed and handled by managed apps on mobile devices. App protection policies can prevent the printing of corporate data from managed apps on iOS devices by using theRestrict cut, copy, and paste with other appssetting. This setting can be configured to block printing from the iOS share menu. An app configuration policy is used to customize the behavior of a managed app, such as specifying a VPN profile or a web link. A security baseline is a collection of recommended security settings for Windows 10 devices that are managed by Intune.An iOS app provisioning profile is a file that contains information about the app's identity, entitlements, and distribution method

Question 4

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

MD-102 Mix Questions IN THIS CASE STUDY

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

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

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

NOTE: Each correct selection is worth one point.

Options:

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

Answer:

A, E

Question 5

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

MD-102 Mix Questions IN THIS CASE STUDY

-

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

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

All the devices will be reimaged and licensed by using subscription activation.

The devices are assigned to the users shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

See the Answer in the Premium Version!

Question 6

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

MD-102 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 subscription.

You plan to enable Microsoft Intune enrollment for the following types of devices:

* Existing Windows 11 devices managed by using Configuration Manager

* Personal iOS devices

The solution must minimize user disruption.

Which enrollment method should you use for each device type? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

See the Answer in the Premium Version!

Question 7

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

MD-102 Mix Questions IN THIS CASE STUDY

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

Name	Platform	Encryption	Secure Boot	Member of
Device1	Windows 10	Yes	No	Group1
Device2	Windows 10	No	Yes	Group2
Device3	Android	No	*Not applicable*	Group3

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

Name	Platform	Encryption	Secure Boot
Policy1	Windows 10	Not configured	Not configured
Policy2	Windows 10	Not configured	Required
Policy3	Windows 10	Required	Required
Policy4	Android	Not configured	*Not applicable*

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group1
Policy2	Group1, Group2
Policy3	Group3
Policy4	Group3

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

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	○	○
Device2 is marked as compliant.	○	○
Device3 is marked as compliant.	○	○

Answer:

See the Answer in the Premium Version!

Question 8

Question Type: Hotspot

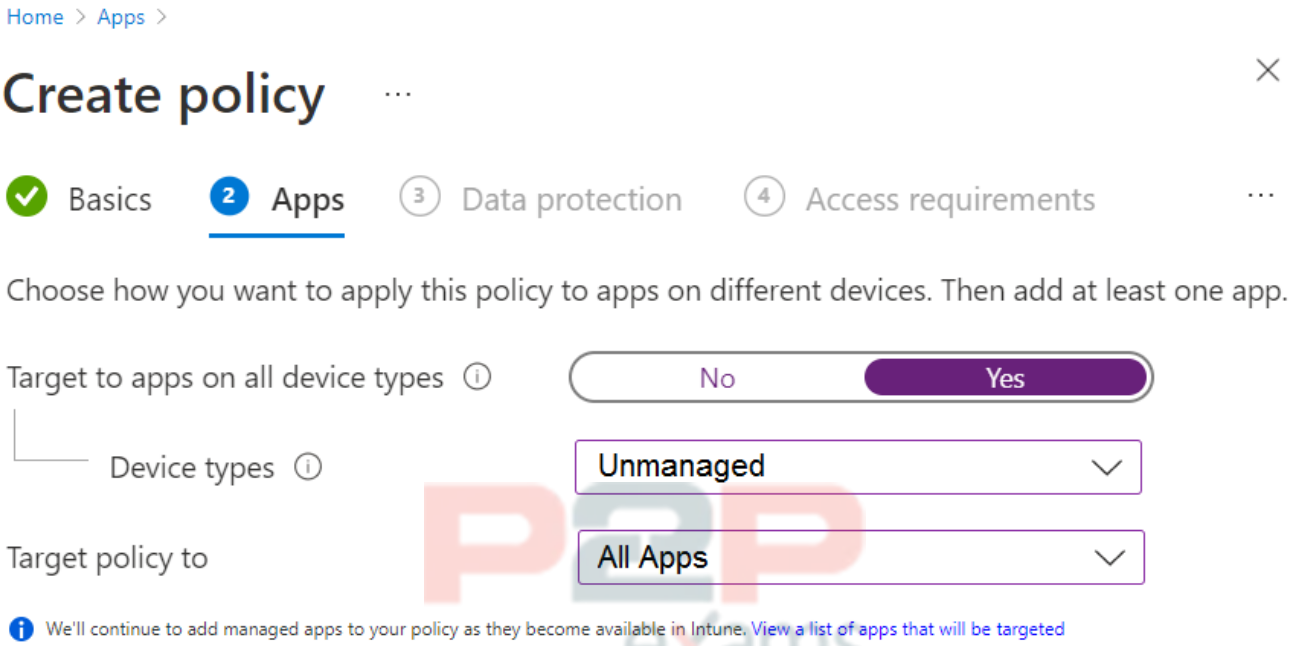
Case Study: Mix Questions

Mix Questions

MD-102 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 E5 subscription.

You create an app protection policy for Android device named Policy1 as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Answer Area

To apply Policy1 to an Android device, you must
- 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 Purview compliance portal

When Policy1 is assigned, the policy will apply to
- users only
- devices only
- users and devices

Answer:

See the Answer in the Premium Version!

Question 9

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

MD-102 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 subscription that contains two security groups named Group1 and Group2. Microsoft 365 uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to assign roles in Intune to meet the following requirements:

* The members of Group1 must manage Intune roles and assignments.

* The members of Group2 must assign existing apps and policies to users and devices.

The solution must follow the principle of least privilege.

Which role should you assign to each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

See the Answer in the Premium Version!

Question 10

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

MD-102 Mix Questions IN THIS CASE STUDY

You have an Azure AD tenant named contoso.com.

You need to ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com.

What should you configure?

Options:

A- Windows Autopilot
B- provisioning packages for Windows
C- Security defaults in Azure AD
D- Device settings in Azure AD

Answer:

D

Explanation:

To ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com, you should configure the Device settings in Azure AD. The Device settings allow you to manage which users can join devices to Azure AD and whether they are added as local administrators or standard users.By default, users who join devices to Azure AD are added to the local Administrators group, but you can change this setting to None or Selected1.

The other options are not relevant for this scenario because:

Windows Autopilot is a service that allows you to pre-configure new devices and enroll them automatically to Azure AD and Microsoft Intune.It does not control the local administrator role of the users who join the devices2.

Provisioning packages for Windows are files that contain custom settings and policies that can be applied to Windows devices during the setup process.They do not affect the Azure AD join process or the local administrator role of the users3.

Security defaults in Azure AD are a set of basic identity security mechanisms that are enabled by default to protect your organization from common attacks.They do not include any settings related to device management or local administrator role4.