MD-102 Q&As

Endpoint Administrator

Pass Microsoft MD-102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/md-102.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You have a Microsoft 365 E5 subscription that contains a user named User1 and a web app named App1.

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 App1.

Which condition should you add to CAPolicy1?

A. Filter for devices

B. Device platforms

C. User risk

D. Sign-in risk

E. Client apps

Correct Answer: E

Create a Conditional Access policy (see step 7 below).

The following steps will help create a Conditional Access policy to block legacy authentication requests. This policy is put in to Report-only mode to start so administrators can determine the impact they\\'ll have on existing users. When

administrators are comfortable that the policy applies as they intend, they can switch to On or stage the deployment by adding specific groups and excluding others.

Sign in to the Azure portal as a Conditional Access Administrator, Security Administrator, or Global 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.

Under Assignments, select Users or workload identities.

Under Include, select All users.

Under Exclude, select Users and groups and choose any accounts that must maintain the ability to use legacy authentication. Exclude at least one account to prevent yourself from being locked out. If you don\\'t exclude any

account, you won\\'t

be able to create this policy.

6.

Under Cloud apps or actions, select All cloud apps.

7.

Under Conditions > Client apps, set Configure to Yes.

Check only the boxes Exchange ActiveSync clients and Other clients.

Select Done.

8.

Under Access controls > Grant, select Block access.

Select Select.

9.

Confirm your settings and set Enable policy to Report-only.

10.

Select Create to create to enable your policy.

After confirming your settings using report-only mode, an administrator can move the Enable policy toggle from Report-only to On.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-block-legacy

QUESTION 2

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

1.

Ensure that you can manage the personal devices by using Microsoft Intune.

2.

Ensure that users can access company data seamlessly from their personal devices.

3.

Ensure that users can only sign in to their personal devices by using their personal account. What should you use to add the devices to Azure AD?

A. Azure AD registered

B. hybrid Azure AD join

C. Azure AD joined

Correct Answer: A

Azure AD registered devices are personal devices that are associated with Azure AD. This allows users to access company data from their personal devices without having to join the devices to the company\\'s domain. Additionally, Azure AD registered devices can be managed by Microsoft Intune.

QUESTION 3

You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You have a device named Devic1 that is enrolled in Intune.

You need to ensure that User1 can use Remote Help from the Intune admin center for Device1.

Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Deploy the Remote Help app to Device1.

B. Assign the Help Desk Operator role to User1.

C. Assign the Intune Administrator role to User1.

D. Assign a Microsoft 365 E5 license to User1.

E. Rerun device onboarding on Device1.

F. Assign the Remote Help add-on license to User1.

Correct Answer: ABF

QUESTION 4

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have 500 corporate-owned Android devices enrolled as fully managed devices.

You need to prepare an app named App1 for deployment to the devices.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the Intune Company Portal, download App1.

B. Sync App1 with Intune.

C. From the Managed Google Play Store, approve App1.

D. Create an OEMConfig profile.

Correct Answer: BC

C: Add a Managed Google Play store app in the Managed Google Play console (Alternative)

If you prefer to synchronize a Managed Google Play app with Intune rather than adding it directly using Intune, use the following steps.

1.

Go to the Managed Google Play store. Sign in with the same account you used to configure the connection between Intune and Android Enterprise.

2.

Search the store and select the app you want to assign by using Intune.

3.

On the page that displays the app, click Approve.

In the following example, the Microsoft Excel app has been chosen.

A window for the app opens asking you to give permissions for the app to perform various operations.

4.

Select Approve to accept the app permissions and continue.

5.

Select an option for handling new app permission requests, and then select Save.

(B) The app is approved, and it is displayed in your IT admin console. Next, you can Sync a Managed Google Play app with Intune.

Reference:

https://learn.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work

QUESTION 5

You have a Microsoft 365 tenant that uses Microsoft Intune.

You use the Company Portal app to access and install published apps to enrolled devices.

From the Microsoft Intune admin center, you add a Microsoft Store app.

Which two App information types are visible in the Company Portal?

NOTE: Each correct selection is worth one point.

A. Privacy URL

B. Information URL

C. Developer

D. Owner

Correct Answer: AB

In the Microsoft Store App information page available through Microsoft Endpoint Manager admin center, the app details include:

*

Privacy URL: Optionally, enter the URL of a website that contains privacy information for this app. The URL is displayed to users in the company portal.

*

Developer: Optionally, enter the name of the app developer.

Information URL or Owner are not included.

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/store-apps-windows