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.geekcert.com/md-102.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

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 have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You use Windows Autopilot to deploy Windows 11 to devices.

A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device.

You need to ensure that when a deployment fails, the deployment logs can be collected.

What should you configure?

A. the automatic enrollment settings

B. the Windows Autopilot deployment profile

C. the enrollment status page (ESP) profile

D. the device configuration profile

Correct Answer: C

Troubleshooting the Enrollment Status Page

To troubleshoot ESP issues, it\\'s important to get more information about the ESP settings that are received by the device, and the applications and policies that are tracked at each stage. All ESP settings and tracking information are logged in

the device registry.

Collect logs

You can enable the ability for users to collect ESP logs in the ESP policy. When a timeout occurs in the ESP, the user can select the option to Collect logs.

Note: Windows Autopilot diagnostics page

On Windows 11, you can open the Autopilot diagnostic page to view additional detailed troubleshooting information about the Autopilot provisioning process. To enable the Autopilot diagnostics page:

Go to the ESP profile where the Autopilot diagnostics page needs to be enabled.

Make sure that Show app and profile configuration progress is selected to Yes.

Make sure that Turn on log collection and diagnostics page for end users is selected to Yes.

Reference:

https://learn.microsoft.com/en-us/troubleshoot/mem/intune/device-enrollment/understand-troubleshoot-esp

QUESTION 3

You have an Azure AD tenant named contoso.com.

You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.

Name	Memory	TPM
Device1	16 GB	*None*
Device2	8 GB	Version 1.2
Device3	4 GB	Version 2.0

Which devices can be configured by using Windows Autopilot self-deploying mode?

A. Device2 only

B. Device3 only

C. Device1 and Device3 only

D. Device1, Device2, and Device3

Correct Answer: B

Self-deploying mode uses a device\\'s TPM 2.0 hardware to authenticate the device into an organization\\'s Azure AD tenant. Therefore, devices without TPM 2.0 can\\'t be used with this mode.

Reference: https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/self-deploying

QUESTION 4

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 Intune admin center?

A. Premium add-ons

B. Connectors and tokens

C. Tenant enrollment

D. Microsoft Tunnel Gateway

Correct Answer: C

https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

QUESTION 5

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

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

You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings.

What should you do?

A. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy.

B. From the Microsoft Intune admin center, create a custom device profile.

C. From the Microsoft Intune admin center, create an Administrative Templates device profile.

D. From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy.

Correct Answer: B

Creating the policy Let\\'s create a new policy in Intune to control the GP vs. MDM winner 1) Navigate to portal.azure.com and locate Intune 2) Select “Device configuration à Profiles à Create profile” 3) Under Platform select

Windows 10 and later 4) Under Profile type select “custom” and “add” 5) Name the custom setting with something intuitive 6) For OMA-URI add the policy OMA-URI string: ./Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP 7) For Data type select Integer and add the number

Note: The following describes which policy wins according to Windows 10 version.

Windows 10 versions 1709 and earlier Group Policy will override MDM policies, even if an identical policy is configured in MDM.

Windows 10 version 1803 and beyond there is a new Policy CSP (configuration service provider) setting called ControlPolicyConflict that includes the policy of MDMWinsOverGP, where the preference of which policy wins can be controlled,

i.e. Microsoft Intune MDM policy.

Note 2: the ControlPolicyConflict policy allows the IT admin to control which policy will be used whenever both the MDM policy and its equivalent Group Policy (GP) are set on the device.

Reference: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict https://uem4all.com/2018/04/02/windows-10-group-policy-vs-intune-mdm-policy-who-wins/