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.pass4itsure.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 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

Correct Answer: C

Onboard Windows devices to Defender for Endpoint using Intune

Enable Microsoft Defender for Endpoint in Intune

The first step you take is to set up the service-to-service connection between Intune and Microsoft Defender for Endpoint. Set up requires administrative access to both the Microsoft Defender Security Center, and to Intune.

Onboard Windows devices

(After you connect Intune and Microsoft Defender for Endpoint, Intune receives an onboarding configuration package from Microsoft Defender for Endpoint. You use a device configuration profile for Microsoft Defender for Endpoint to deploy

the package to your Windows devices.

The configuration package configures devices to communicate with Microsoft Defender for Endpoint services to scan files and detect threats. The device also reports its risk level to Microsoft Defender for Endpoint based on your compliance

policies.

After onboarding a device using the configuration package, you don\\'t need to do it again.)

You can also onboard devices using:

*-> Endpoint detection and response (EDR) policy. Intune EDR policy is part of endpoint security in Intune. Use EDR policies to configure device security without the overhead of the larger body of settings found in device configuration profiles.

You can also use EDR policy with tenant attached devices, which are devices you manage with Configuration Manager.

Reference:

https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure#enable-microsoft-defender-for-endpoint-in-intune

QUESTION 3

You have a Microsoft 365 E5 subscription and 100 computers that run Windows 10.

You need to deploy Microsoft Office Professional Plus 2019 to the computers by using Microsoft Office Deployment Tool (ODT).

What should you use to create a customization file for ODT?

A. the Microsoft 365 admin center

B. the Microsoft Intune admin center

C. the Microsoft Purview compliance portal

D. the Microsoft 365 Apps admin center

Correct Answer: D

To work with configuration files in the cloud, sign in to the Microsoft 365 Apps admin center and go to the Device Configuration page under Customization. From that page, you can do the following actions:

To create a new file, select Create, create a configuration file, and then select Done. The configuration file is automatically saved to the cloud as part of your tenant.

To edit an existing file, select the name of the file, make your changes, and then select Done.

To get a link to a configuration file, select the file, select Get Link, and then select Copy. You can use the link to refer to the configuration file when you use the Office Deployment Tool.

Reference:

https://learn.microsoft.com/en-us/deployoffice/admincenter/overview-office-customization-tool

QUESTION 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

Correct Answer: D

Restart frequency in endpoint analytics.

In endpoint analytics startup performance, we\\'ve provided insights into PC boot times, and how to improve the reboot times of poorly performing devices. Reboot frequency can be just as impactful to the user experience since a device that

reboots daily because of Stop errors will have a poor user experience even if the boot times are fast. We\\'ve recently added insights into restart frequencies within your organization to help you identify problematic devices.

Prerequisites

Devices are enrolled in endpoint analytics.

Enroll Configuration Manager devices

Enroll Intune devices

After enrollment, client devices require a restart to fully enable all analytics.

Etc.

Reference:

https://learn.microsoft.com/en-us/mem/analytics/restart-frequency

QUESTION 5

You need to configure Delivery Optimization to meet the technical requirements. Which download mode should you use?

A. Simple (99)

B. Group (2)

C. Internet (3)

D. HTTP Only (0)

E. Bypass (100)

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimizationreference#download-mode