MD-101 Q&As

Managing Modern Desktops

Pass Microsoft MD-101 Exam with 100% Guarantee

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

https://www.pass2lead.com/md-101.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 an Azure Active Directory (Azure AD) tenant named contoso.com.

You have a workgroup computer named Computer1 that runs Windows 10.

You need to add Computer1 to contoso.com.

What should you use?

A. the Settings app

B. Computer Management

C. netdom.exe

D. dsregcmd.exe

Correct Answer: D

If you want to manually join the computer to Azure AD, you can execute the dsregcmd /join command. This command should be run in SYSTEM context (using psexec for example) and will force an attempt to Azure AD.

Reference: https://365bythijs.be/2019/11/02/troubleshooting-hybrid-azure-ad-join/

QUESTION 2

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company\\'s environment includes a Microsoft 365 subscription.

Users in the company\\'s sales division have personal iOS or Android devices that are enrolled in Microsoft Intune. New users are added to the sales division on a monthly basis.

After a mobile application is created for users in the sales division, you are instructed to make sure that the application can only be downloaded by the sales division users

Solution: You start by adding the application to Intune.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: A

Before you can configure, assign, protect, or monitor apps, you must add them to Microsoft Intune.

Reference: https://docs.microsoft.com/en-us/intune/apps-add

QUESTION 3

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.

You have an Azure Directory group named Group1 that contains Windows 10 Enterprise devices and Windows 10 Pro devices.

From Microsoft Intune, you create a device configuration profile named Profile1.

You need to ensure that Profile1 applies to only the Windows 10 Enterprise devices in Group1.

Solution: You create a scope tag, and then you add the scope tag to the Windows 10 Enterprise devices and Profile1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead: You configure an applicability rule for Profile1. You assign Profile1 to Group1.

Note: Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10/11 devices group. And, you only want the profile

assigned to devices running Windows Enterprise.

To do this task, create an applicability rule.

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

QUESTION 4

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Description
Group1	Azure AD group that contains a user named User1
Group2	Azure AD group that contains iOS devices

You create a Conditional Access policy named CAPolicy1 that will block access to Microsoft Exchange Online from iOS

devices. You assign CAPolicy1 to Group1.

You discover that User1 can still connect to Exchange Online from an iOS device.

You need to ensure that CAPolicy1 is enforced.

What should you do?

A. Configure a new terms of use (TOU).

B. Assign CAPolicy1 to Group2.

C. Enable CAPolicy1

D. Add a condition in CAPolicy1 to filter for devices.

Correct Answer: B

Common signals that Conditional Access can take in to account when making a policy decision include the following signals:

User or group membership

Policies can be targeted to specific users and groups giving administrators fine-grained control over access.

Device

Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Use filters for devices to target policies to specific devices like privileged access workstations.

Etc.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

QUESTION 5

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

Correct Answer: A

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-lifetime