SC-300Q&As

Microsoft Identity and Access Administrator

Pass Microsoft SC-300 Exam with 100% Guarantee

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

https://www.passapply.com/sc-300.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You configure a new Microsoft 36S tenant to use a default domain name of contosso.com.

You need to ensure that you can control access to Microsoft 365 resource-, by using conditional access policy.

What should you do first?

A. Disable the User consent settings.

B. Disable Security defaults.

C. Configure a multi-factor authentication (Ml A) registration policy1.

D. Configure password protection for Windows Server Active Directory.

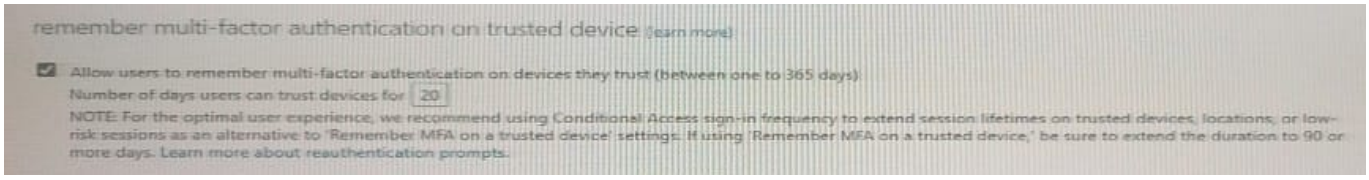
Correct Answer: B

QUESTION 2

You create the Azure Active Directory (Azure AD) users shown in the following table.

Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

On February 1, 2021, you configure the multi-factor authentication (MFA) settings as shown in the following exhibit.



The users authentication to Azure AD on their devices as shown in the following table.

Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

On February 26, 2021, what will the multi-factor auth status be for each user?

A.

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

B.

Name	Multi-factor auth status
User1	Enabled
User2	Enabled
User3	Enabled

C.

Name	Multi-factor auth status
User1	Enforced
User2	Enforced
User3	Enforced

D.

Name	Multi-factor auth status
User1	Disabled
User2	Enforced
User3	Enforced

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

QUESTION 3

You have an Azure Active Directory (Azure AD) tenant that uses Azure AD Identity Protection and contains the resources shown in the following table.

Name	Type	Configuration
Risk1	User risk policy	Users that have a high severity risk must reset their password upon next sign-in.
User1	User	*Not applicable*

Azure Multi-factor Authentication (MFA) is enabled for all users.

User1 triggers a medium severity alert that requires additional investigation.

You need to force User1 to reset his password the next time he signs in. The solution must minimize administrative effort.

What should you do?

A. Reconfigure the user risk, policy to trigger on medium or low severity.

B. Mark User1 as compromised.

C. Reset the Azure MIFA registration for User1.

D. Configure a sign-in risk policy.

Correct Answer: B

QUESTION 4

You have a Microsoft 365 E5 subscription.

You need to create a Microsoft Defender for Cloud Apps session policy.

What should you do first?

A. From the Microsoft Defender for Cloud Apps portal, select User monitoring.

B. From the Microsoft Defender for Cloud Apps portal, select App onboarding/maintenance

C. From the Azure Active Directory admin center, create a Conditional Access policy.

D. From the Microsoft Defender for Cloud Apps portal, create a continuous report.

Correct Answer: C

QUESTION 5

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

All users who run applications registered in Azure AD are subject to conditional access policies.

You need to prevent the users from using legacy authentication.

What should you include in the conditional access policies to filter out legacy authentication attempts?

A. a cloud apps or actions condition

B. a user risk condition

C. a client apps condition

D. a sign-in risk condition

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication