SC-300^{Q&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.leads4pass.com/sc-300.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 that has Azure AD Identity Protection policies enforced.

You create an Azure Sentinel instance and configure the Azure Active Directory connector.

You need to ensure that Azure Sentinel can generate incidents based on the risk alerts raised by Azure AD Identity Protection.

What should you do first?

A. Add an Azure Sentinel data connector.

B. Configure the Notify settings in Azure AD Identity Protection.

C. Create an Azure Sentinel playbook.

D. Modify the Diagnostics settings in Azure AD.

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection

QUESTION 2

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The tenant has the authentication methods shown in the following table.

Method	Target	Enabled
FIDO2	Group2	Yes
Microsoft Authenticator app	Group1	Yes
SMS	Group3	Yes

Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?

A. User1 only

B. User2 only

C. User3 only

D. User1 and User2 only

E. User2 and User3 only

Correct Answer: A

QUESTION 3

You implement the planned changes for SSPR.

What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Number of authentication methods required: | 2 ▼ |

Authentication methods that can be used: | Email and phone only ▼ |

Correct Answer:

Answer Area

Number of authentication methods required: | 2 ▼ |

Authentication methods that can be used: | Email and phone only ▼ |

QUESTION 4

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.

User1 has the devices shown in the following table.

Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings:

Name: Terms1 Display name: Contoso terms of use Require users to expand the terms of use: On Require users to consent on every device: On Expire consents: On Expire starting on: December 10, 2020 Frequency: Monthly

On November 15, 2020, User1 accepts Terms1 on Device3.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	O	O
On December 11, 2020, User1 can accept Terms1 on Device2.	O	O
On December 7, 2020, User1 can accept Terms1 on Device3.	O	O

Correct Answer:

Answer Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	●	O
On December 11, 2020, User1 can accept Terms1 on Device2.	●	O
On December 7, 2020, User1 can accept Terms1 on Device3.	O	●

QUESTION 5

You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements. What should you include in the configuration?

A. named locations that have a private IP address range

B. named locations that have a public IP address range

C. trusted IPs that have a public IP address range

D. trusted IPs that have a private IP address range

Correct Answer: C

Location offer your country set, IP ranges MFA trusted IP and corporate network VPN gateway IP address: This is the public IP address of the VPN device for your on-premises network. The VPN device requires an IPv4 public IP address.

Specify a valid public IP address for the VPN device to which you want to connect. It must be reachable by Azure

Client Address space: List the IP address ranges that you want routed to the local onpremises network through this gateway. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges

of other networks your virtual network connects to, or with the address ranges of the virtual network itself.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

[Latest SC-300 Dumps](https://www.leads4pass.com/sc-300.html)   [SC-300 Study Guide](https://www.leads4pass.com/sc-300.html)   [SC-300 Exam Questions](https://www.leads4pass.com/sc-300.html)