MS-500 Q&As

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

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

https://www.leads4pass.com/ms-500.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 several Microsoft Defender for Office 365 policies in a Microsoft 365 subscription.

You need to allow a user named User1 to view Microsoft Defender for Office 365 reports in the Threat management dashboard.

Which role provides User1 with the required role permissions?

A. Security reader

B. Compliance administrator

C. Information Protection administrator

D. Exchange administrator

Correct Answer: A

In order to view and use the reports described in this article, you need to be a member of one of the following role groups in the Microsoft 365 Defender portal: Organization Management Security Administrator Security Reader Global Reader Note: There are several versions of this question in the exam. The question has two possible correct answers:

1.

Security Administrator

2.

Security Reader Other incorrect answer options you may see on the exam include the following: Message center reader Service administrator Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-mdo

QUESTION 2

What should User6 use to meet the technical requirements?

A. Supervision in the Security and Compliance admin center

B. Service requests in the Microsoft 365 admin center

C. Security and privacy in the Microsoft 365 admin center

D. Data subject requests in the Security and Compliance admin center

Correct Answer: B

https://learn.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide

QUESTION 3

DRAG DROP

You have a Microsoft 365 E5 subscription.

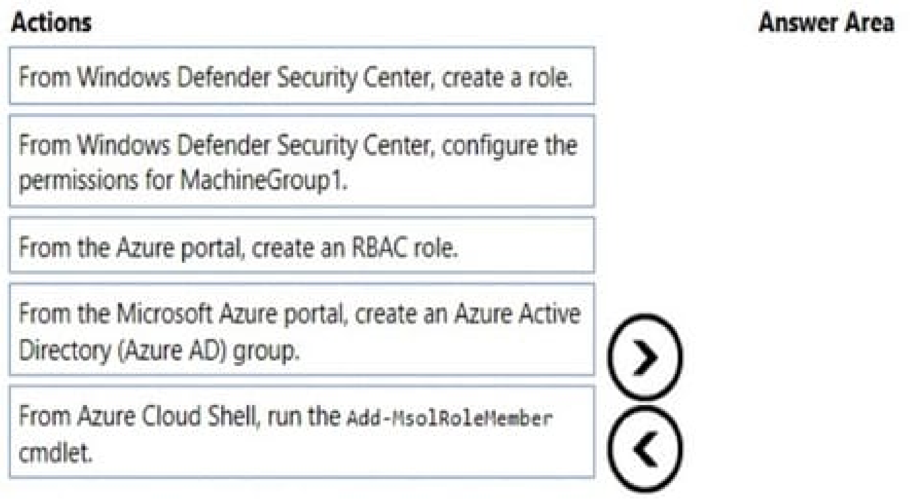
All computers run Windows 10 and are onboarded to Windows Defender Advanced Threat Protection (Windows Defender ATP).

You create a Windows Defender machine group named MachineGroup1.

You need to enable delegation for the security settings of the computers in MachineGroup1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

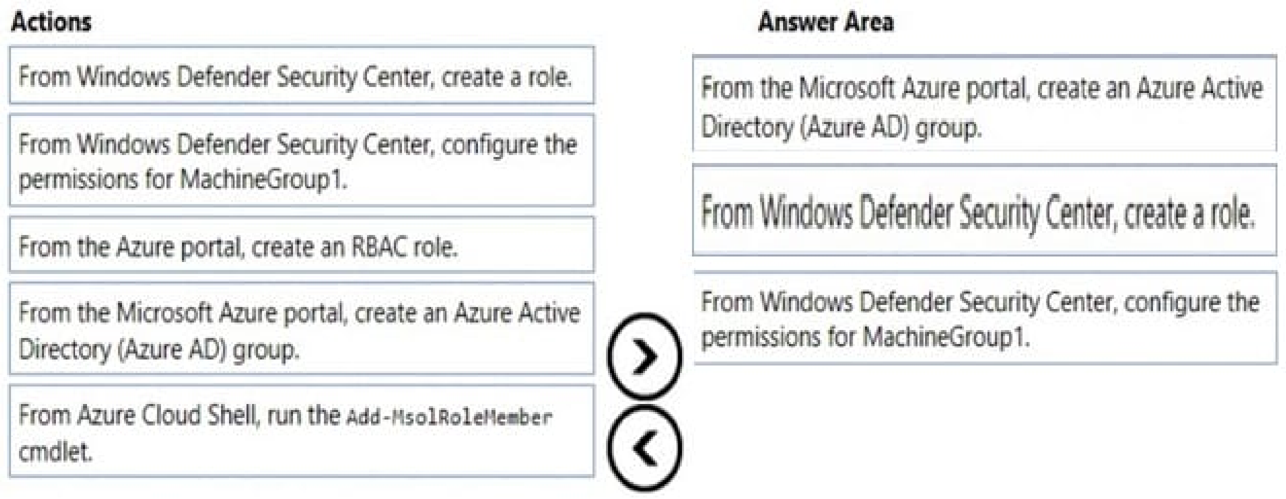


Actions

- From Windows Defender Security Center, create a role.
- From Windows Defender Security Center, configure the permissions for MachineGroup1.
- From the Azure portal, create an RBAC role.
- From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
- From Azure Cloud Shell, run the `Add-MsolRoleMember` cmdlet.

Answer Area

Correct Answer:



Actions

- From Windows Defender Security Center, create a role.
- From Windows Defender Security Center, configure the permissions for MachineGroup1.
- From the Azure portal, create an RBAC role.
- From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
- From Azure Cloud Shell, run the `Add-MsolRoleMember` cmdlet.

Answer Area

- From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
- From Windows Defender Security Center, create a role.
- From Windows Defender Security Center, configure the permissions for MachineGroup1.

QUESTION 4

You need to protect against phishing attacks. The solution must meet the following requirements:

1.

Phishing email messages must be quarantined if the messages are sent from a spoofed domain.

2.

As many phishing email messages as possible must be identified.

The solution must apply to the current SMTP domain names and any domain names added later.

To complete this task, sign in to the Microsoft 365 admin center.

Correct Answer: See explanation below.

1.

After signing in to the Microsoft 365 admin center, select Security, Threat Management, Policy, then ATP Anti-phishing.

2.

Select Default Policy to refine it.

3.

In the Impersonation section, select Edit.

4.

Go to Add domains to protect and select the toggle to automatically include the domains you own.

5.

Go to Actions, open the drop-down If email is sent by an impersonated user, and choose the Quarantine message action. Open the drop-down If email is sent by an impersonated domain and choose the Quarantine message action.

6.

Select Turn on impersonation safety tips. Choose whether tips should be provided to users when the system detects impersonated users, domains, or unusual characters. Select Save.

7.

Select Mailbox intelligence and verify that it\\'s turned on. This allows your email to be more efficient by learning usage patterns.

8.

Choose Add trusted senders and domains. Here you can add email addresses or domains that shouldn\\'t be classified as an impersonation.

9.

Choose Review your settings, make sure everything is correct, select Save, then Close.

Reference:

https://support.office.com/en-us/article/protect-against-phishing-attempts-in-microsoft-365-86c425e1-1686-430a-9151-f7176cce4f2c#ID0EAABAAA=Try_it!

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#example-anti-phishing-policy-to-protect-a-user-and-a-domain

QUESTION 5

You have a Microsoft 365 E5 subscription.

You plan to create a conditional access policy named Policy1.

You need to be able to use the sign-in risk level condition in Policy1.

What should you do first?

A. Connect Microsoft Endpoint Manager and Microsoft Defender for Endpoint.

B. From the Azure Active Directory admin center, configure the Diagnostics settings.

C. From the Endpoint Management admin center, create a device compliance policy.

D. Onboard Azure Active Directory (Azure AD) Identity Protection.

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk