MS-203 Q&As

Microsoft 365 Messaging

Pass Microsoft MS-203 Exam with 100% Guarantee

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

https://www.passapply.com/ms-203.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.

A user attempts to send an email message to an external recipient and receives the following error message: "Your message couldn\\'t be delivered because you weren\\'t recognized as a valid sender. The most common reason for this is that

your email address is suspected of sending spam and it\\'s no longer allowed to send messages outside of your organization. Contact your mail admin for assistance. Remote Server returned `550 5.1.8 Access denied, bad outbound sender\\'."

You need to ensure that the user send email to external recipients.

What should you do?

A. compliance management in the Exchange admin center

B. Data loss prevention in the Security and Compliance admin center

C. Threat management in the Security and Compliance admin center

D. action center in the Exchange admin center

Correct Answer: C

http://automatica.com.au/2020/01/office-365-single-users-unable-to-send-email-access-denied-bad-outbound-sender-error/

QUESTION 2

You have a Microsoft 365 environment that contains 1,000 mobile devices.

You need to recommend a solution to prevent all the mobile devices that use the Exchange ActiveSync protocol from authenticating by using Basic authentication.

Which two solutions should you recommend? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Configure the CAS mailbox settings for each mailbox.

B. Implement Azure Multi-Factor Authentication (MFA).

C. Create an authentication policy.

D. Create a conditional access policy.

E. Create a device access rule.

Correct Answer: CD

Reference: https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-

basicauthentication-in-exchange-online https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

QUESTION 3

You have a Microsoft Exchange Online tenant that contains a user named User1 and a shared mailbox named Project1.

You plan to delegate User1 permission to send email messages from Project1.

You need to ensure that the messages appear to come directly from Project1.

Which permission should you assign to User1?

A. Full Access

B. Contributor

C. Send As

D. Send on Behalf

Correct Answer: C

Explanation:

Which permissions should you use?

You can use the following permissions with a shared mailbox.

Send As: The Send As permission lets a user impersonate the shared mailbox when sending mail. For example, if Kweku logs into the shared mailbox Marketing Department and sends an email, it will look like the Marketing Department sent

the email.

Incorrect:

Full Access: The Full Access permission lets a user open the shared mailbox and act as the owner of that mailbox. After accessing the shared mailbox, a user can create calendar items; read, view, delete, and change email messages; create

tasks and calendar contacts. However, a user with Full Access permission can\\'t send email from the shared mailbox unless they also have Send As or Send on Behalf permission.

Send on Behalf: The Send on Behalf permission lets a user send email on behalf of the shared mailbox. For example, if John logs into the shared mailbox Reception Building 32 and sends an email, it looks like the mail was sent by "John on

behalf of Reception Building 32". You can\\'t use the EAC to grant Send on Behalf permissions, you must use Set-Mailbox cmdlet with the GrantSendonBehalf parameter.

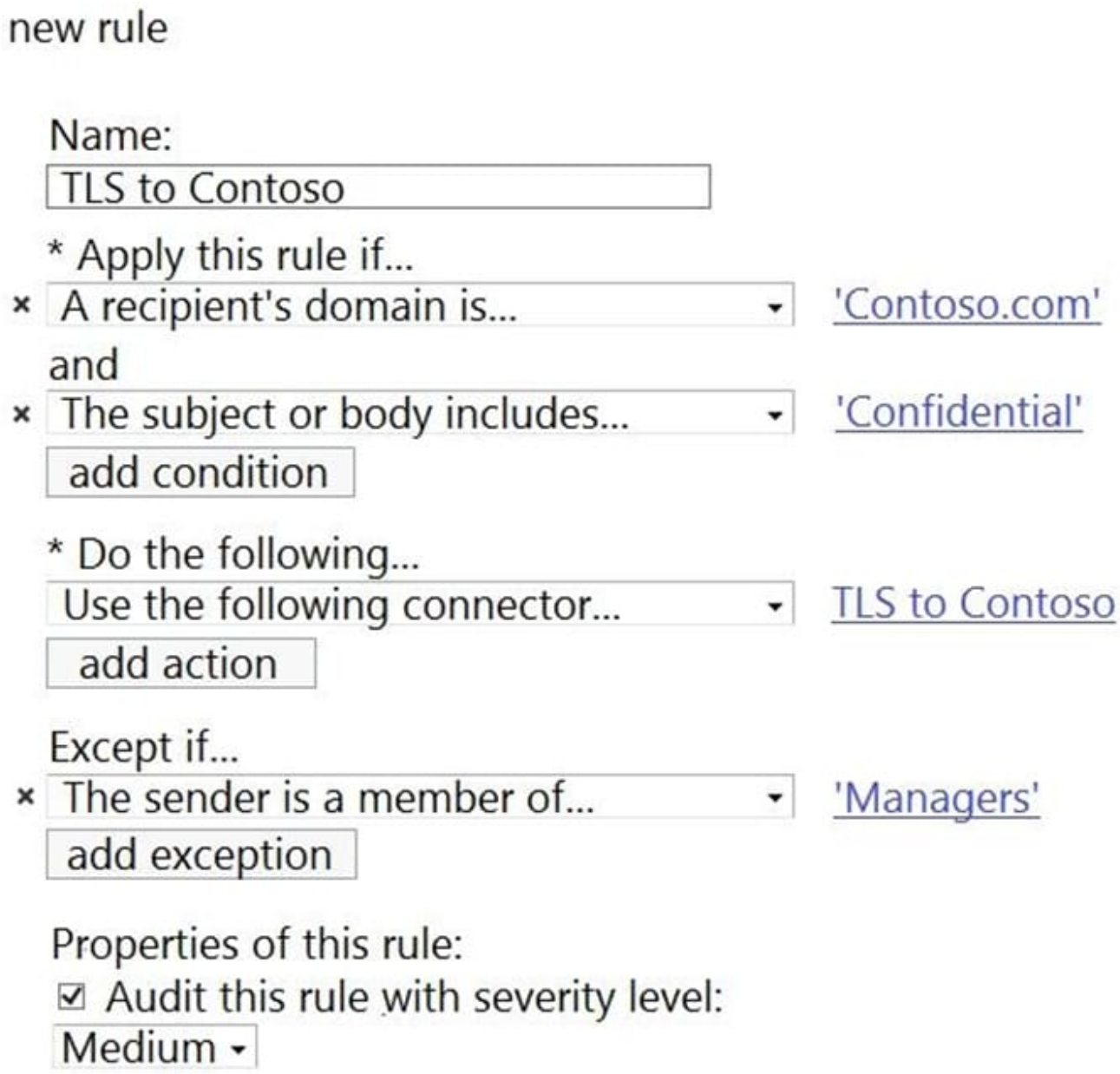
Reference: https://learn.microsoft.com/en-us/exchange/collaboration-exo/shared-mailboxes

QUESTION 4

HOTSPOT

You have a Microsoft Exchange Online subscription that uses a namespace of litwareinc.com.

You create a connector in Exchange Online that is configured as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
All email sent to contoso.com is TLS-encrypted.	○	○
The message sent by User1 uses the TLS to Contoso connector.	○	○
The message sent by User2 uses the TLS to Contoso connector.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
All email sent to contoso.com is TLS-encrypted.	○	○
The message sent by User1 uses the TLS to Contoso connector.	○	○
The message sent by User2 uses the TLS to Contoso connector.	○	○

QUESTION 5

You have a Microsoft 365 subscription that uses a default domain named contoso.com.

Users report that email messages from a domain named fabrikam.com are identified as spam even though the messages are legitimate.

You need to prevent messages from fabrikam.com from being identified as spam.

What should you do?

A. Create a new remote domain.

B. Edit a spam filter policy.

C. Enable the safe list on a connection filter.

D. Enable the Zero-hour auto purge (ZAP) email protection feature.

Correct Answer: C

Safe list: The safe list is a dynamic allow list in the Microsoft datacenter that requires no customer configuration. Microsoft identifies these trusted email sources from subscriptions to various third-party lists. You enable or disable the use of the safe list; you can\\'t configure the source email servers on the safe list. Spam filtering is skipped on incoming

messages from the email servers on the safe list.

Incorrect:

*

Remote Domains are an organizational setting that allow you to control certain message types such as “Out of Office” and “Non-Delivery Reports”.

*

In Microsoft 365 organizations with mailboxes in Exchange Online, zero-hour auto purge (ZAP) is an email protection feature that retroactively detects and neutralizes malicious phishing, spam, or malware messages that have already been delivered to Exchange Online mailboxes.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-the-connection-filter-policy?view=o365-worldwide