**Vendor:**Microsoft

**Exam Code:**MS-203

**Exam Name:**Microsoft 365 Messaging

**Version:**Demo

**QUESTION 1**

HOTSPOT

You have a Microsoft 365 E5 tenant that contains two Azure Active Directory (Azure AD) security groups named Finance and Marketing. The tenant contains the users and devices shown in the following table.

## Answer Area

The email was not received from a known open relay:

- BCL:7
- IPV:NLI
- SFV:SPM
- SCL:5

The message is from a bulk sender:

- BCL:7
- IPV:NLI
- SCL:5
- SFV:SPM

The devices are configured as shown in the following table.

**Answer Area**

The email was not received from a known open relay:

- BCL:7
- IPV:NLI
- SFV:SPM
- SCL:5

The message is from a bulk sender:

- BCL:7
- IPV:NLI
- SCL:5
- SFV:SPM

A conditional access policy is configured as shown in the following exhibit.

## Answer Area

Group type:

- Distribution list
- Microsoft 365
- Security

Configuration:

- Add CustomerSupport as a member of the group.
- Assign the group the Contributor role for CustomerSupport.
- Configure the Send As settings.
- Configure the Send on Behalf settings.

From Microsoft Exchange Online PowerShell, you run the following cmdlet.

Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default

-ConditionalAccessPolicy ReadOnly

All the users connect to Exchange Online by using Outlook on the web.

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**

Group type:

- Distribution list
- Microsoft 365
- Security

Configuration:

- Add CustomerSupport as a member of the group.
- Assign the group the Contributor role for CustomerSupport.
- Configure the Send As settings.
- Configure the Send on Behalf settings.

Correct Answer:

| Name | Role |
|---|---|
| Admin1 | Exchange Administrator |
| Admin2 | Security Administrator |

---

**QUESTION 2**

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 a Microsoft Exchange Online tenant that contains the following email domains:

1.

Adatum.com

2.

Contoso.com

3.

Fabrikam.com

When external recipients receive email messages from the users in the tenant, all the messages are delivered by using the @contoso.com email domain.

You need to ensure that the users send email by using the @fabrikam.com email domain.

Solution: From the Microsoft 365 portal, you set fabrikam.com as the default domain.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq?view=o365-worldwide#how-do-i-set-or-change-the-default-domain-in-microsoft-365

---

**QUESTION 3**

You have 1,000 user accounts that are each licensed for Microsoft 365. Each user account has a Microsoft Exchange Online mailbox.

Ten of the user accounts are configured as service accounts for applications. The applications send event notifications to the mailboxes of the service accounts by using SMTP. The developers of each application have delegated access to the mailbox of their respective application. You need to ensure that all the event notifications sent by the applications are retained in the service account mailboxes so that new developers can review older notifications. The developers must be able to view only the notifications for their

respective application. The solution must minimize licensing costs. What should you do?

A. Convert the service account mailboxes into shared mailboxes.

B. Replace the service account mailboxes with a mail-enabled group.

C. Convert the service account mailboxes into mail-enabled contacts.

D. Convert the service account mailboxes into mail-enabled users.

Correct Answer: A

When you convert a user\\'s mailbox to a shared mailbox, all of the existing email and calendar is retained. Only now it\\'s in a shared mailbox where several people will be able to access it instead of one person. Reference: https://docs.microsoft.com/en-us/microsoft-365/admin/email/convert-user-mailbox-to-shared-mailbox?view=o365-worldwide

---

**QUESTION 4**

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.

Your company has a Microsoft 365 subscription.

Several users in the finance department of the company recently accessed unsafe websites by clicking on links in email messages.

Users in the marketing department of the company report that they must be able to access all the links embedded in email messages.

You need to reduce the likelihood of the finance department users accessing unsafe websites. The solution must affect only the finance department users.

Solution: You create a new safe links policy and apply the policy to finance department users.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-safe-links-policies?view=o365-worldwide

---

**QUESTION 5**

You have a Microsoft Exchange Online tenant that contains a user named User1.

You need to grant User1 the Send on Behalf permission for 20 mailboxes.

Which PowerShell cmdlet should you use?

A. Add-MailboxPermission

B. Add-MailboxFolderPermission

C. Set-Mailbox

D. Add-RecipientPermission

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/exchange/recipients/mailbox-permissions?view=exchserver-2019

---

**QUESTION 6**

You need to encrypt email between Fabrikam and Litware to support the planned changes. What should you configure in the Exchange admin center?

A. a connector

B. an organization relationship

C. a sharing policy

D. a remote domain

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/set-up-connectors-for-secure-mail-flow-with-a-partner

---

**QUESTION 7**

You have two mailboxes named Mailbox1 and Mailbox2 that have the ProhibitSendReceiveQuota parameter set to 50 GB. From a Microsoft Exchange Online tenant, you run the following PowerShell command.

## Mail flow scenario

From: Office 365

To: Partner organization

## Name

TLS to Contoso

## Description

None

## Status

Turn it on after saving

## When to use the connector

Use only when I have a transport rule set up that redirects messages to this connector.

## Routing method

Use the MX record associated with the partner's domain.

## Security restrictions

Always use Transport Layer Security (TLS) and connect only if the recipient's email server has a digital certificate.

You receive the license status of each mailbox and discover the configurations shown in the following table.

| Name | Configuration |
|---|---|
| DC1 | Domain controller |
| EXCH1 | Exchange Server 2019 Mailbox server |
| EDGE1 | Edge Transport server |
| SRV1 | Azure AD Connect server |

You need to increase the quota for Mailbox1 and Mailbox2. What should you do first?

A. Assign a license to each mailbox.

B. Convert each mailbox into an equipment mailbox.

C. Enable an archive for each mailbox.

D. Place both mailboxes on retention hold.

Correct Answer: A

Shared and resource mailboxes don\\'t require a license. However, without a license, these mailboxes are limited to 50 GB. To increase the mailbox size, an E3 or E5 license must be assigned. This will increase the mailbox to 100 GB.

Reference: https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits

---

**QUESTION 8**

You have a Microsoft Exchange Online tenant that uses a third-party email hygiene system named Service1. Service1 blocks all encrypted email.

All external email is routed through Service1 by using a connector.

Users classify email by using sensitivity labels. Emails classified as Secret are encrypted automatically.

You need to ensure that the users can send emails classified as Secret to external recipients.

Which two items should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a remote domain

B. a connector

C. a data loss prevention (DLP) policy

D. a mail flow rule

E. a label policy

Correct Answer: BD

Use an additional Connector and a Mail Flow Rule to bypass the third-party email hygiene system for emails that have the Secret sensitivity label. Emails with the sensitivity label will use the new connector. All other emails will use the existing connector.

Reference: https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/conditional-mail-routing

---

**QUESTION 9**

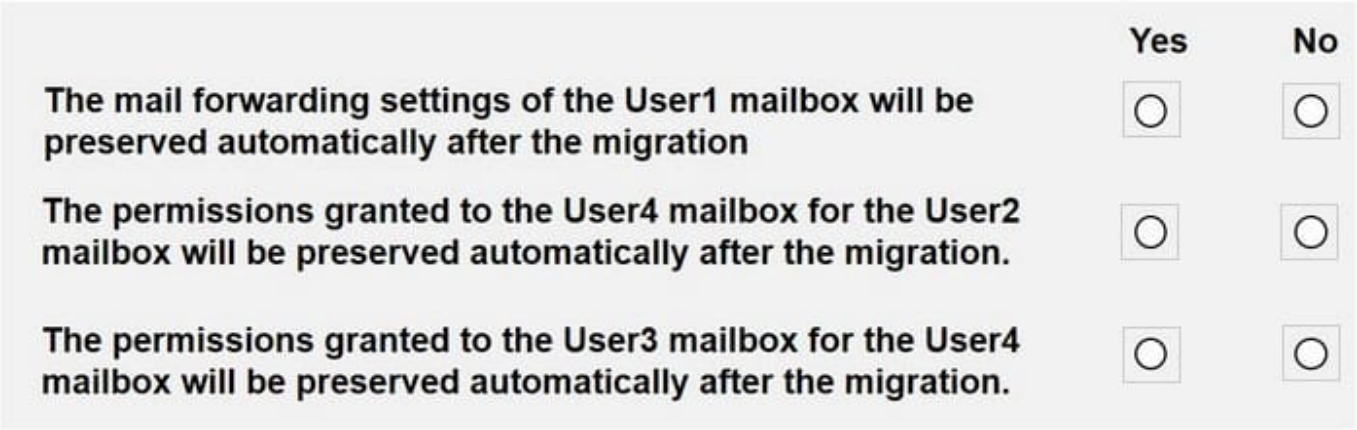
DRAG DROP

You have a Microsoft Exchange Online tenant that does NOT contain any public folders.

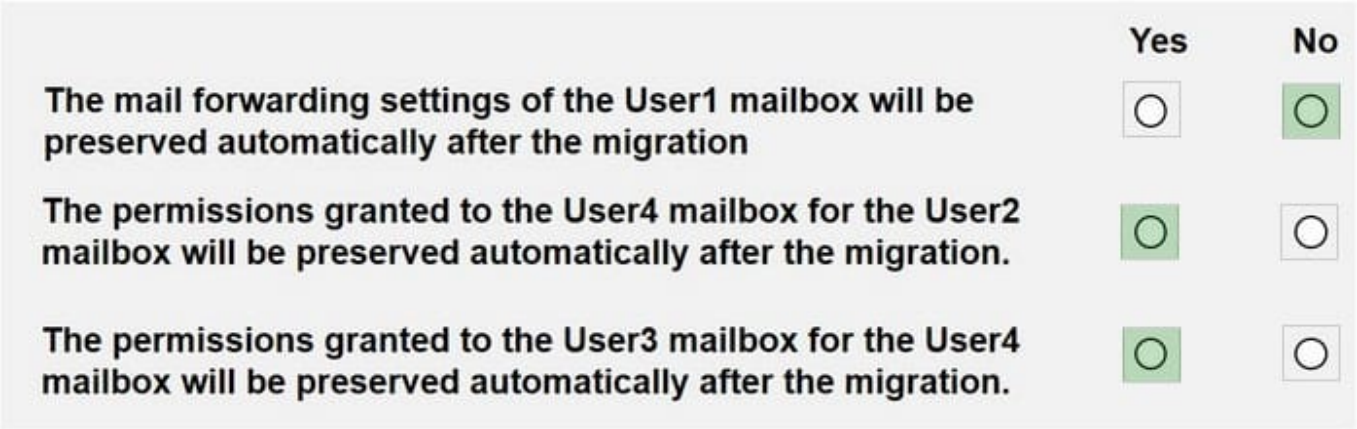
You need to create a new public folder. The solution must ensure that users can create a post by sending an email to the folder.

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

Select and Place:




Correct Answer:




Reference: https://docs.microsoft.com/en-us/exchange/collaboration-exo/public-folders/create-public-folder

https://docs.microsoft.com/en-us/exchange/collaboration-exo/public-folders/enable-or-disable-mail-for-public-folder

---

**QUESTION 10**

HOTSPOT

You have a Microsoft Exchange Online tenant that contains three users named User1, User2, and User3.

Mobile device mailbox policies are configured as shown in the following exhibit.

**Answer Area**

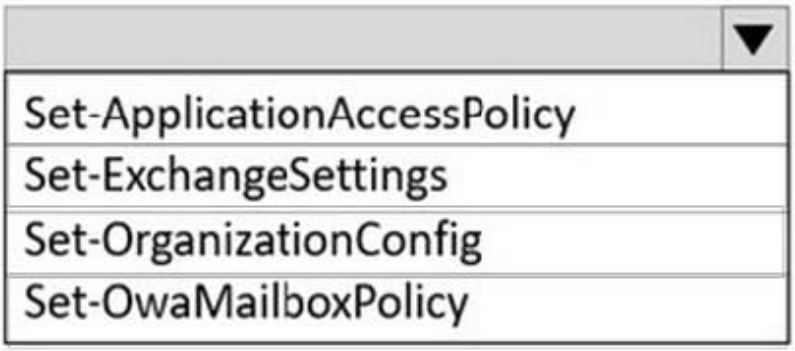
| Statements | Yes | No |
|---|---|---|
| If an email message sent from the Internet contains malware, the message will be delivered successfully to the recipient's mailbox | ○ | ○ |
| To prevent an email message from the Internet that contains malware from being delivered to an internal recipient, the default antimalware policy must be modified | ○ | ○ |
| To prevent an email message from the Internet that contains malware from being delivered to an internal recipient, the priority of the malware agent must be modified | ○ | ○ |

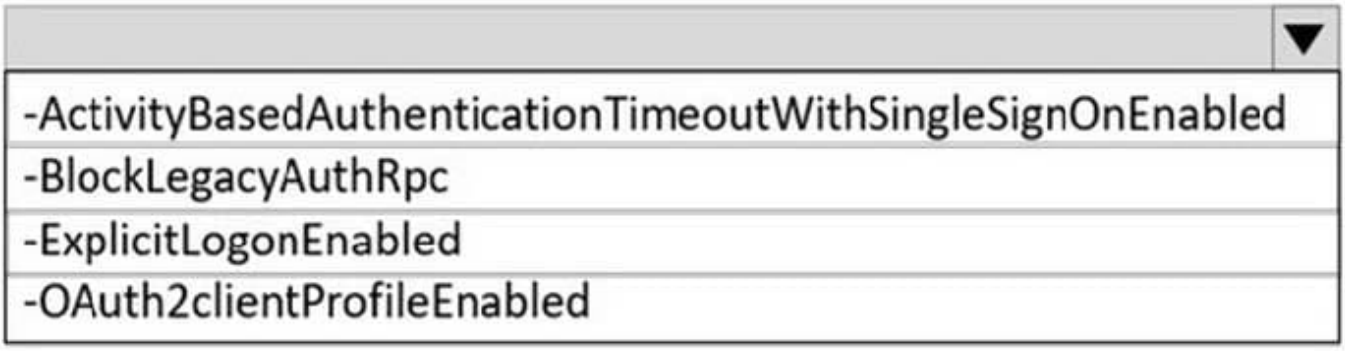
The users are configured as shown in the following table.

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| If an email message sent from the Internet contains malware, the message will be delivered successfully to the recipient's mailbox | ○ | ○ |
| To prevent an email message from the Internet that contains malware from being delivered to an internal recipient, the default antimalware policy must be modified | ○ | ○ |
| To prevent an email message from the Internet that contains malware from being delivered to an internal recipient, the priority of the malware agent must be modified | ○ | ○ |

You create a new mobile device mailbox policy as shown in the following exhibit.

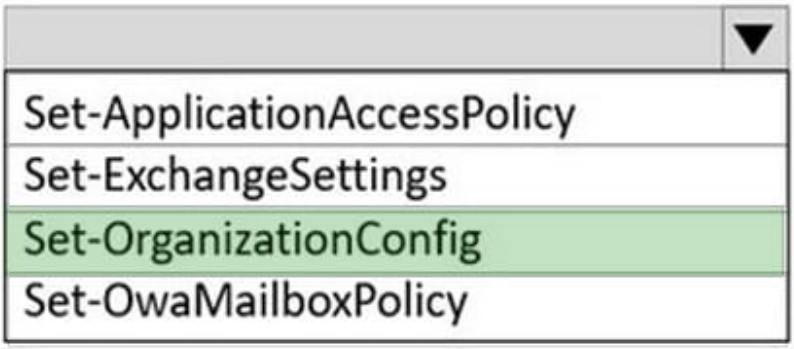


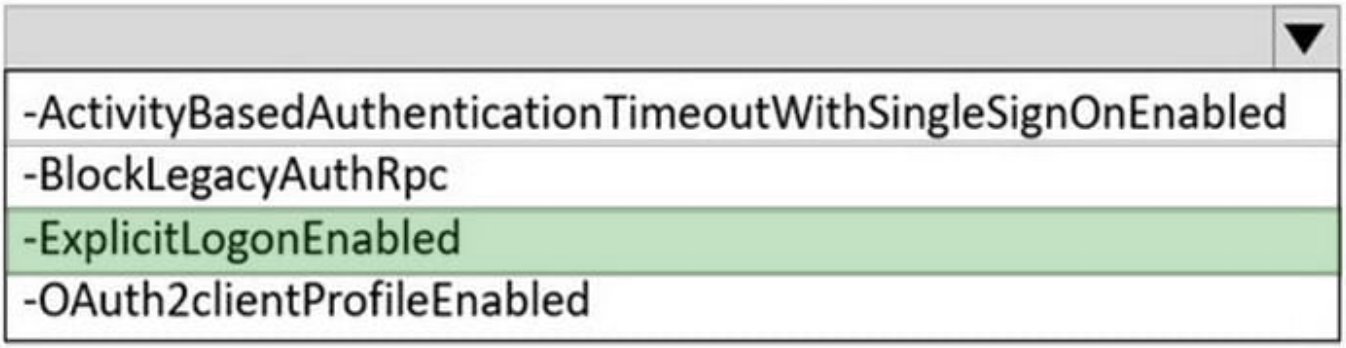




For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:




Correct Answer:

| Name | Email address | Title | Country |
|---|---|---|---|
| User1 | User1@contoso.com | Sales & Marketing Director | Canada |
| User2 | User2@contoso.com | Sales Manager | France |
| User3 | User3@sales.contoso.com | Marketing | Canada |

Reference: https://docs.microsoft.com/en-us/exchange/create-or-modify-a-mobile-device-mailbox-policy-exchange-2013-help

---

**QUESTION 11**

You have a Microsoft 365 E3 subscription that uses Microsoft Exchange Online.

You need to ensure that Safe Links and Safe Attachments protection is enabled for users.

What should you do?

A. Enable the Strict protection preset security policy.

B. Assign a Microsoft 365 E5 license to each user.

C. Create an Enhanced Filtering for Connectors rule.

D. Create an anti-malware policy and enable the common attachments filter.

Correct Answer: A

Explanation:

Preset security policies in EOP and Microsoft Defender for Office 365

Preset security policies provide a centralized location for applying all of the recommended spam, malware, and phishing policies to users at once. The policy settings are not configurable. Instead, they are set by us and are based on our

observations and experiences in the datacenters for a balance between keeping harmful content away from users and avoiding unnecessary disruptions.

Policies in preset security policies

Preset security policies use the corresponding policies from the various protection features in EOP and Microsoft Defender for Office 365. These policies are created after you assign the Standard protection or Strict protection preset security

policies to users. You can\\'t modify the settings in these policies.

Microsoft Defender for Office 365 policies: These policies are in organizations with Microsoft 365 E5 or Defender for Office 365 add-on subscriptions:

*

Safe Links policies named Standard Preset Security Policy, Strict Preset Security Policy, and Built-in Protection Policy.

*

Safe Attachments policies named Standard Preset Security Policy, Strict Preset Security Policy, and Built-in Protection Policy.

*

Anti-phishing policies in Defender for Office 365 named Standard Preset Security Policy and Strict Preset Security Policy, which include:

The same spoof settings that are available in the EOP anti-phishing policies.

Impersonation settings

Note also:

Exchange Online Protection (EOP) policies: These policies are in all Microsoft 365 organizations with Exchange Online mailboxes and standalone EOP organizations without Exchange Online mailboxes:

Anti-spam policies named Standard Preset Security Policy and Strict Preset Security Policy.

Anti-malware policies named Standard Preset Security Policy and Strict Preset Security Policy.

Anti-phishing policies (spoofing protection) named Standard Preset Security Policy and Strict Preset Security Policy (spoof settings).

Incorrect:

Not B: To use Safe Links and Safe Attachments, one must have Microsoft 365 Advanced Threat Protection Plan 1 or 2.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/preset-security-policies

---

**QUESTION 12**

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.

Your company has an Exchange Online tenant that contains 2,000 mailboxes.

A partner company named Fabrikam, Inc. uses a third-party messaging solution. The outbound SMTP server for Fabrikam uses an IP address of 131.107.2.22.

You discover that several email messages from the fabrikam.com domain are erroneously marked as spam.

You need to ensure that all the email messages sent from the fabrikam.com domain are delivered successfully to the user mailboxes of your company.

Solution: You create a remote domain. Does this meet the goal?

A. Yes

B. No

Correct Answer: B