faq

QUESTION 56
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 Server 2019 hybrid deployment. All user mailboxes are hosted in Microsoft 365. All outbound SMTP email is routed through the on-premises Exchange organization.

A corporate security policy requires that you must prevent credit card numbers from being sent to internet recipients by using email.

You need to configure the deployment to meet the security policy requirement.

Solution: From Microsoft 365, you create a data loss prevention (DLP) policy.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

QUESTION 57
You have a Microsoft Exchange Server 2019 organization.

You purchase a Microsoft Office 365 E5 subscription.

You plan to implement Exchange Modern Hybrid and free/busy sharing.

Which two components should you configure for the planned implementations? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a sharing policy
B. a federation trust
C. a relying party trust
D. Active Directory Lightweight Directory Services (AD LDS)
E. an organization relationship

Correct Answer: BE
Explanation:
https://docs.microsoft.com/en-us/exchange/shared-free-busy

QUESTION 58
You have a Microsoft 365 subscription.

Several users report today that they cannot access email from their mobile device. They successfully accessed their email from the same device yesterday.

You need to identify which mobile device access rule applies to the devices.

Which cmdlet should you run?

A.   Get-MsolDevice
B.   Get-DeviceTenantRule
C.   Get-MobileDevice
D.   Get- ActiveSyncMailboxPolicy

Correct Answer: C
Explanation:
The Get-MobileDevice cmdlet returns identification, configuration, and status information for each mobile device.

Note: The Get-MobileDeviceStatistics cmdlet can also be used.

Reference:
https://docs.microsoft.com/en-us/powershell/module/exchange/devices/get-mobiledevice?view=exchange-ps

QUESTION 59
You have a Microsoft Exchange Online tenant.

All users are assigned only an Office 365 Enterprise E3 license.

You need to ensure that the users can use only Microsoft Outlook to connect to their Microsoft 365 mailbox when they connect from an Android device.

What should you create?

A.   a conditional access policy in Azure Active Directory (Azure AD)
B.   a connection filter policy in Exchange Online Protection (EOP)
C.   an Outlook Web App policy in Exchange Online
D.   an app protection policy in Microsoft Endpoint Manager

Correct Answer: A
Explanation:
Office 365 Enterprise E3 includes Azure Active Directory Premium P1 which is required for Azure conditional access policies.

QUESTION 60
You have a Microsoft Exchange Server 2019 organization.

You purchase a Microsoft 365 subscription and configure Active Directory synchronization.

You use a smart host for all email communication between the organization and the Internet. The smart host performs email hygiene and alerts message headers.

You plan to run the Hybrid Configuration wizard to create an Exchange hybrid deployment and change the MX record to point to Exchange Online.

You need to decommission the smart host from the organization.

What should you do first?

A. Create a Receive connector that allows anonymous authentication.
B. Modify the InternalSmtpServer value by running the Set-TransportConfig cmdlet.
C. Modify the Send connector to use DNS delivery.
D. Modify the TLSReceiveDomainSecureList value by running the Set-TransportConfig cmdlet.

Correct Answer: C

QUESTION 61
You have a hybrid deployment that contains a Microsoft exchange Online tenant and anon premises Exchange Server 2019 server named Server1. Alt users use an email address suffix of @contoso.com.

On Server1, you create a new mailbox that uses an email address of user1@contoso.com

Users hosted in Exchange Online report that they receive a non-delivery report (NDR) When they attempt to send email messages to user1@contoso.com. The NDR contains the following text: "User1 wasn't found at contoso.com."

You verify that the Exchange Online users can send email successfully to the other mailboxes hosted on Server1. Users hosted on Server1 can send email to user1@contoso.com successfully.

You need to identify what causes the email delivery to fail. What should you use?

A. the Azure Active Directory admin center
B. the Exchange admin center
C. Azure AD Connect Health
D. the on-premises Exchange admin center

Correct Answer: C
Explanation:
It's likely that the new user account hasn't replicated to Azure Active Directory. Azure AD Connect is responsible for account replication between on-prem AD and Azure AD.

QUESTION 62
HOTSPOT
Your company has an Exchange Online tenant.

A partner company named Fourth Coffee also uses Exchange Online.

You need to ensure that the users at your company share free busy information with the users at Fourth Coffee. The solution must ensure that the meeting details included in the calendars of your company users remain hidden from the Fourth Coffee users.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
┌──────────────────────────┬──▼──┐  -Name "Fourth Coffee" -DomainNames "fourthcoffee.com"
│ New-SharingPolicy        │     │
│ New-AvailabilityConfig   │     │
│ New-OrganizationRelationship │
└──────────────────────────┴─────┘
-FreeBusyAccessEnabled $true -FreeBusyAccessLevel ┌──────────────┬──▼──┐ -FreeBusyAccessScope "Executives"
                                                  │ None         │     │
                                                  │ LimitedDetails │   │
                                                  │ AvailabilityOnly │ │
                                                  └──────────────┴─────┘
```

Correct Answer:

Answer Area

```
┌──────────────────────────┬──▼──┐  -Name "Fourth Coffee" -DomainNames "fourthcoffee.com"
│ New-SharingPolicy        │     │
│ New-AvailabilityConfig   │     │
│ New-OrganizationRelationship │  ← (selected)
└──────────────────────────┴─────┘
-FreeBusyAccessEnabled $true -FreeBusyAccessLevel ┌──────────────┬──▼──┐ -FreeBusyAccessScope "Executives"
                                                  │ None         │     │
                                                  │ LimitedDetails │   │
                                                  │ AvailabilityOnly │ │ ← (selected)
                                                  └──────────────┴─────┘
```

QUESTION 63
You have a Microsoft Exchange Server 2019 organization.

You need to configure the organization to use Exchange Online Protection (EOP) for the message hygiene of all inbound and outbound email.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Install an Exchange hybrid server.
B. For the organization, configure an MX record that points to Microsoft Office 365.
C. Create a hybrid organization relationship.
D. From the on-premises organization, create a connector to relay outbound email to Microsoft Office 365.

E.   Create a Microsoft Office 365 Connector to the on-premises organization.
F.   Create on-premises transport rules to control the outbound message flow.
Correct Answer: BDE
Explanation:
https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/setup-connectors-to-route-mail

QUESTION 64
You have a Microsoft Exchange Online tenant named contoso.com.

Several users report that email messages sent to the users at another company named fabrikam.com contain a Winmail.dat attachment.

You need to prevent the fabrikam.com users from receiving Winmail.dat attachments.

What should you do?

A.   Configure a remote domain that has the TNEFEnabled parameter set to $False.
B.   Create an Outbound connector that has the validationRecipients parameter set to contoso.com.
C.   Create an Outbound connector that has the validationRecipients parameter set to fabrikam.com.
D.   Configure a remote domain that has the TrustedMailoutboundEnabled parameter set to $False.

Correct Answer: A
Explanation:
https://gcits.com/knowledge-base/how-to-fix-the-winmail-dat-attachment-issue/

QUESTION 65
HOTSPOT
Your company has a Microsoft Exchange Server 2019 hybrid deployment.

The company has four departments that have the mailboxes shown in the following table.

Department	Number of mailboxes	Location
Finance	500	On-premises
Manufacturing	15,000	Exchange Online
Sales	5,000	On-premises
Marketing	2,000	Exchange Online

The mailboxes are configured as shown in the following table.