Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator

NEW QUESTION 1

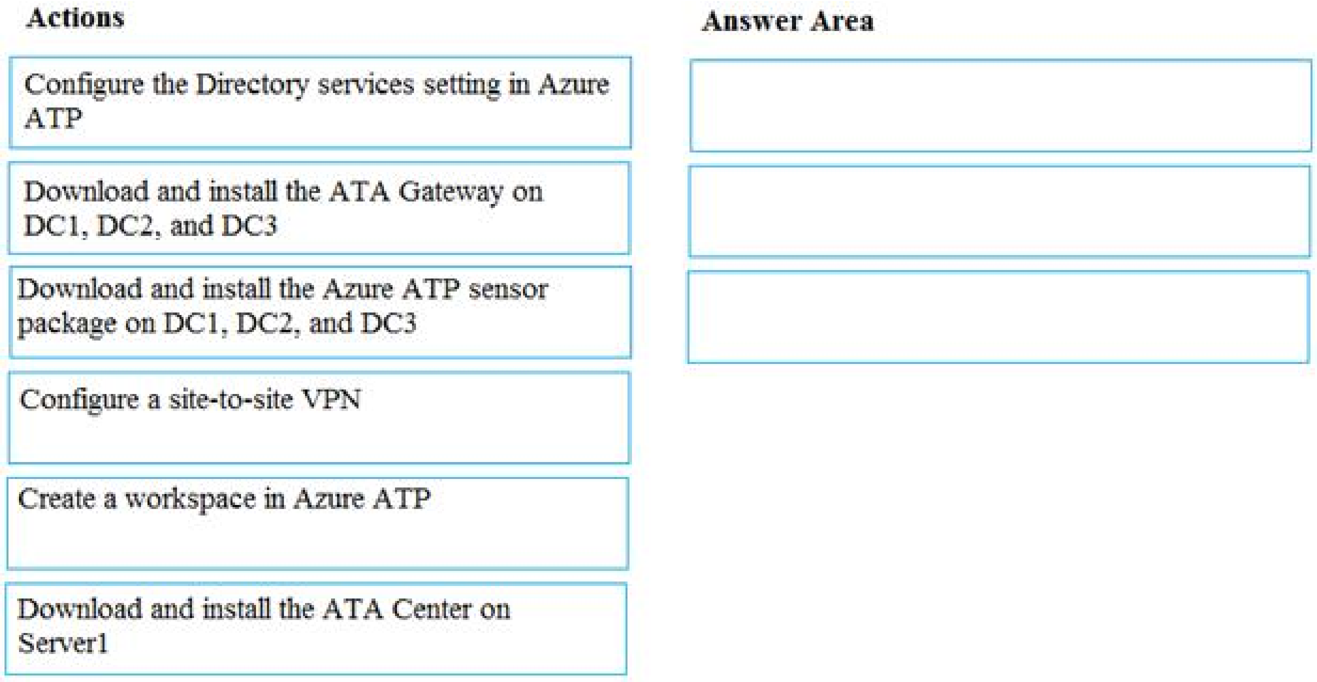
You need to recommend a solution that meets the technical and security requirements for sharing data with the partners.
What should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Create an access review.
B. Assign the Global administrator role to User1.
C. Assign the Guest inviter role to User1.
D. Modify the External collaboration settings in the Azure Active Directory admin center.

Answer: AC

NEW QUESTION 2

DRAG DROP
You need to configure threat detection for Active Directory. The solution must meet the security requirements.
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.



Actions

Configure the Directory services setting in Azure ATP

Download and install the ATA Gateway on DC1, DC2, and DC3

Download and install the Azure ATP sensor package on DC1, DC2, and DC3

Configure a site-to-site VPN

Create a workspace in Azure ATP

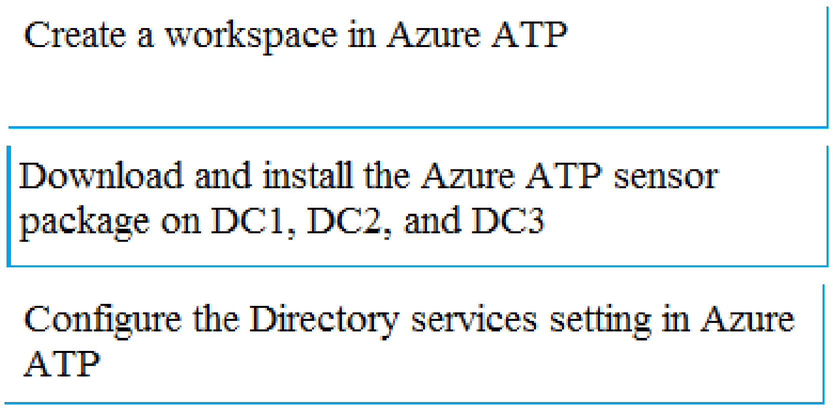
Download and install the ATA Center on Server1

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



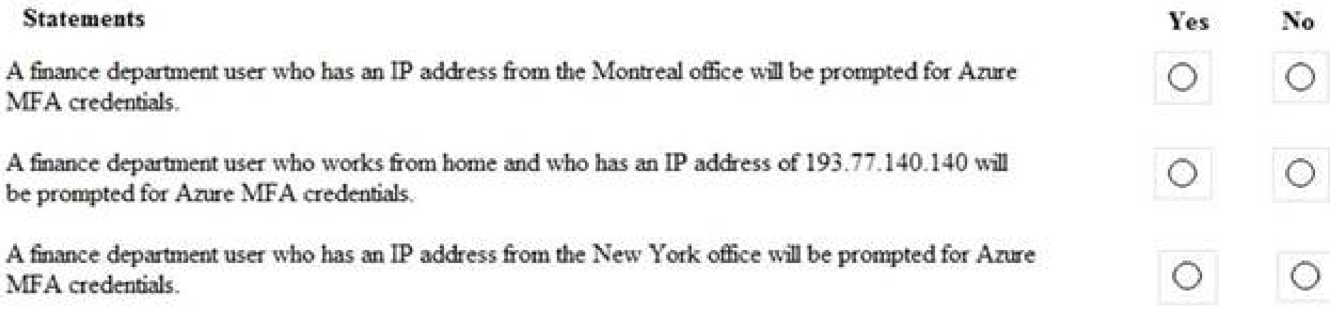
Create a workspace in Azure ATP

Download and install the Azure ATP sensor package on DC1, DC2, and DC3

Configure the Directory services setting in Azure ATP

NEW QUESTION 3

HOTSPOT
You are evaluating which finance department users will be prompted for Azure MFA credentials. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

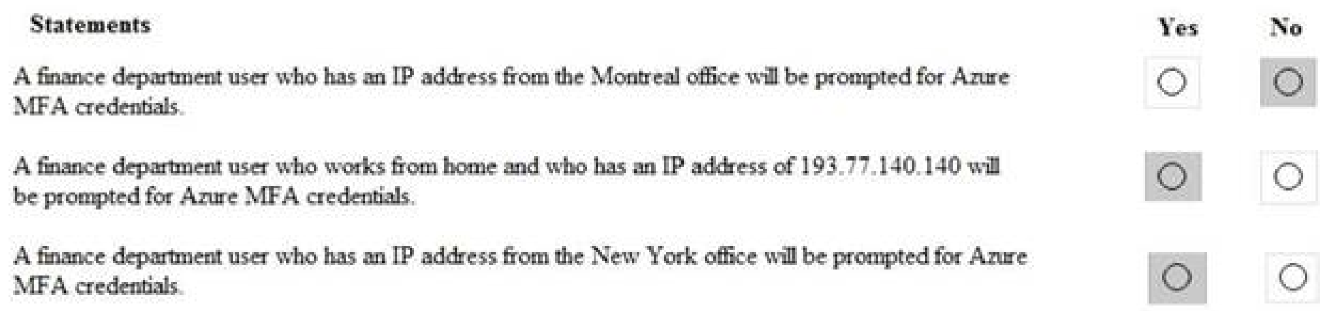


Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	○	○
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	○	○
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

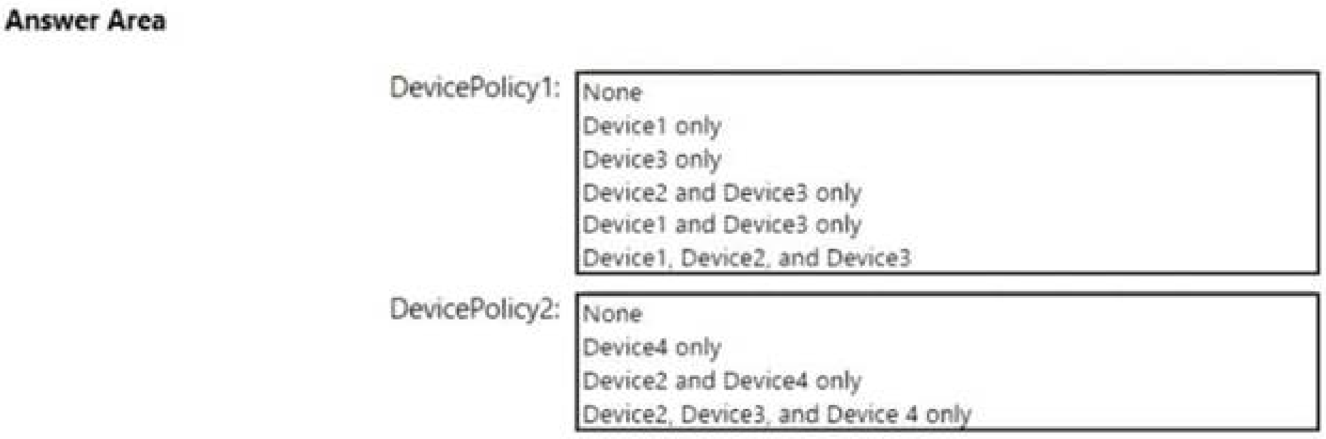


Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	○	[✓ ○]
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	[✓ ○]	○
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	[✓ ○]	○

NEW QUESTION 4

HOTSPOT

Which policies apply to which devices? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

DevicePolicy1:
- None
- Device1 only
- Device3 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device3

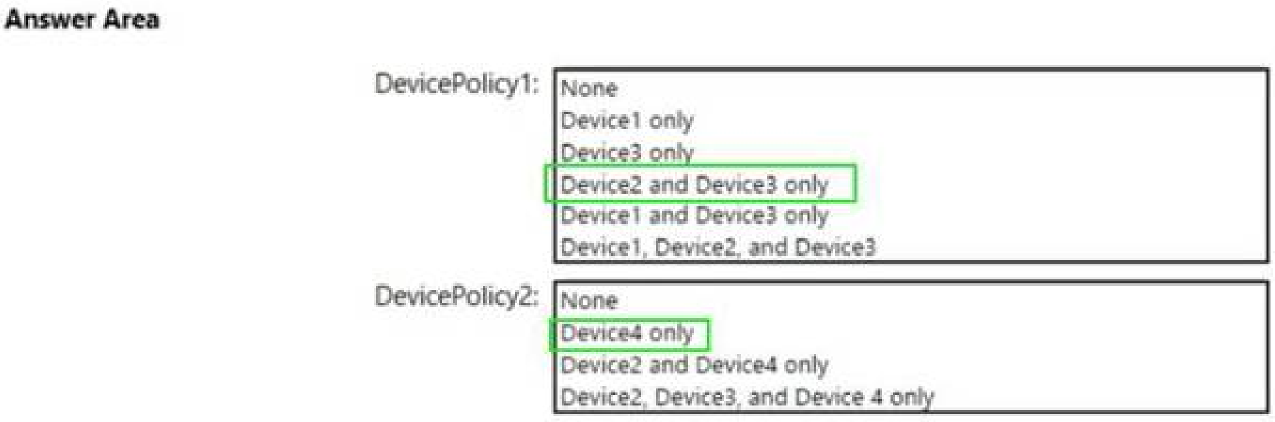
DevicePolicy2:
- None
- Device4 only
- Device2 and Device4 only
- Device2, Device3, and Device 4 only

A. Mastered

B. Not Mastered

Answer: A

Explanation:



Answer Area

DevicePolicy1:
- None
- Device1 only
- Device3 only
- [✓ Device2 and Device3 only]
- Device1 and Device3 only
- Device1, Device2, and Device3

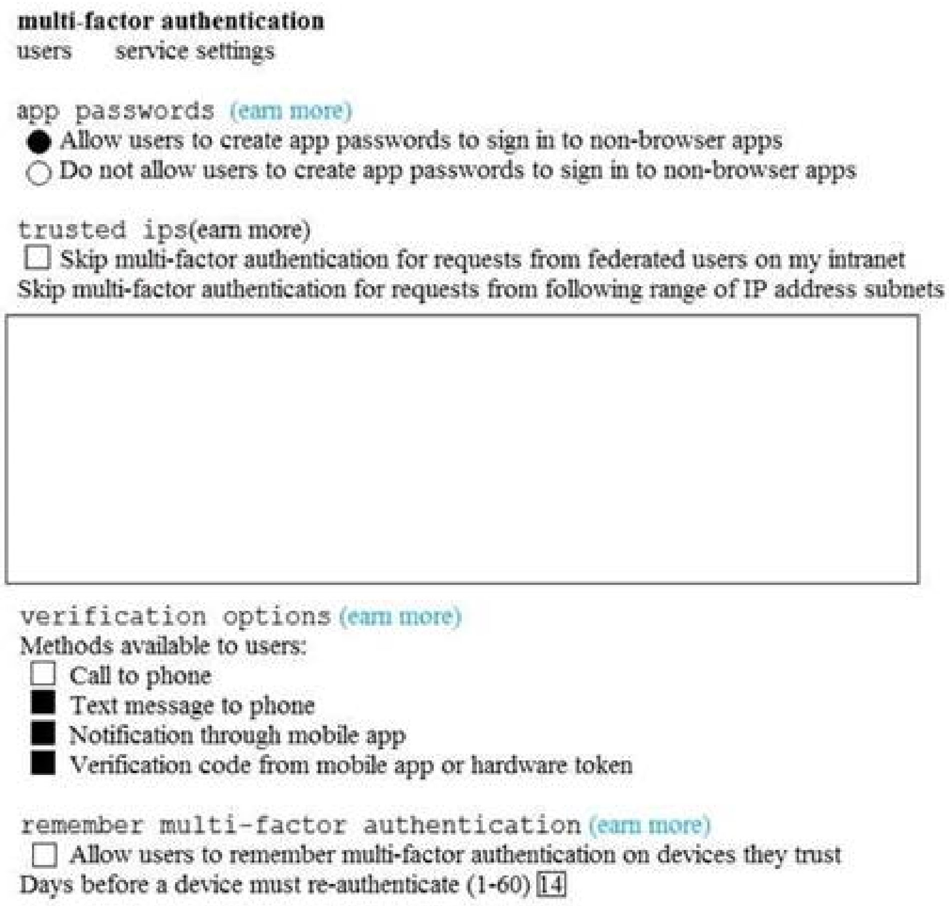
DevicePolicy2:
- None
- [✓ Device4 only]
- Device2 and Device4 only
- Device2, Device3, and Device 4 only

NEW QUESTION 5

HOTSPOT

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

The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Clock the Exhibit tab.)



multi-factor authentication
users service settings

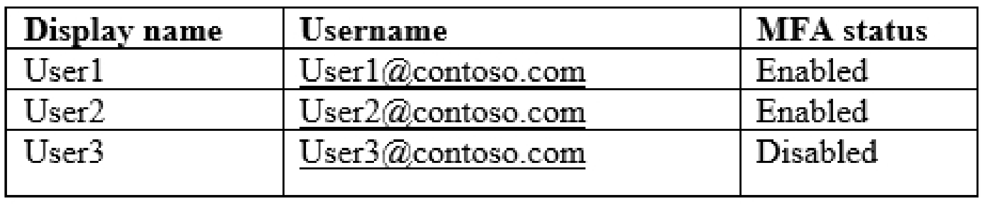
app passwords (earn more)
● Allow users to create app passwords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips(earn more)
□ Skip multi-factor authentication for requests from federated users on my intranet
Skip multi-factor authentication for requests from following range of IP address subnets

verification options (earn more)
Methods available to users:
□ Call to phone
■ Text message to phone
■ Notification through mobile app
■ Verification code from mobile app or hardware token

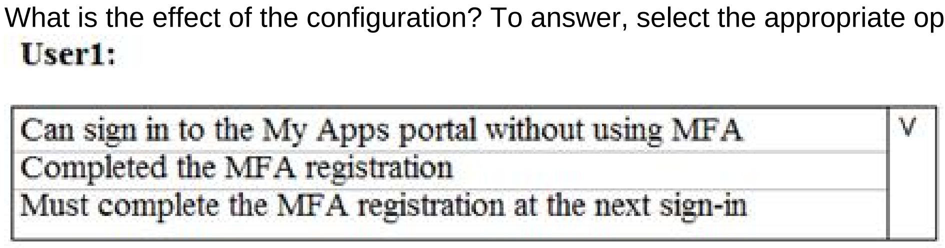
remember multi-factor authentication (earn more)
□ Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60) 14

In contoso.com, you create the users shown in the following table.



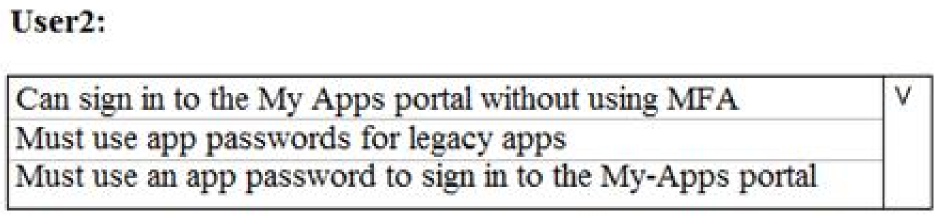
Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

What is the effect of the configuration? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



User1:

Can sign in to the My Apps portal without using MFA
Completed the MFA registration
Must complete the MFA registration at the next sign-in



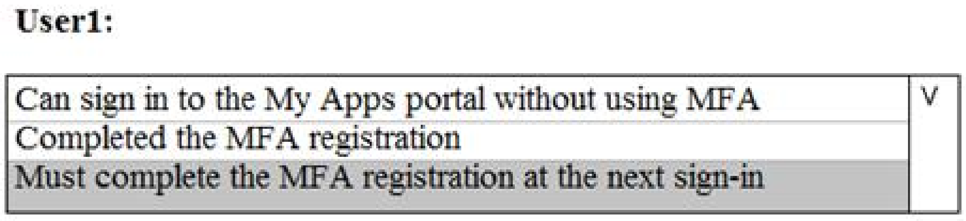
User2:

Can sign in to the My Apps portal without using MFA
Must use app passwords for legacy apps
Must use an app password to sign in to the My-Apps portal

A. Mastered
B. Not Mastered

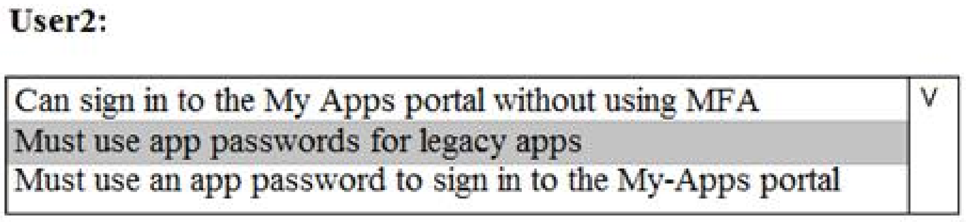
Answer: A

Explanation:



User1:

Can sign in to the My Apps portal without using MFA
Completed the MFA registration
Must complete the MFA registration at the next sign-in



User2:

Can sign in to the My Apps portal without using MFA
Must use app passwords for legacy apps
Must use an app password to sign in to the My-Apps portal

NEW QUESTION 6
You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune.
You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on- premises network.
What should you do first?

A. From the Azure Active Directory admin center, create a new certificate
B. Enable Application Proxy in Azure AD
C. From Active Directory Administrative Center, create a Dynamic Access Control policy
D. From the Azure Active Directory admin center, configure authentication methods

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn- connectivitywindows10

NEW QUESTION 7
You have a Microsoft 365 subscription.
From the Microsoft 365 admin center, you create a new user. You plan to assign the Reports reader role to the user.
You need to see the permissions of the Reports reader role. Which admin center should you use?

A. Azure Active Directory
B. Cloud App Security
C. Security & Compliance
D. Microsoft 365

Answer: A

NEW QUESTION 8
You have a Microsoft 365 subscription.
You need to ensure that all users who are assigned the Exchange administrator role have multi-factor authentication (MFA) enabled by default.
What should you use to achieve the goal?

A. Security & Compliance permissions
B. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
C. Microsoft Azure AD group management
D. Microsoft Office 365 user management

Answer: B

NEW QUESTION 9
You have a Microsoft 365 Enterprise E5 subscription.
You use Windows Defender Advanced Threat Protection (Windows Defender ATP). You plan to use Microsoft Office 365 Attack simulator.
What is a prerequisite for running Attack simulator?

A. Enable multi-factor authentication (MFA)
B. Configure Advanced Threat Protection (ATP)
C. Create a Conditional Access App Control policy for accessing Office 365
D. Integrate Office 365 Threat Intelligence and Windows Defender ATP

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

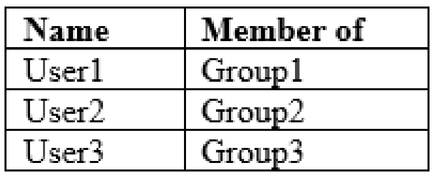
NEW QUESTION 10
You have a Microsoft 365 E5 subscription.
You implement Advanced Threat Protection (ATP) safe attachments policies for all users.
User reports that email messages containing attachments take longer than expected to be received. You need to reduce the amount of time it takes to receive email messages that contain attachments. The solution must ensure that all attachments are scanned for malware. Attachments that have malware must be blocked.
What should you do from ATP?

A. Set the action to Block
B. Add an exception
C. Add a condition
D. Set the action to Dynamic Delivery

Answer: D

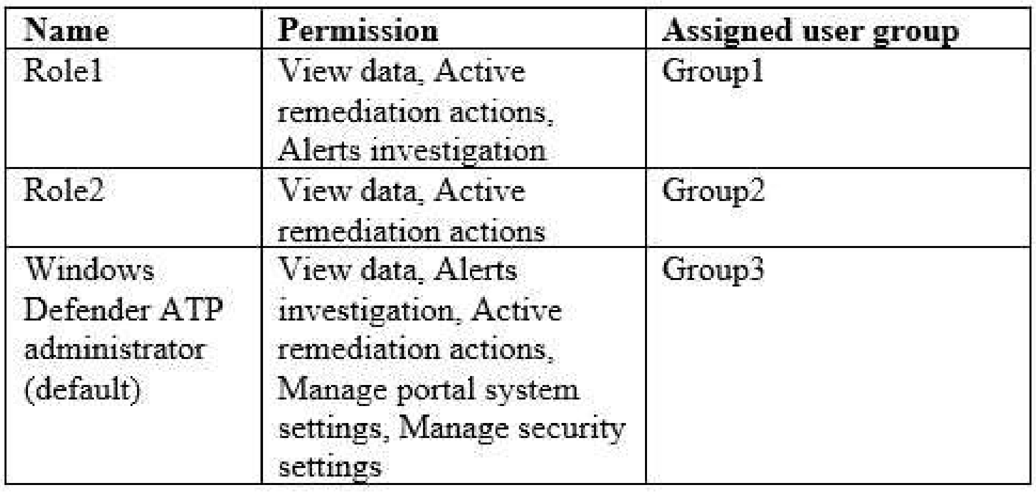
Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-previewing

NEW QUESTION 10
HOTSPOT
Your company has a Microsoft 365 subscription that contains the users shown in the following table.



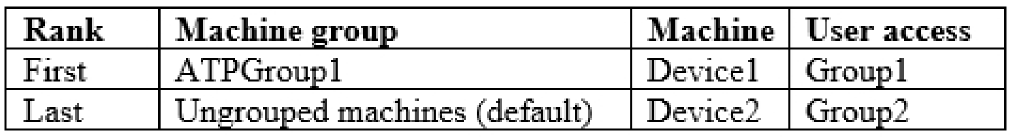
Name	Member of
User1	Group1
User2	Group2
User3	Group3

The company implements Windows Defender Advanced Threat Protection (Windows Defender ATP). Windows Defender ATP includes the roles shown in the following table:



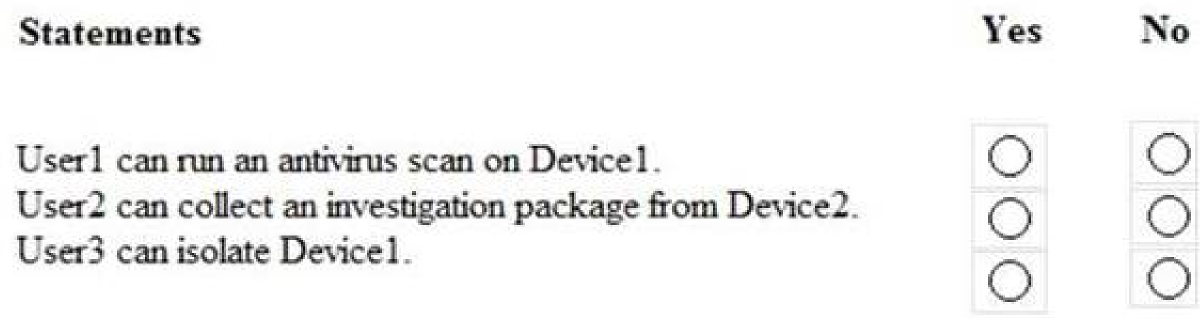
Name	Permission	Assigned user group
Role1	View data, Active remediation actions, Alerts investigation	Group1
Role2	View data, Active remediation actions	Group2
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Windows Defender ATP contains the machine groups shown in the following table:



Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

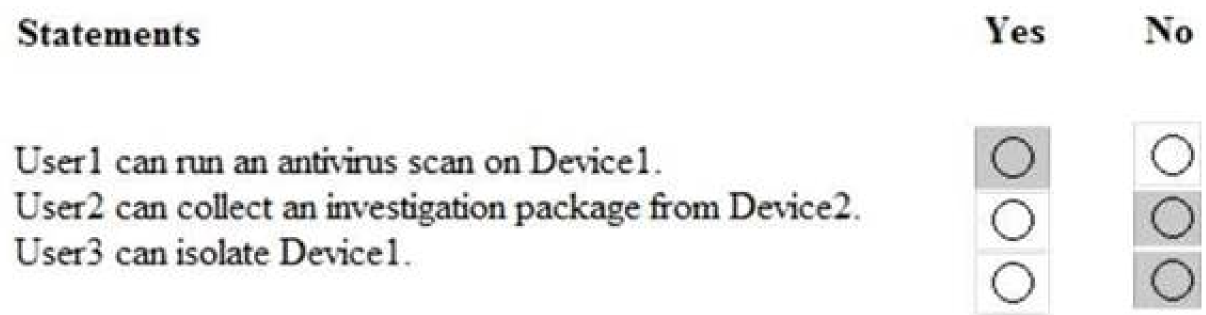


Statements	Yes	No
User1 can run an antivirus scan on Device1.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Statements	Yes	No
User1 can run an antivirus scan on Device1.	●	○
User2 can collect an investigation package from Device2.	○	●
User3 can isolate Device1.	○	●

NEW QUESTION 12
Your company uses Microsoft Azure Advanced Threat Protection (ATP).
You enable the delayed deployment of updates for an Azure ATP sensor named Sensor1. How long after the Azure ATP cloud service is updated will Sensor1 be updated?

A. 7 days
B. 24 hours
C. 1 hour
D. 48 hours
E. 12 hours

Answer: B

Explanation:
Note: The delay period was 24 hours. In ATP release 2.62, the 24 hour delay period has been increased to 72 hours.

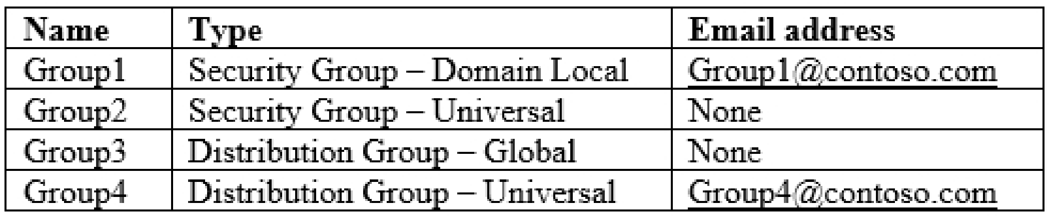
NEW QUESTION 16
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.
You add CompanyConfidential to a global policy.
A user protects an email message by using CompanyConfidential and sends the label to several external
recipients. The external recipients report that they cannot open the email message.
You need to ensure that the external recipients can open protected email messages sent to them. Solution: You modify the encryption settings of the label.
Does this meet the goal?

A. Yes
B. No

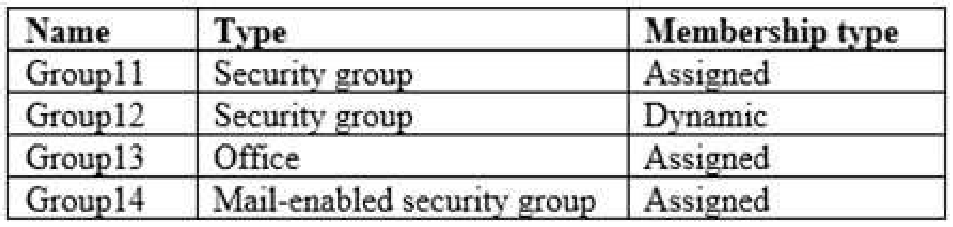
Answer: B

NEW QUESTION 20
HOTSPOT
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.



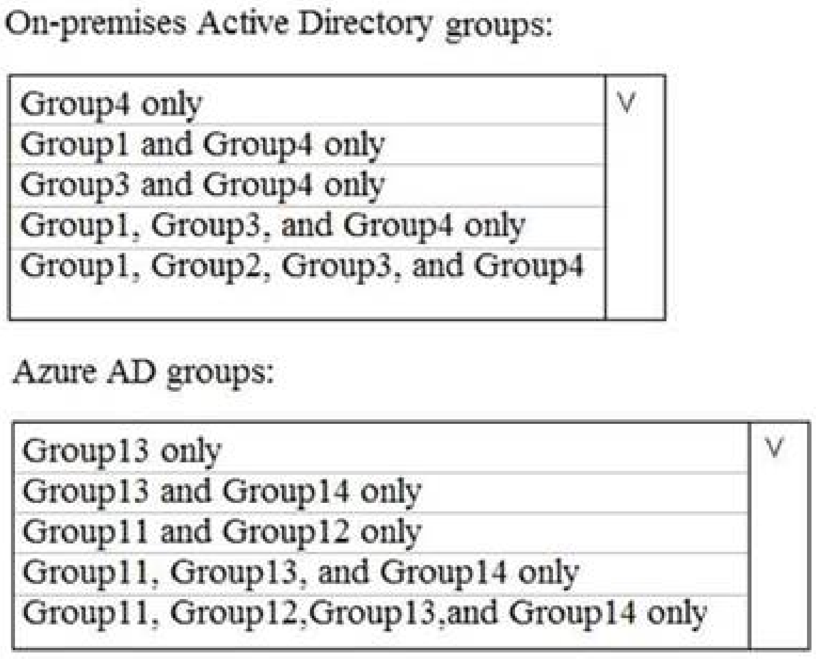
Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.



Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Office	Assigned
Group14	Mail-enabled security group	Assigned

You create an Azure Information Protection policy named Policy1. You need to apply Policy1.
To which groups can you apply Policy1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



On-premises Active Directory groups:

- Group4 only
- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Azure AD groups:

- Group13 only
- Group13 and Group14 only
- Group11 and Group12 only
- Group11, Group13, and Group14 only
- Group11, Group12,Group13,and Group14 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/prepare

NEW QUESTION 23
You have a Microsoft 365 subscription.
A user reports that changes were made to several files in Microsoft OneDrive.
You need to identify which files were modified by which users in the user's OneDrive. What should you do?

A. From the Azure Active Directory admin center, open the audit log
B. From the OneDrive admin center, select Device access
C. From Security & Compliance, perform an eDiscovery search
D. From Microsoft Cloud App Security, open the activity log

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/activity-filters

NEW QUESTION 27

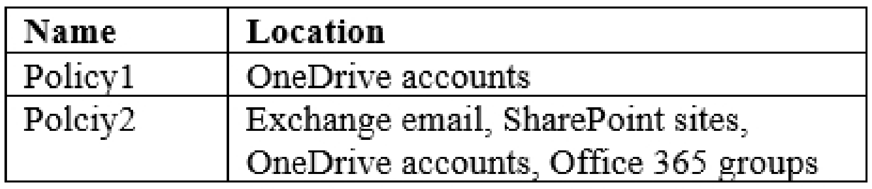
You have a Microsoft 365 subscription. You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. From the Cloud App Security admin center, create a file policy.
B. From the SharePoint admin center, modify the Site Settings.
C. From the SharePoint & Compliance admin center, create a label.
D. From the SharePoint admin center, modify the records management settings.
E. From the Security & Compliance admin center, publish a label.

Answer: CE

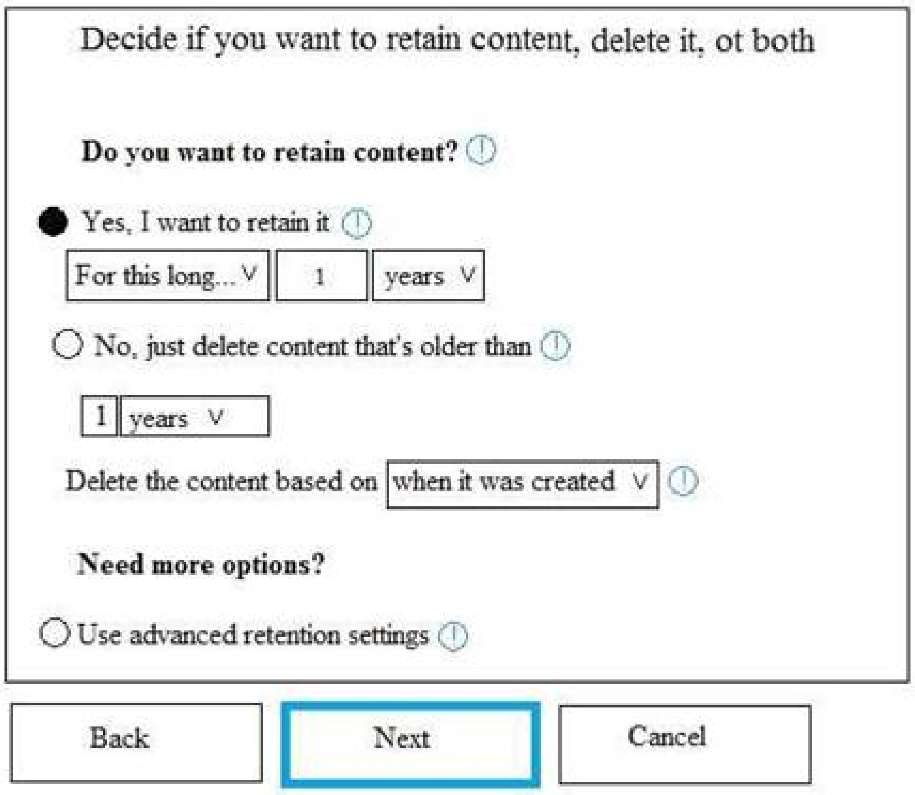
Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-office-365-labels-and-dlp

NEW QUESTION 28
HOTSPOT
You have a Microsoft 365 subscription. From the Security & Compliance admin center, you create the retention policies shown in the following table.



Name	Location
Policy1	OneDrive accounts
Polciy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

Policy1 if configured as showing in the following exhibit.



Decide if you want to retain content, delete it, ot both

Do you want to retain content?

● Yes, I want to retain it

For this long... ∨ | 1 | years ∨

○ No, just delete content that's older than

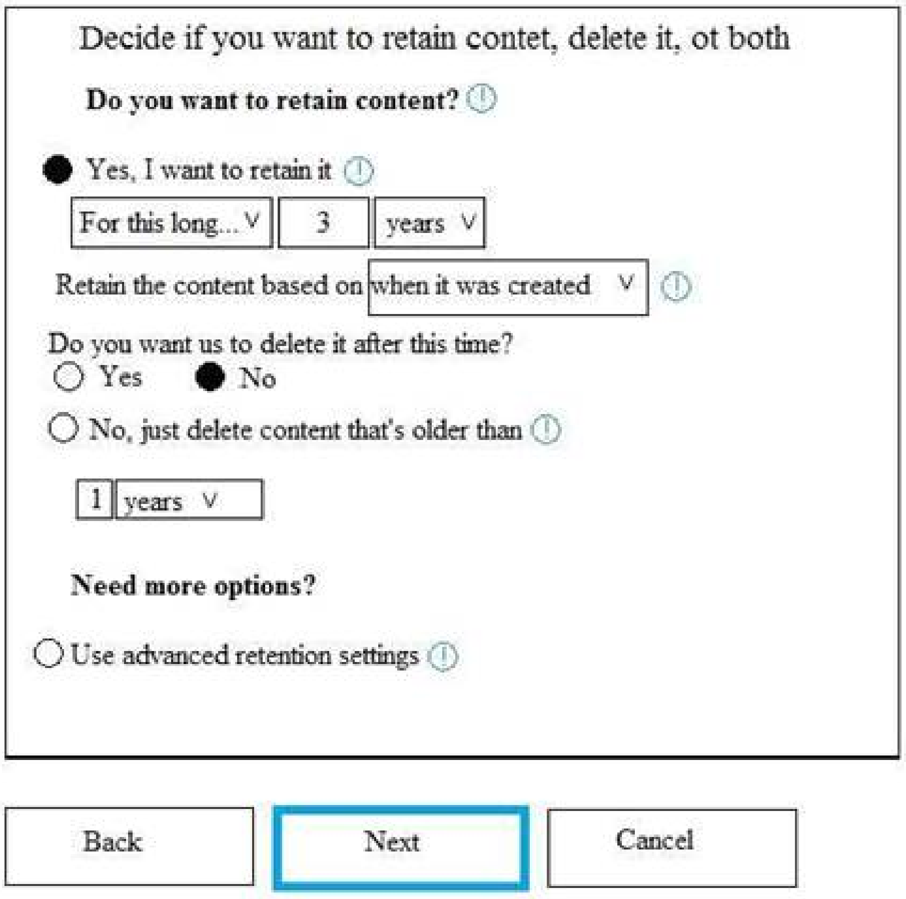
1 | years ∨

Delete the content based on when it was created ∨

Need more options?

○ Use advanced retention settings

Policy2 is configured as shown in the following exhibit.



Decide if you want to retain contet, delete it, ot both

Do you want to retain content?

● Yes, I want to retain it

For this long... ∨ | 3 | years ∨

Retain the content based on when it was created ∨

Do you want us to delete it after this time?
○ Yes ● No

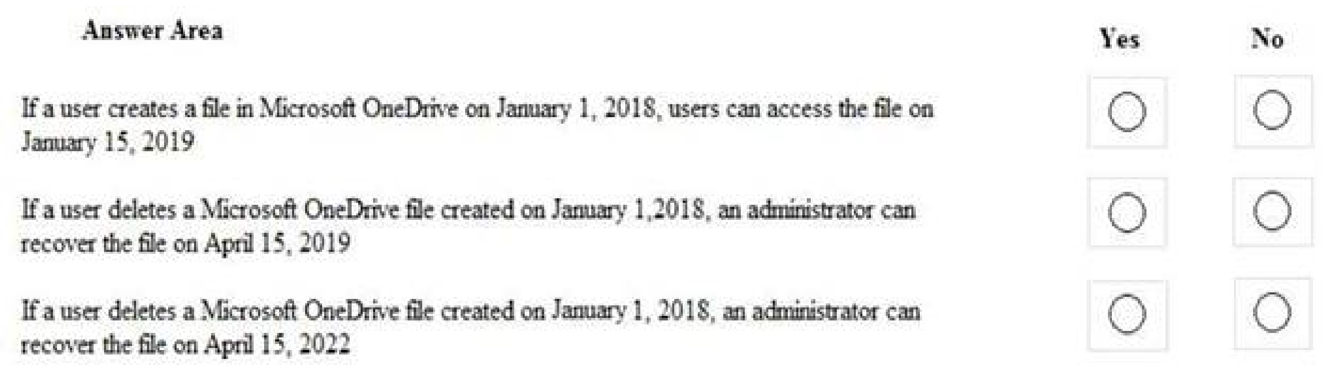
○ No, just delete content that's older than

1 | years ∨

Need more options?

○ Use advanced retention settings

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



Answer Area

	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	○	○
If a user deletes a Microsoft OneDrive file created on January 1,2018, an administrator can recover the file on April 15, 2019	○	○
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the-principles-of-retention-or-what-takes-precedence

NEW QUESTION 30
You have a Microsoft 365 subscription that includes a user named Admin1.
You need to ensure that Admin1 can preserve all the mailbox content of users, including their deleted items.
The solution must use the principle of least privilege. What should you do?

A. From the Microsoft 365 admin center, assign the Exchange administrator role to Admin1.
B. From the Exchange admin center, assign the Discovery Management admin role to Admin1.
C. From the Azure Active Directory admin center, assign the Service administrator role to Admin1.
D. From the Exchange admin center, assign the Recipient Management admin role to Admin1.

Answer: B

NEW QUESTION 34
You have a Microsoft 365 subscription.
Yesterday, you created retention labels and published the labels to Microsoft Exchange Online mailboxes.
You need to ensure that the labels will be available for manual assignment as soon as possible. What should you do?

A. From the Security & Compliance admin center, create a label policy
B. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning
C. From Exchange Online PowerShell, run Start-ManagedFolderAssistant
D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

Answer: C

NEW QUESTION 37
Your company has a main office and a Microsoft 365 subscription.
You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.
What should you include in the configuration?

A. a user risk policy
B. a sign-in risk policy
C. a named location in Azure Active Directory (Azure AD)
D. an Azure MFA Server

Answer: C

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

NEW QUESTION 39
You have a Microsoft 365 Enterprise E5 subscription.
You use Windows Defender Advanced Threat Protection (Windows Defender ATP).
You need to integrate Microsoft Office 365 Threat Intelligence and Windows Defender ATP. Where should you configure the integration?

A. From the Microsoft 365 admin center, select Settings, and then select Services & add-ins.
B. From the Security & Compliance admin center, select Threat management, and then select Explorer.
C. From the Microsoft 365 admin center, select Reports, and then select Security & Compliance.
D. From the Security & Compliance admin center, select Threat management and then select Threat tracker.

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-office-365-ti-with-wdatp

NEW QUESTION 40
Your network contains an on-premises Active Directory domain. The domain contains servers that run
Windows Server and have advanced auditing enabled.
The security logs of the servers are collected by using a third-party SIEM solution.
You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.
What should you do?

A. Configure auditing in the Office 365 Security & Compliance center.
B. Turn off Delayed updates for the Azure ATP sensors.
C. Modify the Domain synchronizer candidate’s settings on the Azure ATP sensors.
D. Integrate SIEM and Azure ATP.

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5

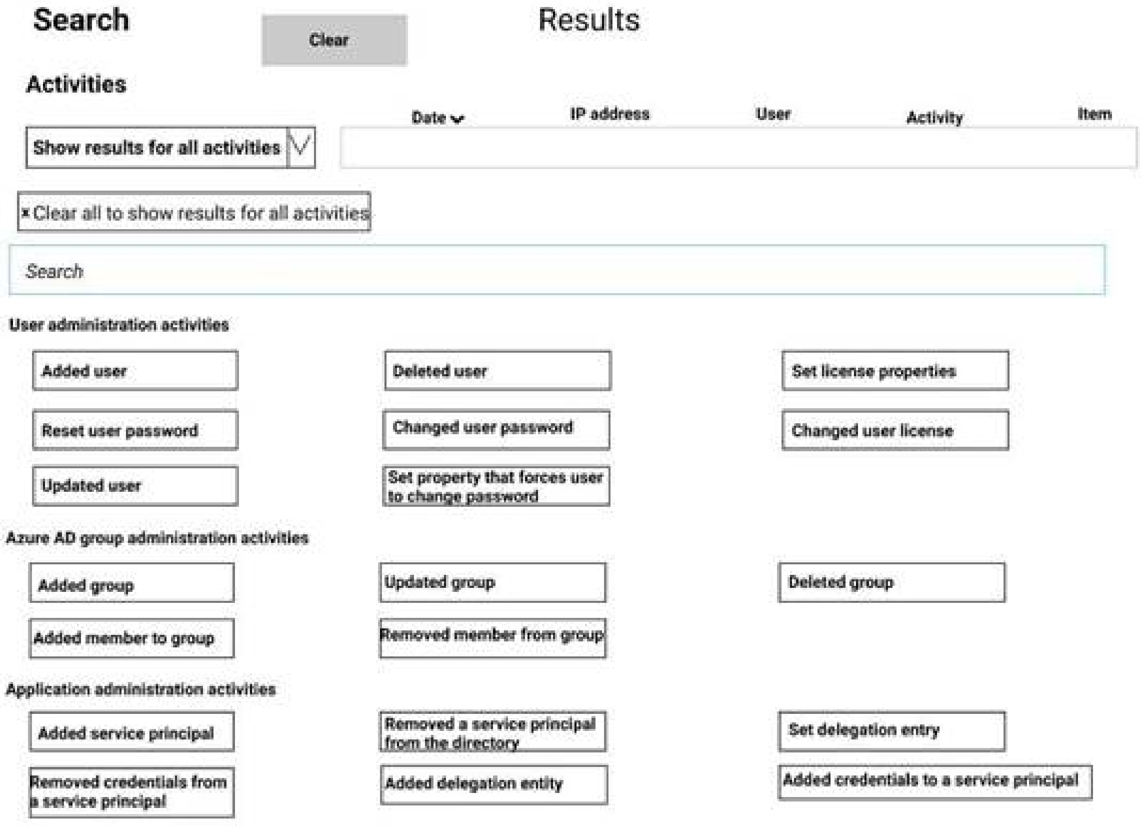
NEW QUESTION 44
You have a Microsoft 365 subscription.
A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.
You need to limit alert notifications to actionable DLP events.
What should you do?

A. From the Security & Compliance admin center, modify the Policy Tips of a DLP policy.
B. From the Cloud App Security admin center, apply a filter to the alerts.
C. From the Security & Compliance admin center, modify the User overrides settings of a DLP policy.
D. From the Security & Compliance admin center, modify the matched activities threshold of an alert policy.

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

NEW QUESTION 47
HOTSPOT
You have a Microsoft 365 subscription. Auditing is enabled.
A user named User1 is a member of a dynamic security group named Group1. You discover that User1 is no longer a member of Group1.
You need to search the audit log to identify why User1 was removed from Group1.
Which two actions should you use in the search? To answer, select the appropriate activities in the answer area.
NOTE: Each correct selection is worth one point.


Search
Clear
Results
Activities
Date
IP address
User
Activity
Item
Show results for all activities
×Clear all to show results for all activities
Search
User administration activities
Added user
Deleted user
Set license properties
Reset user password
Changed user password
Changed user license
Updated user
Set property that forces user to change password
Azure AD group administration activities
Added group
Updated group
Deleted group
Added member to group
Removed member from group
Application administration activities
Added service principal
Removed a service principal from the directory
Set delegation entry
Removed credentials from a service principal
Added delegation entity
Added credentials to a service principal

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

NEW QUESTION 49
You have a Microsoft 365 subscription.
All users are assigned a Microsoft 365 E5 license. How long will auditing data be retained?

A. 30 days
B. 90 days
C. 365 days
D. 5 years

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

NEW QUESTION 54
You have a Microsoft 365 subscription.
You have a team named Team1 in Microsoft Teams. You plan to place all the content in Team1 on hold.
You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.
Which cmdlet should you use?

A. Get-UnifiedGroup
B. Get-MailUser
C. Get-TeanMessagingSettings
D. Get-TeamChannel

Answer: A

NEW QUESTION 59
Several users in your Microsoft 365 subscription report that they received an email message without the attachment. You need to review the attachments that were removed from the messages. Which two tools can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. the Exchange admin center
B. the Azure ATP admin center
C. Microsoft Azure Security Center
D. the Security & Compliance admin center
E. Outlook on the web

Answer: AD

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages- and-files

NEW QUESTION 60
You have a Microsoft 365 subscription. You enable auditing for the subscription.
You plan to provide a user named Auditor with the ability to review audit logs. You add Auditor to the Global administrator role group.
Several days later, you discover that Auditor disabled auditing.
You remove Auditor from the Global administrator role group and enable auditing.

A. Security operator
B. Security reader
C. Security administrator
D. Compliance administrator

Answer: D

NEW QUESTION 64
Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.
The security logs of the servers are collected by using a third-party SIEM solution.
You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.
What should you do?

A. Configure Event Forwarding on the domain controllers
B. Configure auditing in the Office 365 Security & Compliance center.
C. Turn on Delayed updates for the Azure ATP sensors.
D. Enable the Audit account management Group Policy setting for the servers.

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

NEW QUESTION 68

......