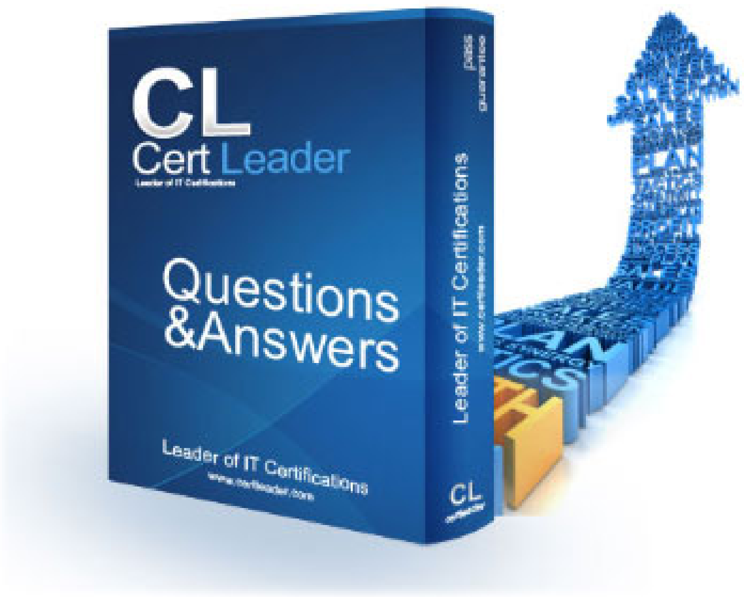
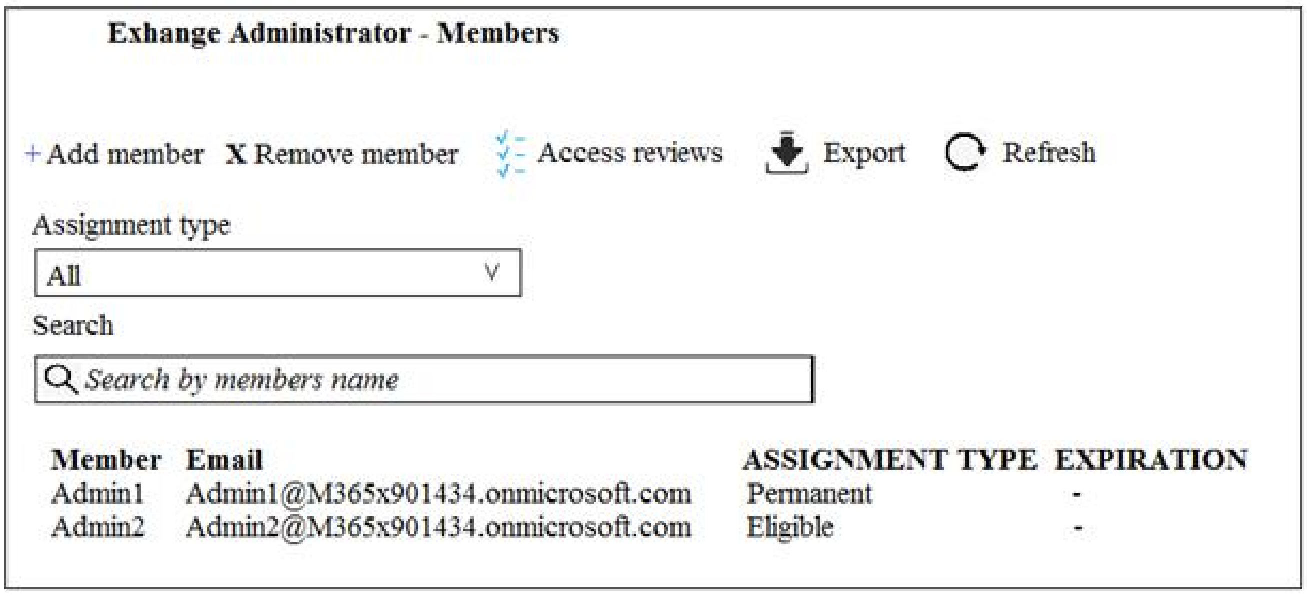
MS-500 Dumps

Microsoft 365 Security Administrator

https://www.certleader.com/MS-500-dumps.html



NEW QUESTION 1
An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.



Exhange Administrator - Members

Assignment type: All

Search: Search by members name

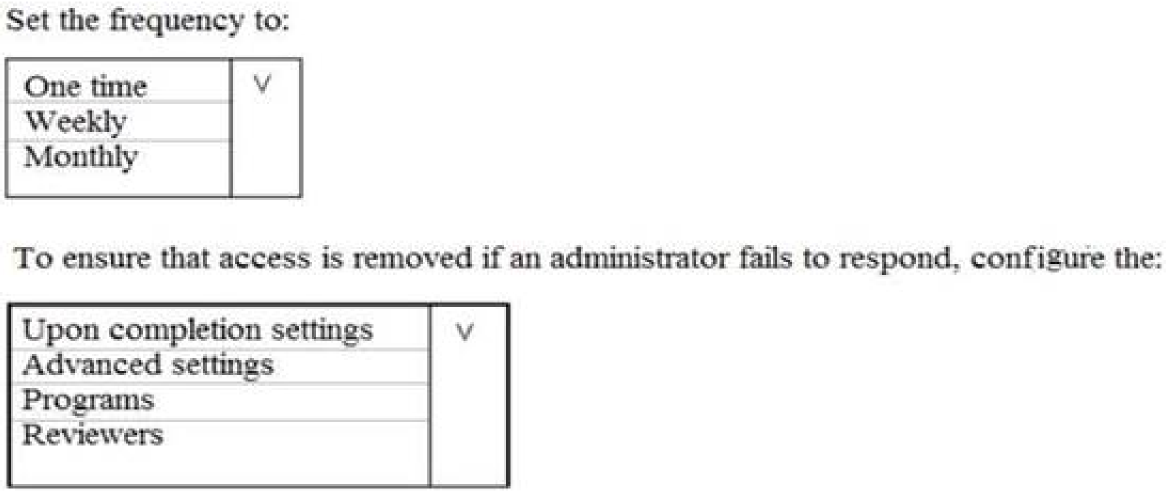
Member	Email	ASSIGNMENT TYPE	EXPIRATION
Admin1	Admin1@M365x901434.onmicrosoft.com	Permanent	-
Admin2	Admin2@M365x901434.onmicrosoft.com	Eligible	-

What should you do to meet the security requirements?

A. Change the Assignment Type for Admin2 to Permanent
B. From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
C. From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
D. Change the Assignment Type for Admin1 to Eligible

Answer: D

NEW QUESTION 2
HOTSPOT
You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.
Which other settings should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Set the frequency to:

- One time
- Weekly
- Monthly

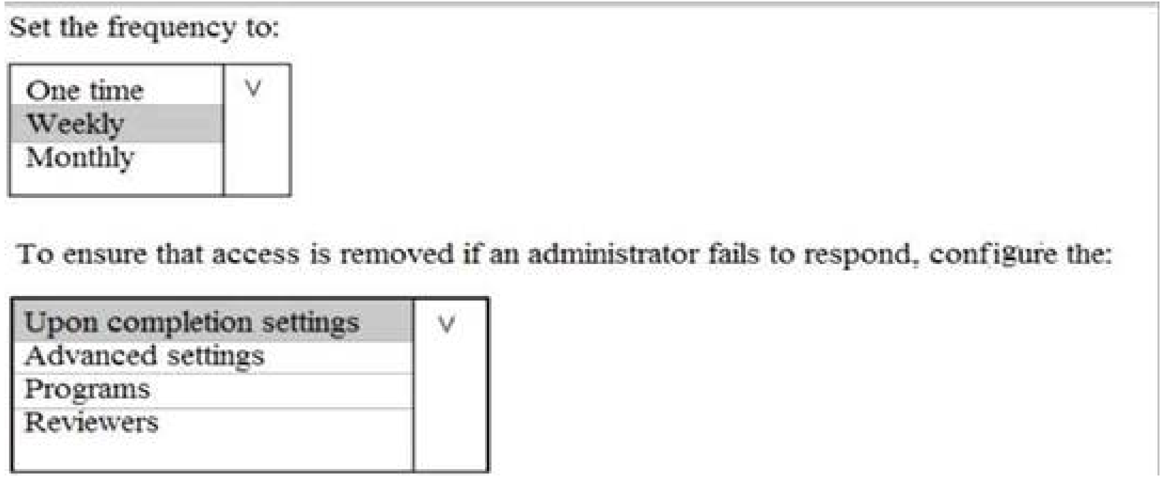
To ensure that access is removed if an administrator fails to respond, configure the:

- Upon completion settings
- Advanced settings
- Programs
- Reviewers

A. Mastered
B. Not Mastered

Answer: A

Explanation:



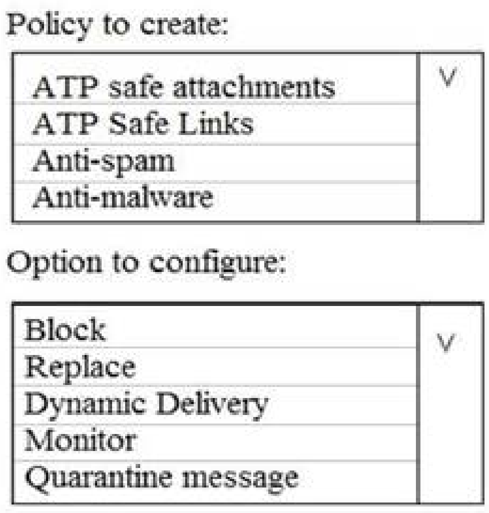
Set the frequency to:

- One time
- Weekly
- Monthly

To ensure that access is removed if an administrator fails to respond, configure the:

- Upon completion settings
- Advanced settings
- Programs
- Reviewers

NEW QUESTION 3
HOTSPOT
You need to recommend an email malware solution that meets the security requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Policy to create:

- ATP safe attachments
- ATP Safe Links
- Anti-spam
- Anti-malware

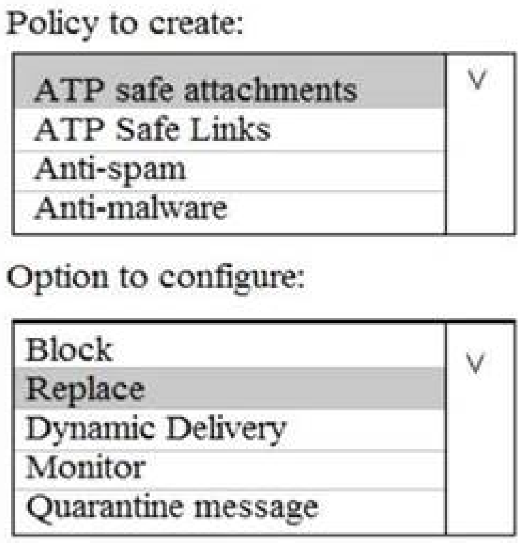
Option to configure:

- Block
- Replace
- Dynamic Delivery
- Monitor
- Quarantine message

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Policy to create:

- ATP safe attachments
- ATP Safe Links
- Anti-spam
- Anti-malware

Option to configure:

- Block
- Replace
- Dynamic Delivery
- Monitor
- Quarantine message

NEW QUESTION 4

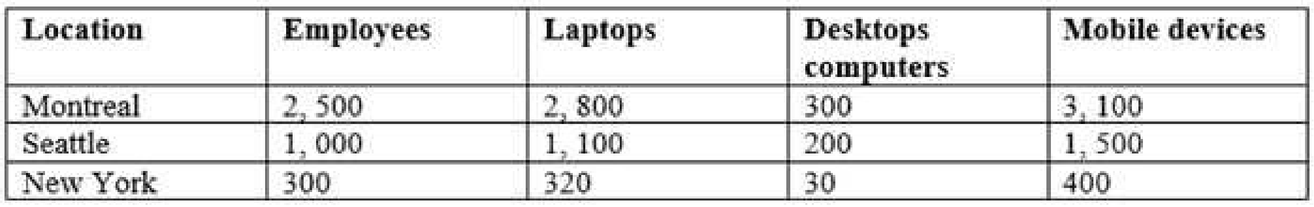
You need to implement Windows Defender ATP to meet the security requirements. What should you do?

A. Configure port mirroring
B. Create the ForceDefenderPassiveMode registry setting
C. Download and install the Microsoft Monitoring Agent
D. Run WindowsDefenderATPOnboardingScript.cmd

Answer: C

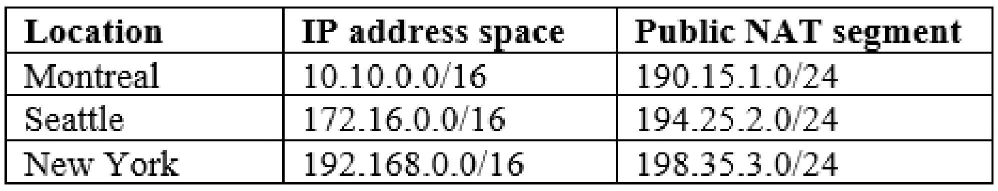
Explanation:

Case Study: 3 Contoso, Ltd Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, and New York.
The company has the offices shown in the following table.



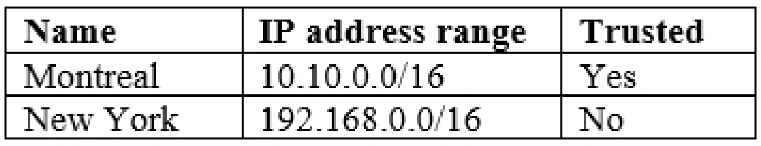
Location	Employees	Laptops	Desktops computers	Mobile devices
Montreal	2, 500	2, 800	300	3, 100
Seattle	1, 000	1, 100	200	1, 500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.
Existing Environment Infrastructure
The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.
The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.
Each client computer has a single volume.
Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.



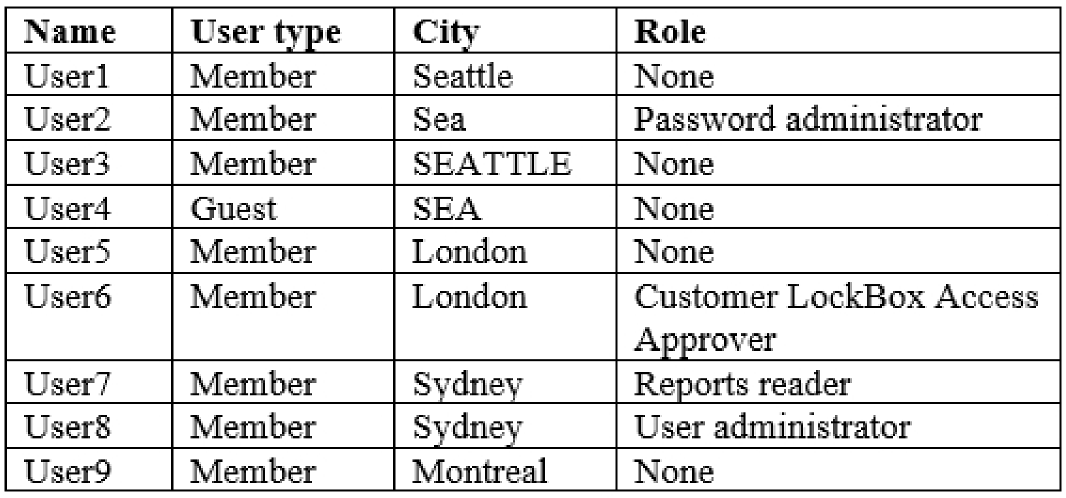
Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.



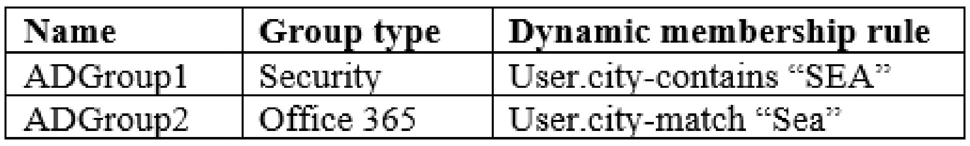
Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.
Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department. The tenant contains the users shown in the following table.



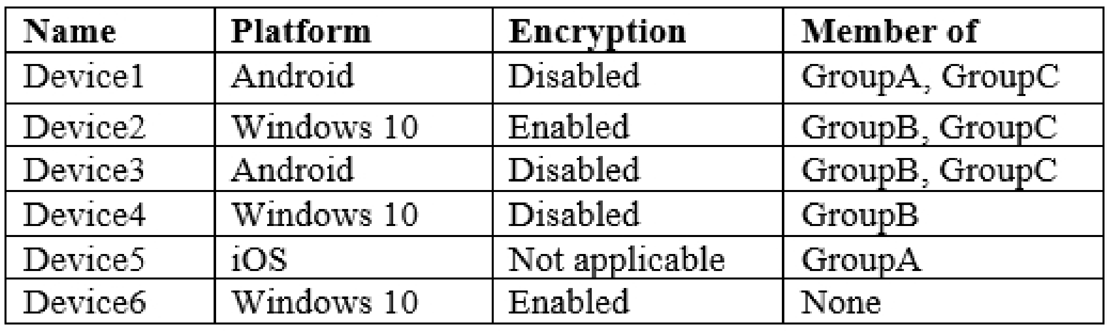
Name	User type	City	Role
User1	Member	Seattle	None
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	None
User4	Guest	SEA	None
User5	Member	London	None
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	None

The tenant contains the groups shown in the following table.



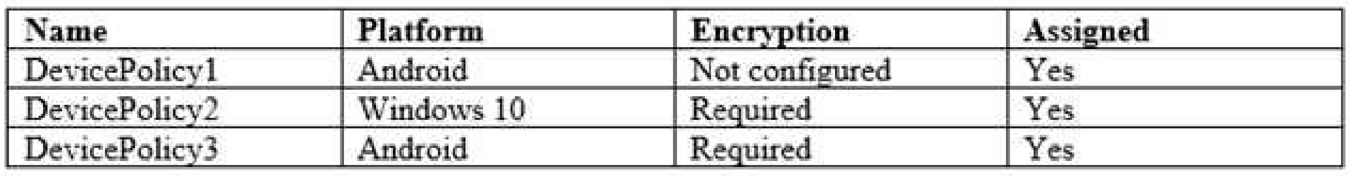
Name	Group type	Dynamic membership rule
ADGroup1	Security	User.city-contains "SEA"
ADGroup2	Office 365	User.city-match "Sea"

Customer Lockbox is enabled in Microsoft 365. Microsoft Intune Configuration
The devices enrolled in Intune are configured as shown in the following table.



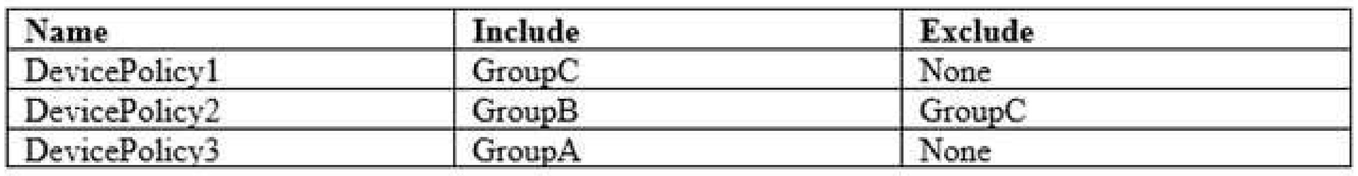
Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	Not applicable	GroupA
Device6	Windows 10	Enabled	None

The device compliance policies in Intune are configured as shown in the following table.



Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

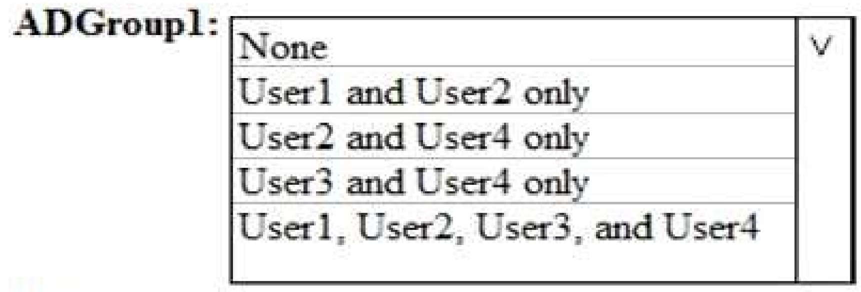
The device compliance policies have the assignments shown in the following table.



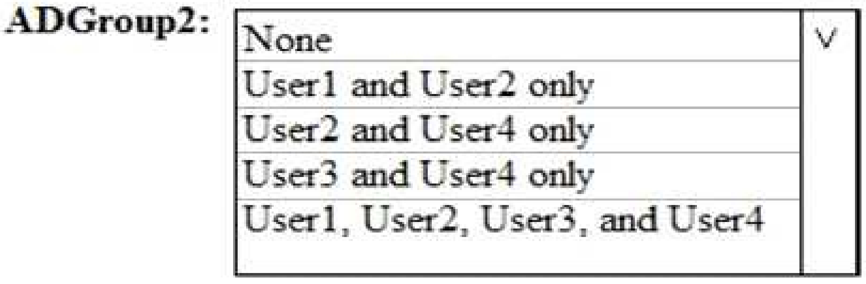
Name	Include	Exclude
DevicePolicy1	GroupC	None
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	None

The Mark devices with no compliance policy assigned as setting is set to Compliant.
Requirements
Technical Requirements
Contoso identifies the following technical requirements:
•Use the principle of least privilege
•Enable User1 to assign the Reports reader role to users
•Ensure that User6 approves Customer Lockbox requests as quickly as possible
•Ensure that User9 can implement Azure AD Privileged Identity Management

NEW QUESTION 5
HOTSPOT
Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



ADGroup1:
- None
- User1 and User2 only
- User2 and User4 only
- User3 and User4 only
- User1, User2, User3, and User4



ADGroup2:
- None
- User1 and User2 only
- User2 and User4 only
- User3 and User4 only
- User1, User2, User3, and User4

A. Mastered

B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

NEW QUESTION 6
Which user passwords will User2 be prevented from resetting?

A. User6 and User7
B. User4 and User6
C. User4 only
D. User7 and User8
E. User8 only

Answer: C

NEW QUESTION 7
You need to meet the technical requirements for User9. What should you do?

A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9
B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9
C. Assign the Security administrator role to User9
D. Assign the Global administrator role to User9

Answer: A

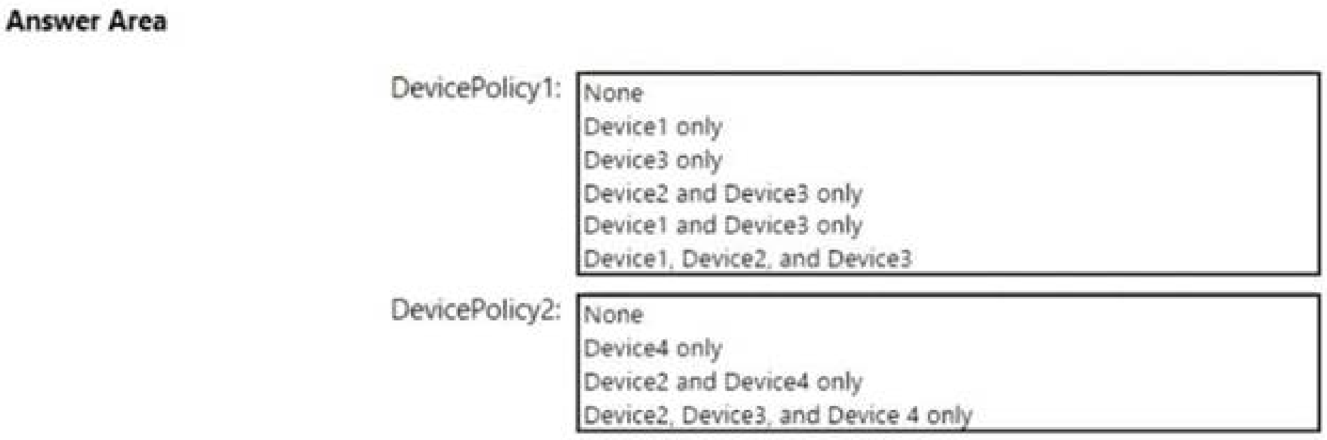
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access-to-pim

NEW QUESTION 8
What should User6 use to meet the technical requirements?

A. Supervision in the Security & Compliance admin center
B. Service requests in the Microsoft 365 admin center
C. Security & privacy in the Microsoft 365 admin center
D. Data subject requests in the Security & Compliance admin center

Answer: B

NEW QUESTION 9
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

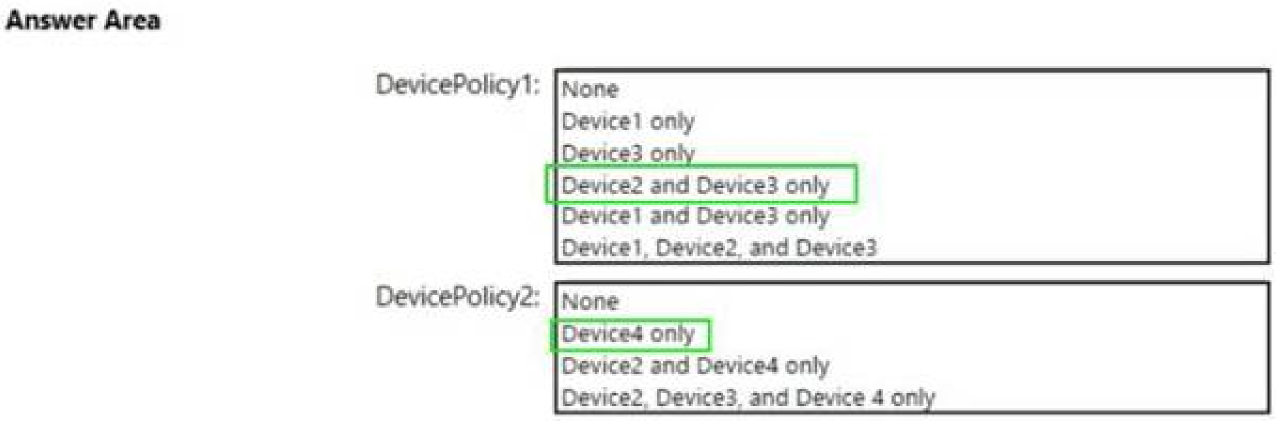
DevicePolicy1:
None
Device1 only
Device3 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

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

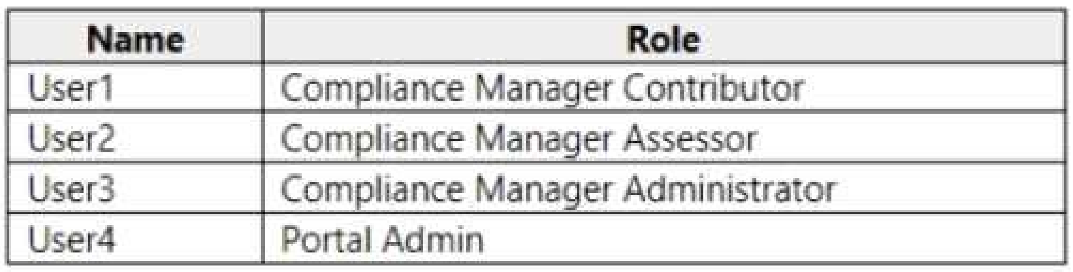
DevicePolicy2:
None
[✓ Device4 only]
Device2 and Device4 only
Device2, Device3, and Device 4 only

NEW QUESTION 10

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 365 subscription that contains the users shown in the following table.



Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports. The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend assigning the Compliance Manager Reader role to User1. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 10

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 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

•Source Anchor: objectGUID
•Password Hash Synchronization: Disabled
•Password writeback: Disabled
•Directory extension attribute sync: Disabled
•Azure AD app and attribute filtering: Disabled
•Exchange hybrid deployment: Disabled
•User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution: You modify the Azure AD app and attribute filtering settings.

Does that meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 14

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 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

•Source Anchor: objectGUID
•Password Hash Synchronization: Disabled
•Password writeback: Disabled
•Directory extension attribute sync: Disabled
•Azure AD app and attribute filtering: Disabled
•Exchange hybrid deployment: Disabled
•User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Source Anchor settings.

Does that meet the goal?

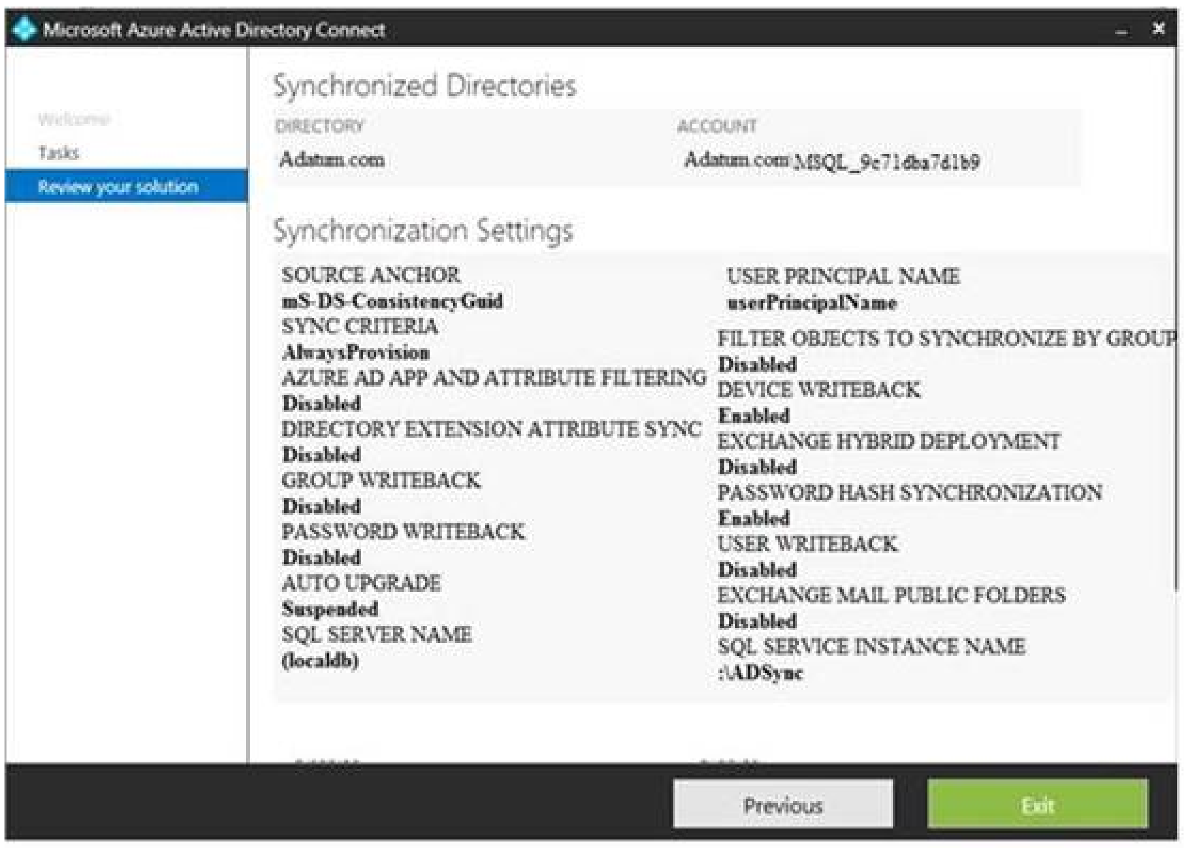
A. Yes
B. No

Answer: B

NEW QUESTION 16

HOTSPOT

You configure Microsoft Azure Active Directory (Azure AD) Connect as shown in the following exhibit.



Synchronized Directories

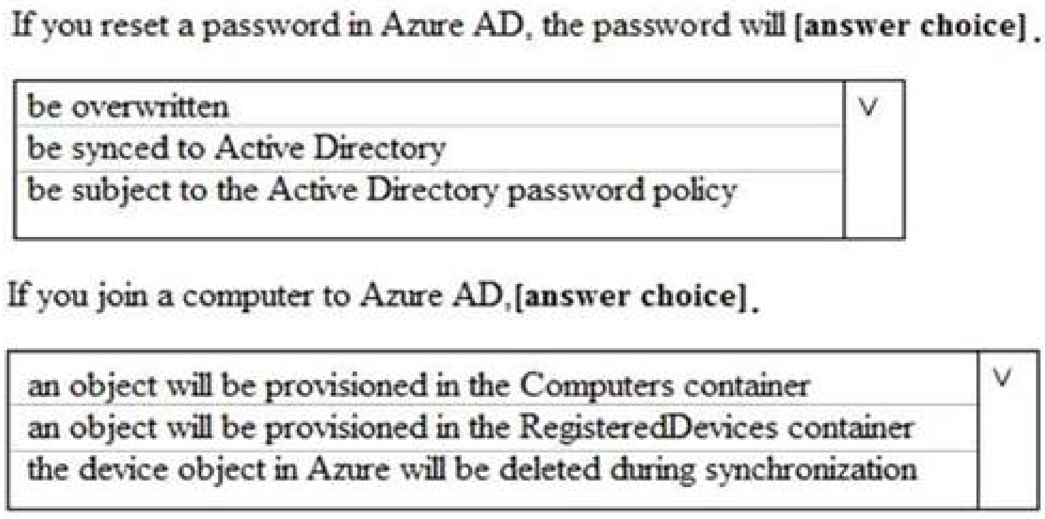
DIRECTORY	ACCOUNT
Adatum.com	Adatum.com\MSQL_9e71dba7d1b9

Synchronization Settings

SOURCE ANCHOR
mS-DS-ConsistencyGuid
SYNC CRITERIA
AlwaysProvision
AZURE AD APP AND ATTRIBUTE FILTERING
Disabled
DIRECTORY EXTENSION ATTRIBUTE SYNC
Disabled
GROUP WRITEBACK
Disabled
PASSWORD WRITEBACK
Disabled
AUTO UPGRADE
Suspended
SQL SERVER NAME
(localdb)

USER PRINCIPAL NAME
userPrincipalName
FILTER OBJECTS TO SYNCHRONIZE BY GROUP
Disabled
DEVICE WRITEBACK
Enabled
EXCHANGE HYBRID DEPLOYMENT
Disabled
PASSWORD HASH SYNCHRONIZATION
Enabled
USER WRITEBACK
Disabled
EXCHANGE MAIL PUBLIC FOLDERS
Disabled
SQL SERVICE INSTANCE NAME
:\ADSync

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.



If you reset a password in Azure AD, the password will **[answer choice]**.

- be overwritten
- be synced to Active Directory
- be subject to the Active Directory password policy

If you join a computer to Azure AD,**[answer choice]**.

- an object will be provisioned in the Computers container
- an object will be provisioned in the RegisteredDevices container
- the device object in Azure will be deleted during synchronization

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback

NEW QUESTION 17
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 22
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 23
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 27
You have a Microsoft 365 subscription.
You create an Advanced Threat Protection (ATP) safe attachments policy to quarantine malware. You need to configure the retention duration for the attachments in quarantine.
Which type of threat management policy should you create from the Security&Compliance admin center?

A. ATP anti-phishing
B. DKIM
C. Anti-spam
D. Anti-malware

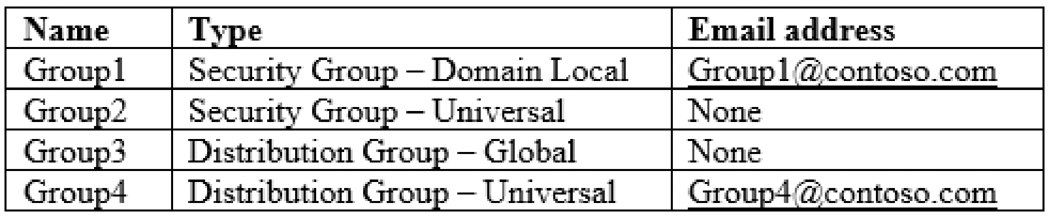
Answer: D

NEW QUESTION 31
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 create a new label in the global policy and instruct the user to resend the email message.
Does this meet the goal?

A. Yes
B. No

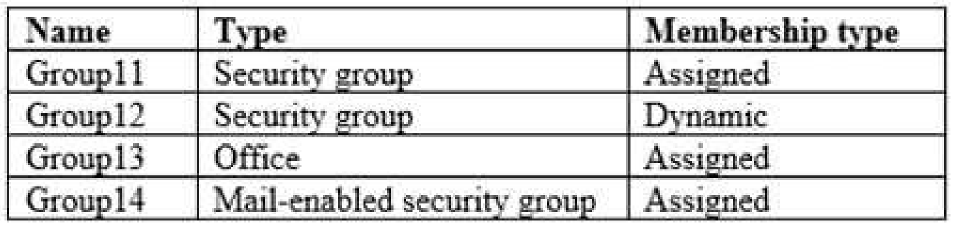
Answer: A

NEW QUESTION 34
HOTSPOT
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.



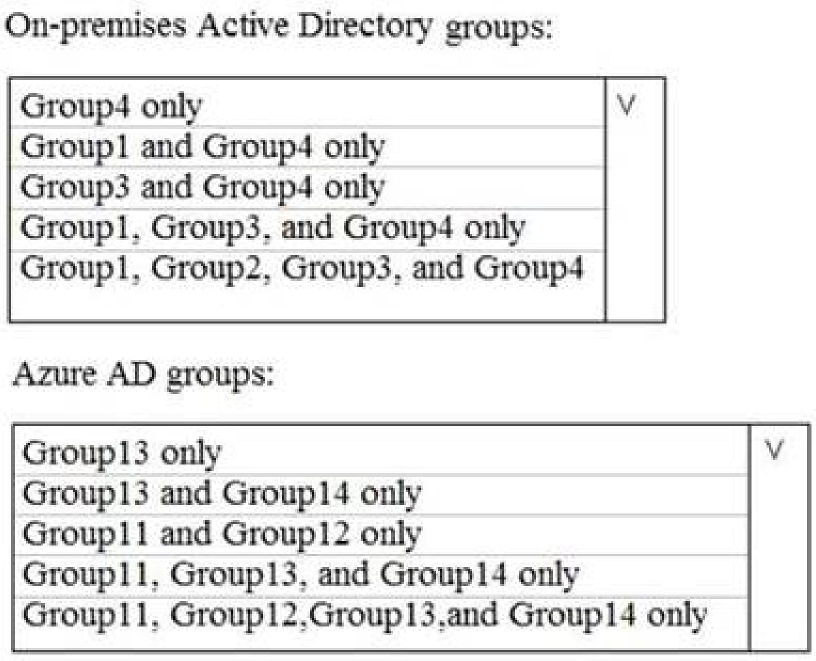
Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

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:

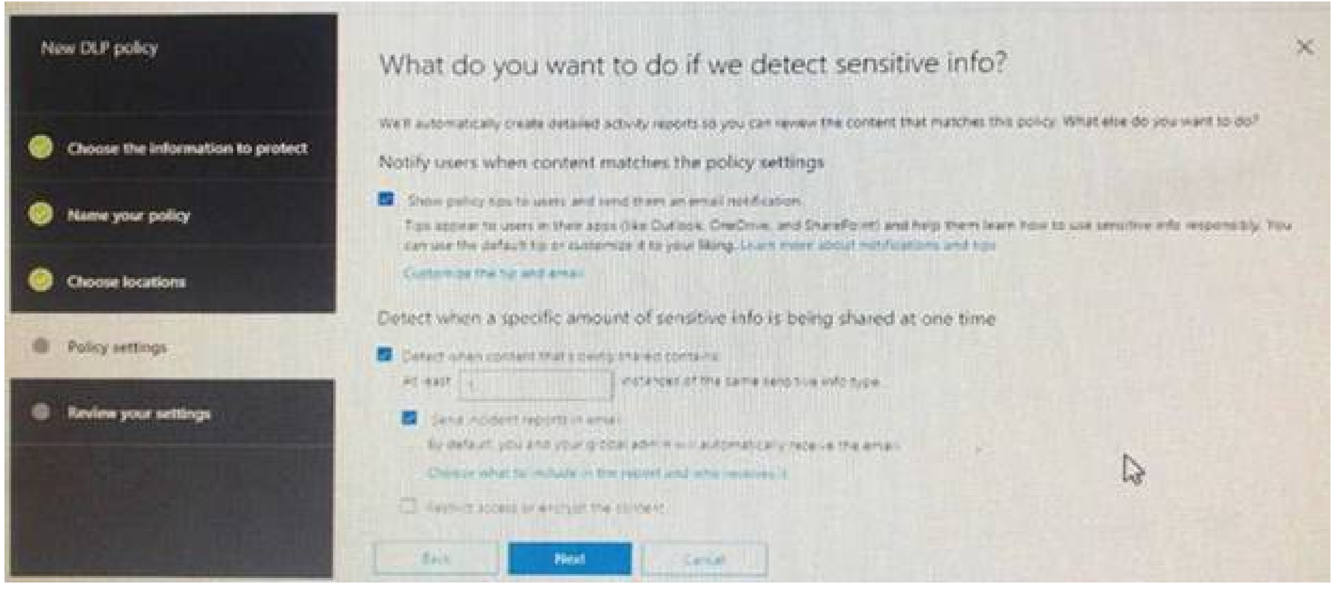
- Group13 only
- Group13 and Group14 only
- Group11 and Group12 only
- Group11, Group13, and Group14 only
- Group11, Group12,Group13,and Group14 only

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 37
You create a data loss prevention (DLP) policy as shown in the following shown:



What do you want to do if we detect sensitive info?

We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?

Notify users when content matches the policy settings

☑ Show policy tips to users and send them an email notification.
Tips appear to users in their apps (like Outlook, OneDrive, and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. Learn more about notifications and tips
Customize the tip and email

Detect when a specific amount of sensitive info is being shared at one time

☑ Detect when content that's being shared contains:
At least 1 instances of the same sensitive info type.
☑ Send incident reports in email
By default, you and your global admin will automatically receive the email.
Choose what to include in the report and who receives it
□ Restrict access or encrypt the content

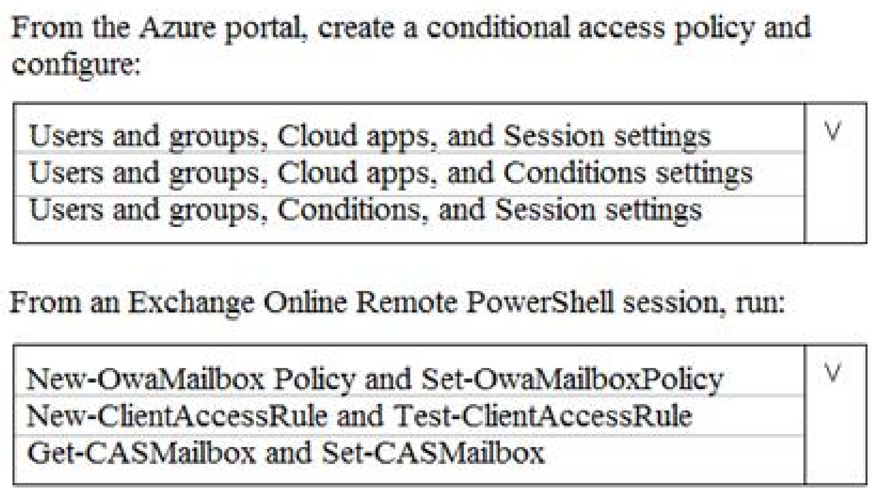
What is the effect of the policy when a user attempts to send an email messages that contains sensitive information?

A. The user receives a notification and can send the email message
B. The user receives a notification and cannot send the email message
C. The email message is sent without a notification
D. The email message is blocked silently

Answer: A

Explanation:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

NEW QUESTION 40
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Microsoft Azure Active Directory (Azure AD), you create a security group named Group1. You add 10 users to Group1.
You need to apply app enforced restrictions to the members of Group1 when they connect to Microsoft Exchange Online from non-compliant devices, regardless of their location.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



From the Azure portal, create a conditional access policy and configure:

- Users and groups, Cloud apps, and Session settings
- Users and groups, Cloud apps, and Conditions settings
- Users and groups, Conditions, and Session settings

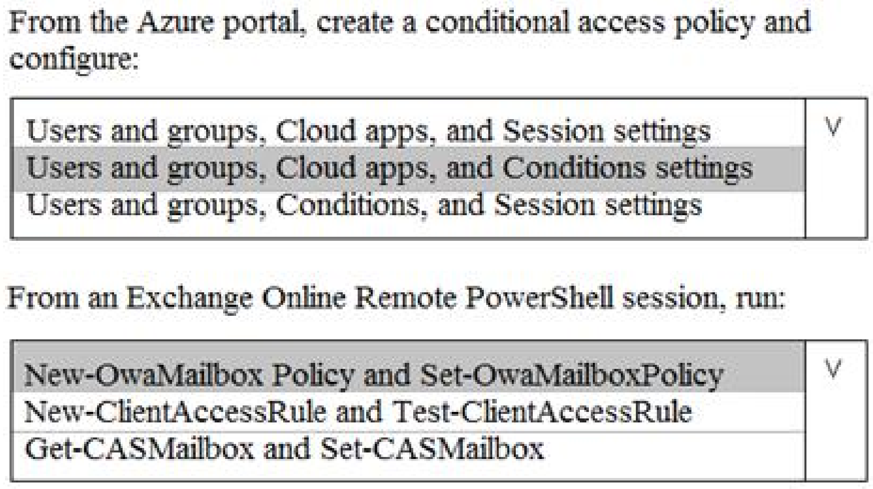
From an Exchange Online Remote PowerShell session, run:

- New-OwaMailbox Policy and Set-OwaMailboxPolicy
- New-ClientAccessRule and Test-ClientAccessRule
- Get-CASMailbox and Set-CASMailbox

A. Mastered
B. Not Mastered

Answer: A

Explanation:



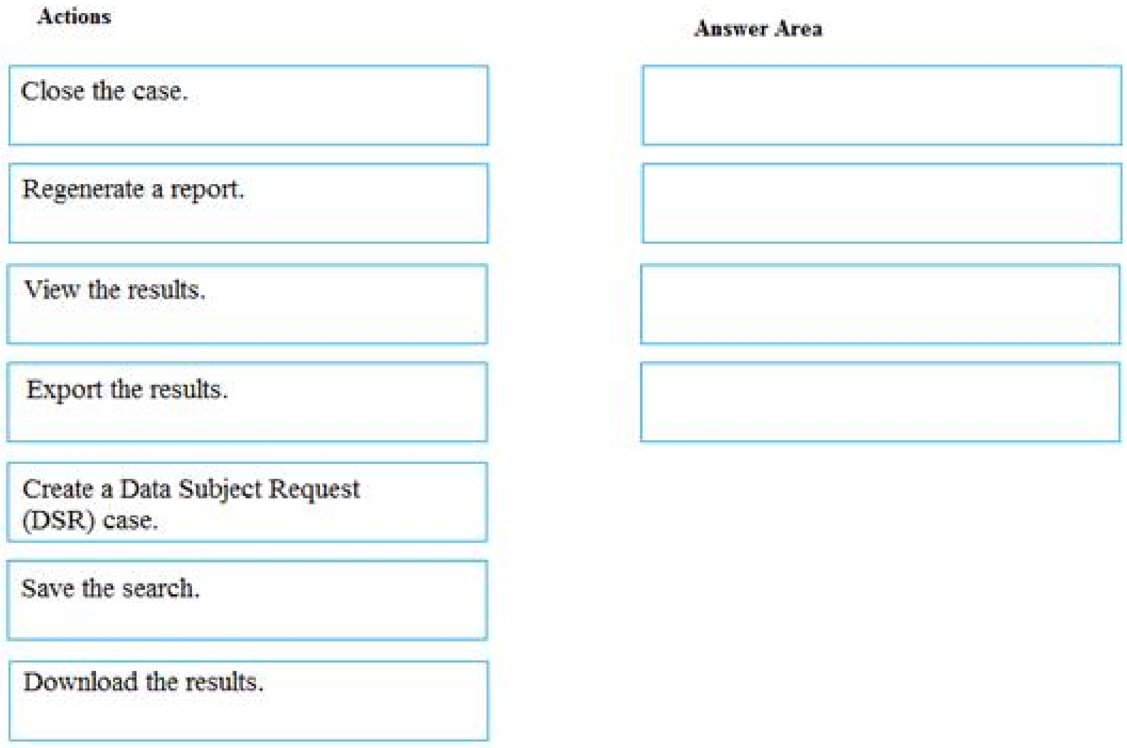
From the Azure portal, create a conditional access policy and configure:

- Users and groups, Cloud apps, and Session settings
- [✓ Users and groups, Cloud apps, and Conditions settings]
- Users and groups, Conditions, and Session settings

From an Exchange Online Remote PowerShell session, run:

- [✓ New-OwaMailbox Policy and Set-OwaMailboxPolicy]
- New-ClientAccessRule and Test-ClientAccessRule
- Get-CASMailbox and Set-CASMailbox

NEW QUESTION 42
DRAG DROP
You have a Microsoft 365 subscription.
A customer requests that you provide her with all documents that reference her by name. You need to provide the customer with a copy of the content.
Which four 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

- Close the case.
- Regenerate a report.
- View the results.
- Export the results.
- Create a Data Subject Request (DSR) case.
- Save the search.
- Download the results.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365

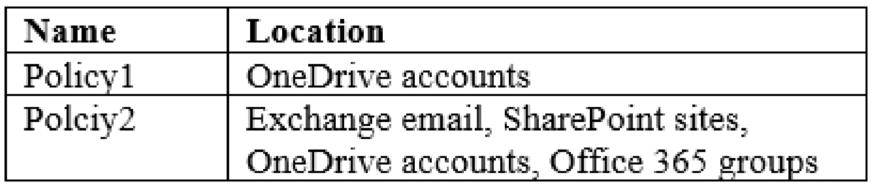
NEW QUESTION 46
You recently created and published several labels policies in a Microsoft 365 subscription.
You need to view which labels were applied by users manually and which labels were applied automatically.

What should you do from the Security & Compliance admin center?

A. From Search & investigation, select Content search
B. From Data governance, select Events
C. From Search & investigation, select eDiscovery
D. From Reports, select Dashboard

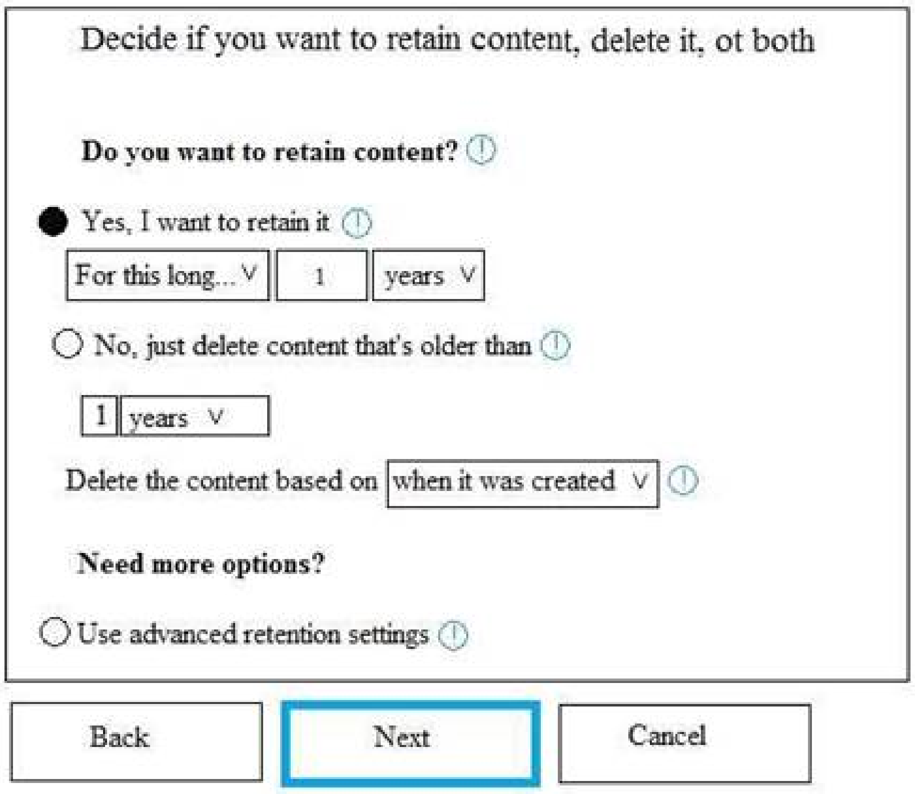
Answer: B

NEW QUESTION 51
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

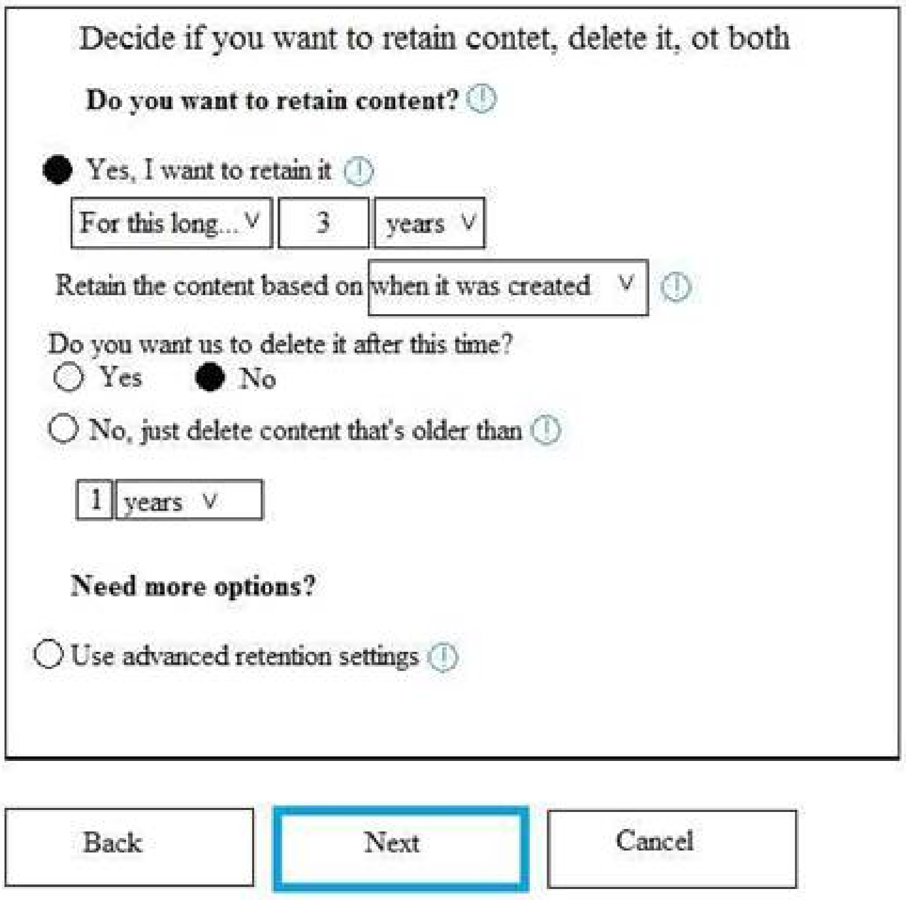
○ No, just delete content that's older than
1 | years

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

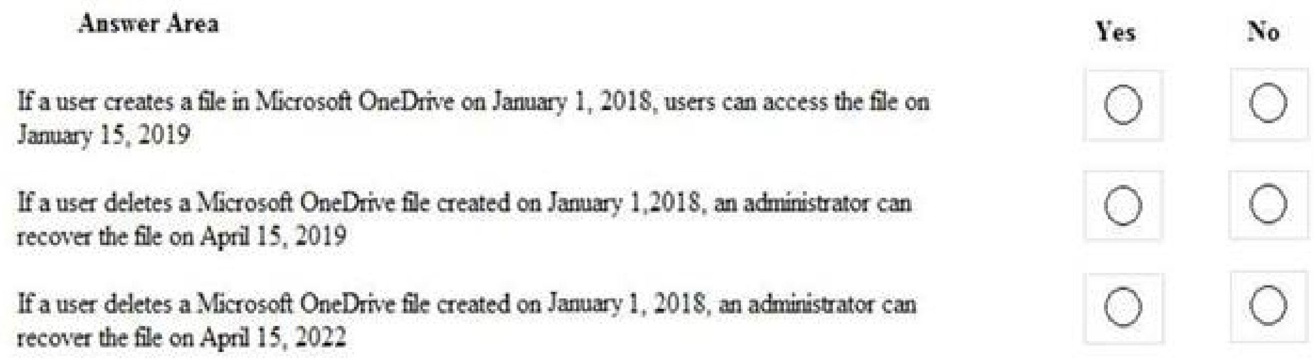
Do you want us to delete it after this time?
○ Yes ● No

○ 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 56
You have a Microsoft 365 subscription.
You need to enable auditing for all Microsoft Exchange Online users. What should you do?

A. From the Exchange admin center, create a journal rule
B. Run the Set-MailboxDatabase cmdlet
C. Run the Set-Mailbox cmdlet
D. From the Exchange admin center, create a mail flow message trace rule.

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing

NEW QUESTION 60
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.

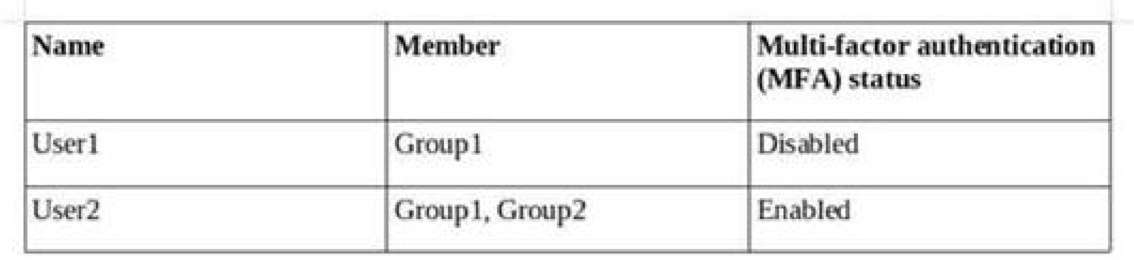
Answer: B

NEW QUESTION 63
You have a hybrid Microsoft 365 environment.
All computers run Windows 10 Enterprise and have Microsoft Office 365 ProPlus installed. All the computers are joined to Active Directory.
You have a server named Server1 that runs Windows Server 2016. Server1 hosts the telemetry database. You need to prevent private details in the telemetry data from being transmitted to Microsoft.
What should you do?

A. On Server1, run readinessreportcreator.exe
B. Configure a registry on Server1
C. Configure a registry on the computers
D. On the computers, run tdadm.exe

Answer: C

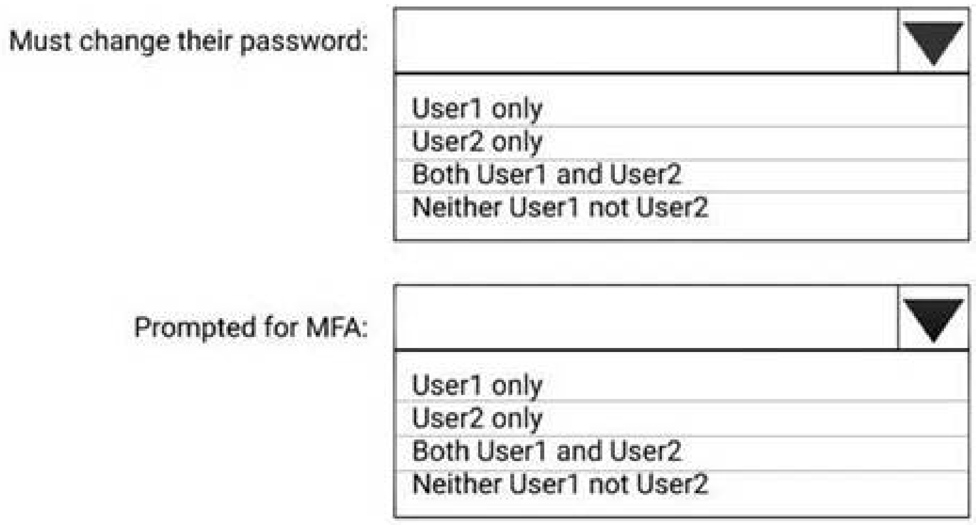
NEW QUESTION 67
HOTSPOT
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.



Name	Member	Multi-factor authentication (MFA) status
User1	Group1	Disabled
User2	Group1, Group2	Enabled

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:
•Assignments: Include Group1, Exclude Group2

•Conditions: Sign in risk of Low and above
•Access: Allow access, Require password change
You need to identify how the policy affects User1 and User2.
What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



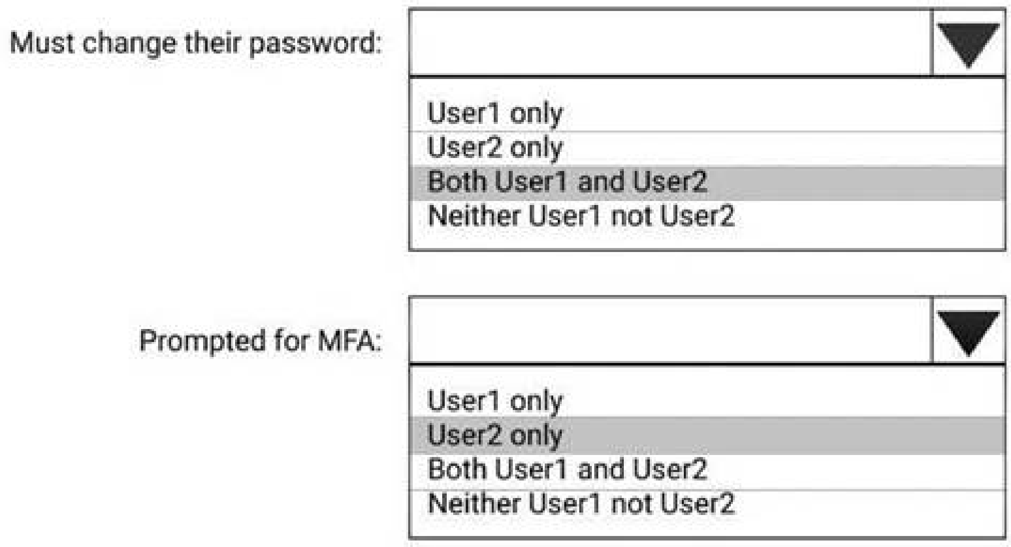
Must change their password:
User1 only
User2 only
Both User1 and User2
Neither User1 not User2

Prompted for MFA:
User1 only
User2 only
Both User1 and User2
Neither User1 not User2

A. Mastered
B. Not Mastered

Answer: A

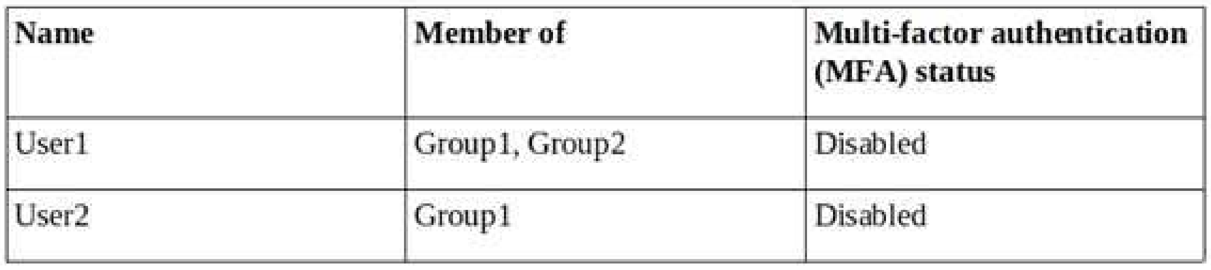
Explanation:



Must change their password:
User1 only
User2 only
[✓ Both User1 and User2]
Neither User1 not User2

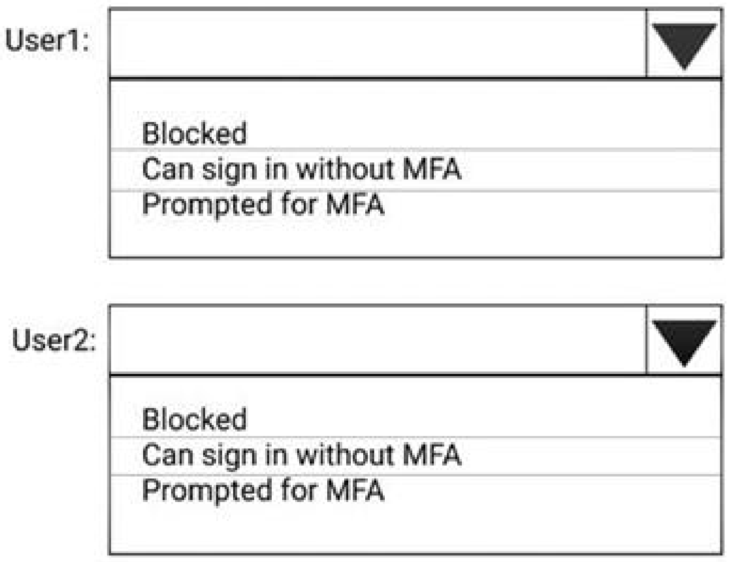
Prompted for MFA:
User1 only
[✓ User2 only]
Both User1 and User2
Neither User1 not User2

NEW QUESTION 72
HOTSPOT
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.



Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:
•Assignments: Include Group1, Exclude Group2
•Conditions: Sign in risk of Low and above
•Access: Allow access, Require password multi-factor authentication You need to identify how the policy affects User1 and User2.
What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



User1:

Blocked
Can sign in without MFA
Prompted for MFA

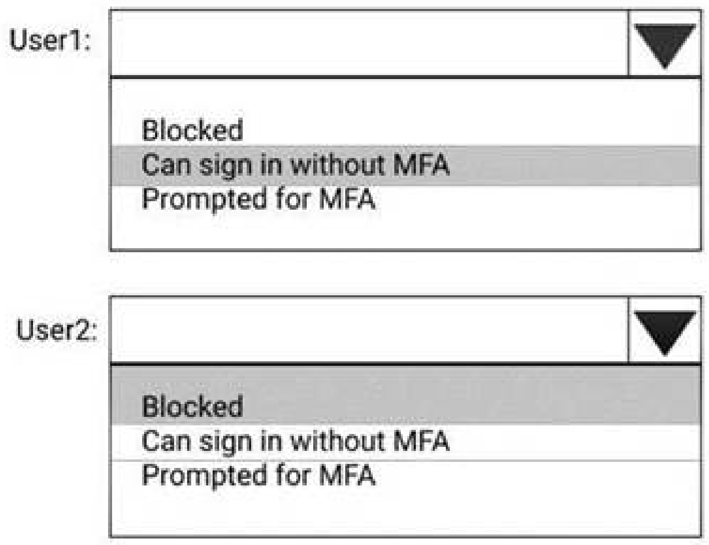
User2:

Blocked
Can sign in without MFA
Prompted for MFA

A. Mastered
B. Not Mastered

Answer: A

Explanation:



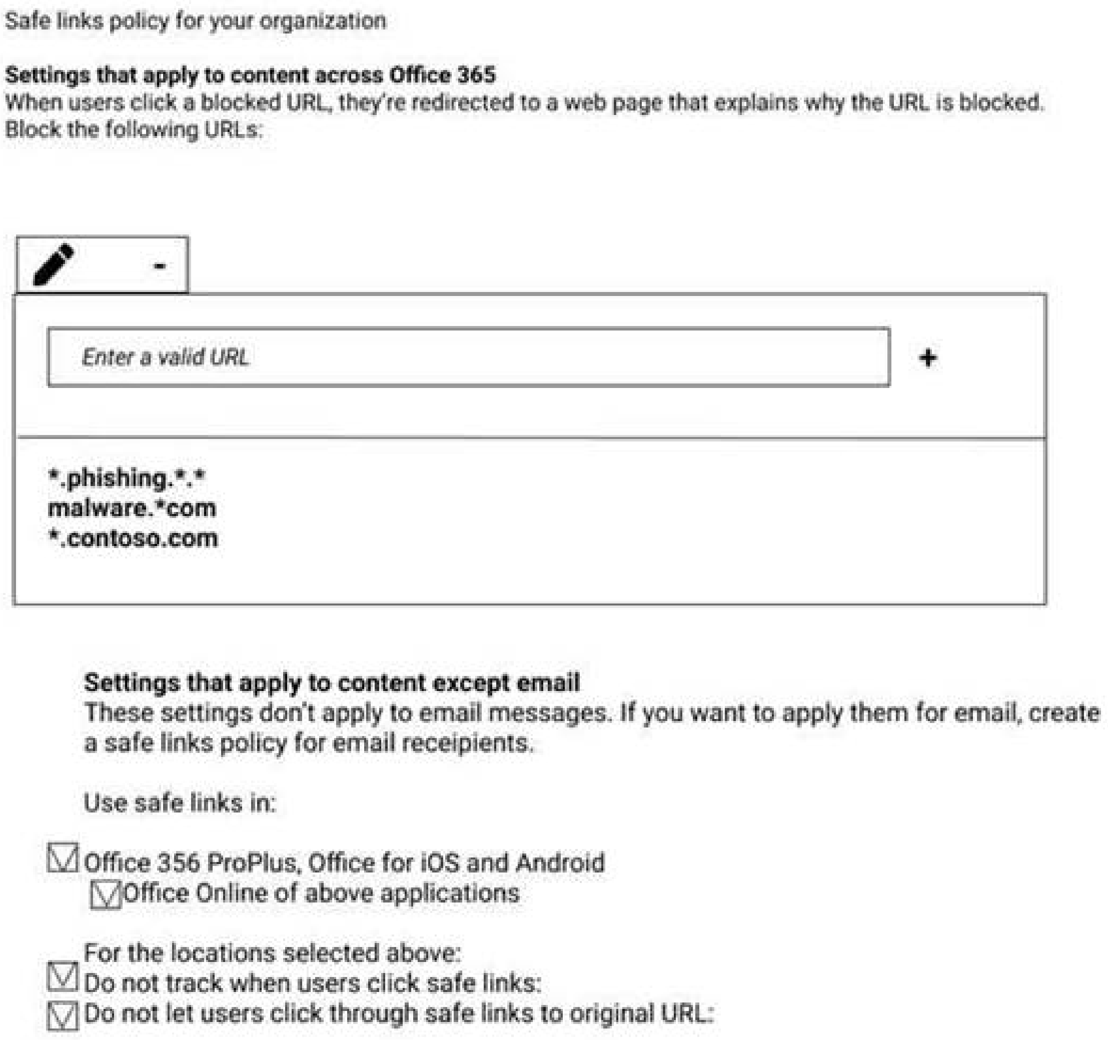
User1:

Blocked
Can sign in without MFA
Prompted for MFA

User2:

Blocked
Can sign in without MFA
Prompted for MFA

NEW QUESTION 73
You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com. You create a safe links policy, as shown in the following exhibit.



Safe links policy for your organization

Settings that apply to content across Office 365
When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.
Block the following URLs:

Enter a valid URL +

.phishing.*.
malware.*com
***.contoso.com**

Settings that apply to content except email
These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email receipients.

Use safe links in:

☑ Office 356 ProPlus, Office for iOS and Android
☑ Office Online of above applications

For the locations selected above:
☑ Do not track when users click safe links:
☑ Do not let users click through safe links to original URL:

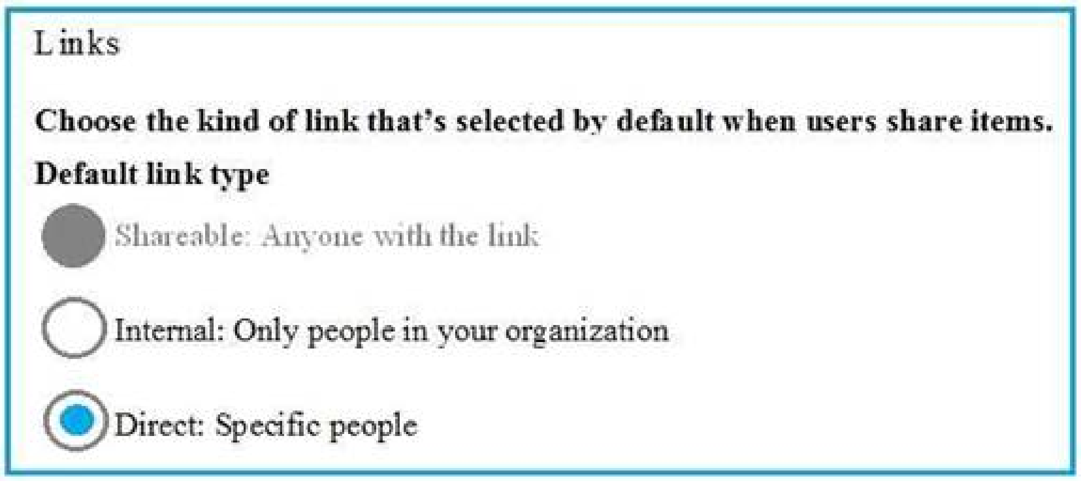
Which URL can a user safely access from Microsoft Word Online?

A. fabrikam.phishing.fabrikam.com
B. malware.fabrikam.com
C. fabrikam.contoso.com
D. www.malware.fabrikam.com

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-a-custom-blocked-urls-list- wtih-atp

NEW QUESTION 78
HOTSPOT
You have a Microsoft 365 subscription that uses a default name of litwareinc.com.
You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.



Links

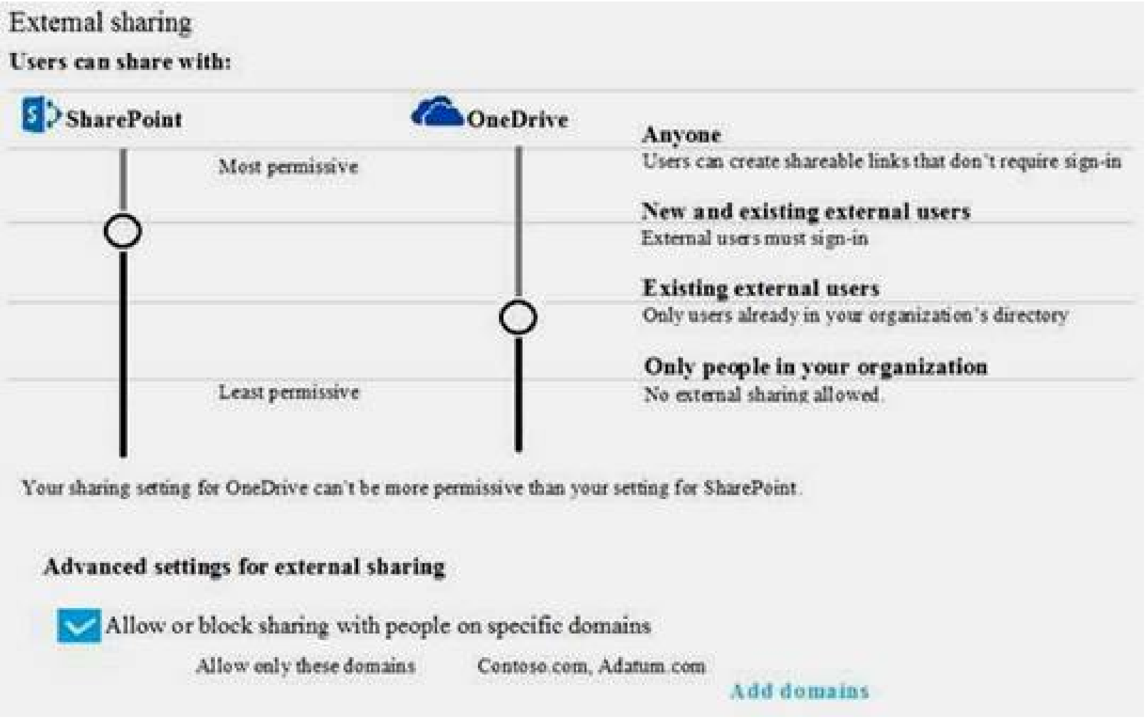
Choose the kind of link that's selected by default when users share items.

Default link type

○ Shareable: Anyone with the link

○ Internal: Only people in your organization

◉ Direct: Specific people



External sharing

Users can share with:

SharePoint	OneDrive	
Most permissive		**Anyone** Users can create shareable links that don't require sign-in
○		**New and existing external users** External users must sign-in
	○	**Existing external users** Only users already in your organization's directory
Least permissive		**Only people in your organization** No external sharing allowed.

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

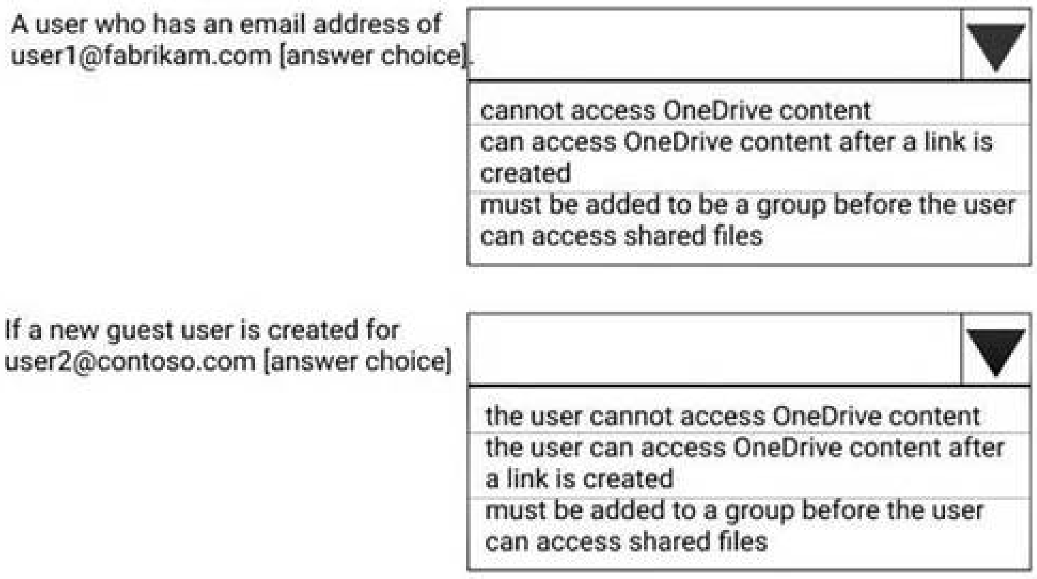
Advanced settings for external sharing

☑ Allow or block sharing with people on specific domains

Allow only these domains   Contoso.com, Adatum.com

Add domains

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.



A user who has an email address of user1@fabrikam.com [answer choice].
- cannot access OneDrive content
- can access OneDrive content after a link is created
- must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]
- the user cannot access OneDrive content
- the user can access OneDrive content after a link is created
- must be added to a group before the user can access shared files

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/onedrive/manage-sharing

NEW QUESTION 82

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 87
You have a Microsoft 365 subscription.
You create and run a content search from the Security & Compliance admin center. You need to download the results of the content search.
What should you obtain first?

A. an export key
B. a password
C. a certificate
D. a pin

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results

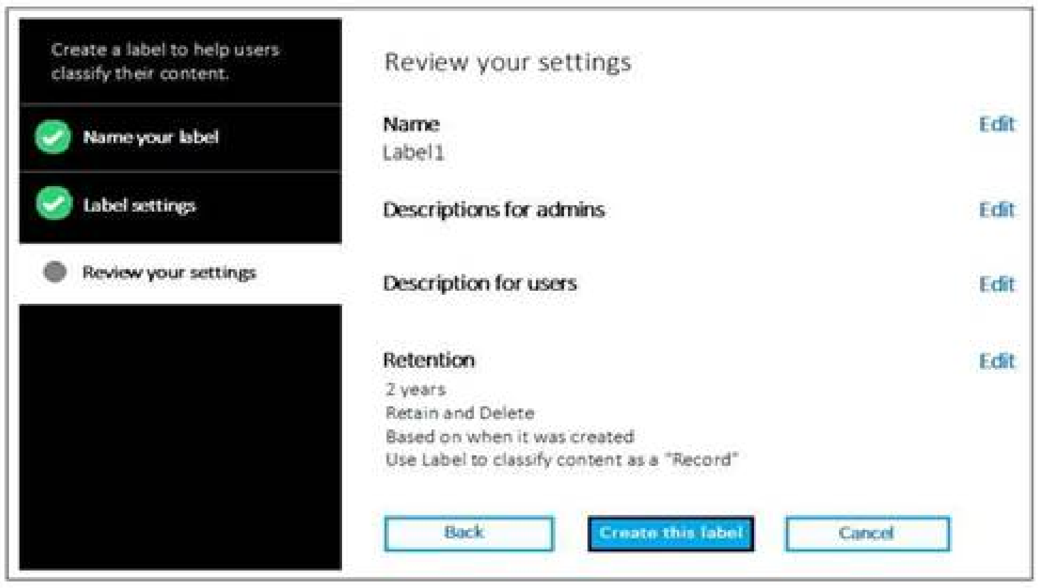
NEW QUESTION 89
You have a Microsoft 365 subscription.
All users are assigned a Microsoft 365 E5 license. How long will auditing data be retained?

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 90
HOTSPOT
You have a Microsoft 365 subscription.
You create a retention label named Label1 as shown in the following exhibit.



Create a label to help users classify their content.

✓ Name your label
✓ Label settings
● Review your settings

Review your settings

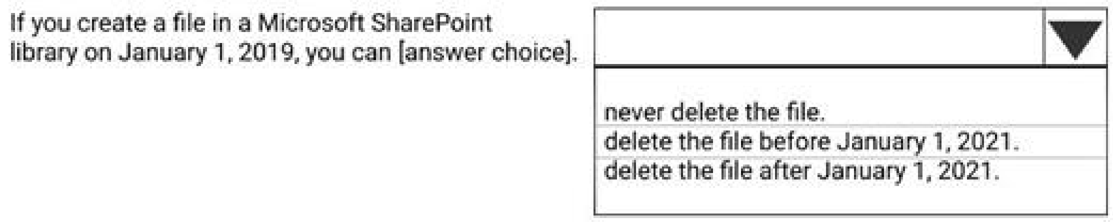
Name — Edit
Label1

Descriptions for admins — Edit

Description for users — Edit

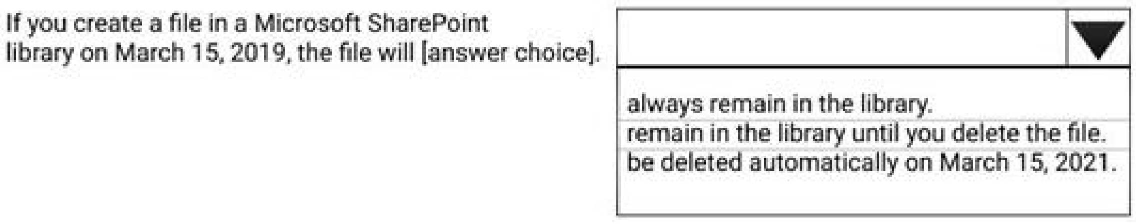
Retention — Edit
2 years
Retain and Delete
Based on when it was created
Use Label to classify content as a "Record"

You publish Label1 to SharePoint sites.
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.



If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

never delete the file.
delete the file before January 1, 2021.
delete the file after January 1, 2021.



If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

always remain in the library.
remain in the library until you delete the file.
be deleted automatically on March 15, 2021.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 92
You have a Microsoft 365 subscription.
You create a retention policy and apply the policy to Exchange Online mailboxes.
You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible.
What should you do?

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

Answer: D

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

NEW QUESTION 94
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 questions 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 an on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events.
You use the System event log on Server1. Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

NEW QUESTION 98
......