Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator

NEW QUESTION 1
You need to recommend a solution for the user administrators that meets the security requirements for auditing.
Which blade should you recommend using from the Azure Active Directory admin center?

A. Sign-ins
B. Azure AD Identity Protection
C. Authentication methods
D. Access review

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

NEW QUESTION 2
You need to recommend a solution to protect the sign-ins of Admin1 and Admin2. What should you include in the recommendation?

A. a device compliance policy
B. an access review
C. a user risk policy
D. a sign-in risk policy

Answer: C

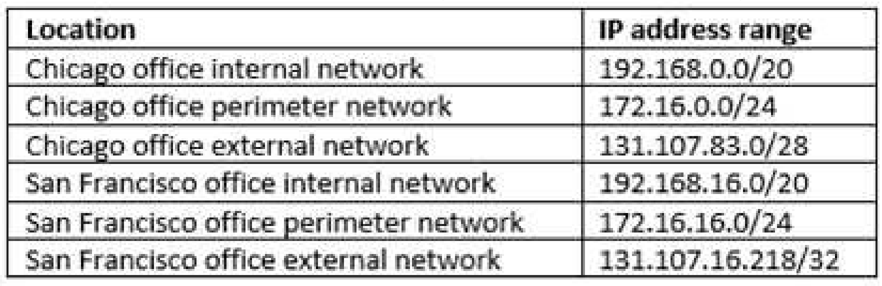
Explanation:
References:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy

NEW QUESTION 3
You need to resolve the issue that targets the automated email messages to the IT team. Which tool should you run first?

A. Synchronization Service Manager
B. Azure AD Connect wizard
C. Synchronization Rules Editor
D. IdFix

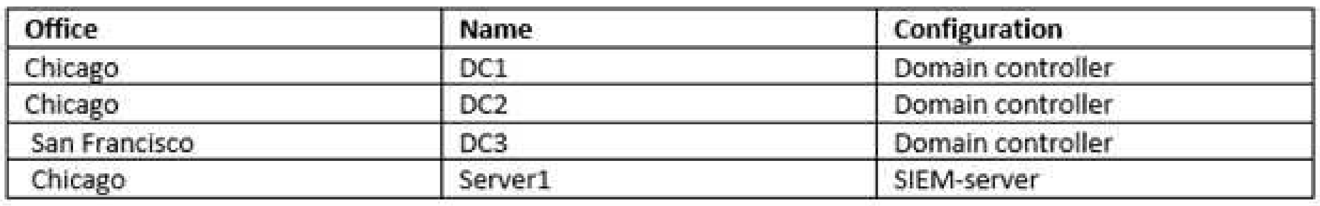
Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization
Case Study: 2 Litware, Inc Overview
Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in
a branch office in San Francisco.
Existing Environment
Internal Network Infrastructure
The network contains a single domain forest. The forest functional level is Windows Server 2016. Users are subject to sign-in hour restrictions as defined in Active Directory.
The network has the IP address range shown in the following table.



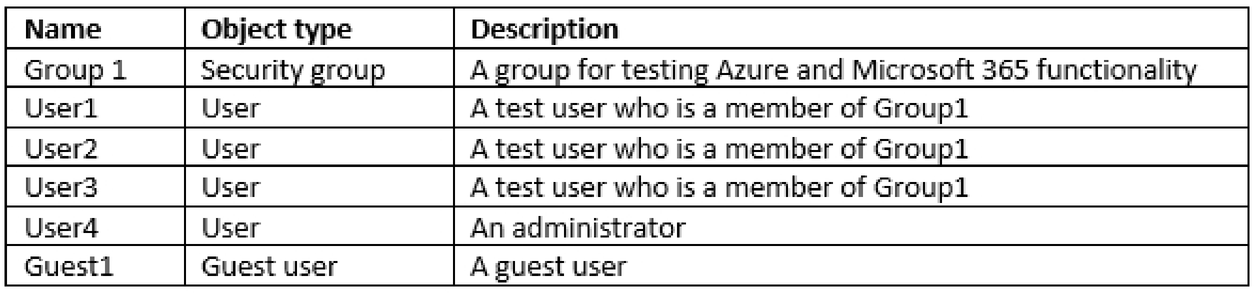
Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).
The following operating systems are used on the network:
•Windows Server 2016
•Windows 10 Enterprise
•Windows 8.1 Enterprise
The internal network contains the systems shown in the following table.



Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.
Cloud Infrastructure
Litware recently purchased Microsoft 365 subscription licenses for all users.
Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.
You have the Microsoft 365 users and groups shown in the following table.



Name	Object type	Description
Group 1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Planned Changes
Litware plans to implement the following changes: Migrate the email system to Microsoft Exchange Online Implement Azure AD Privileged Identity Management
Security Requirements
Litware identities the following security requirements:
•Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
•Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
•Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
•Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
•Implement a permanent eligible assignment of the Compliance administrator role for User1
•Integrate Windows Defender and Windows Defender ATP on domain-joined servers
•Prevent access to Azure resources for the guest user accounts by default
•Ensure that all domain-joined computers are registered to Azure AD
Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts. You identify the following requirements for testing MFA. Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
If an authentication attempt is suspicious, MFA must be used, regardless of the user location Any disruption of legitimate authentication attempts must be minimized
General Requirements
Litware want to minimize the deployment of additional servers and services in the Active Directory forest.

NEW QUESTION 4
You need to create Group2.
What are two possible ways to create the group?

A. an Office 365 group in the Microsoft 365 admin center
B. a mail-enabled security group in the Microsoft 365 admin center
C. a security group in the Microsoft 365 admin center
D. a distribution list in the Microsoft 365 admin center
E. a security group in the Azure AD admin center

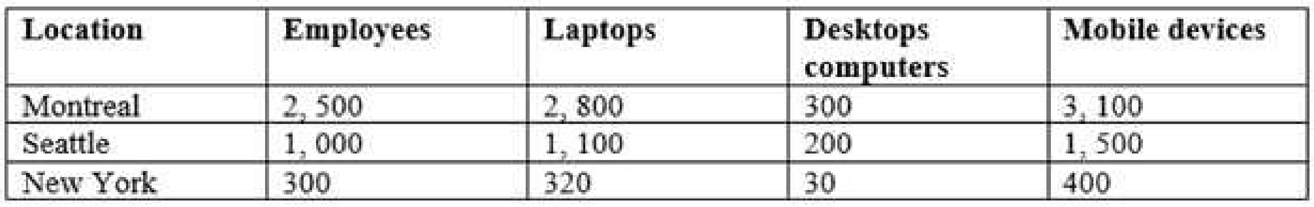
Answer: CE

NEW QUESTION 5
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

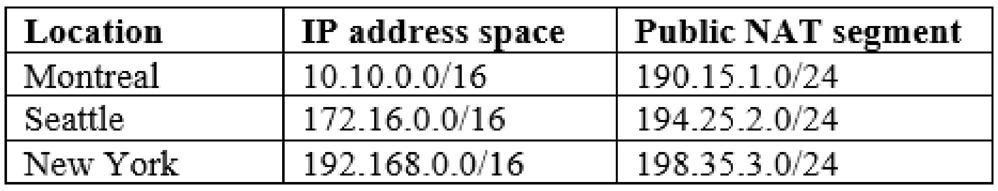
Answer: C

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.



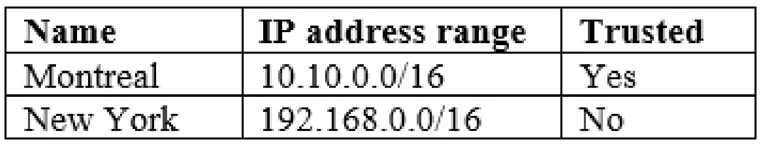
Location	Employees	Laptops	Desktops computers	Mobile devices
Montreal	2, 500	2, 800	300	3, 100
Seattle	1, 000	1, 100	200	1, 500
New York	300	320	30	400

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.



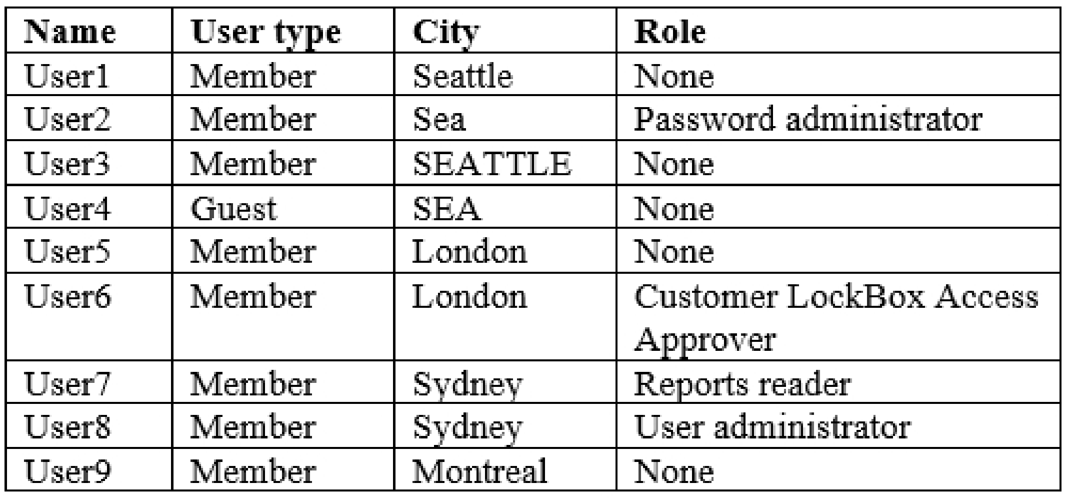
Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

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



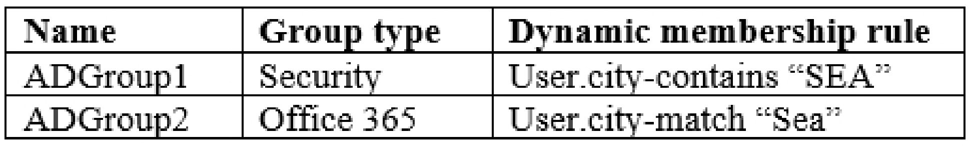
Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

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.



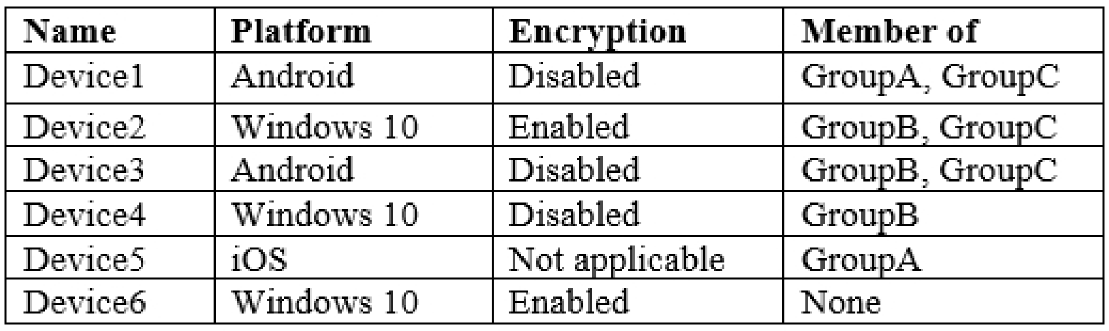
Name	User type	City	Role
User1	Member	Seattle	None
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	None
User4	Guest	SEA	None
User5	Member	London	None
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member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

The tenant contains the groups shown in the following table.



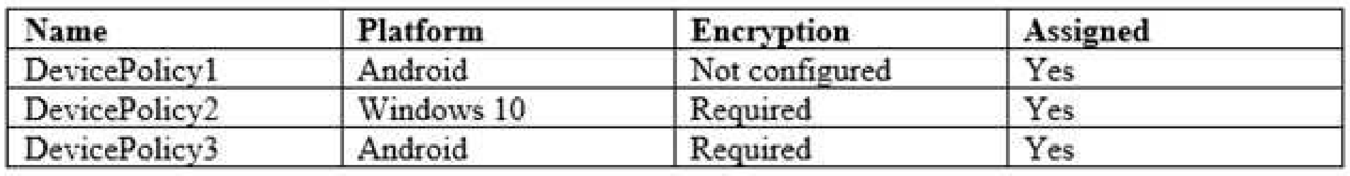
Name	Group type	Dynamic membership rule
ADGroup1	Security	User.city-contains “SEA”
ADGroup2	Office 365	User.city-match “Sea”

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



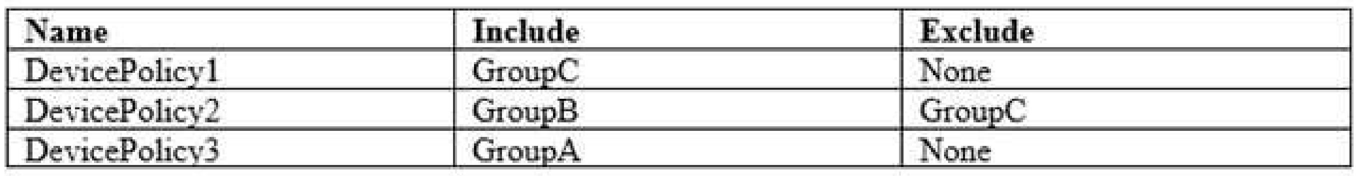
Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	Not applicable	GroupA
Device6	Windows 10	Enabled	None

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

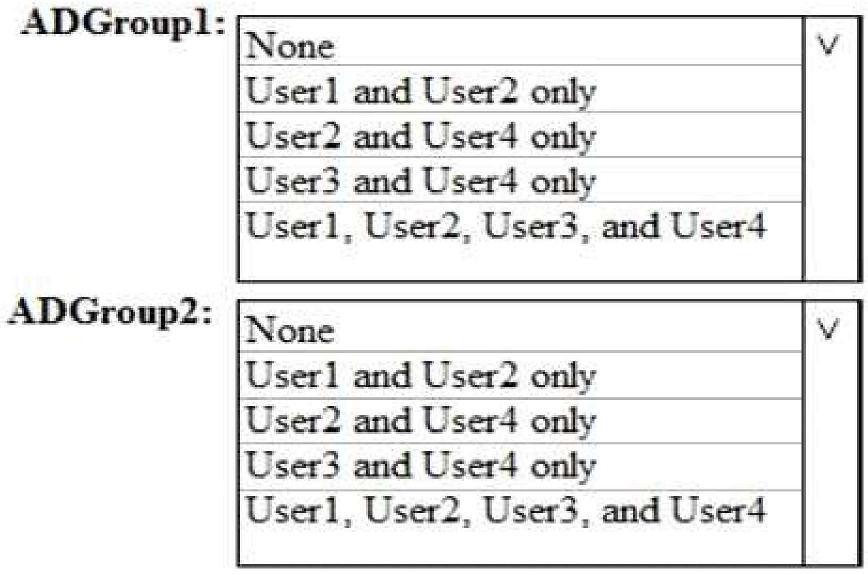
The device compliance policies have the assignments shown in the following table.



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 6
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:

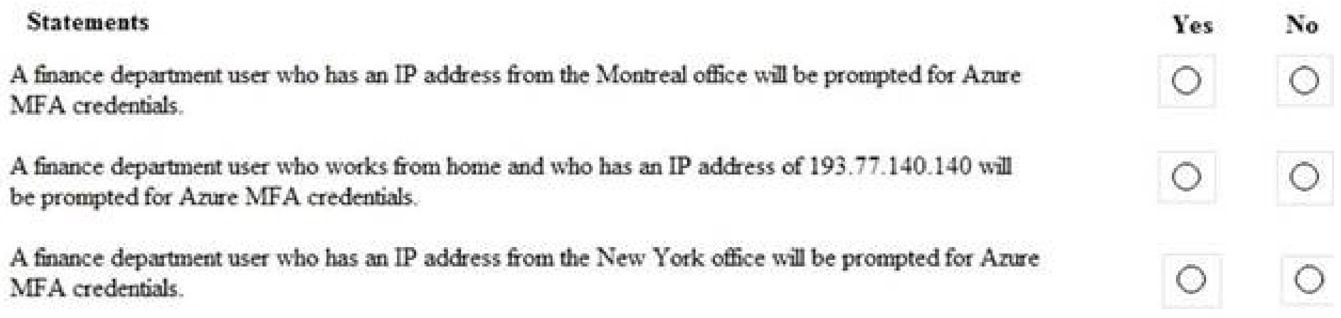
- None
- User1 and User2 only
- User2 and User4 only
- User3 and User4 only
- User1, User2, User3, and User4

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 7
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.

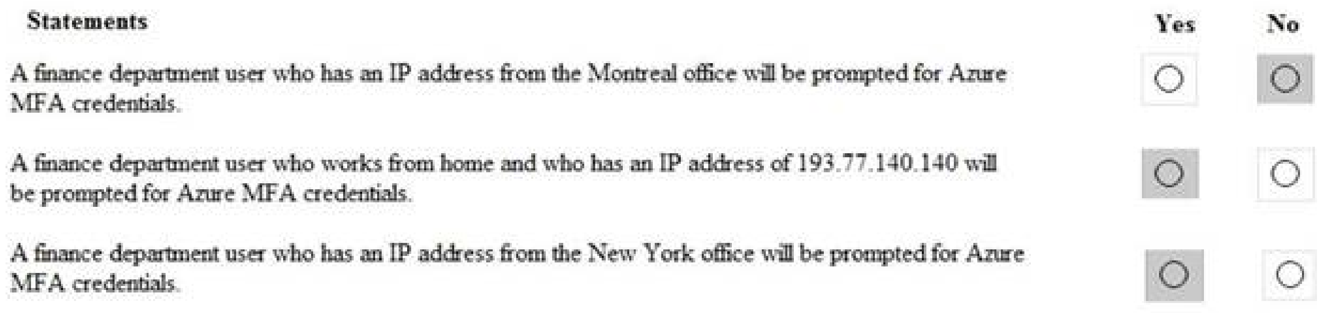


Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	○	○
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	○	○
A finance department user 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 8
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 9
Which role should you assign to User1?

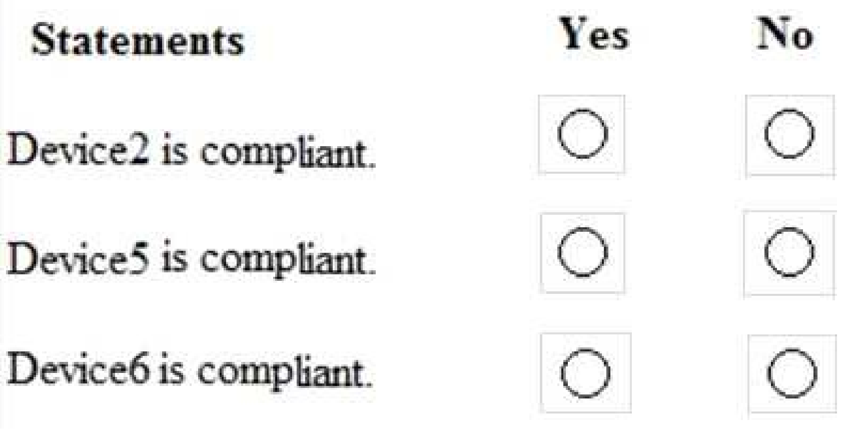
A. Global administrator

B. User administrator
C. Privileged role administrator
D. Security administrator

Answer: D

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

NEW QUESTION 10
HOTSPOT
You are evaluating which devices are compliant in Intune.
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

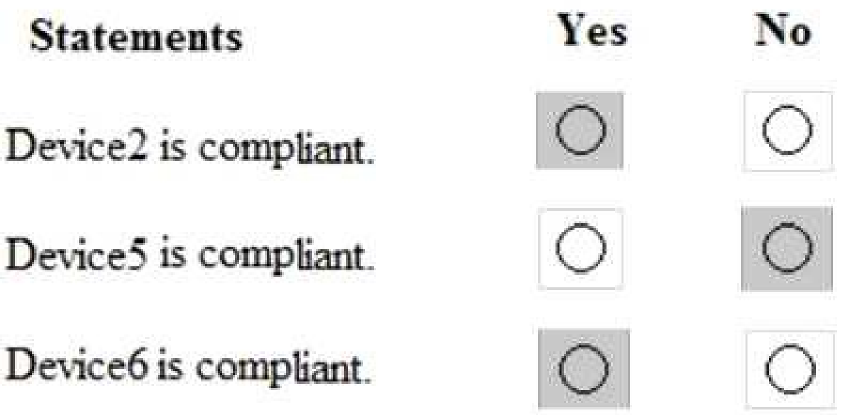


Statements	Yes	No
Device2 is compliant.	○	○
Device5 is compliant.	○	○
Device6 is compliant.	○	○

A. Mastered
B. Not Mastered

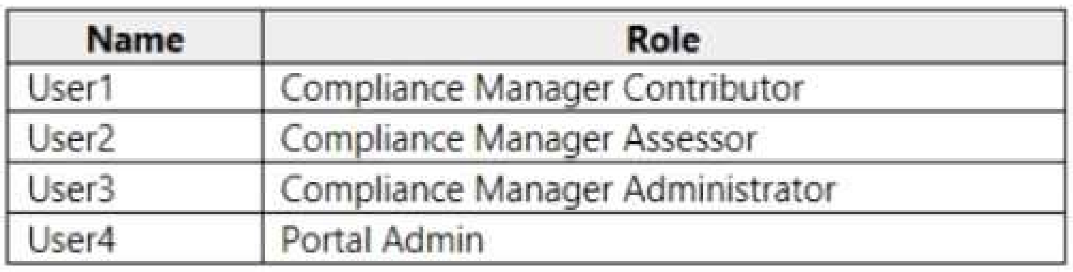
Answer: A

Explanation:



Statements	Yes	No
Device2 is compliant.	●	○
Device5 is compliant.	○	●
Device6 is compliant.	●	○

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 modifying the licenses assigned to User5. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Case Study: 4 Mix Questions

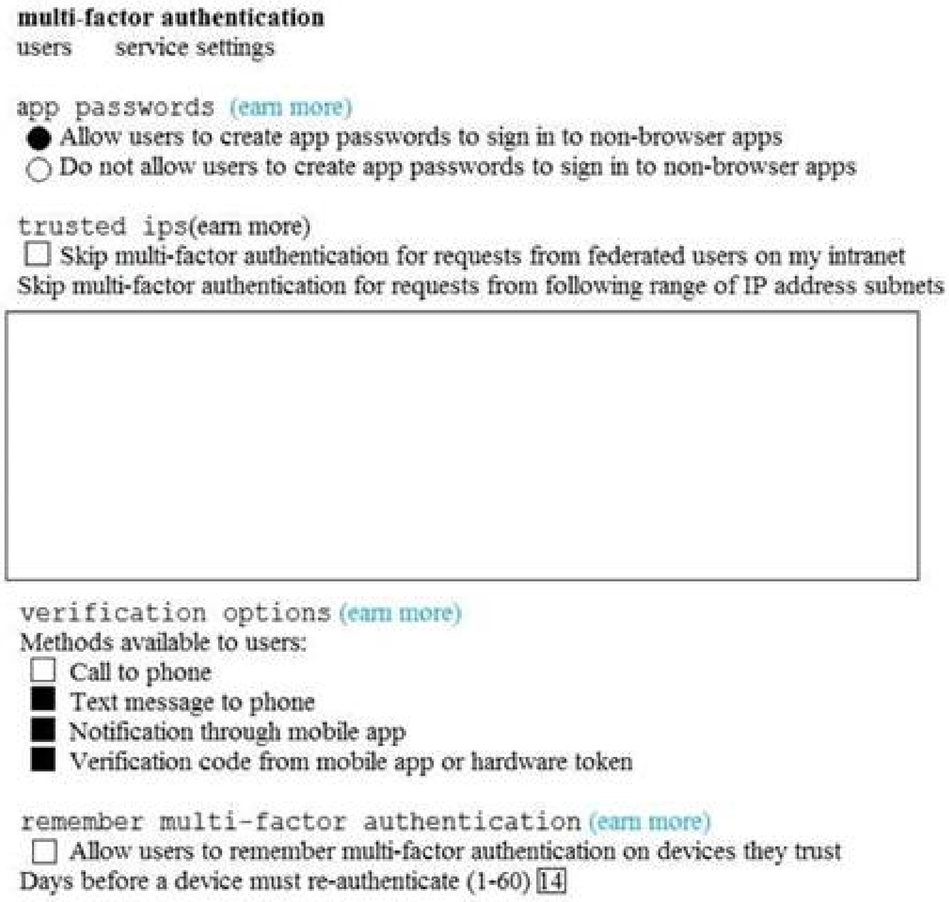
NEW QUESTION 15
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After 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 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

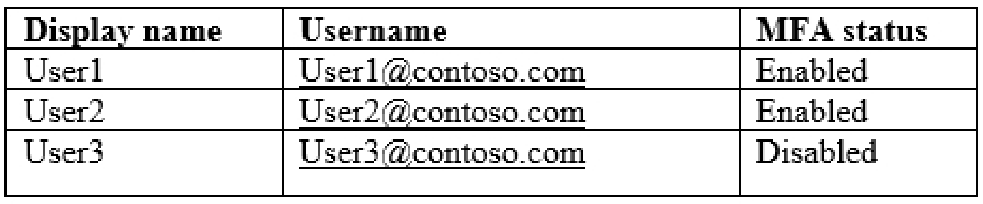
app passwords (earn more)
● Allow users to create app passwords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

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

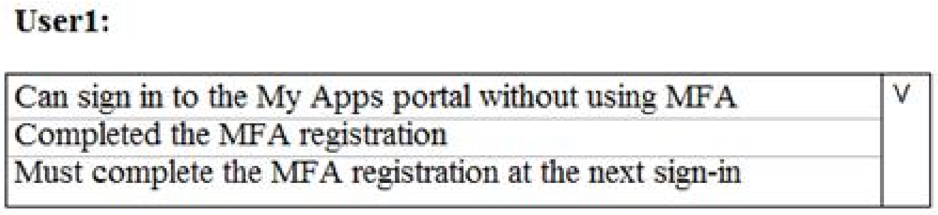
remember multi-factor authentication (earn more)
□ Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60) 14

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

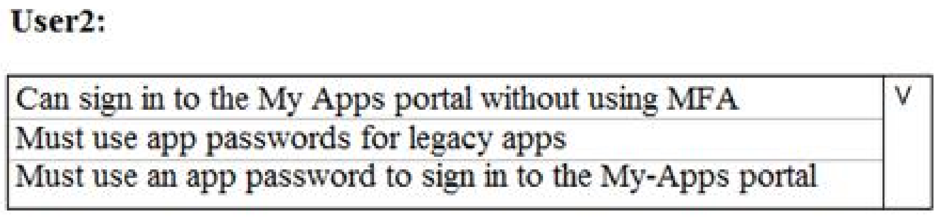


Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

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

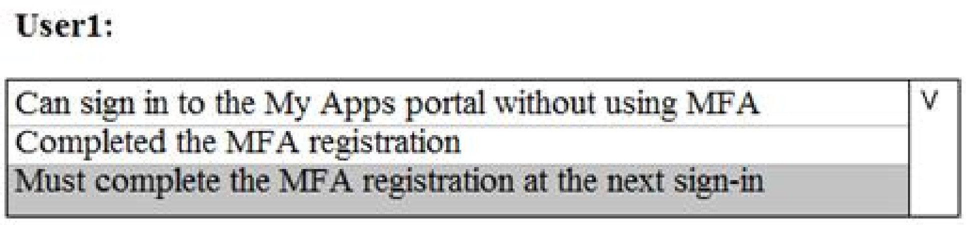


User2:
Can sign in to the My Apps portal without using MFA
Must use app passwords for legacy apps
Must use an app password to sign in to the My-Apps portal

A. Mastered
B. Not Mastered

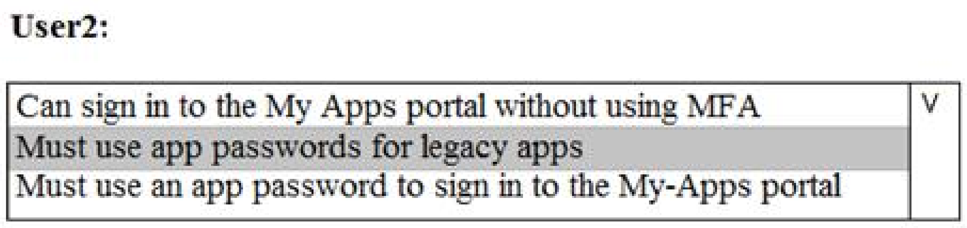
Answer: A

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 18
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 20
Your company has a Microsoft 365 subscription.
The company forbids users to enroll personal devices in mobile device management (MDM). Users in the sales department have personal iOS devices.
You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.
The users must be prevented from backing up the app’s data to iCloud. What should you create?

A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
B. an app protection policy in Microsoft Intune
C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
D. a device compliance policy in Microsoft Intune

Answer: B

NEW QUESTION 23
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 27
You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.
Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.
You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members.
The email address that you intend to spoof belongs to the Executive group members. What should you do first?

A. From Azure ATP admin center, configure the primary workspace settings
B. From the Microsoft Azure portal, configure the user risk settings in Azure AD Identity Protection
C. Enable MFA for the Research group members
D. Migrate the Executive group members to Exchange Online

Answer: C

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

NEW QUESTION 28
You have a Microsoft 365 E5 subscription.

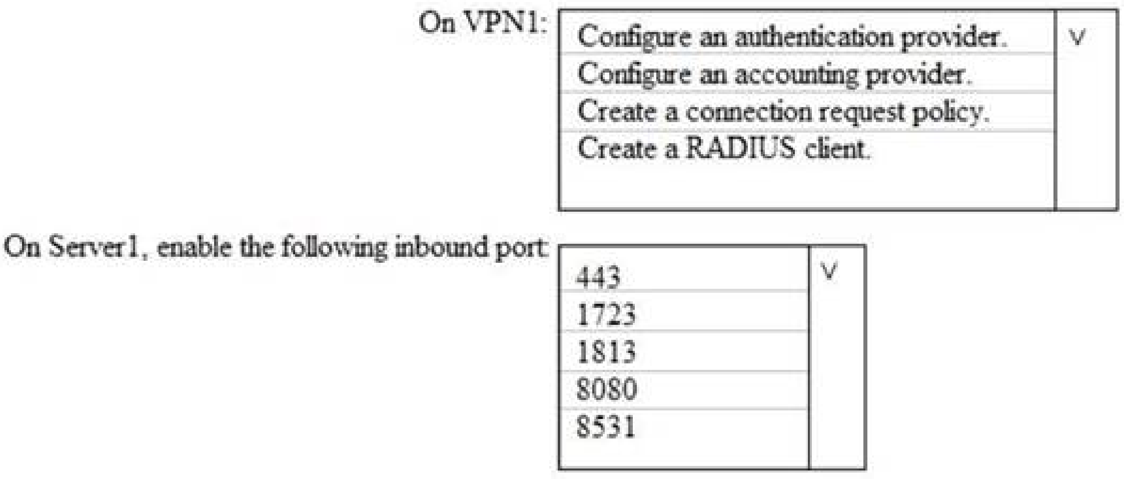
You implement Advanced Threat Protection (ATP) safe attachments policies for all users.
User reports that email messages containing attachments take longer than expected to be received. You need to reduce the amount of time it takes to receive email messages that contain attachments. The solution must 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 32
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed. You have a Microsoft Azure subscription.
You are deploying Azure Advanced Threat Protection (ATP)
You install an Azure ATP standalone sensor on a server named Server1 that runs Windows Server 2016.
You need to integrate the VPN and Azure ATP.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



On VPN1:
- Configure an authentication provider.
- Configure an accounting provider.
- Create a connection request policy.
- Create a RADIUS client.

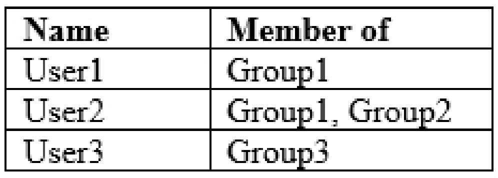
On Server1, enable the following inbound port
- 443
- 1723
- 1813
- 8080
- 8531

A. Mastered
B. Not Mastered

Answer: A

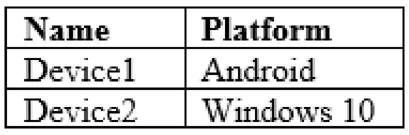
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn

NEW QUESTION 35
HOTSPOT
You have a Microsoft 365 subscription that uses a default domain name of contoso.com. Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.



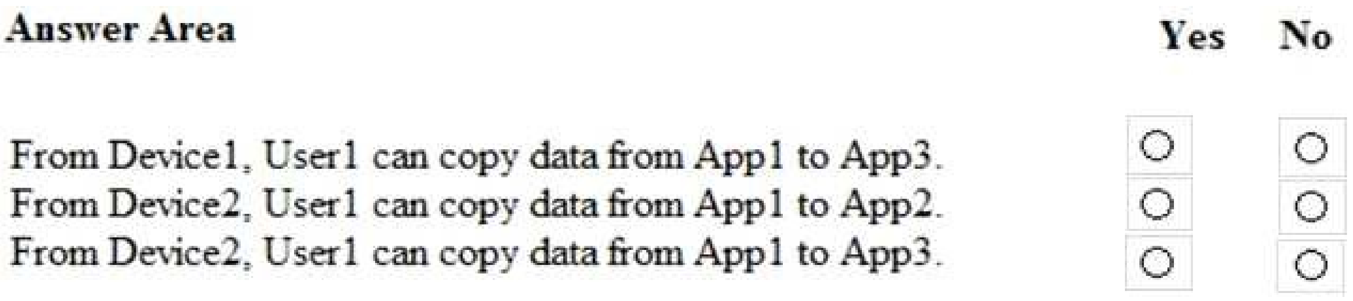
Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Intune has two devices enrolled as shown in the following table:



Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.
You create an app protection policy named ProtectionPolicy1 that has the following settings:
•Protected apps: App1
•Exempt apps: App2
•Windows Information Protection mode: Block
You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1. For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

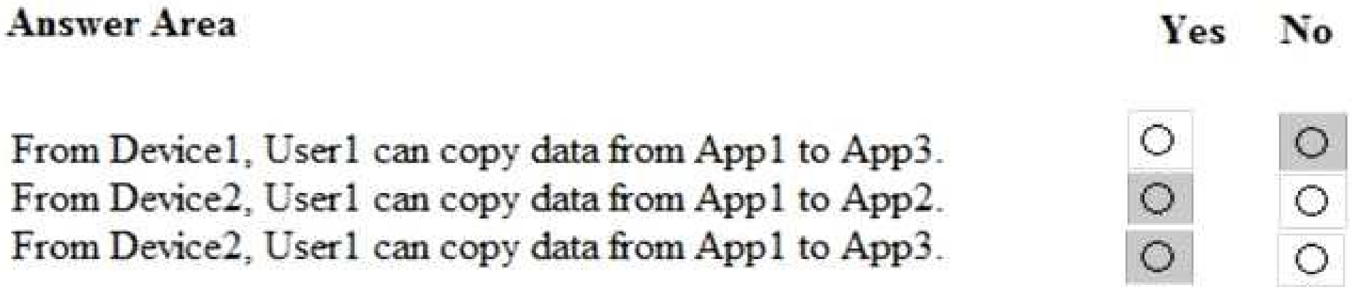


Answer Area	Yes	No
From Device1, User1 can copy data from App1 to App3.	○	○
From Device2, User1 can copy data from App1 to App2.	○	○
From Device2, User1 can copy data from App1 to App3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area	Yes	No
From Device1, User1 can copy data from App1 to App3.	○	●
From Device2, User1 can copy data from App1 to App2.	●	○
From Device2, User1 can copy data from App1 to App3.	●	○

NEW QUESTION 36
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

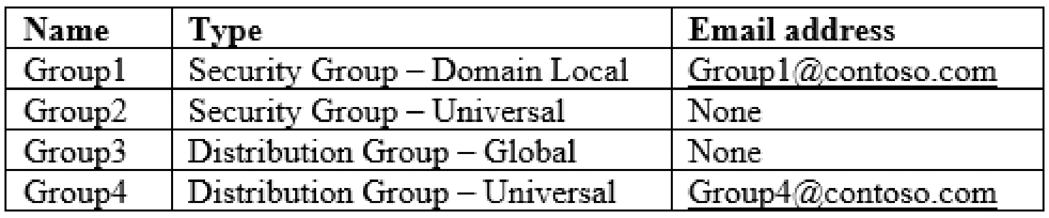
Answer: D

NEW QUESTION 41
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

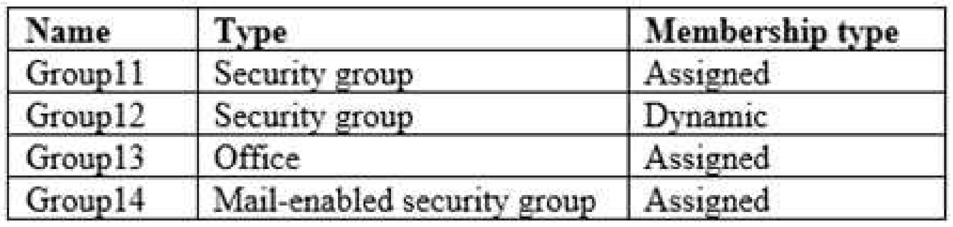
Answer: B

NEW QUESTION 45
HOTSPOT
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.



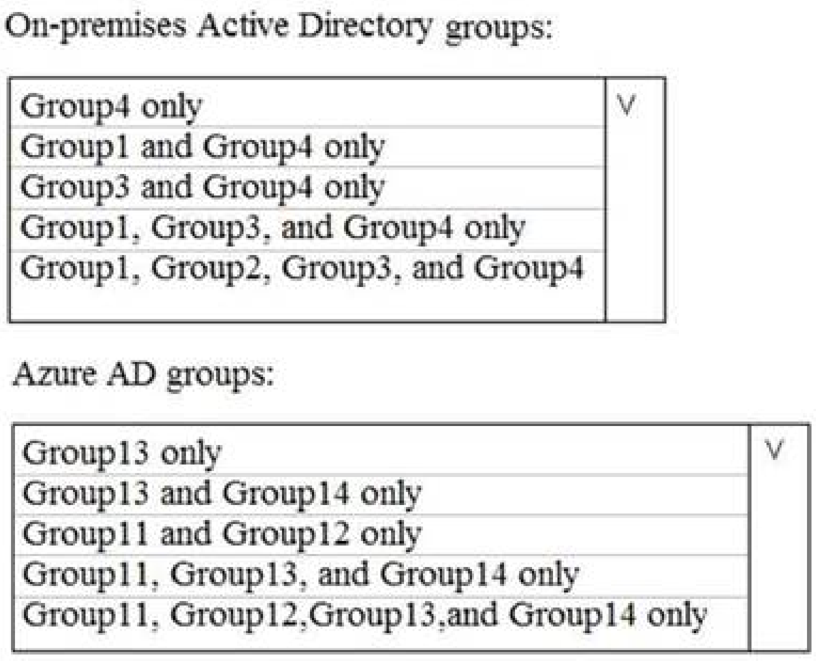
Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

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:

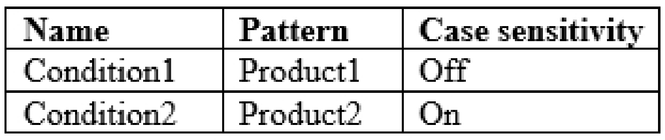
- Group13 only
- Group13 and Group14 only
- Group11 and Group12 only
- Group11, Group13, and Group14 only
- Group11, Group12,Group13,and Group14 only

A. Mastered
B. Not Mastered

Answer: A

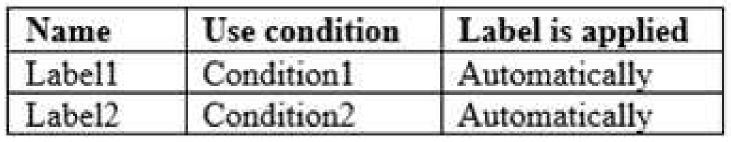
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/prepare

NEW QUESTION 49
HOTSPOT
You have the Microsoft conditions shown in the following table.



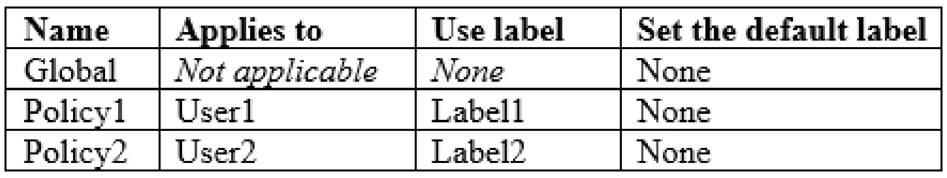
Name	Pattern	Case sensitivity
Condition1	Product1	Off
Condition2	Product2	On

You have the Azure Information Protection labels shown in the following table.



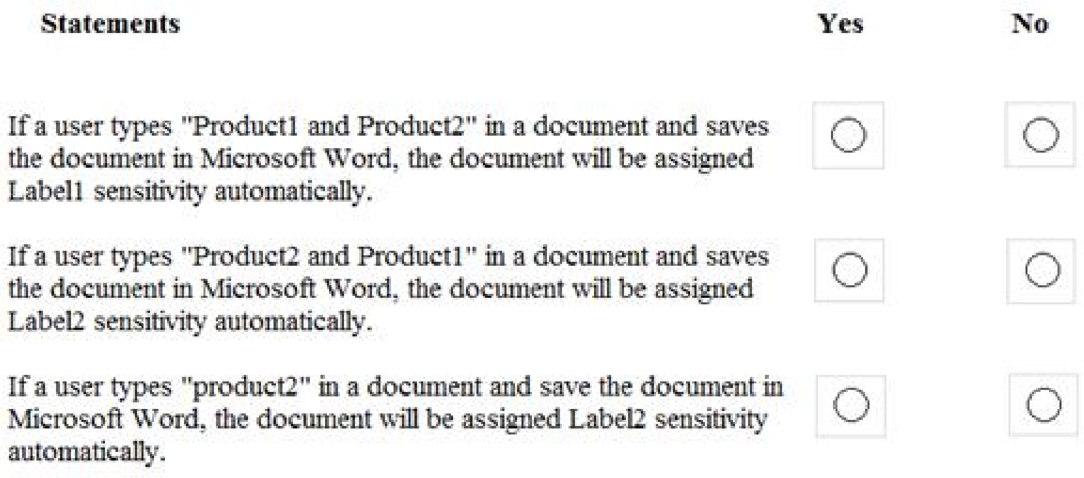
Name	Use condition	Label is applied
Label1	Condition1	Automatically
Label2	Condition2	Automatically

You have the Azure Information Protection policies shown in the following table.



Name	Applies to	Use label	Set the default label
Global	*Not applicable*	*None*	None
Policy1	User1	Label1	None
Policy2	User2	Label2	None

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

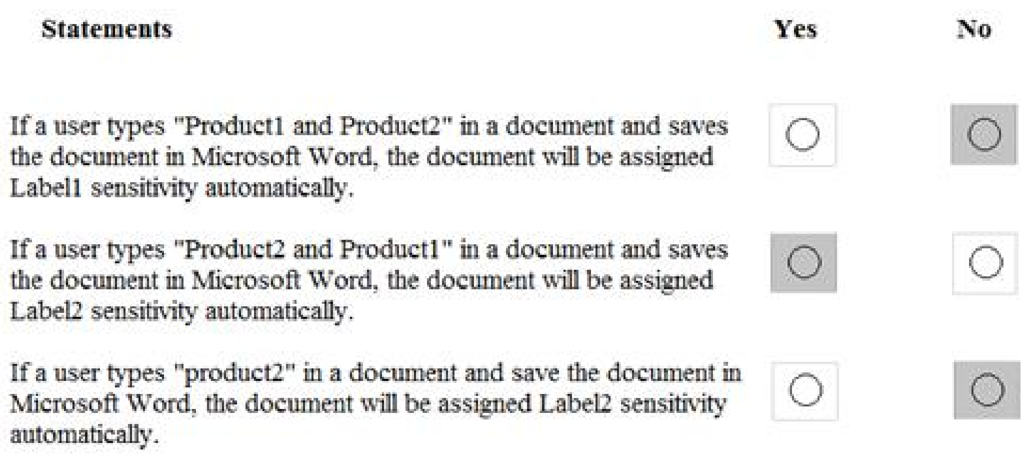


Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	○
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	[✓ ○]
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	[✓ ○]	○
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	[✓ ○]

NEW QUESTION 54

HOTSPOT

You have a Microsoft 365 subscription.

You identify the following data loss prevention (DLP) requirements:

•Send notifications to users if they attempt to send attachments that contain EU social security numbers

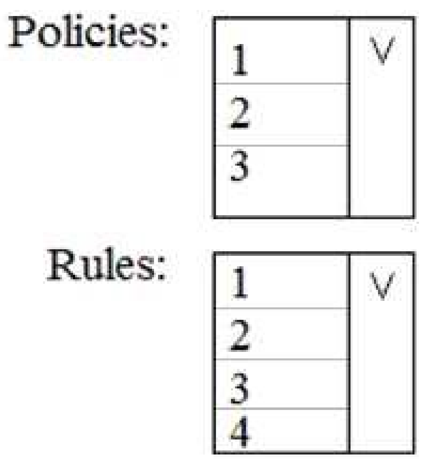
•Prevent any email messages that contain credit card numbers from being sent outside your organization

•Block the external sharing of Microsoft OneDrive content that contains EU passport numbers

•Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Policies: 1 / 2 / 3

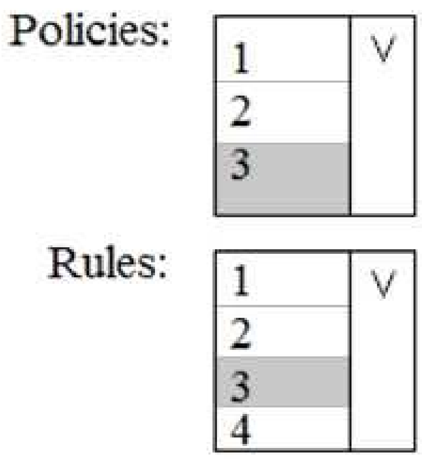
Rules: 1 / 2 / 3 / 4

A. Mastered

B. Not Mastered

Answer: A

Explanation:

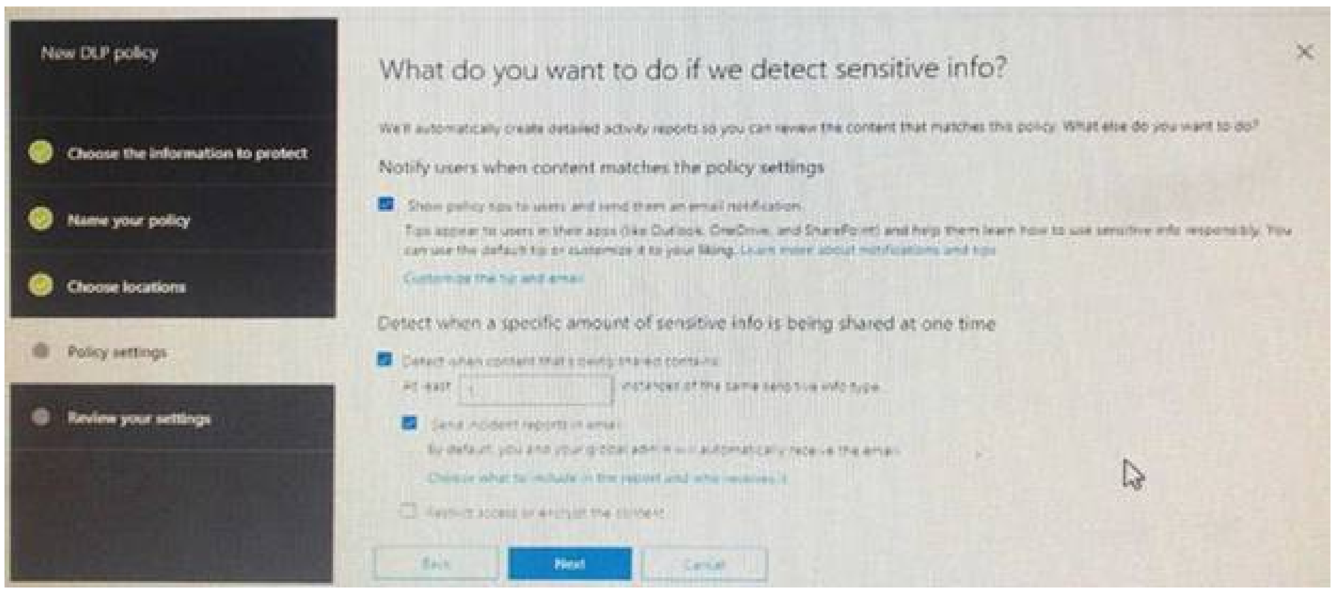


Policies: 1 / 2 / [✓ 3]

Rules: 1 / 2 / [✓ 3] / 4

NEW QUESTION 57

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 59
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 62
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 67
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 72
You have a Microsoft 365 subscription.
The Global administrator role is assigned to your user account. You have a user named Admin1. You create an eDiscovery case named Case1.
You need to ensure that Admin1 can view the results of Case1. What should you do first?

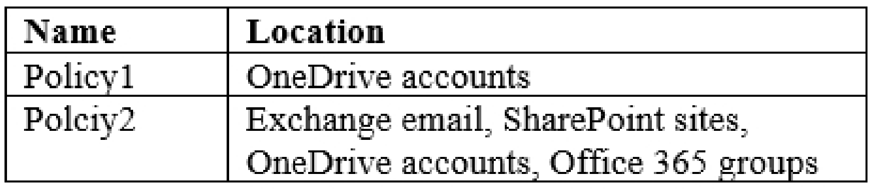
A. From the Azure Active Directory admin center, assign a role group to Admin1.

B. From the Microsoft 365 admin center, assign a role to Admin1.
C. From Security & Compliance admin center, assign a role group to Admin1.

Answer: C

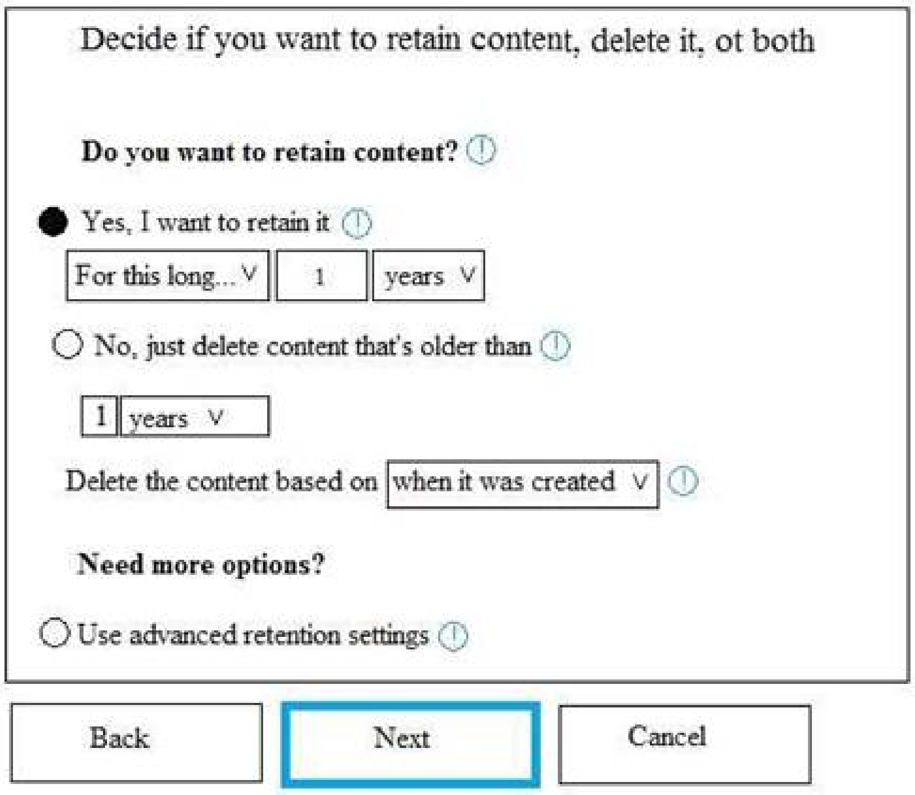
Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions

NEW QUESTION 75
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

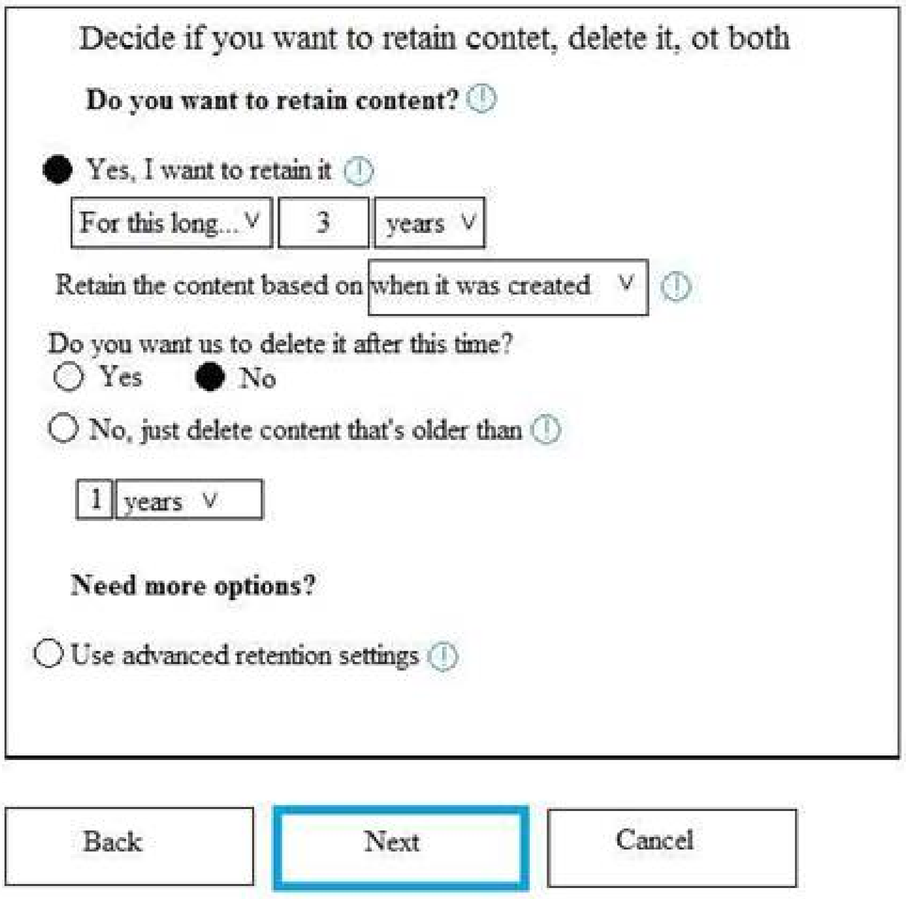
1 | years ∨

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

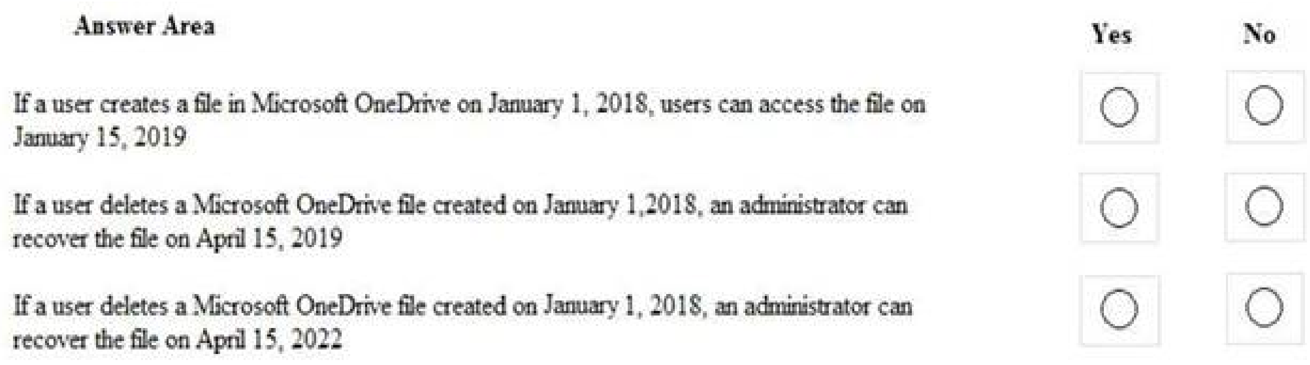
○ No, just delete content that's older than

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 79
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 82
You have a Microsoft 365 subscription.
All computers run Windows 10 Enterprise and are managed by using Microsoft Intune. You plan to view only security-related Windows telemetry data.
You need to ensure that only Windows security data is sent to Microsoft. What should you create from the Intune admin center?

A. a device configuration profile that has device restrictions configured
B. a device configuration profile that has the Endpoint Protection settings configured
C. a device configuration policy that has the System Security settings configured
D. a device compliance policy that has the Device Health settings configured

Answer: A

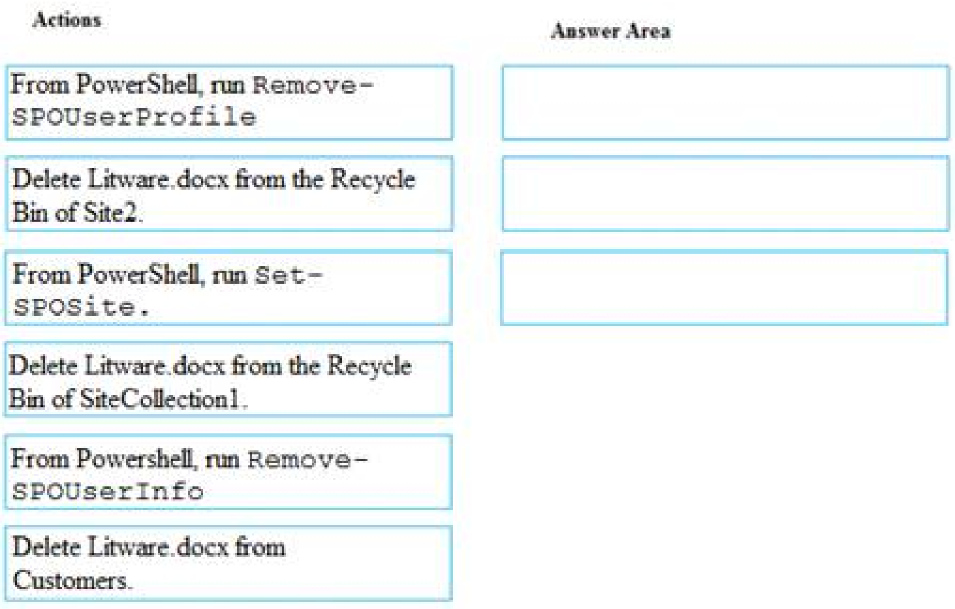
Explanation:
Reference:
https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10#reporting-and-telemetry

NEW QUESTION 83
You create a label that encrypts email data. Users report that they cannot use the label in Outlook on the web to protect the email messages they send.
You need to ensure that the users can use the new label to protect their email. What should you do?

A. Modify the priority order of label policies
B. Wait six hours and ask the users to try again
C. Create a label policy
D. Create a new sensitive information type

Answer: B

NEW QUESTION 86
DRAG DROP
You have a Microsoft 365 subscription.
You have a site collection named SiteCollection1 that contains a site named Site2. Site2 contains a document library named Customers.
Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.
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

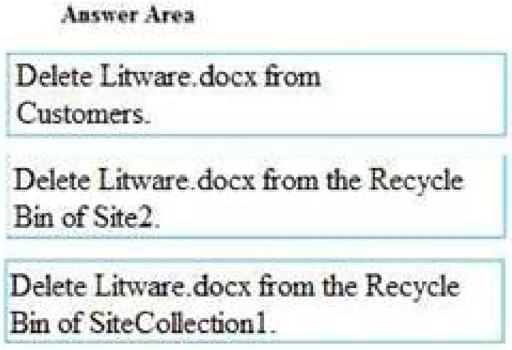
- From PowerShell, run `Remove-SPOUserProfile`
- Delete Litware.docx from the Recycle Bin of Site2.
- From PowerShell, run `Set-SPOSite.`
- Delete Litware.docx from the Recycle Bin of SiteCollection1.
- From Powershell, run `Remove-SPOUserInfo`
- Delete Litware.docx from Customers.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

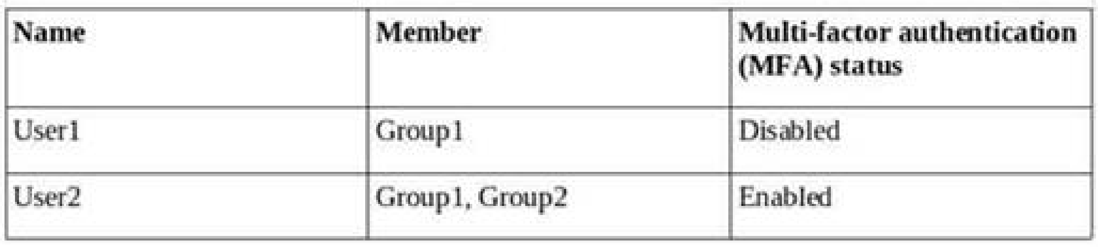
Explanation:



Answer Area

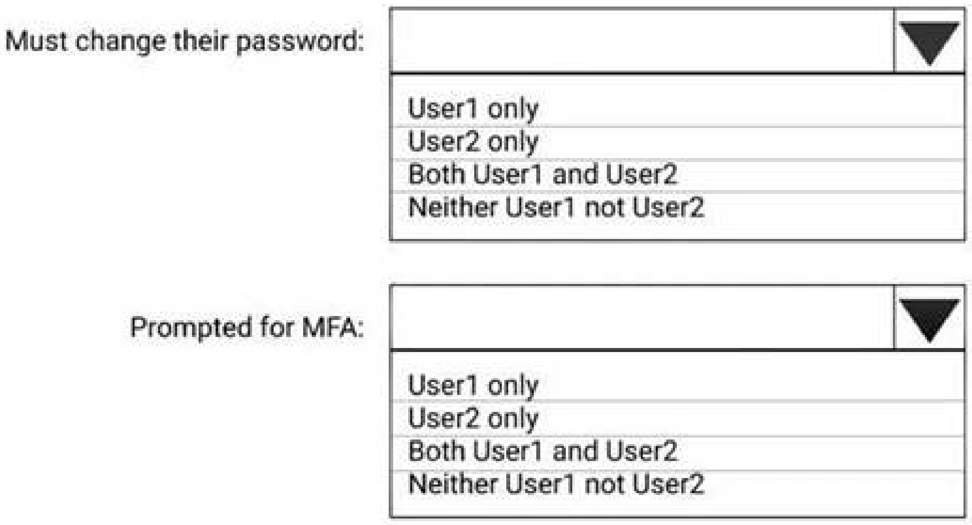
- Delete Litware.docx from Customers.
- Delete Litware.docx from the Recycle Bin of Site2.
- Delete Litware.docx from the Recycle Bin of SiteCollection1.

NEW QUESTION 90
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.



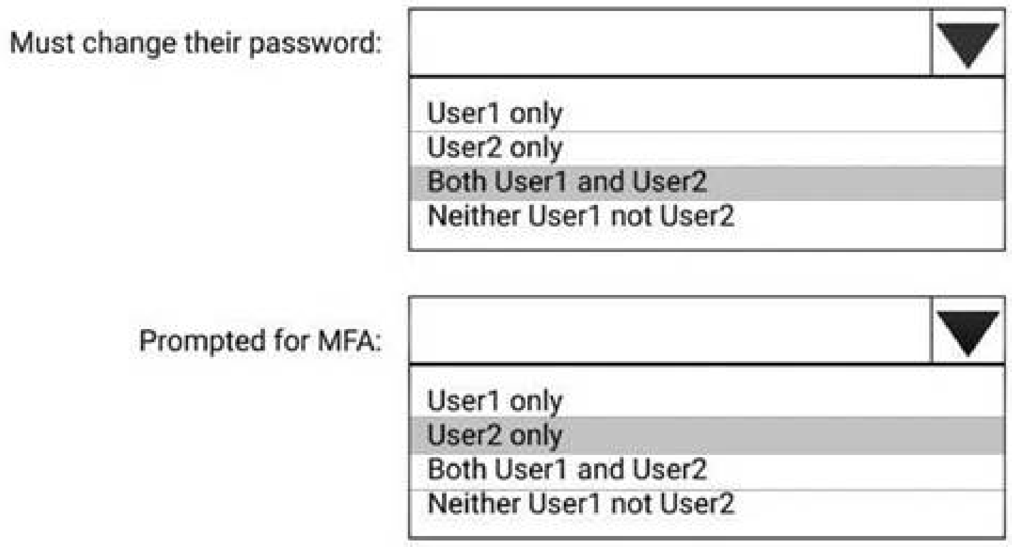
Must change their password:
- User1 only
- User2 only
- Both User1 and User2
- Neither User1 not User2

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 94

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 97

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?

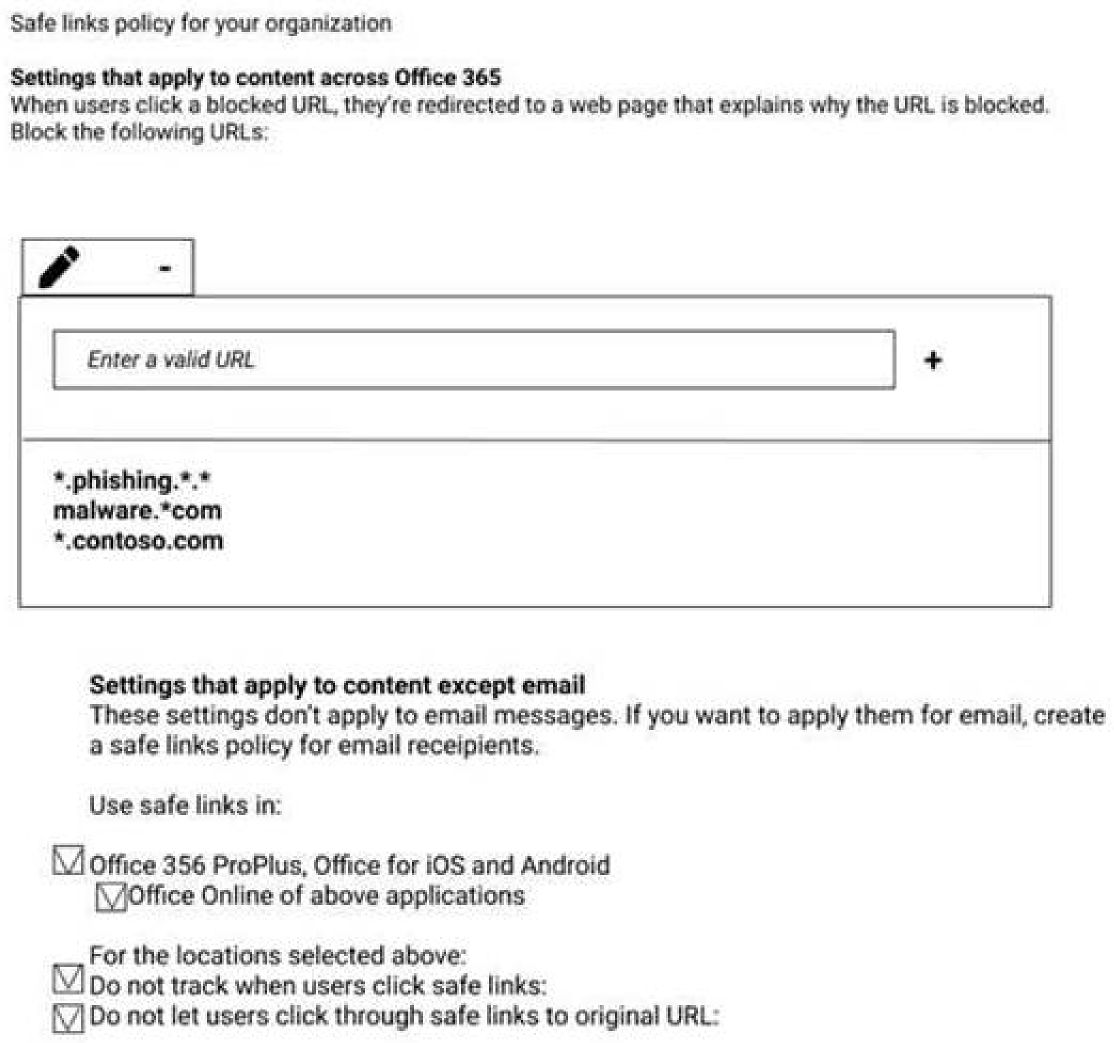
A. Configure auditing in the Office 365 Security & Compliance center.
B. Turn off Delayed updates for the Azure ATP sensors.
C. Modify the Domain synchronizer candidate's settings on the Azure ATP sensors.
D. Integrate SIEM and Azure ATP.

Answer: C

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

NEW QUESTION 102

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:

.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 104
You have a Microsoft 365 subscription that includes a user named User1.
You have a conditional access policy that applies to Microsoft Exchange Online. The conditional access policy is configured to use Conditional Access App Control.
You need to create a Microsoft Cloud App Security policy that blocks User1 from printing from Exchange Online.
Which type of Cloud App Security policy should you create?

A. an app permission policy
B. an activity policy
C. a Cloud Discovery anomaly detection policy
D. a session policy

Answer: D

NEW QUESTION 108
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 a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1. You run the Set-Maibox -Identity "User1" -AuditEnabled $true command. Does that meet the goal?

A. Yes
B. No

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set- mailbox?view=exchange-ps

NEW QUESTION 111
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 a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1. You run the Set-AuditConfig -Workload Exchange command.
Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps

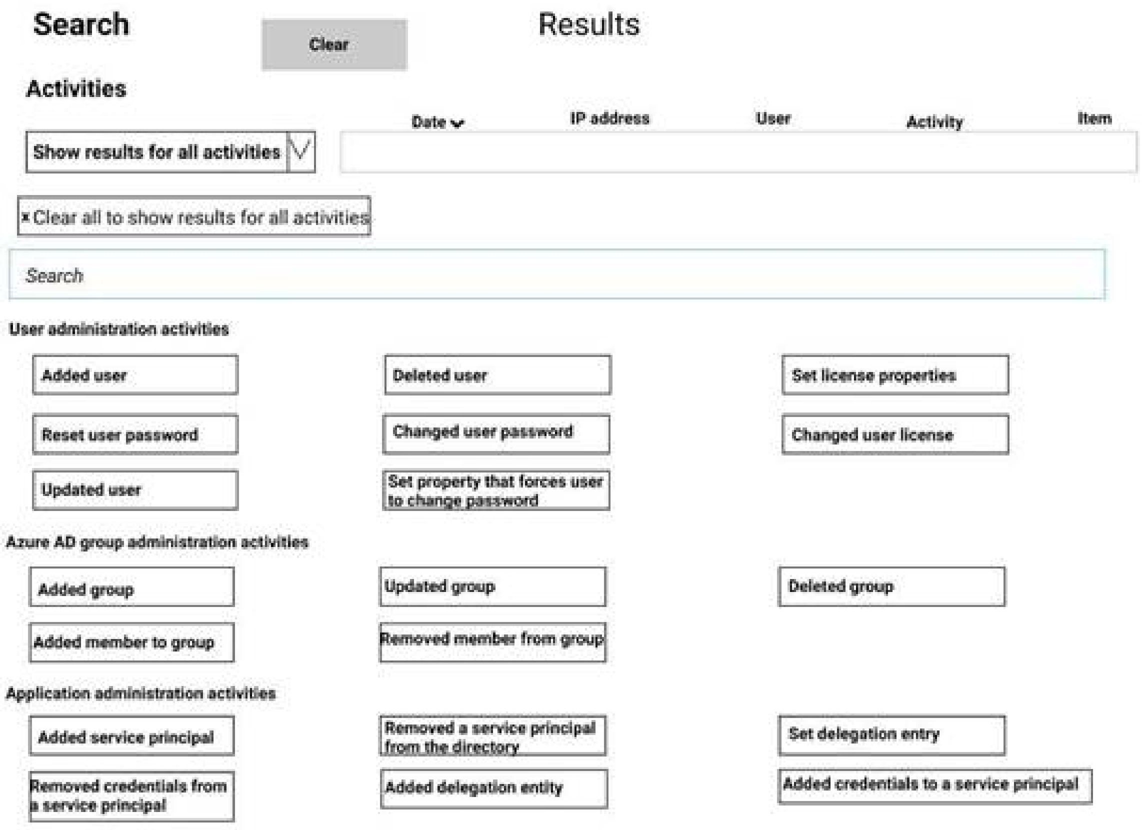
NEW QUESTION 116
You have a Microsoft 365 subscription.
You have a Microsoft SharePoint Online site named Site1. The files in Site1 are protected by using Microsoft Azure Information Protection.
From the Security & Compliance admin center, you create a label that designates personal data. You need to auto-apply the new label to all the content in Site1.
What should you do first?

A. From PowerShell, run Set-ManagedContentSettings.
B. From PowerShell, run Set-ComplianceTag.
C. From the Security & Compliance admin center, create a Data Subject Request (DSR).
D. Remove Azure Information Protection from the Site1 files.

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/apply-labels-to-personal-data-in- office-365

NEW QUESTION 120
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

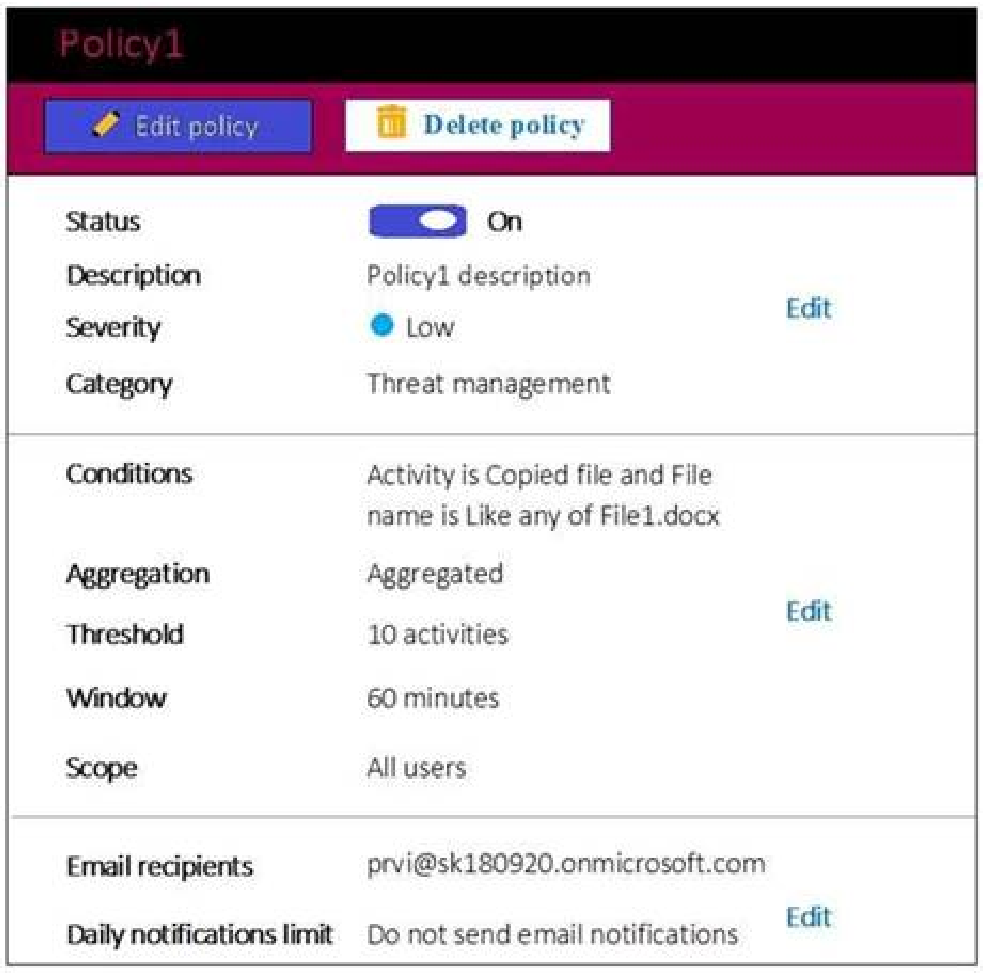
NEW QUESTION 122

HOTSPOT

You have a Microsoft 365 subscription that include three users named User1, User2, and User3.

A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute.

You create an alert policy named Policy1 as shown in the following exhibit.

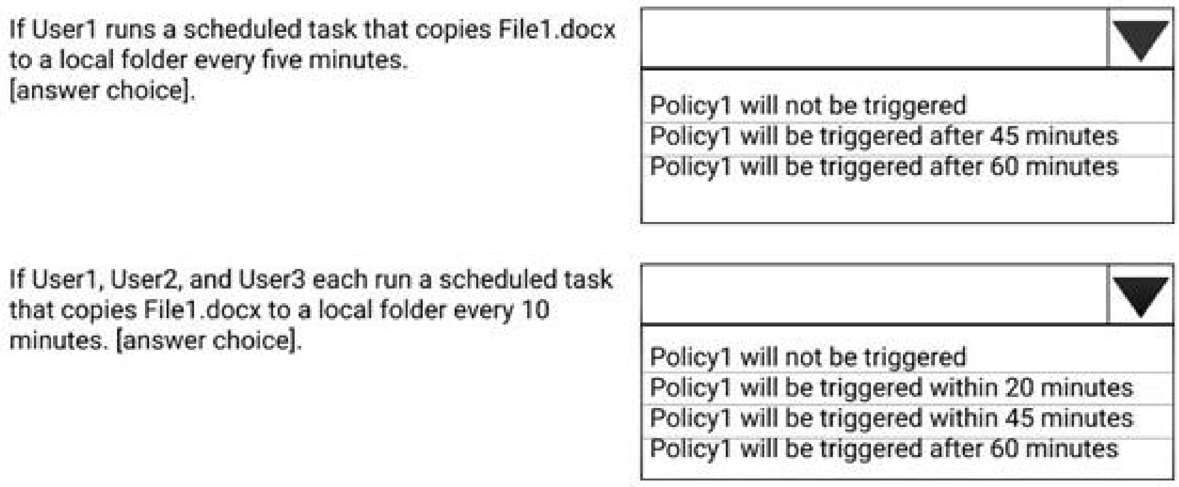


Policy1

Status	On
Description	Policy1 description
Severity	● Low
Category	Threat management
Conditions	Activity is Copied file and File name is Like any of File1.docx
Aggregation	Aggregated
Threshold	10 activities
Window	60 minutes
Scope	All users
Email recipients	prvi@sk180920.onmicrosoft.com
Daily notifications limit	Do not send email notifications

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 User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered after 45 minutes
- Policy1 will be triggered after 60 minutes

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered within 20 minutes
- Policy1 will be triggered within 45 minutes
- Policy1 will be triggered after 60 minutes

A. Mastered
B. Not Mastered

Answer: A

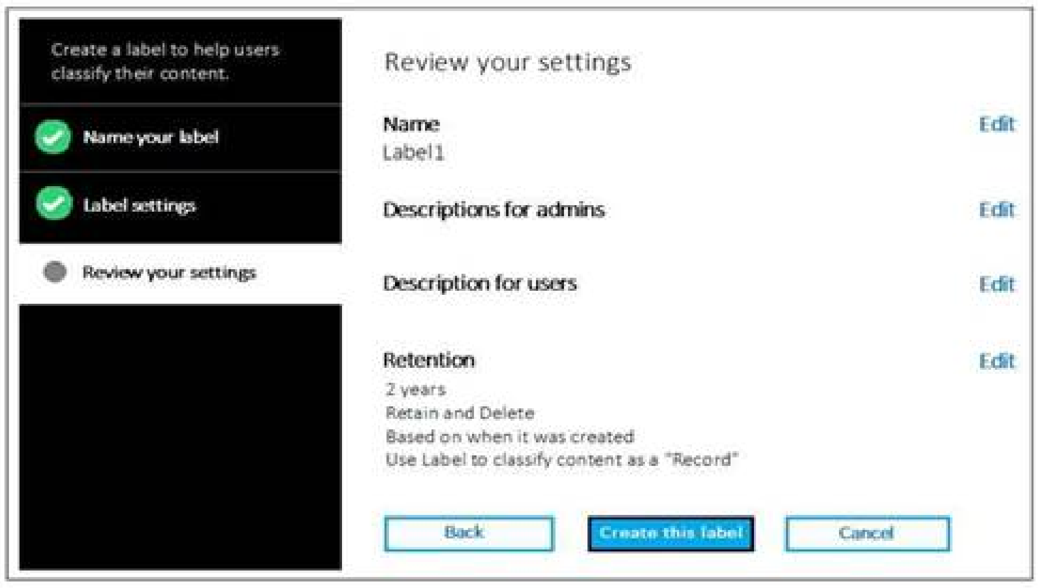
Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

NEW QUESTION 127

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

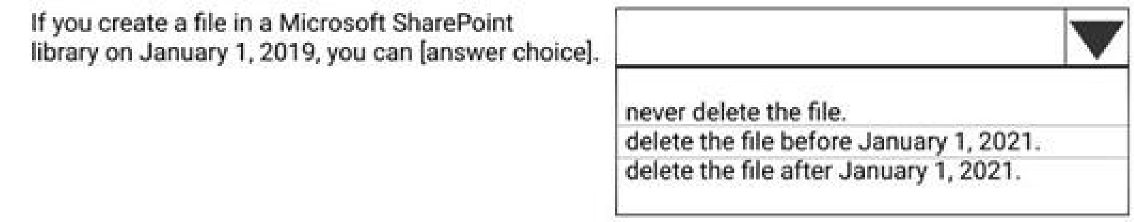
Name — Edit
Label1

Descriptions for admins — Edit

Description for users — Edit

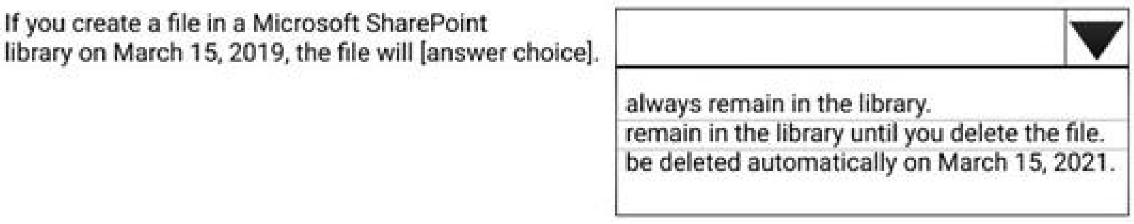
Retention — Edit
2 years
Retain and Delete
Based on when it was created
Use Label to classify content as a "Record"

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].

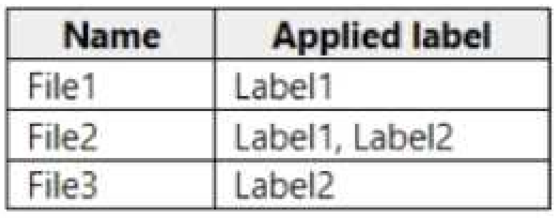
- always remain in the library.
- remain in the library until you delete the file.
- be deleted automatically on March 15, 2021.

A. Mastered
B. Not Mastered

Answer: A

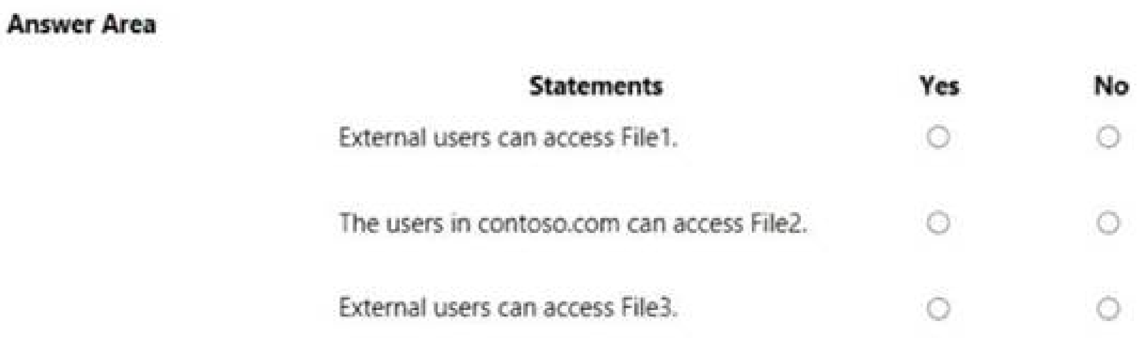
Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/labels

NEW QUESTION 131
HOTSPOT
You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. OneDrive stores files that are shared with external users. The files are configured as shown in the following table.



Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:
•Rulel:
•Conditions: Label 1, Detect content that's shared with people outside my organization
•Actions: Restrict access to the content for external users
•User notifications: Notify the user who last modified the content
•User overrides: On
•Priority: 0
•Rule2:
•Conditions: Label 1 or Label2
•Actions: Restrict access to the content
•Priority: 1
•Rule3:
•Conditions: Label2, Detect content that's shared with people outside my organization
•Actions: Restrict access to the content for external users
•User notifications: Notify the user who last modified the content
•User overrides: On
•Priority: 2
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



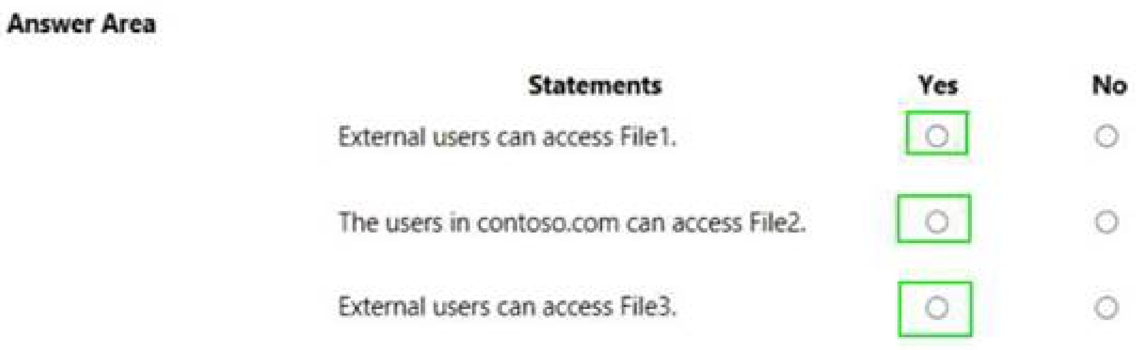
Answer Area

Statements	Yes	No
External users can access File1.	○	○
The users in contoso.com can access File2.	○	○
External users can access File3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
External users can access File1.	[✓ ○]	○
The users in contoso.com can access File2.	[✓ ○]	○
External users can access File3.	[✓ ○]	○

NEW QUESTION 132

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 135

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 139

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 Directory Service 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 142

......