Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam

NEW QUESTION 1
DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You need to automatically label the documents on Site1 that contain credit card numbers. 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	Answer Area
Create a sensitivity label.	
Create an auto-labeling policy.	
Create a sensitive information type.	
Wait 24 hours, and then turn on the policy.	
Publish the label.	
Create a retention label.	
Wait eight hours, and then turn on the policy.	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
Create a sensitivity label.	Create a sensitivity label.
Create an auto-labeling policy.	
Create a sensitive information type.	Publish the label.
Wait 24 hours, and then turn on the policy.	
Publish the label.	Create an auto-labeling policy.
Create a retention label.	
Wait eight hours, and then turn on the policy.	

NEW QUESTION 2
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
You need to implement identity protection. The solution must meet the following requirements:
? Identify when a user's credentials are compromised and shared on the dark web.
? Provide users that have compromised credentials with the ability to self-remediate.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

To identify when users have compromised credentials, configure: [A registration policy / A sign-in risk policy / A user risk policy / A multifactor authentication registration policy]

To enable self-remediation, select: [Generate a temporary password / Require multi-factor authentication / Require password change]

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: A user risk policy
Identify when a user's credentials are compromised and shared on the dark web.

User risk-based Conditional Access policy
Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:
Block access
Allow access but require a secure password change.
A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.
Box 2: Require password change
Provide users that have compromised credentials with the ability to self-remediate.
A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators

NEW QUESTION 3
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to implement device configuration profiles in Microsoft Intune. Which platform can you manage by using the profiles?

A. Ubuntu Linux
B. macOS
C. Android Enterprise
D. Windows 8.1

Answer: D

NEW QUESTION 4
- (Topic 6)
Your company has offices in five cities. The company has a Microsoft 365 tenant.
Each office is managed by a local administrator. You plan to deploy Microsoft Intune.
You need to recommend a solution to manage resources in intune that meets the following requirements:
? Local administrators must be able to manage only the resources in their respective office.
? Local administrators must be prevented from managing resources in other offices.
? Administrative effort must be minimized.
What should you include in the recommendation?

A. device categories
B. scope tags
C. configuration profiles
D. conditional access policies

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

NEW QUESTION 5
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft 365 compliance policies to meet the following requirements:
? Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
? Report on shared documents that contain PII.
What should you create?

A. an alert policy
B. a data loss prevention (DLP) policy
C. a retention policy
D. a Microsoft Cloud App Security policy

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about- dlp?view=o365-worldwide

NEW QUESTION 6
- (Topic 6)
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 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

NEW QUESTION 7
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Service Support Administrator
User3	Cloud Application Administrator
User4	*None*

You plan to provide User4 with early access to Microsoft 365 feature and service updates. You need to identify which Microsoft 365 setting must be configured, and which user can
modify the setting. The solution must use the principle of least privilege.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Microsoft 365 setting:
- Office installation options
- Privileged access
- Release preferences

User:
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Microsoft 365 setting:
- Office installation options
- Privileged access
- Release preferences

User:
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

NEW QUESTION 8
- (Topic 6)

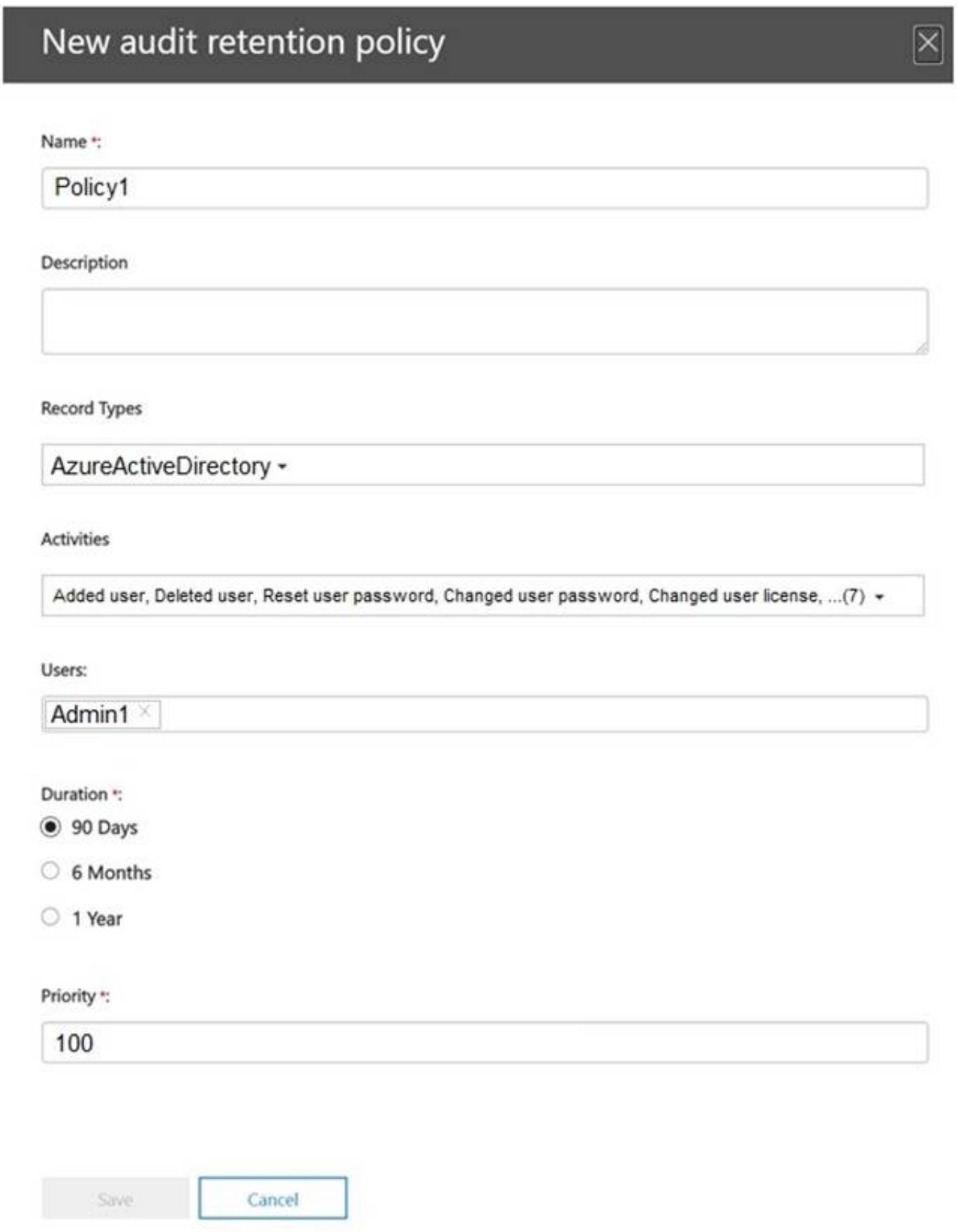
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the Azure AD credentials.
Does this meet the goal?

A. Yes
B. No

Answer: B

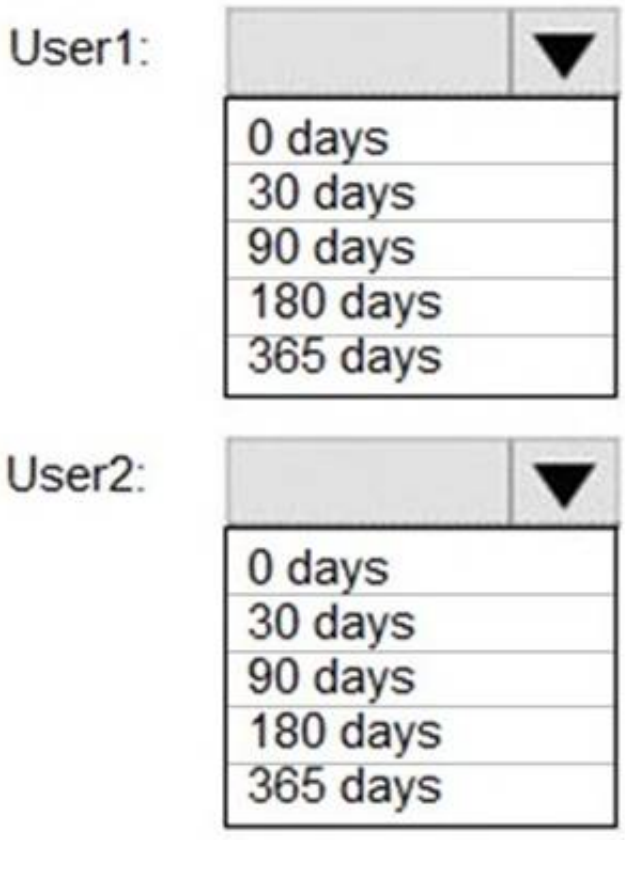
Explanation:
The question states that “all the user account synchronizations completed successfully”. Therefore, the Azure AD credentials are configured correctly in Azure AD Connect. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync- configure-filtering

NEW QUESTION 9
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains two users named Admin1 and Admin2.
All users are assigned a Microsoft 365 Enterprise E5 license and auditing is turned on.
You create the audit retention policy shown in the exhibit. (Click the Exhibit tab.)



After Policy1 is created, the following actions are performed:
? Admin1 creates a user named User1.
? Admin2 creates a user named User2.
How long will the audit events for the creation of User1 and User2 be retained? To answer, select the appropriate options in the answer area.

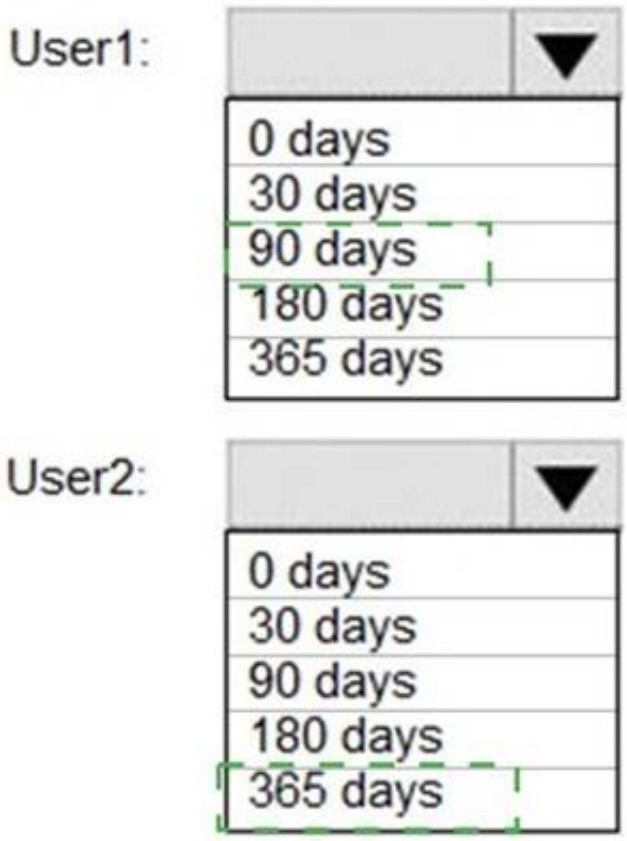
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 10
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription that contains the users in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.

Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	Group3

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

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

NEW QUESTION 10
- (Topic 6)
You purchase a new computer that has Windows 10, version 2004 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

A. Install all the feature updates released since version 2004 and all the quality updates released since version 2004 only.
B. install the West feature update and the latest quality update only.
C. install all the feature updates released since version 2004 and the latest quality update only.
D. install the latest feature update and all the quality updates released since version 2004.

Answer: B

NEW QUESTION 11
- (Topic 6)
Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 10.
You purchase a Microsoft 365 subscription.
You implement password hash synchronization and Azure AD Seamless Single Sign-On (Seamless SSO).
You need to ensure that users can use Seamless SSO from the Windows 10 computers. What should you do?

A. Join the computers to Azure AD.
B. Create a conditional access policy in Azure AD.
C. Modify the Intranet zone settings by using Group Policy.
D. Deploy an Azure AD Connect staging server.

Answer: A

NEW QUESTION 15

- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. A Built-in protection preset security policy is applied to the subscription.
Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

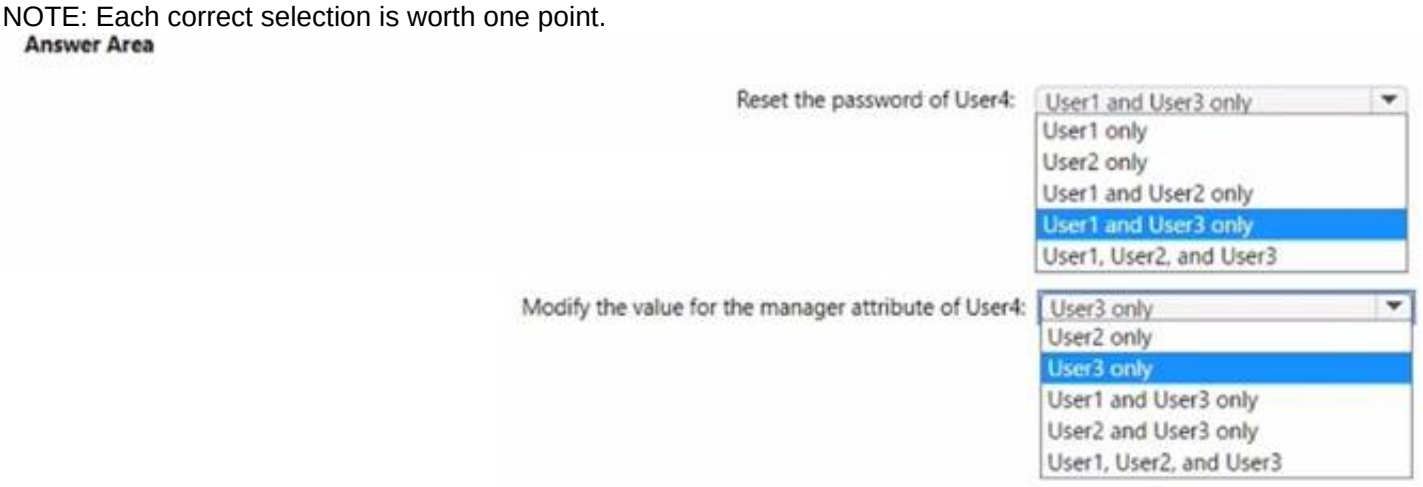
A. Anti-malware
B. Anti-phishing
C. Safe Attachments
D. Anti-spam
E. Safe Links

Answer: CE

NEW QUESTION 20
HOTSPOT - (Topic 6)
Your company has a Azure AD tenant named comoso.onmicrosoft.com that contains the users shown in the following table.

Name	Role
User1	Password Administrator
User2	Security Administrator
User3	User Administrator
User4	None

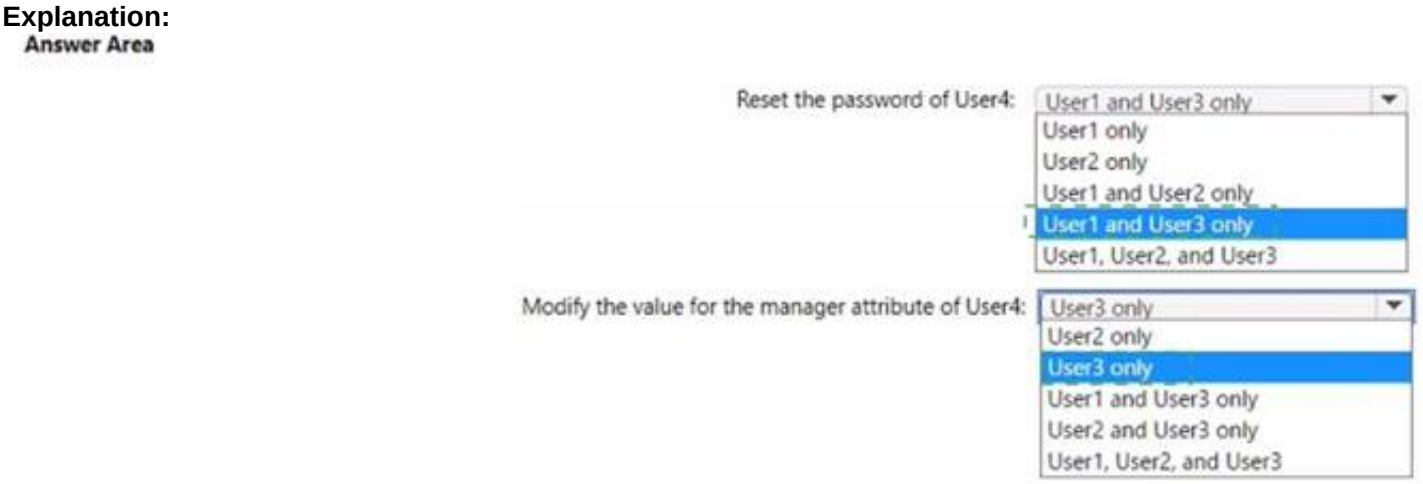
You need to identify which users can perform the following administrative tasks:
• Reset the password of User4.
• Modify the value for the manager attribute of User4.
Which users should you identify for each task? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 23
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365 and contains a mailbox named Mailbox1.
You plan to use Mailbox1 to collect and analyze unfiltered email messages.
You need to ensure that Defender for Office 365 takes no action on any inbound emails delivered to Mailbox1.
What should you do?

A. Configure a retention policy for Mailbox1.
B. Create a mail flow rule.
C. Configure Mailbox! as a SecOps mailbox.
D. Place a litigation hold on Mailbox1.

Answer: D

NEW QUESTION 27
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
On activation, require	Azure MFA
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	15 day(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

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.

Answer Area

A user that is assigned the Global Administrator role as active **[answer choice]**.
- will lose the role after eight hours
- can reactivate the role every eight hours
- can reactivate the role every 15 days
- will lose the role after 15 days

You can make the Global Administrator role available to activation requests **[answer choice]**.
- for up to eight hours
- for up to three months
- for up to 15 days
- until the requests are revoked manually

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: will lose the role after eight hours
From exhibit: Activation, Activation maximum duration (hours): 8 hour(s)
Box 2: for up to three months
We see from exhibit: Assignment, Expire eligible assignment after: 3 month(s)

NEW QUESTION 28
HOTSPOT - (Topic 6)
You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.

Choose the types of content to protect

This policy will protect that matches these requirements. You can choose sensitive info types and existing labels

Content contains

Any of these

Sensitive info type	Match accuracy min	Match accuracy max
Credit Card Number	85	100

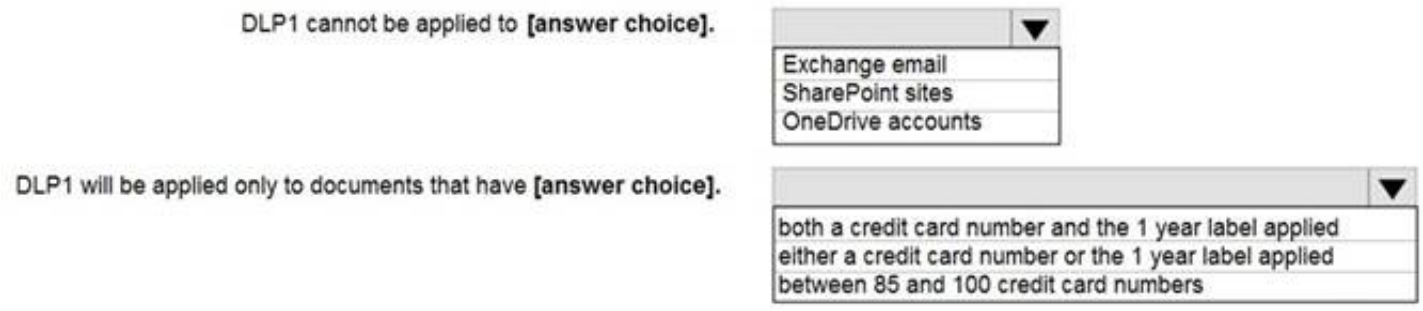
Retention labels
1 year

Add

+ Add group

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. Mastered
B. Not Mastered

Answer: A

Explanation:
Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

NEW QUESTION 30
- (Topic 6)
You have a Microsoft 365 subscription that contains the alerts shown in the following table.

Name	Severity	Status	Comment	Category
Alert1	Medium	Active	Comment1	Threat management
Alert2	Low	Resolved	Comment2	Other

Which properties of the alerts can you modify?

A. Status only
B. Status and Comment only
C. Status and Severity only
D. Status, Severity, and Comment only
E. Status, Severity, Comment and Category

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365-worldwide#limitations

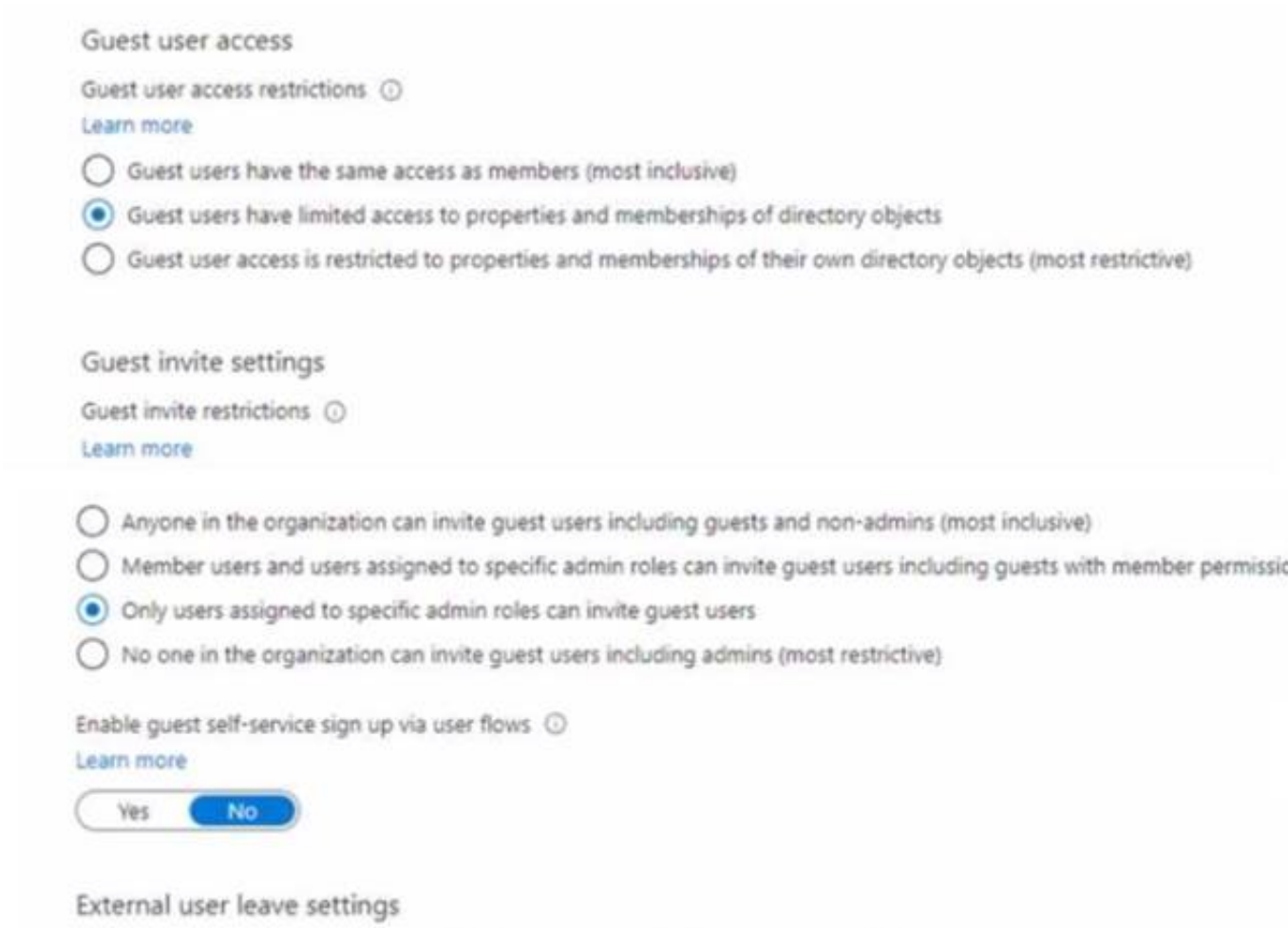
NEW QUESTION 33
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type	Role
Group1	Security	Helpdesk Administrator
Group2	Security	*None*
Group3	Microsoft 365	User Administrator

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

In Azure AD, you configure the External collaboration settings as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

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
User1 can invite guest users.	○	○
User2 can invite guest users.	○	○
User3 can invite guest users.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can invite guest users.	○	○
User2 can invite guest users.	○	○
User3 can invite guest users.	○	○

NEW QUESTION 36
- (Topic 6)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.
The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User1 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes
B. No

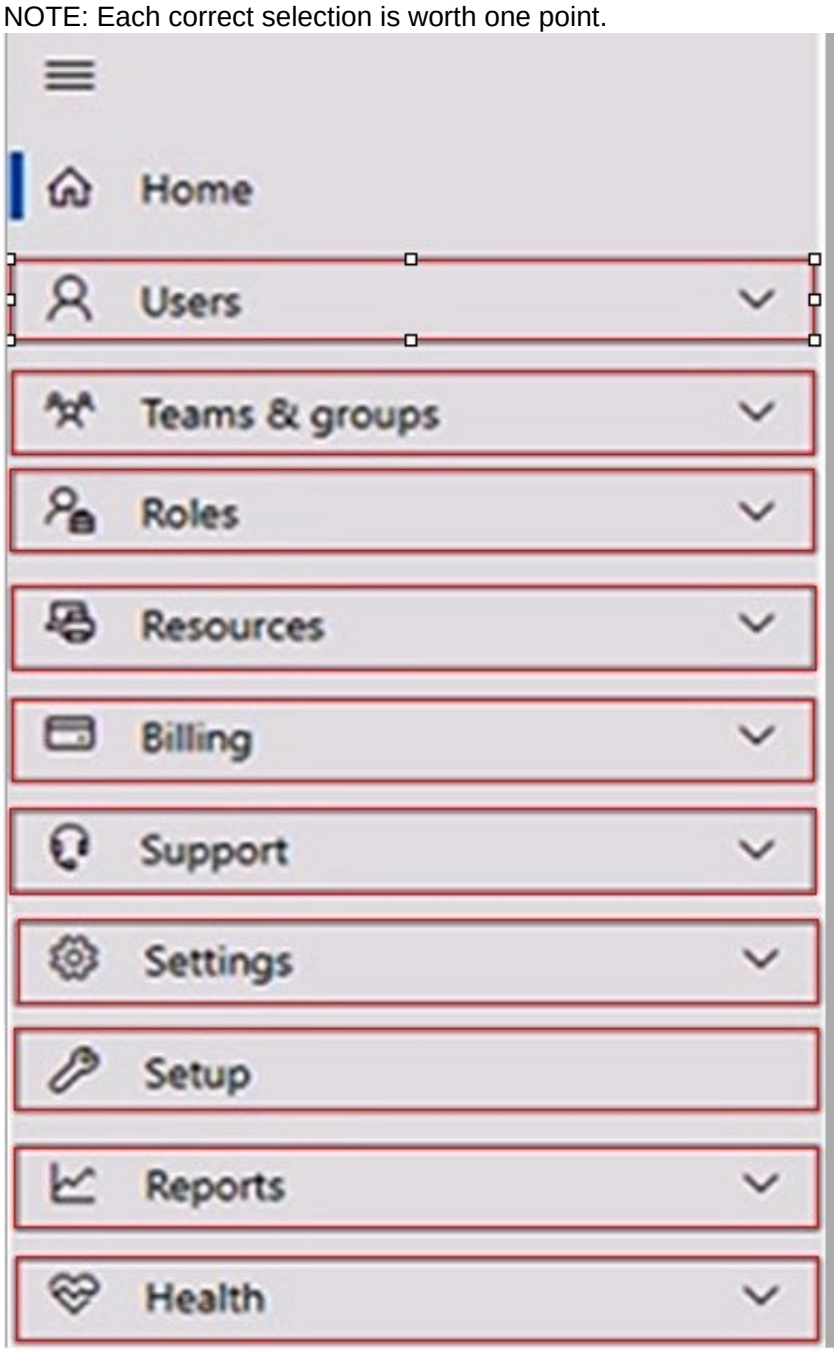
Answer: A

NEW QUESTION 38
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You plan to perform device discovery and authenticated scans of network devices. You install and register the network scanner on a device named Device1.
What should you do next?

A. Connect Defender for Endpoint to Microsoft Intune.
B. Apply for Microsoft Threat Experts - Targeted Attack Notifications.
C. Create an assessment job.
D. Download and run an onboarding package.

Answer: C

NEW QUESTION 43
HOTSPOT - (Topic 6)
HOTSPOT
Your company has a Microsoft 365 E5 subscription. You need to perform the following tasks:
View the Adoption Score of the company. Create a new service request to Microsoft.
Which two options should you use in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Reports
View the Adoption Score of the company.
How to enable Adoption Score To enable Adoption Score:
? Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score
? Select enable Adoption Score. It can take up to 24 hours for insights to become
available.
Box 2: Support
Create a new service request to Microsoft.
Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request. If you're in the admin center, select Support > New service request.

NEW QUESTION 48
- (Topic 6)
You have a Microsoft 365 subscription.
You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.
To which location can the policy be applied?

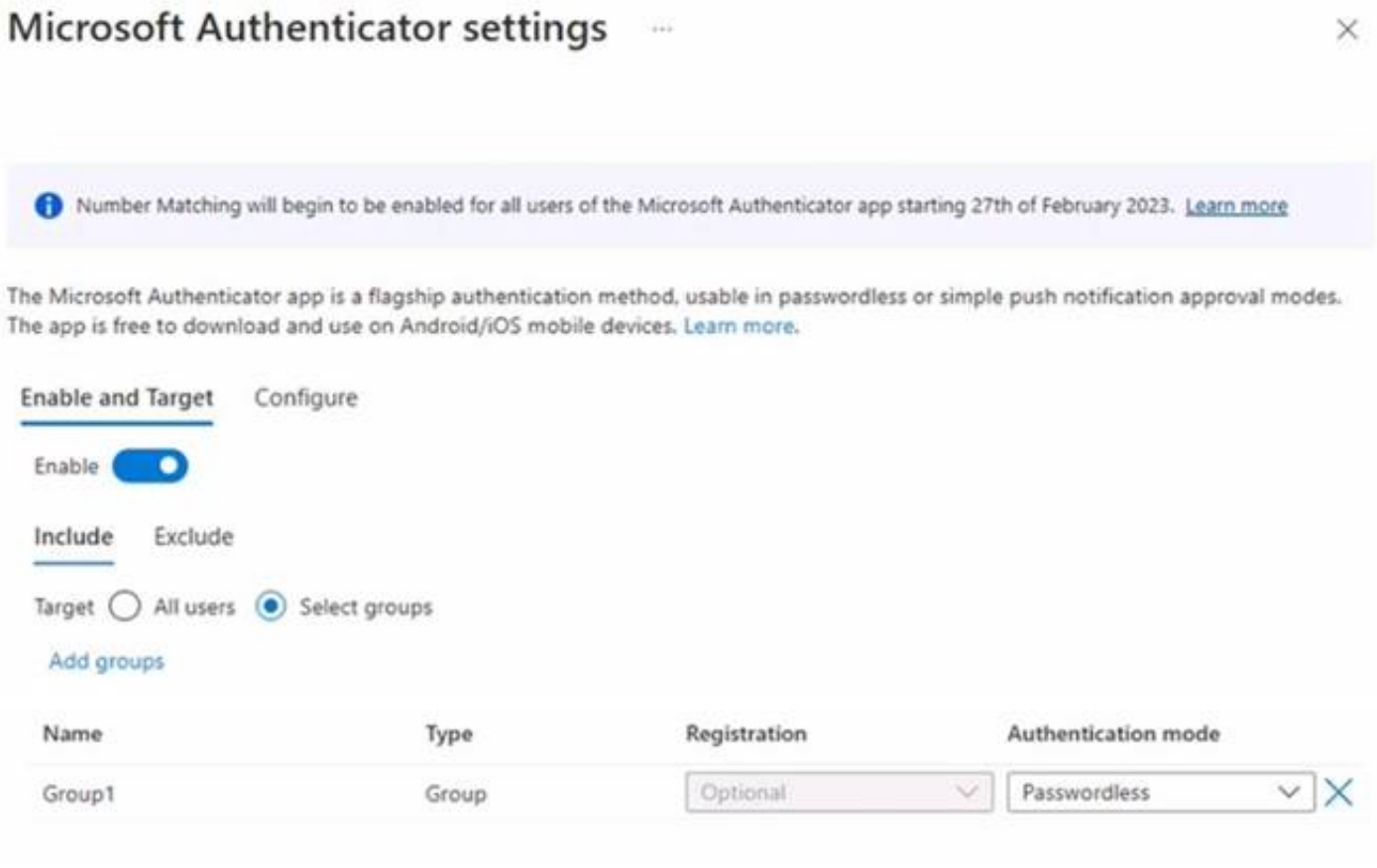
A. OneDrive accounts
B. Exchange email
C. Teams chat and channel messages
D. SharePoint sites

Answer: B

NEW QUESTION 49
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Passwordless capable	Multi-factor authentication (MFA) method registered
User1	Group1	Capable	Microsoft Authenticator app (push notification)
User2	Group2	Capable	Microsoft Authenticator app (push notification)
User3	Group1, Group2	Capable	Mobile phone, Windows Hello for Business

Each user has a device with the Microsoft Authenticator app installed.
From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit tab.)



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
User1 can use number matching during sign-in.	○	○
User2 can use number matching during sign-in.	○	○
User3 can use number matching during sign-in.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can use number matching during sign-in.	○	○
User2 can use number matching during sign-in.	○	○
User3 can use number matching during sign-in.	○	○

NEW QUESTION 54
- (Topic 6)
You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.
You need to prevent the members or Group1 from communicating with the members of Group2 by using Microsoft Teams. The solution must comply with regulatory requirements and must not affect other user in the tenant.
What should you use?

A. information barriers
B. communication compliance policies
C. moderated distribution groups
D. administrator units in Azure Active Directory (Azure AD)

Answer: A

NEW QUESTION 57
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature. You need to block users from downloading a file named File1.exe.
What should you use?

A. an indicator
B. a suppression rule
C. a device configuration profile

Answer: A

NEW QUESTION 59
- (Topic 6)
You have a Microsoft 365 E5 subscription.
From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.
What is the longest time range that can be included in the report?

A. 1 day
B. 7 days
C. 30 days
D. 90 days

Answer: C

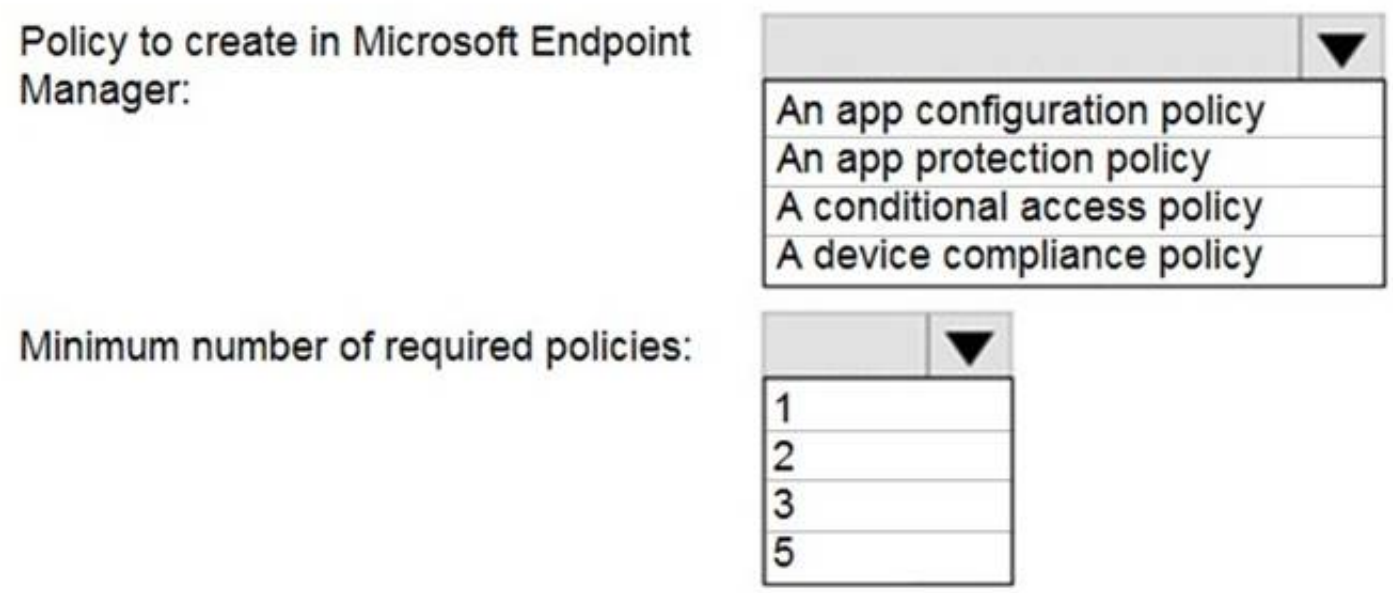
Explanation:
View email security reports in the Microsoft 365 Defender portal
The aggregate view shows data for the last 90 days and the detail view shows data for the last 30 days
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email- security

NEW QUESTION 64
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.
You need to prevent users from copying data from App1 and pasting the data into other apps.
Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in

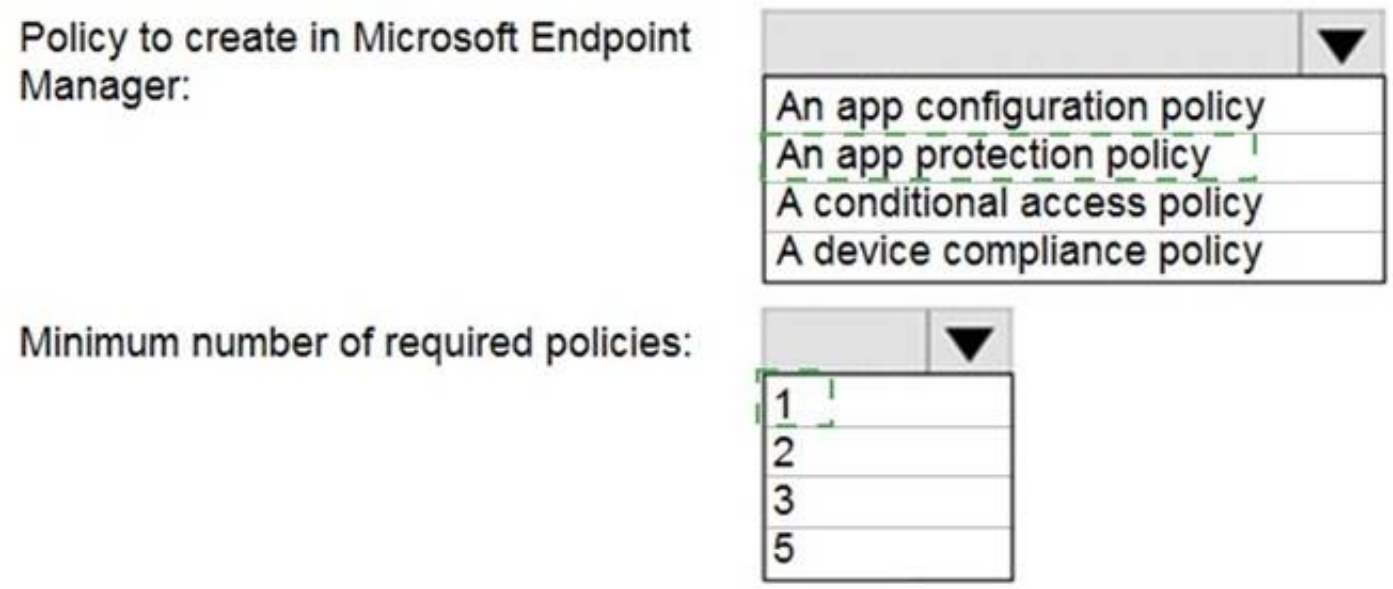
the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 67
- (Topic 6)
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 goats. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. You deploy a Microsoft Entra tenant.
Another administrator configures the domain to synchronize to the Microsoft Entra tenant.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.
You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.
Solution: From Microsoft Entra Connect, you modify the filtering settings. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 72
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1, Group2
User2	Group2, Group3
User3	Group1, Group3

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.

Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

The policies use the settings shown in the following table.

Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

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

Statements	Yes	No
User1 has their cache cleared on close.	○	○
User2 has Cursor movement set to Visual.	○	○
User3 has Cursor movement set to Visual.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 has their cache cleared on close.	○	○
User2 has Cursor movement set to Visual.	○	○
User3 has Cursor movement set to Visual.	○	○

NEW QUESTION 77
- (Topic 6)
You have a Microsoft 365 subscription.
You need to configure a compliance solution that meets the following requirements: Defines sensitive data based on existing data samples
Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages
Which two components should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a trainable classifier
B. a sensitive info type
C. an insider risk policy
D. an adaptive policy scope
E. a data loss prevention (DLP) policy

Answer: AE

Explanation:
A: Classifiers
This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.
Where you can use classifiers
Classifiers are available to use as a condition for: Office auto-labeling with sensitivity labels
Auto-apply retention label policy based on a condition Communication compliance
Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.
Data loss prevention

E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp

NEW QUESTION 82
- (Topic 6)
You have a Microsoft 365 E5 tenant.
industry regulations require that the tenant comply with the ISO 27001 standard. You need to evaluate the tenant based on the standard

A. From Policy in the Azure portal, select Compliance, and then assign a pokey
B. From Compliance Manager, create an assessment
C. From the Microsoft J6i compliance center, create an audit retention policy.
D. From the Microsoft 365 admin center enable the Productivity Score.

Answer: B

NEW QUESTION 86
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.
All the devices in your organization are onboarded to Microsoft Defender for Endpoint.
You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.
What should you do?

A. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
B. From Alerts queue, create a suppression rule and assign an alert.
C. From Advanced hunting, create a query and a detection rule.
D. From the Microsoft Purview compliance portal, create an audit log search.

Answer: C

NEW QUESTION 90
- (Topic 6)
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 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

NEW QUESTION 91
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert
occurs only on a Windows 10 device. The solution must minimize administrative effort. What should you do first?

A. From the Microsoft 365 admin center, create a mail-enabled security group.
B. From the Microsoft 365 Defender portal, create a device group.
C. From the Microsoft Endpoint Manager admin center, create a device category.
D. From the Azure Active Directory admin center, create a dynamic device group.

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide

NEW QUESTION 92
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations: Name: Policy1
Assignments:
- Users and groups: Group1
- Cloud aps or actions: All cloud apps
? Access controls:
? Grant, require multi-factor authentication
? Enable policy: Report-only
You set Enabled Security defaults to Yes for the tenant.
For each of the following settings select Yes, if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:
? Conditional Access policies can be enabled in report-only mode.
? During sign-in, policies in report-only mode are evaluated but not enforced.
? Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
? Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

NEW QUESTION 95
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:
? MDM user scope: Some
? uk.co.certification.simulator.questionpool.PList@184e72e0
? MAM user scope: Some
? uk.co.certification.simulator.questionpool.PList@184e7360 You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

NEW QUESTION 100
- (Topic 6)
You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Exchange Administrator
User2	User Administrator
User3	Global Administrator
User4	None

You add another user named User5 to the User Administrator role. You need to identify which two management tasks User5 can perform.
Which two tasks should you identify? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Delete User2 and User4 only.
B. Reset the password of User4 only
C. Reset the password of any user in Azure AD.
D. Delete User1, User2, and User4 only.
E. Reset the password of User2 and User4 only.
F. Delete any user in Azure AD.

Answer: AE

Explanation:
Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).
Only on users who are non-admins or in any of the following limited admin roles:
• Directory Readers
• Guest Inviter
• Helpdesk Administrator
• Message Center Reader
• Reports Reader
• User Administrator Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#available-roles

NEW QUESTION 101
FILL IN THE BLANK - (Topic 6)
You have a Microsoft 365 subscription.
From Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.
You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.
Solution: From Windows PowerShell, you run the New-complianceSecurityFilter cmdlet with the appropriate parameters.
Does this meet the goal?
A Yes

A. No

Answer: A

NEW QUESTION 106
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 security center. Which Microsoft service source will appear on the Incidents page of the Microsoft 365
security center?

A. Microsoft Cloud App Security
B. Azure Sentinel
C. Azure Web Application Firewall
D. Azure Defender

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate- alerts?view=o365-worldwide

NEW QUESTION 108
HOTSPOT - (Topic 6)
HOTSPOT

				actions				
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.
Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	
The SP800 assessment score will increase by 54 points.	○	
The Data Protection Baseline score will increase by 9 points.	○	

NEW QUESTION 113
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that contains the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to create a compliance policy named Compliance1.
You need to identify the groups that meet the following requirements:
? Can be added to Compliance1 as recipients of noncompliance notifications
? Can be assigned to Compliance1
To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

NEW QUESTION 117
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.com.
For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.
You plan to sync contoso.com to an Azure AD tenant.
You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.
What should you include in the recommendation?

A. pass-through authentication
B. conditional access policies
C. password synchronization
D. Azure AD Identity Protection policies

Answer: A

Explanation:
Reference:
https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

NEW QUESTION 118
- (Topic 6)
You enable the Azure AD Identity Protection weekly digest email. You create the users shown in the following table.

Name	Role
Admin1	Security reader
Admin2	User administrator
Admin3	Security administrator
Admin4	Compliance administrator

Which users will receive the weekly digest email automatically?

A. Admin2, Admin3, and Admin4 only
B. Admin1, Admin2, Admin3, and Admin4
C. Admin2 and Admin3 only
D. Admin3 only
E. Admin1 and Admin3 only

Answer: E

Explanation:
By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or Security Administrators will automatically be added to the recipients list.

NEW QUESTION 119
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	**None**	Purchaser	Group2
User3	**None**	Basic Purchaser	Group3

You perform the following actions:
? Provision the private store in Microsoft Store for Business.
? Add an app named App1 to the private store.
? Set Private store availability for App1 to Specific groups, and then select Group3.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can install App1 from the private store.	○	○
User2 can install App1 from the private store.	○	○
User3 can install App1 from the private store.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can install App1 from the private store.	○	○
User2 can install App1 from the private store.	○	○
User3 can install App1 from the private store.	○	○

NEW QUESTION 123
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription.
You deploy the anti-phishing policy shown in the following exhibit.
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.

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the **[answer choice]** setting.

- Add trusted senders and domains
- Enable domains to protect
- Enable users to protect
- Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the **[answer choice]** setting.

- Add trusted senders and domains
- Enable intelligence for impersonation protection
- Enable spoof intelligence

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Enable users to protect
Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.
User impersonation protection
User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.
You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation
is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).
When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender's email address, the action for impersonated users is applied to the message.
Box 2: Add trusted senders and domains Trusted senders and domains
Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren't applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.

NEW QUESTION 127
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You create an account tor a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.
Does this meet the goal?

A. Yes
B. no

Answer: B

NEW QUESTION 128
- (Topic 6)
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Department
User1	Human resources
User2	Research
User3	Human resources
User4	Marketing

You need to configure group-based licensing to meet the following requirements:
? To all users, deploy an Office 365 E3 license without the Power Automate license option.
? To all users, deploy an Enterprise Mobility + Security E5 license.
? To the users in the research department only, deploy a Power BI Pro license.
? To the users in the marketing department only, deploy a Visio Plan 2 license.
What is the minimum number of deployment groups required?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: C

Explanation:
One for all users, one for the research department, and one for the marketing department.

Note: What are Deployment Groups?
With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers on-premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.
Reference:
https://devblogs.microsoft.com/devops/deployment-groups-is-now-generally-available-sharing-of-targets-and-more

NEW QUESTION 129
- (Topic 6)
You have a Microsoft 365 subscription.
You plan to implement Microsoft Purview Privileged Access Management. Which Microsoft Office 365 workloads support privileged access?

A. Microsoft Exchange Online only
B. Microsoft Teams only
C. Microsoft Exchanqe Online and SharePoint Online only
D. Microsoft Teams and SharePoint Online only
E. Microsoft Teams, Exchanqe Online, and SharePoint Online

Answer: A

Explanation:
Privileged access management
Having standing access by some users to sensitive information or critical network configuration settings in Microsoft Exchange Online is a potential pathway for compromised accounts or internal threat activities. Microsoft Purview Privileged Access Management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. Instead of administrators having constant access, just-in-time access rules are implemented for tasks that need elevated permissions. Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.
Note: When will privileged access support Office 365 workloads beyond Exchange? Privileged access management will be available in other Office 365 workloads soon.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access- management-solution-overview
https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management

NEW QUESTION 131
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

Name	Type
Policy1	Anti-phishing
Policy2	Anti-spam
Policy3	Anti-malware
Policy4	Safe Attachments

All the policies are configured to send malicious email messages to quarantine. Which policies support a customized quarantine retention period?

A. Policy1 and Policy2 only
B. Policy2 and Policy4 only
C. Policy3 and Policy4 only
D. Policy1 and Policy3only

Answer: A

NEW QUESTION 132
- (Topic 6)
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 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp

NEW QUESTION 135
- (Topic 6)
You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.
From Microsoft Defender Security Center, you perform a security investigation. You need to run a PowerShell script on the device to collect forensic information.

Which action should you select on the device page?

A. Initiate Live Response Session
B. Initiate Automated Investigation
C. Collect investigation package
D. Go hunt

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

NEW QUESTION 136
- (Topic 6)
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant includes a user named User1.
You enable Azure AD Identity Protection.
You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.
To which role should you add User1?

A. Security Reader
B. Global Administrator
C. Owner
D. User Administrator

Answer: A

NEW QUESTION 137
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of	Device
User1	Group1	Device1
User2	Group1	Device2, Device3

The devices are configured as shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Joined
Device3	Android	Registered

You have a Conditional Access policy named CAPolicy1 that has the following settings: 1.Assignments
? Users or workload identities: Group1
? Cloud apps or actions: Office 365 SharePoint Online
? Conditions
- Filter for devices: Exclude filtered devices from the policy
- Rule syntax: device.displayName -startsWith "Device" 2.Access controls
? Grant
- Grant: Block access
? Session: 0 controls selected 3.Enable policy: On
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
User1 can access Site1 from Device1.	○	○
User2 can access Site1 from Device2.	○	○
User2 can access Site1 from Device3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
User1 is member of Group1 and has Device1.
Device1 is not Azure AD joined.
Note: Requiring a hybrid Azure AD joined device is dependent on your devices already being hybrid Azure AD joined.
Box 2: Yes
User2 is member of Group1 and has devices Device2 and Device3. Device2 is Azure AD joined.
Device2 is excluded from CAPolicy1 (which would block access to Site1). Box 3: Yes
User2 is member of Group1 and has devices Device2 and Device3.
Device3 is Android and is Azure AD registered.
Device3 is excluded from CAPolicy1 (which would block access to Site1).
Note: On Windows 7, iOS, Android, macOS, and some third-party web browsers, Azure AD identifies the device using a client certificate that is provisioned when the device is registered with Azure AD. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.

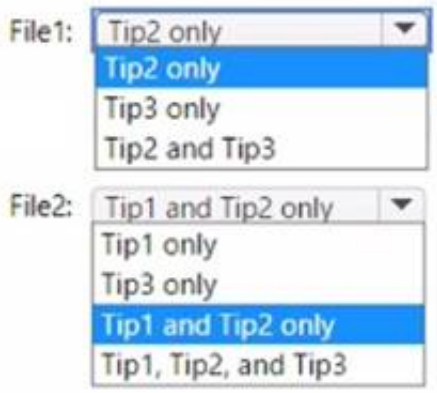
NEW QUESTION 142
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. Site! contains the files shown in the following table.

Name	Number of IP addresses in the file
File1	2
File2	3

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	If there is a match, stop processing	Priority
Rule1	3 or more IP addresses	Tip1	No	0
Rule2	1 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

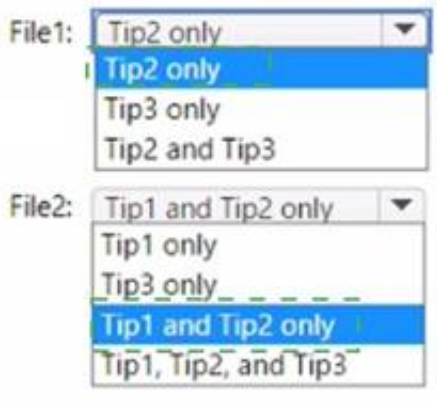
You apply DLP1 to Site1.
Which policy tip is displayed for each file? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area



A. Mastered
B. Not Mastered

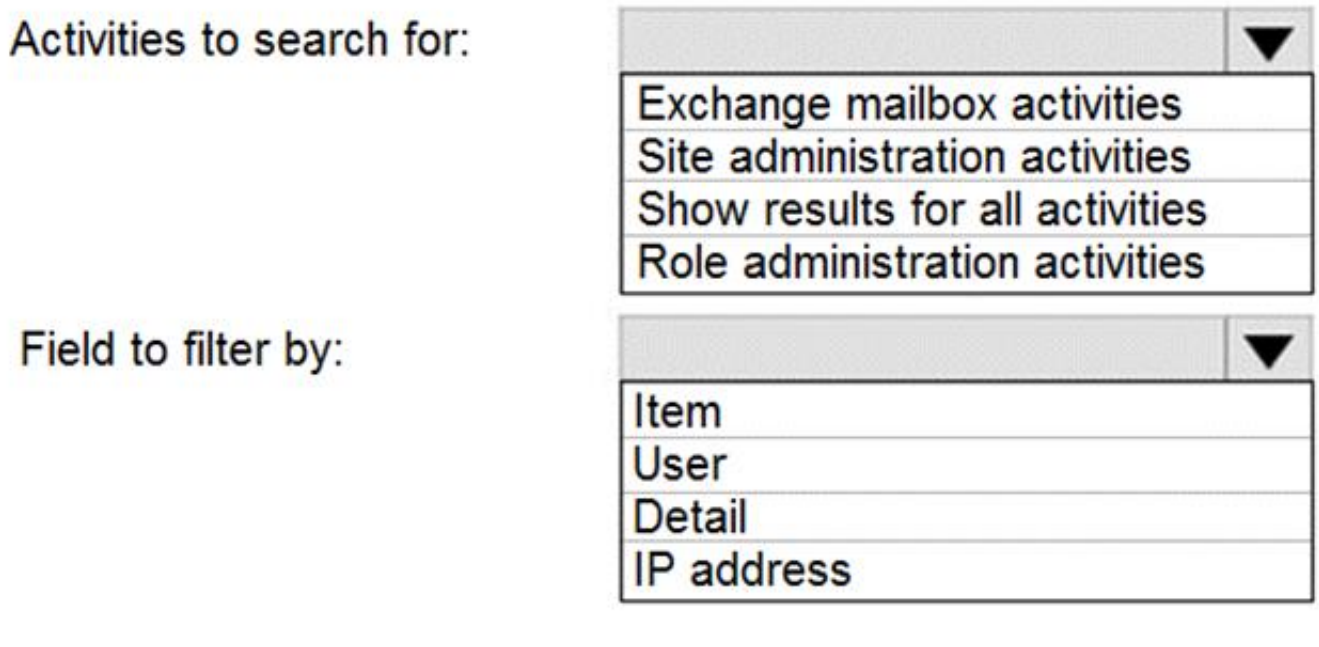
Answer: A

Explanation:
Answer Area



NEW QUESTION 143

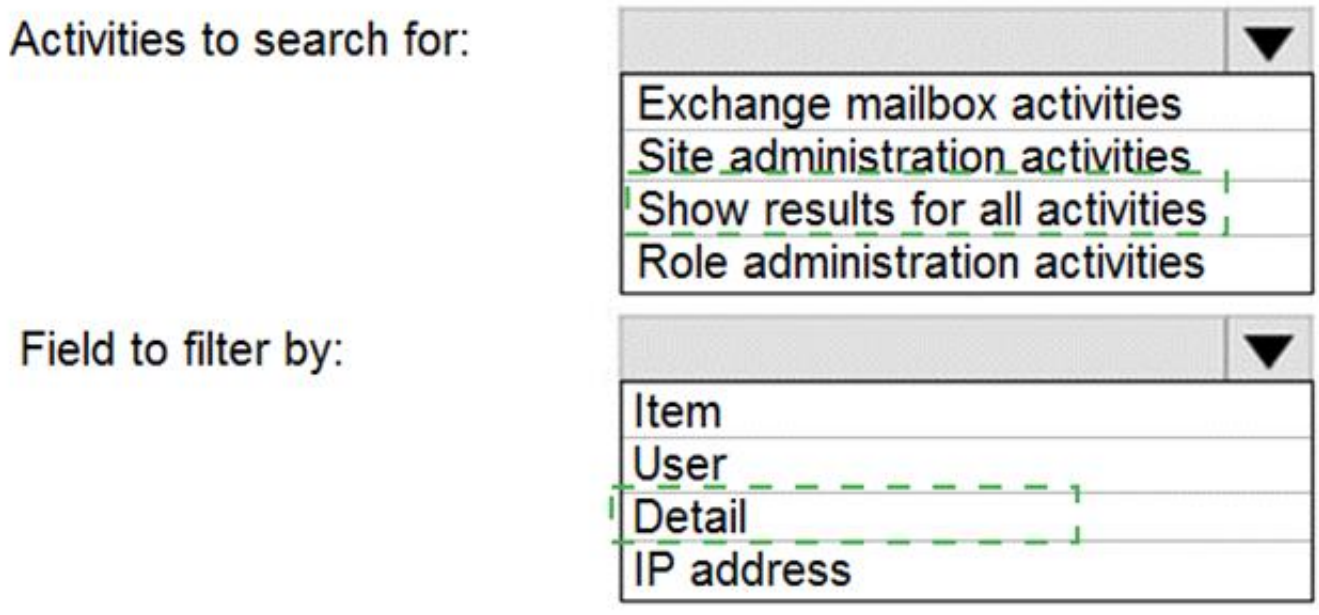
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription.
Your network uses an IP address space of 51.40.15.0/24.
An Exchange Online administrator recently created a role named Role1 from a computer on the network.
You need to identify the name of the administrator by using an audit log search.
For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 146
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

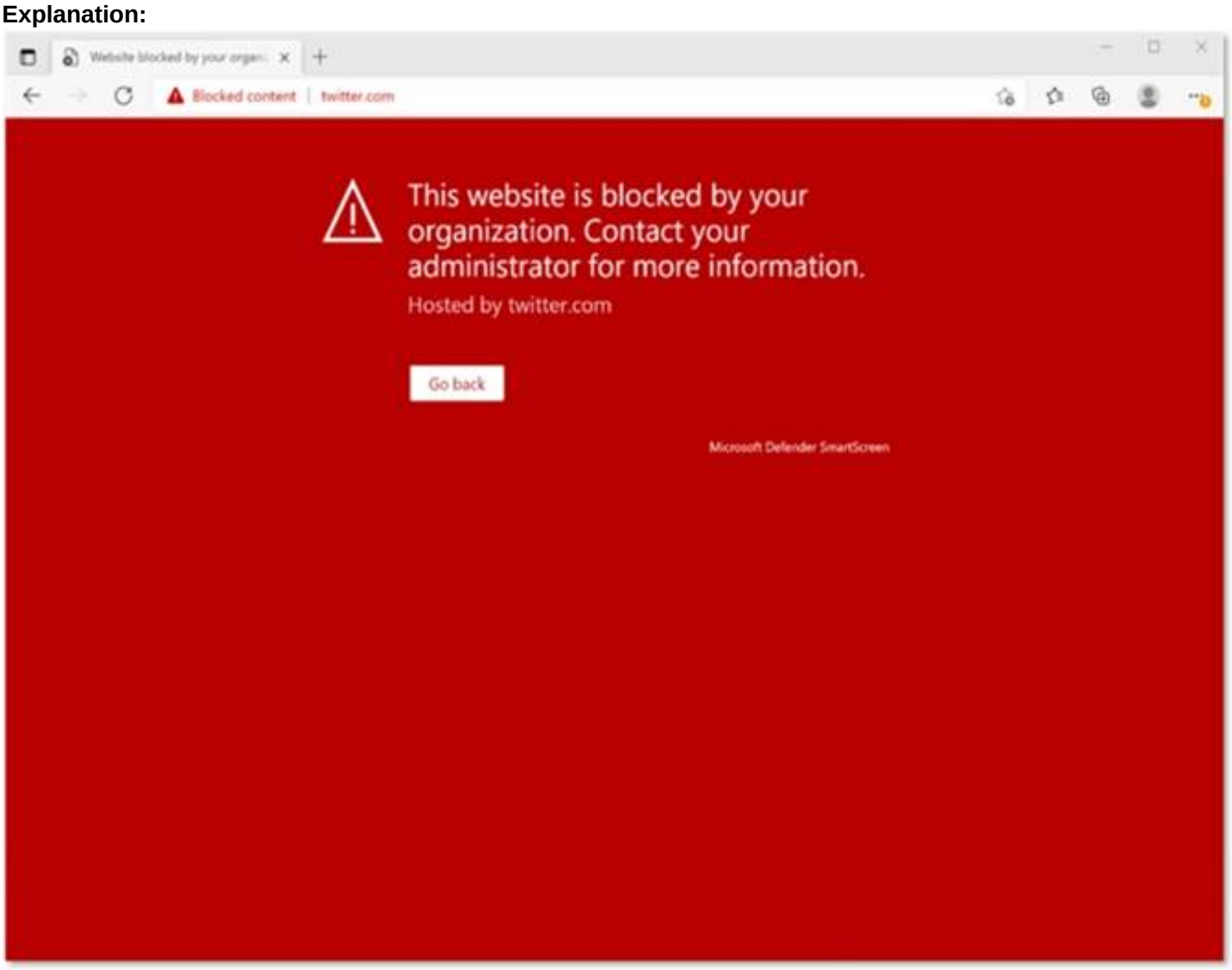
You need to enable user access to the partner company's portal. Which Microsoft Defender for Endpoint setting should you modify?

A. Alert notifications
B. Alert suppression
C. Custom detections
D. Advanced hunting

E. Indicators

Answer: E

Explanation:

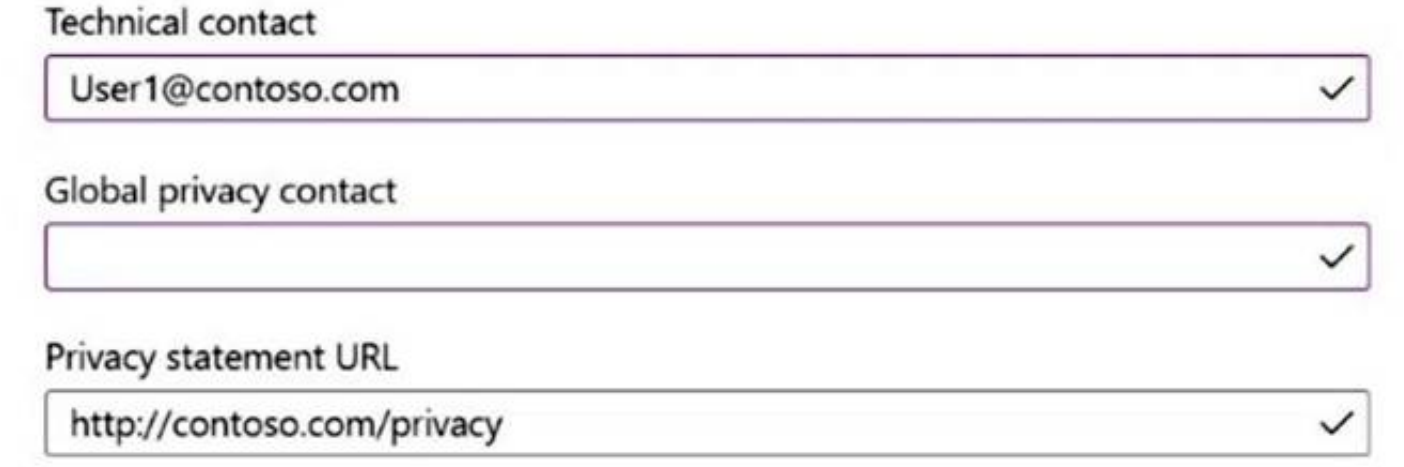


This Website Is Blocked By Your Organization
Custom indicators will block malicious IPs, URLs, and domains. Then, they will display the above message for the user.
Reference: https://jadexstrategic.com/web-protection/

NEW QUESTION 149
- (Topic 6)
You have a Microsoft 365 subscription.
You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Global Administrator
User3	Service Support Administrator

You configure Tenant properties as shown in the following exhibit.



Which users will be contacted by Microsoft if the tenant experiences a data breach?

A. Used only
B. User2 only
C. User3 only
D. Used and User2 only
E. User2 and User3 only

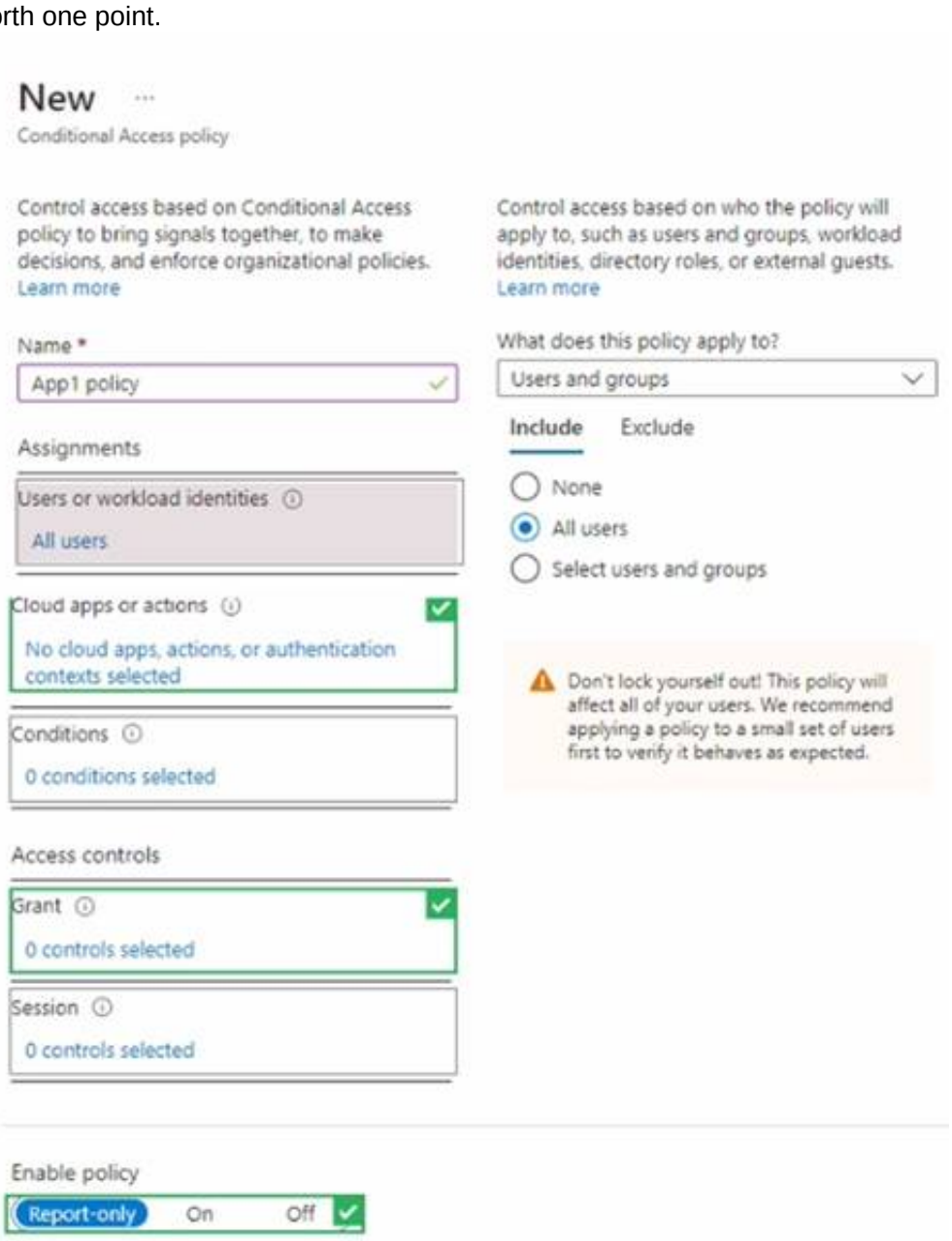
Answer: B

Explanation:
Microsoft 365 is committed to notifying customers within 72 hours of breach declaration.
The customer's tenant administrator will be notified.

Reference:
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365

NEW QUESTION 153
HOTSPOT - (Topic 6)
You have a Microsoft 365 Enterprise E5 subscription.
You add a cloud-based app named App1 to the Azure AD enterprise applications list.
You need to ensure that two-step verification is enforced for all user accounts the next time they connect to App1.
Which three settings should you configure from the policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

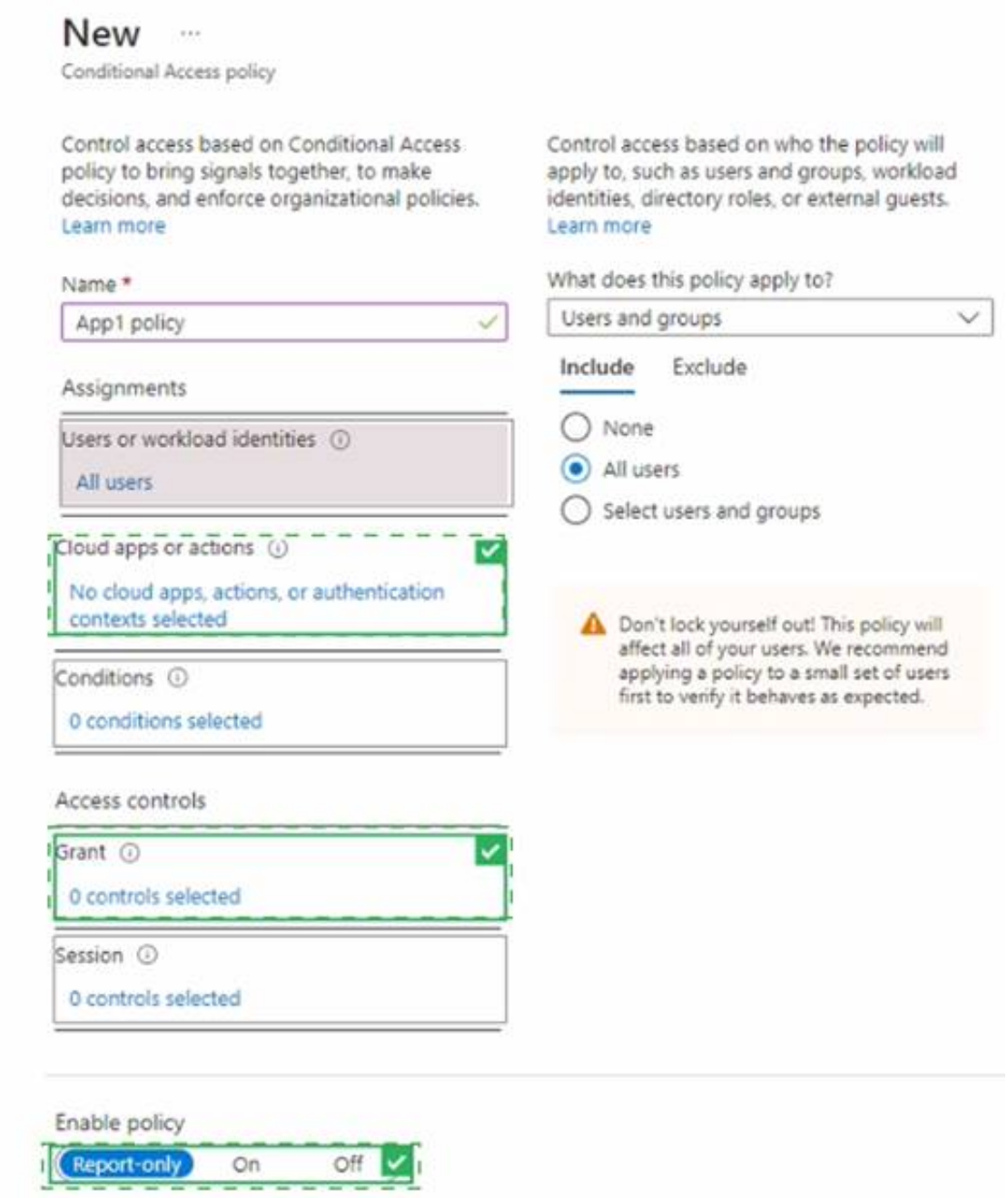


A. Mastered
B. Not Mastered

Answer: A

Explanation:

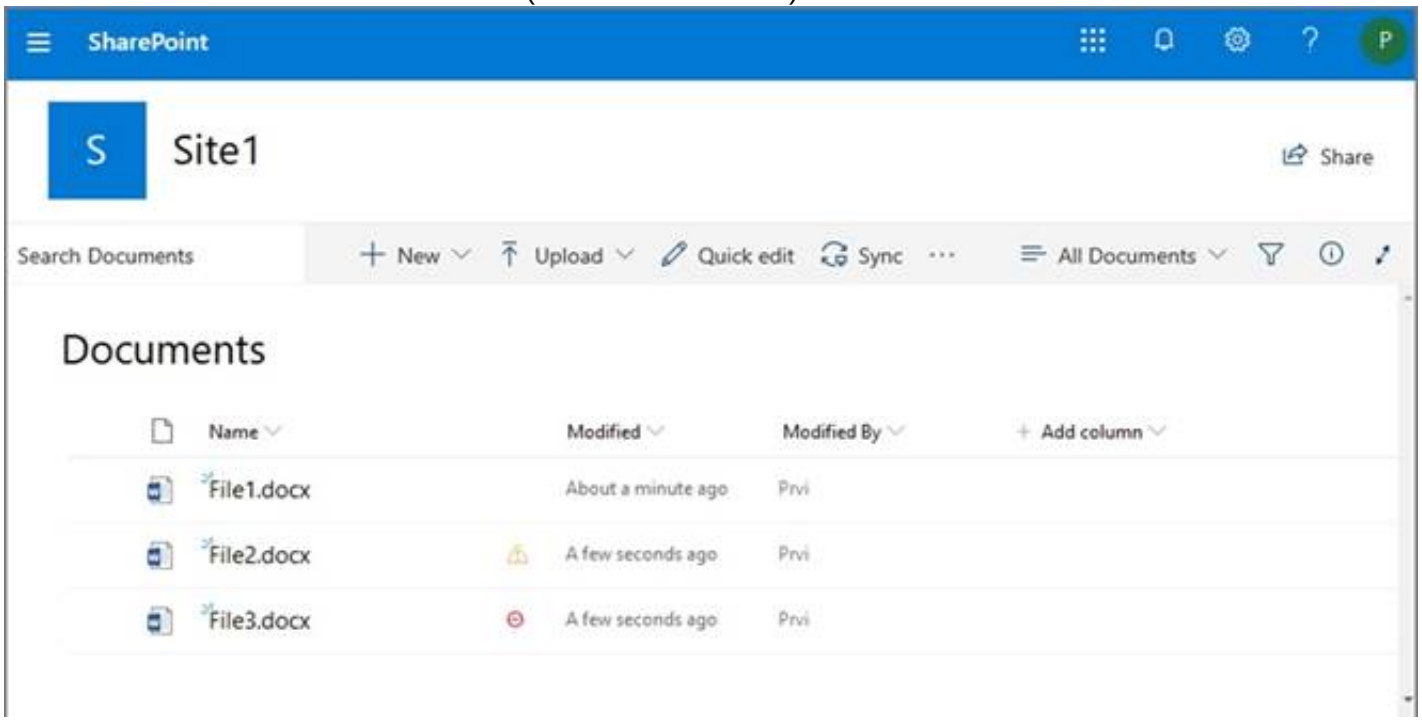
Answer Area



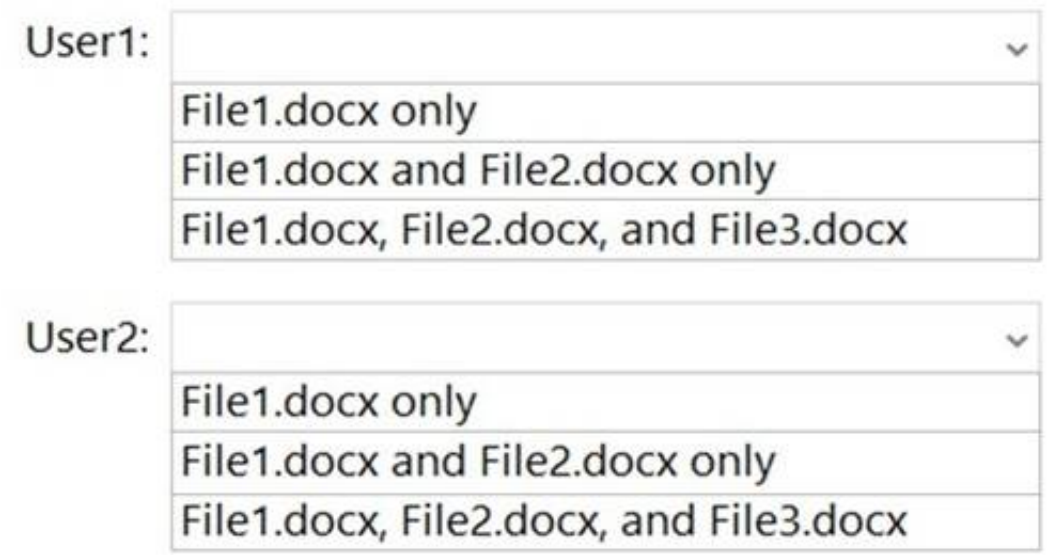
NEW QUESTION 155
HOTSPOT - (Topic 6)
From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)



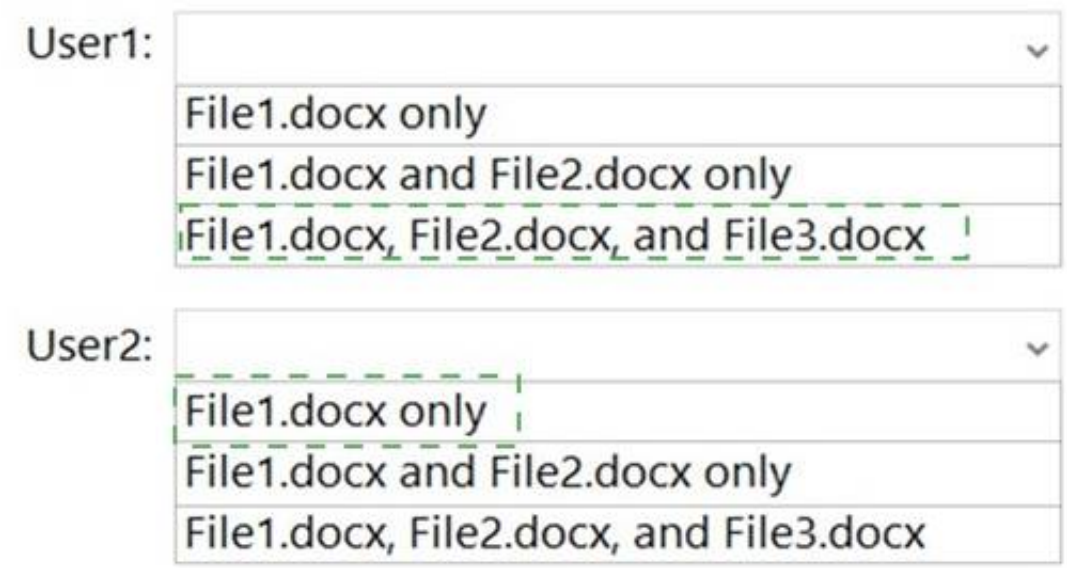
Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 156
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Passwordless authentication	Multi-factor authentication (MFA) method registered
User1	Not configured	Microsoft Authenticator app (push notification)
User2	Configured	Microsoft Authenticator app (push notification)
User3	Not configured	Mobile phone
User4	Not configured	Email

You plan to create a Conditional Access policy that will use GPS-based named locations. Which users can the policy protect?

A. User2 and User4 only
B. User1 and User3 only
C. Userl1 only
D. User1, User2. User3. and User4

Answer: C

NEW QUESTION 159
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription and an Azure AD tenant named contoso.com.
All users have computers that run Windows 11, are joined to contoso.com, and are protected by using BitLocker Drive Encryption (BitLocker).
You plan to create a user named Admin1 that will perform following tasks:
• View BitLocker recovery keys.
• Configure the usage location for the users in contoso.com.
You need to assign roles to Admin1 to meet the requirements. The solution must use the principle of least privilege. Which two roles should you assign? To answer, select the appropriate roles in the answer area.
NOTE: Each correct selection is worth one point

Answer Area

Devices

- [ ] Cloud Device Administrator
- [ ] Desktop Analytics Administrator
- [ ] Intune Administrator
- [ ] Printer Administrator
- [ ] Printer Technician
- [ ] Windows 365 Administrator

Global

- [ ] Global Administrator

Identity

- [ ] Application Administrator
- [ ] Application Developer
- [ ] Authentication Administrator
- [ ] Cloud Application Administrator
- [ ] Conditional Access Administrator
- [ ] Domain Name Administrator
- [ ] External Identity Provider Administrator
- [ ] Guest Inviter
- [ ] Helpdesk Administrator
- [ ] Hybrid Identity Administrator
- [ ] License Administrator
- [ ] Password Administrator

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Devices

- [ ] Cloud Device Administrator
- [ ] Desktop Analytics Administrator
- [ ] Intune Administrator
- [ ] Printer Administrator
- [ ] Printer Technician
- [ ] Windows 365 Administrator

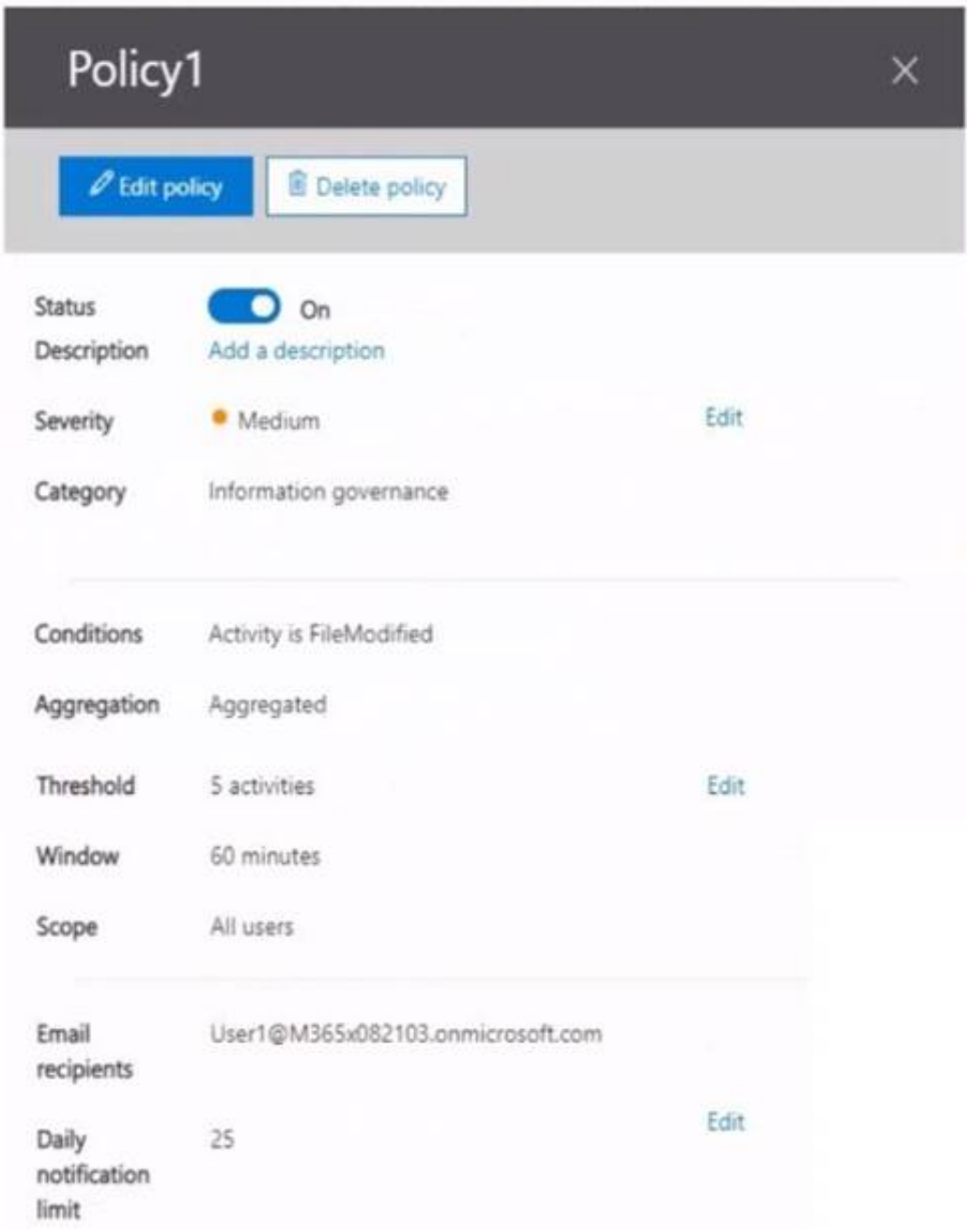
Global

- [ ] Global Administrator

Identity

- [ ] Application Administrator
- [ ] Application Developer
- [ ] Authentication Administrator
- [ ] Cloud Application Administrator
- [ ] Conditional Access Administrator
- [ ] Domain Name Administrator
- [ ] External Identity Provider Administrator
- [ ] Guest Inviter
- [ ] Helpdesk Administrator
- [ ] Hybrid Identity Administrator
- [ ] License Administrator
- [ ] Password Administrator

NEW QUESTION 163
- (Topic 6)
You have a Microsoft 365 tenant that contains two users named User1 and User2. You create the alert policy shown in the following exhibit.



User2 runs a script that modifies a file in a Microsoft SharePoint Online library once every four minutes and runs for a period of two hours.
How many alerts will User1 receive?

A. 2
B. 5
C. 10
D. 25

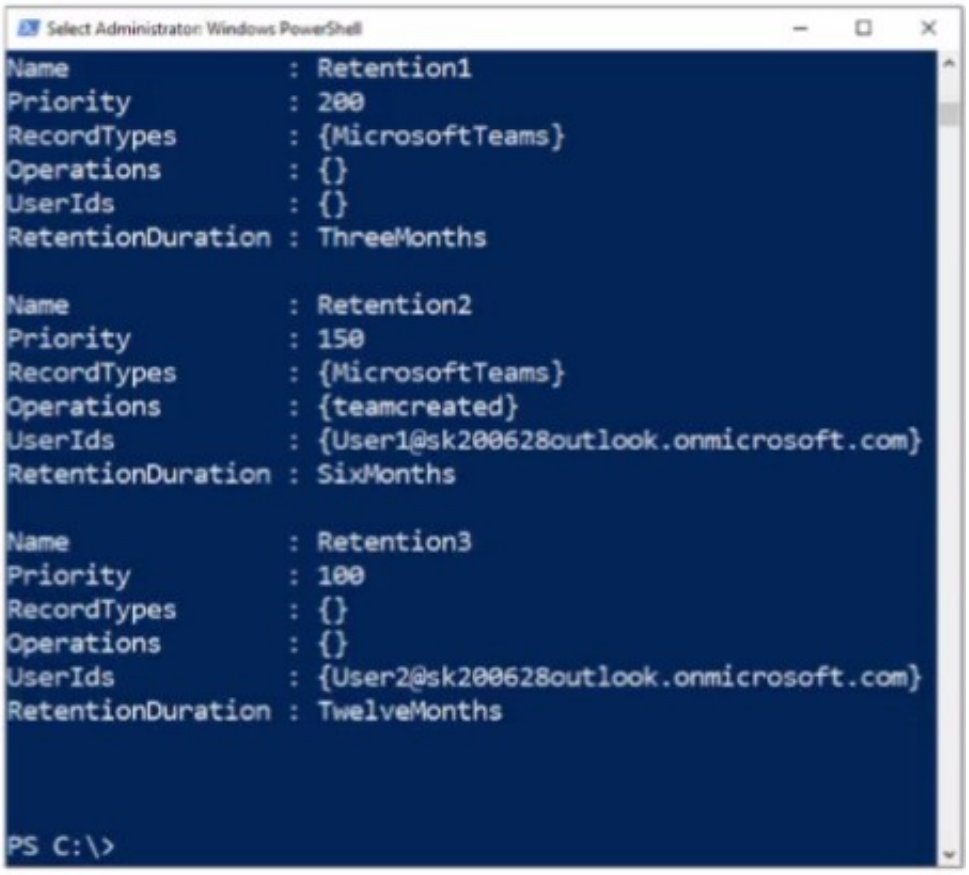
Answer: D

NEW QUESTION 167
- (Topic 6)
You have a Microsoft 365 subscription that uses Security & Compliance retention policies.
You implement a preservation lock on a retention policy that is assigned to all executive users.
Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point?

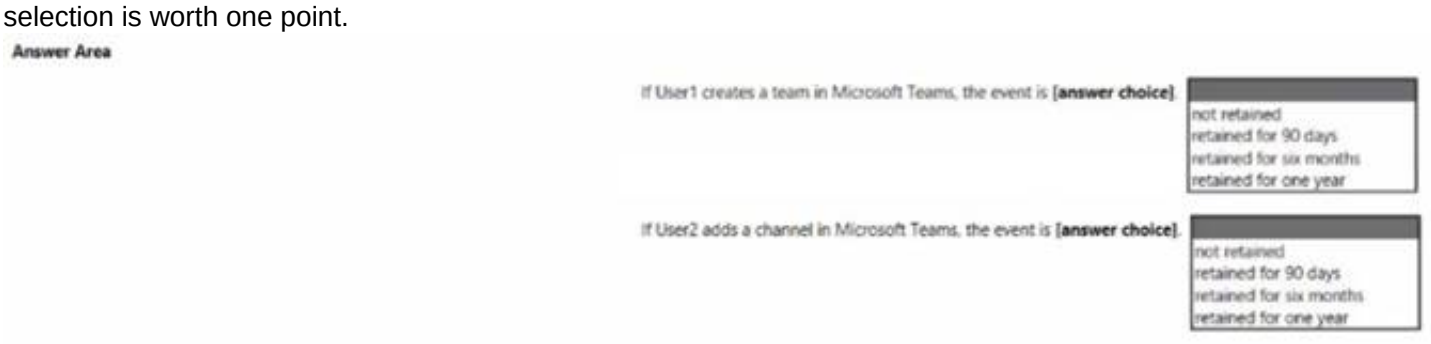
A. Add locations to the policy
B. Reduce the duration of policy
C. Remove locations from the policy
D. Extend the duration of the policy
E. Disable the policy

Answer: AB

NEW QUESTION 171
HOTSPOT - (Topic 6)
You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.



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. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 175
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users have the devices shown in the following table.

Name	Platform	Owner	Enrolled in Microsoft Endpoint Manager
Device1	Android	User1	Yes
Device2	Android	User1	No
Device3	iOS	User1	No
Device4	Windows 10	User2	Yes
Device5	Windows 10	User2	No
Device6	iOS	User2	Yes

On which devices can you manage apps by using app configuration policies in Microsoft Endpoint Manager?

A. Device1, Device4, and Device6
B. Device2, Device3, and Device5
C. Device1, Device2, Device3, and Device6
D. Device1, Device2, Device4, and Device5

Answer: C

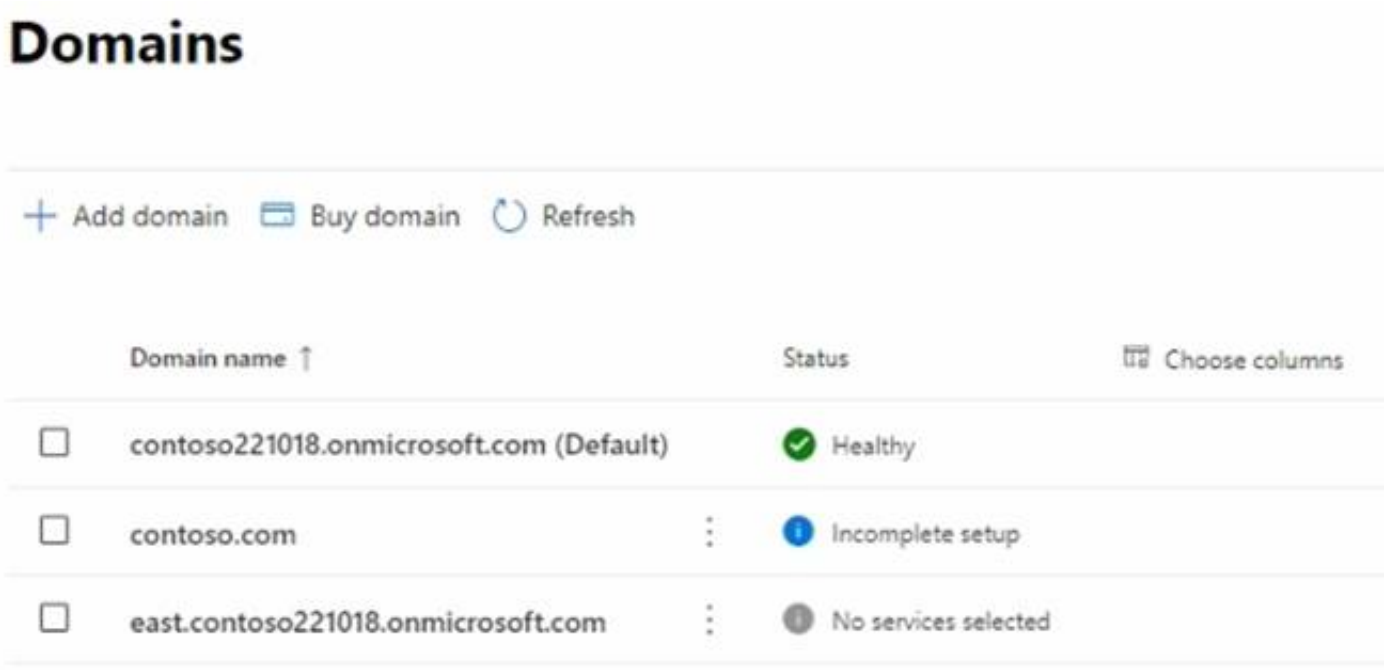
Explanation:
You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

NEW QUESTION 177
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Endpoint security.
You need to create a group and assign the Endpoint Security Manager role to the group. Which type of group can you use?

A. Microsoft 365 only
B. security only
C. mail-enabled security and security only
D. mail-enabled security, Microsoft 365, and security only
E. distribution, mail-enabled security, Microsoft 365, and security

Answer: D

NEW QUESTION 178
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 subscription That contains the domains shown in the following exhibit.



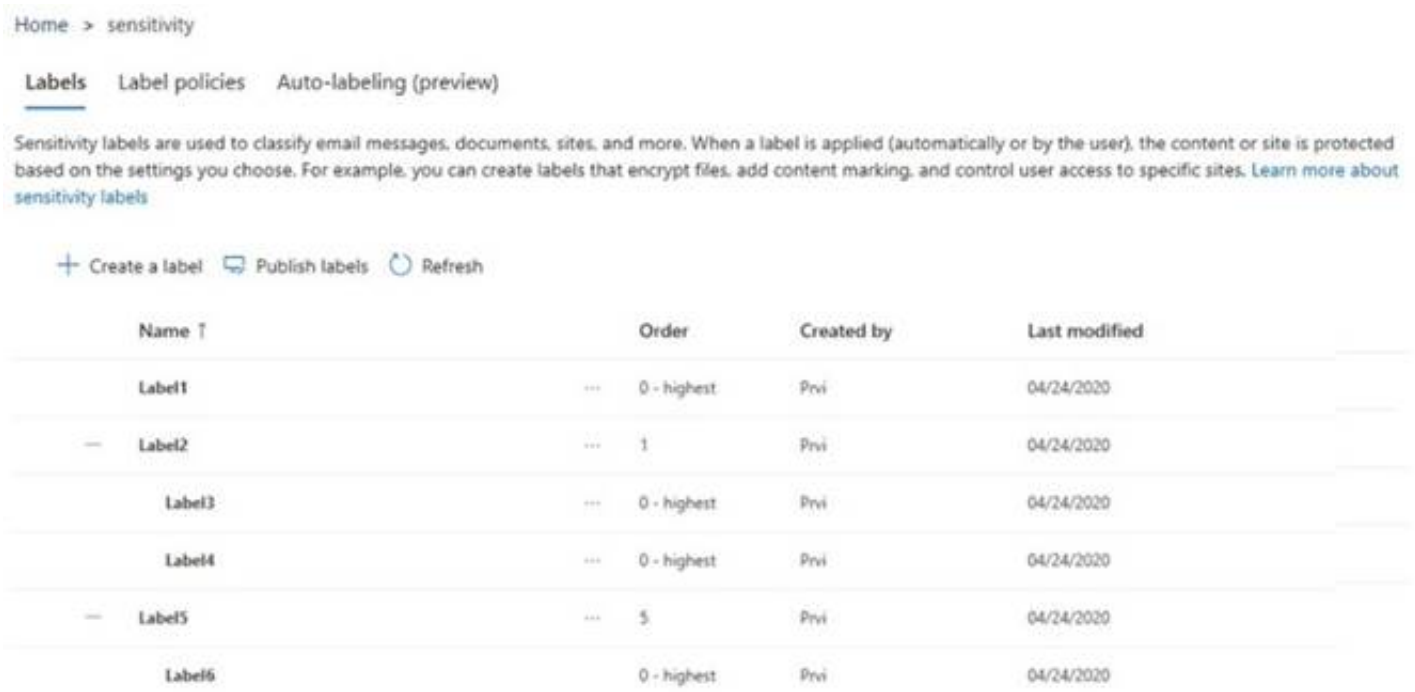
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE; Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 180
- (Topic 6)
You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.



Which labels can users apply to content?

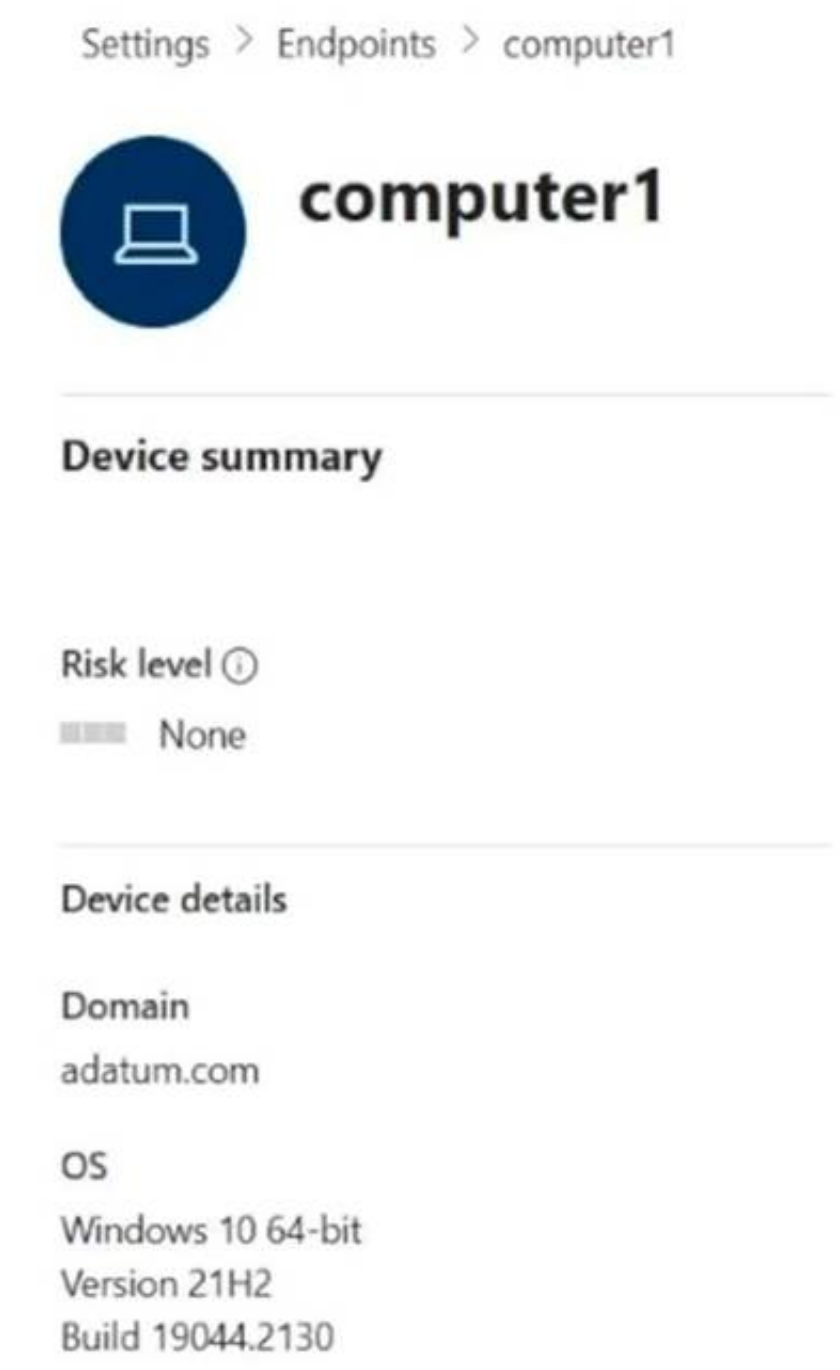
A. Label1, Label2, and Label5 only
B. Label3. Label4, and Label6 only
C. Label1, Label3, Labe2, and Label6 only
D. Label1, Label2, Label3, Label4, Label5. and Label6

Answer: C

NEW QUESTION 181
HOTSPOT - (Topic 6)
HOTSPOT
Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Device group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped devices (default)	*Not applicable*

You onboard a computer named computer1 to Microsoft Defender for Endpoint as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement.
NOTE: Each correct selection is worth one point.

Answer Area

Computer1 will be a member of **[answer choice]**.
- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of **[answer choice]**.
- Group1 only
- Group1 and Group2 only
- Group1, Group2, Group3, and Group4
- Ungrouped devices

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Group3 and Group4 only Computer1 has no Demo Tag.
Computer1 is in the adatum domain and OS is Windows 10. Box 2: Group1, Group2, Group3 and Group4

NEW QUESTION 184
- (Topic 6)
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
User5	User5@gmail.com	Guest

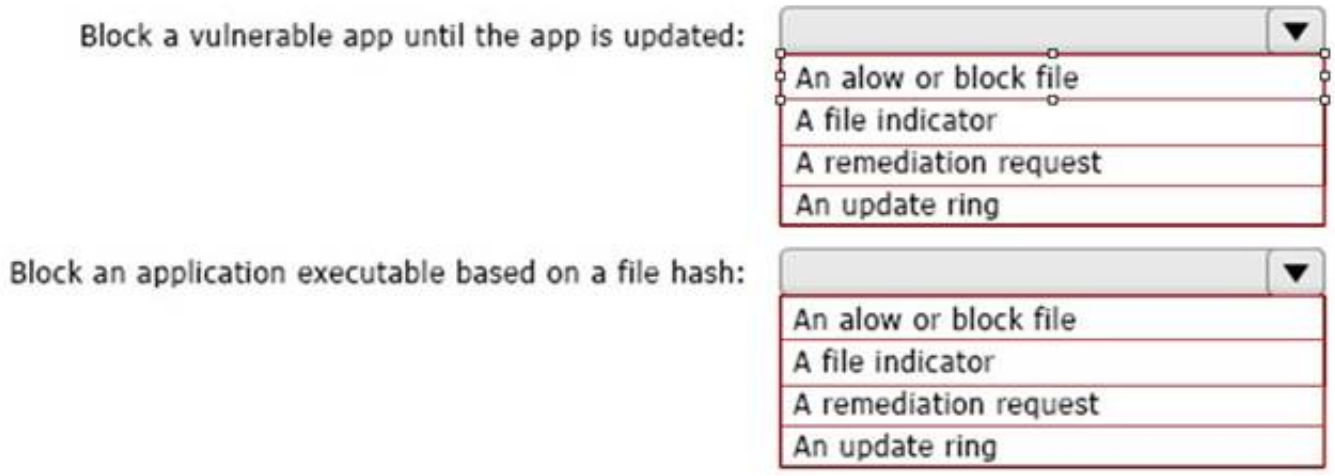
You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (Pll) from being emailed to users outside your organization.
To which users can User! send documents that contain Pll?

A. User2only
B. User2and User3only
C. User2, User3, and User4 only
D. User2, User3, User4, and User5

Answer: B

NEW QUESTION 188
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.
You need to configure Defender for Endpoint to meet the following requirements:
? Block a vulnerable app until the app is updated.
? Block an application executable based on a file hash.
The solution must minimize administrative effort.
What should you configure for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: A remediation request
Block a vulnerable app until the app is updated.
Block vulnerable applications
How to block vulnerable applications
? Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.
? Select a security recommendation to see a flyout with more information.
? Select Request remediation.
? Select whether you want to apply the remediation and mitigation to all device groups or only a few.
? Select the remediation options on the Remediation request page. The remediation options are software update, software uninstall, and attention required.
? Pick a Remediation due date and select Next.
? Under Mitigation action, select Block or Warn. Once you submit a mitigation action, it is immediately applied.
? Review the selections you made and Submit request. On the final page you can
choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.
Box 2: A file indicator
Block an application executable based on a file hash.
While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.
The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

NEW QUESTION 189
HOTSPOT - (Topic 6)
Your company uses Microsoft Defender for Endpoint.
The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

The alerts visible in the Microsoft Defender for Endpoint alerts queue are shown in the following table.

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:
• Triggering IOC: Any IOC
• Action: Hide alert
• Suppression scope: Alerts on ATP1 device group
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
After you create the suppression rule, Alert1 is visible in the alerts queue.	○	○
After you create the suppression rule, Alert3 is visible in the alerts queue.	○	○
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	○	○
After you create the suppression rule, Alert3 is visible in the alerts queue.	○	○
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	○	○

NEW QUESTION 192
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. You need to perform the following tasks:
• Create a sensitive info type named SIT1 based on a regular expression.
• Add a watermark to all new documents that are matched by SIT1.
Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 196
- (Topic 6)
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 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp

NEW QUESTION 201
- (Topic 6)
: 241
You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?

A. Microsoft Store for Business
B. Apple Business Manager
C. Apple iTunes Store
D. Apple Configurator

Answer: B

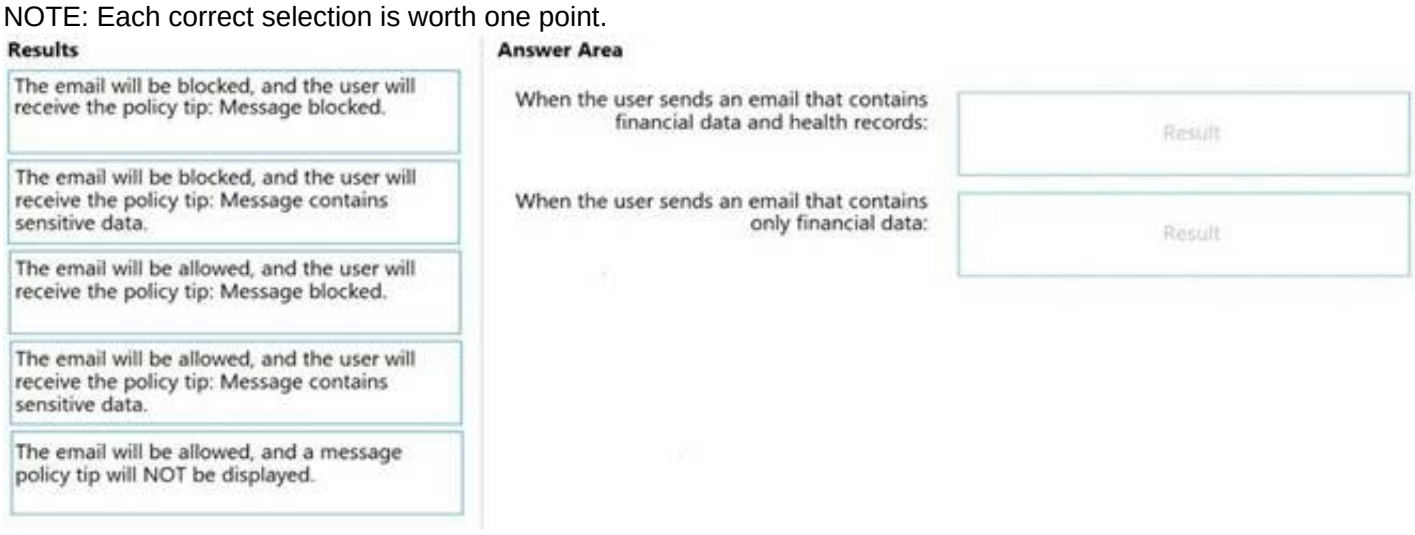
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios

NEW QUESTION 202
- (Topic 6)
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.
From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.
You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.
Solution: From the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 203
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 subscription.
In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:
? Block emails that contain financial data.
? Display the following policy tip text: Message blocked.
From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:
? Use the following location: Exchange email.
? Display the following policy tip text: Message contains sensitive data.
? When a user sends an email, notify the user if the email contains health records.
What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked. If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.
Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

NEW QUESTION 206
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Al users have Mac computers. ATI the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender for Endpoint.

You need to configure Microsoft Defender for Endpoint on the computers. What should you create from the Endpoint Management admin center?

A. a Microsoft Defender for Endpoint baseline profile
B. an update policy for iOS
C. a device configuration profile
D. a mobile device management (MDM) security baseline profile

Answer: D

NEW QUESTION 211
- (Topic 6)
You have a Microsoft 365 subscription.
You have a data loss prevention (DLP) policy that blocks sensitive data from being shared in email messages.
You need to modify the policy so that when an email message containing sensitive data is sent to both external and internal recipients, the message is only prevented from being delivered to the external recipients.
What should you modify?

A. the policy rule exceptions
B. the DLP policy locations
C. the policy rule conditions
D. the policy rule actions

Answer: C

NEW QUESTION 216
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.
You deploy a third-party antivirus solution to the devices.
You need to ensure that the devices are marked as compliant.
Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

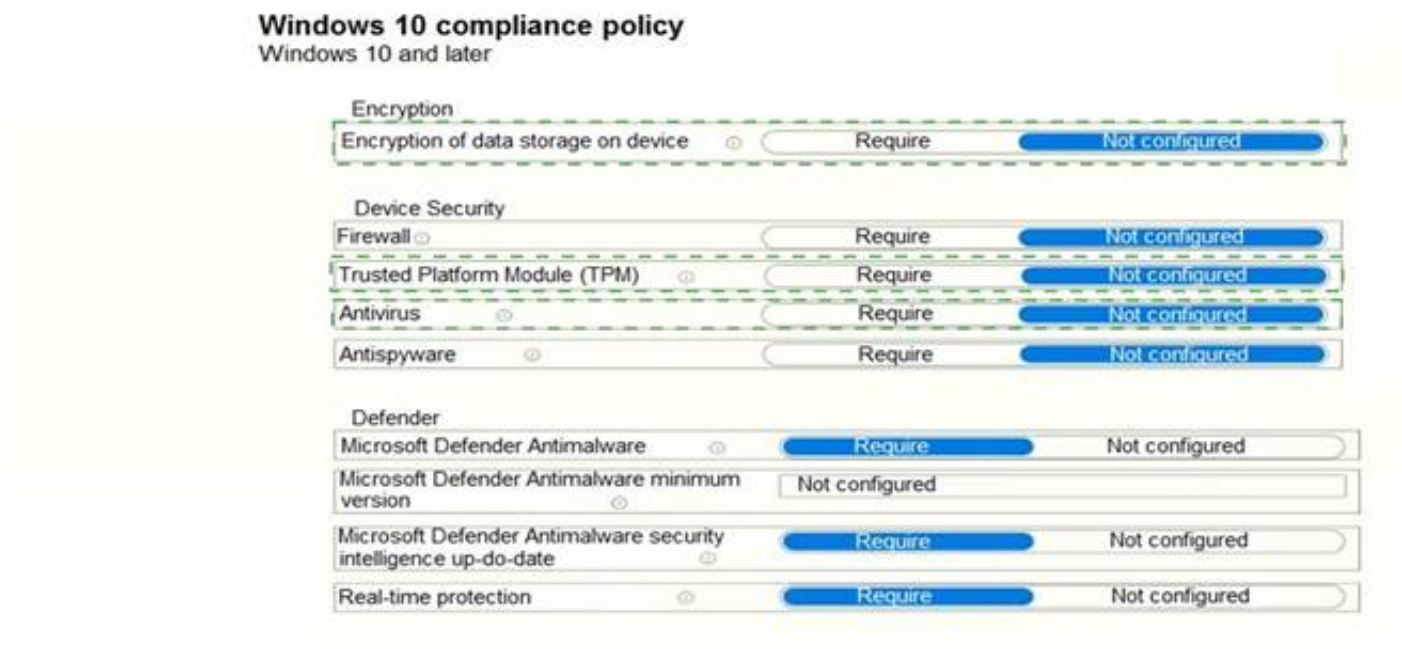
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 218
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Office 365 role group
User1	*None*	Compliance Data Administrator
User2	Global Administrator	*None*

You create a retention label named Label 1 that has the following configurations:
• Retains content for five years
• Automatically deletes all content that is older than five years
You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:
• Applies to content that contains the word Merger
• Specifies the OneDrive accounts and SharePoint sites locations You run the following command.
Set-RetentionConpliancePolicy Policy1 -RestrictiveRetention Strue -Force
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
User1 can add Exchange email as a location to Policy1.	○	○
User2 can remove SharePoint sites from Policy1.	○	○
User2 can add the word Acquisition to Policy1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	○	○
User2 can remove SharePoint sites from Policy1.	○	○
User2 can add the word Acquisition to Policy1.	○	○

NEW QUESTION 220
- (Topic 6)
You have a Microsoft 365 subscription.
Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de- fghij.
You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.
D18912E1457D5D1DDCBD40AB3BF70D5D
What should you create to ensure that the DLP policy can detect the customer IDs?

A. a sensitive information type
B. a sensitivity label
C. a supervision policy
D. a retention label

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide

NEW QUESTION 221
- (Topic 6)
You have a new Microsoft 365 E5 tenant.
You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.

What should you do first?

A. Enable auditing.
B. Enable Microsoft 365 usage analytics.
C. Create an Insider risk management policy.
D. Create a communication compliance policy.

Answer: A

Explanation:
Microsoft Purview auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.
Note: Permissions alert policies
Example: Elevation of Exchange admin privilege
Generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in Exchange Online.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies

NEW QUESTION 223
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the security groups shown in the following table.

Name	Membership type	Membership rule
Group1	Assigned	*Not applicable*
Group2	Dynamic	(user.department -eq "Finance")
Group3	Dynamic	(user.department -eq "R&D")

The subscription contains the users shown in the following table.

Name	Department	Assigned group membership
User1	Finance	Group1
User2	Technical	*None*
User3	R&D	Group1

You have a Conditional Access policy that has the following settings:
• Assignments o Users
Include: Group1
Exclude: Group2. Group3 o Target resources
Cloud apps App1
Access controls Grant
Block access
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
User1 can sign in to App1.	○	○
User2 can sign in to App1.	○	○
User3 can sign in to App1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Statements	Yes	No
User1 can sign in to App1.	○	○
User2 can sign in to App1.	○	○
User3 can sign in to App1.	○	○

NEW QUESTION 226
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription. You need to meet the following requirements:
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label. Which two settings should you use in the Microsoft Purview compliance portal? To answer,
select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

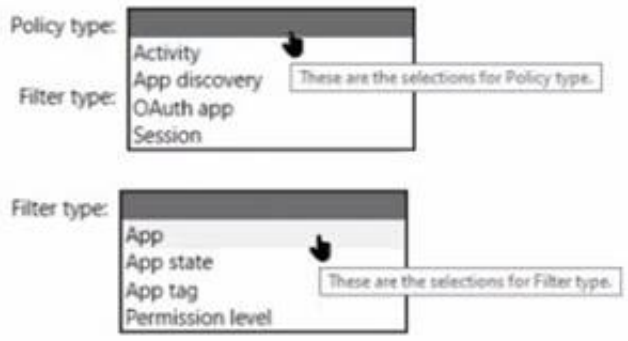
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Information protection
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection
All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files
without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.
To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels:
In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information Protection -> Microsoft Information Protection.
Note: Encryption of data at rest
Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.
BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology. Box 2: Settings
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.
* 1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.

* 2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
* 3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
* 4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
* 5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.

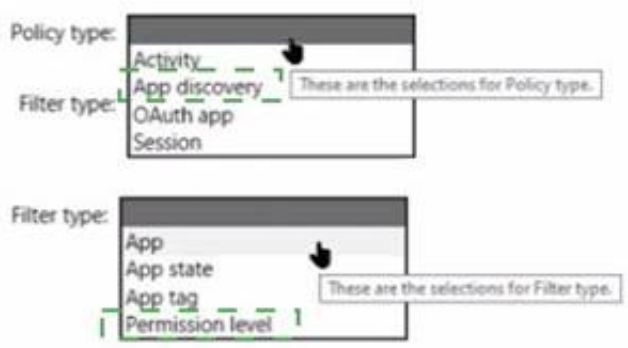
NEW QUESTION 227
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to create a policy that will generate an email alert when a banned app is detected requesting permission to access user information or data in the subscription.
What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 231
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains a user named User1.
You plan to implement insider risk management.
You need to ensure that User1 can perform the following tasks:
? Review alerts.
? Manage cases.
? Create notice templates.
? Review user emails by using Content explorer.
The solution must use the principle of least privilege. To which role group should you add User1?

A. Insider Risk Management
B. Insider Risk Management Analysts
C. Insider Risk Management Investigators
D. Insider Risk Management Admin

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide

NEW QUESTION 234
- (Topic 6)
You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.
Company policy requires that the devices have the following configurations:
? Require complex passwords.
? Require the encryption of removable data storage devices.
? Have Microsoft Defender Antivirus real-time protection enabled.
You need to configure the devices to meet the requirements.
What should you use?

A. an app configuration policy
B. a compliance policyC a security baseline profile D a conditional access policy

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION 239
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).
The tenant has two Compliance Manager assessments as shown in the following table.

Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Regulations
Establish a threat intelligence program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline
Establish and document a configuration management program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline

You perform the following actions:
? For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.
? Enable multi-factor authentication (MFA) for all users.
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
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

NEW QUESTION 244
HOTSPOT - (Topic 6)
You have device compliance policies shown in the following table.

Name	Platform	Assignment
Policy1	Windows 10 and later	Device1
Policy2	Windows 10 and later	Device1
Policy3	Windows 10 and later	Device2
Policy4	Windows 10 and later	Device2
Policy5	iOS/iPadOS	Device3
Policy6	iOS/iPadOS	Device3

The device compliance state for each policy is shown in the following table.

Policy	State
Policy1	Compliant
Policy2	In grace period
Policy3	Compliant
Policy4	Not compliant
Policy5	In grace period
Policy6	Compliant

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	○	○
Device2 has an overall compliance state of Not compliant.	○	○
Device3 has an overall compliance state of In grace period.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	○	○
Device2 has an overall compliance state of Not compliant.	○	○
Device3 has an overall compliance state of In grace period.	○	○

NEW QUESTION 247
- (Topic 6)
Your company has a Microsoft 365 E5 subscription.
Users in the research department work with sensitive data.
You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents.
Users in other departments must not be restricted.
What should you do?

A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
B. Modify the safe links policy Global settings.
C. Create a data loss prevention (DLP) policy that has a Content contains condition.
D. Create a new safe links policy.

Answer: D

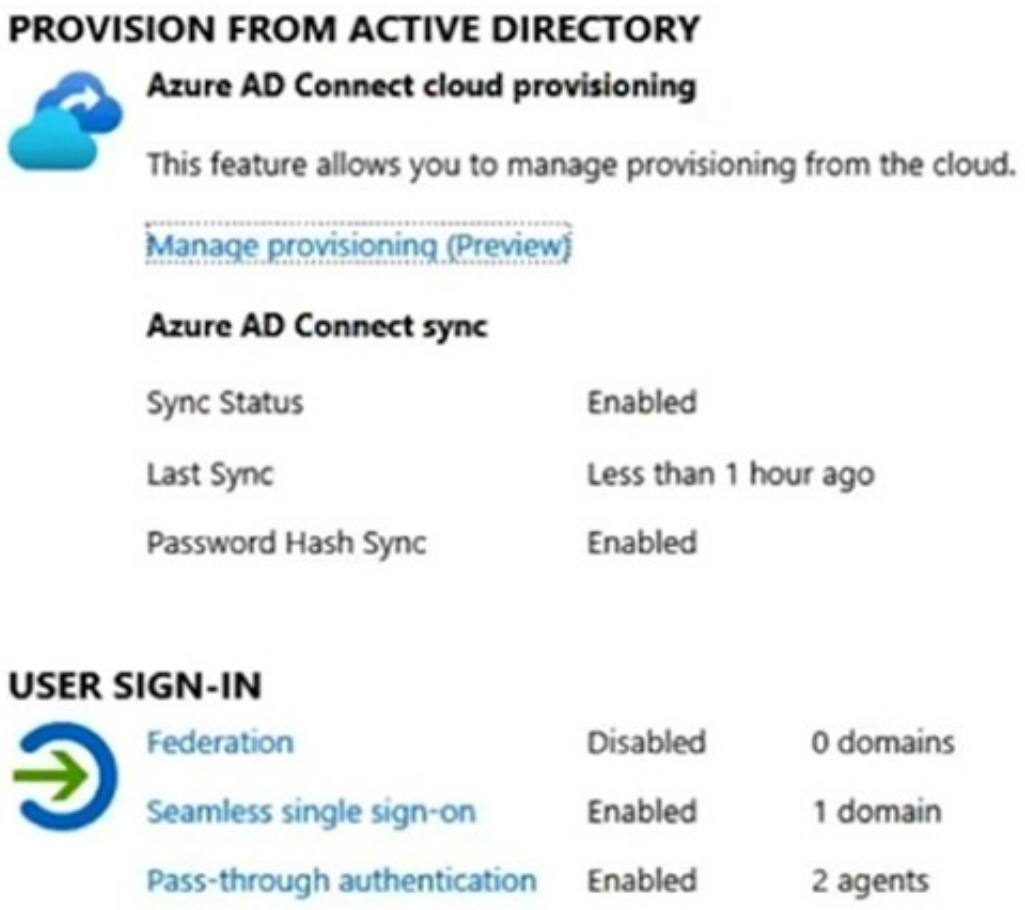
Explanation:
Use the Microsoft 365 Defender portal to create Safe Links policies
In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & Collaboration > Policies & Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use https://security.microsoft.com/safelinksv2.
* 1. On the Safe Links page, select Create to start the new Safe Links policy wizard.
* 2. On the Name your policy page, configure the following settings: Name: Enter a unique, descriptive name for the policy.
Description: Enter an optional description for the policy.
* 3. When you're finished on the Name your policy page, select Next.
* 4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions):
Users: The specified mailboxes, mail users, or mail contacts.
*-> Groups:
Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren't supported).
The specified Microsoft 365 Groups.
Domains: All recipients in the specified accepted domains in your organization. Etc.
Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links- policies-configure

NEW QUESTION 248
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
This is not a permissions issue.
The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

NEW QUESTION 250
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the following user:
? Name: User1
? UPN: user1@contoso.com
? Email address: user1@marketmg.contoso.com
? MFA enrollment status: Disabled
When User1 attempts to sign in to Outlook on the web by using the user1@marketing.contoso.com email address, the user cannot sign in.
You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com.
What should you do?

A. Assign an MFA registration policy to User1.
B. Reset the password of User1.
C. Add an alternate email address for User1.
D. Modify the UPN of User1.

Answer: D

Explanation:
Microsoft’s recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN’s to match.
Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user's email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only

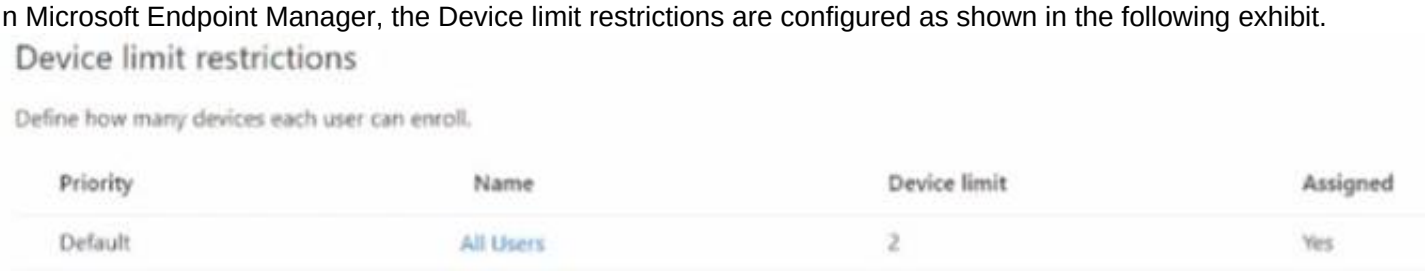
needs to remember a single name.
Configure the Azure AD multifactor authentication registration policy
Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.
Reference:
https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname

NEW QUESTION 254
- (Topic 6)
You have a Microsoft 365 subscription. You add a domain named contoso.com.
When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.com.
You need to change the email address used to verify the domain. What should you do?

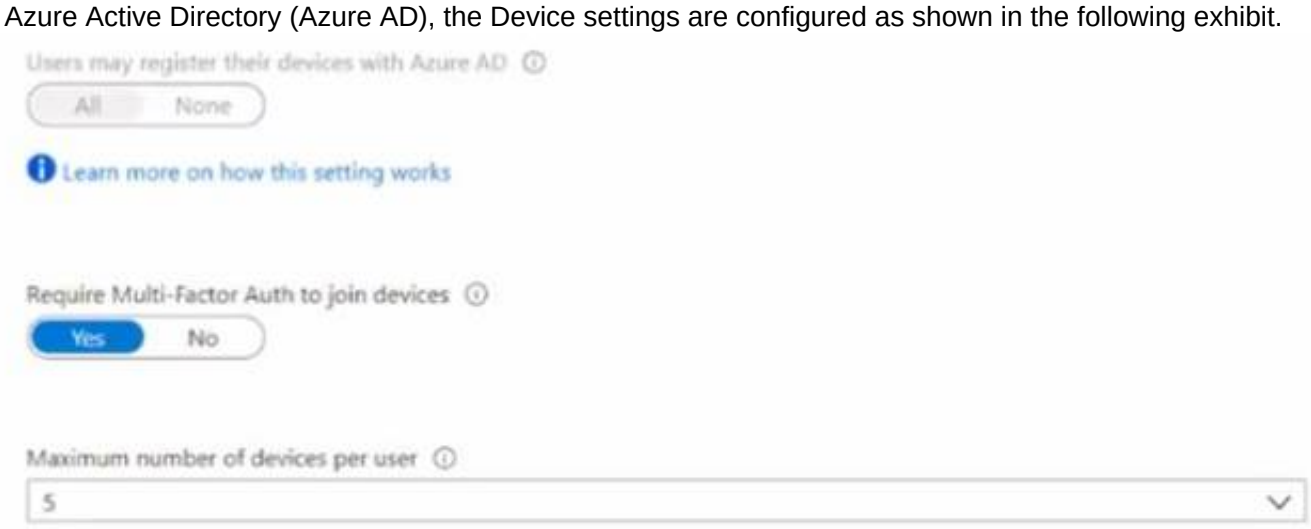
A. From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription.
B. Add a TXT record to the DNS zone of the domain.
C. From the domain registrar, modify the contact information of the domain.
D. Modify the NS records for the domain.

Answer: C

NEW QUESTION 256
HOTSPOT - (Topic 6)
You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.
In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.



In Azure Active Directory (Azure AD), the Device settings are configured as shown in the following exhibit.



From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).
For each of the following statement, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	○	○
User1 can join only five devices to Azure AD.	○	○
User2 can enroll all the devices in Intune.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	○	○
User1 can join only five devices to Azure AD.	○	○
User2 can enroll all the devices in Intune.	○	○

NEW QUESTION 261

HOTSPOT - (Topic 6)
You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

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

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Not configured	15	Yes

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

Name	Assigned to
Policy2	Group2
Policy3	Group3

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
Device1 is marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

NEW QUESTION 266
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	*None*	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	*None*	iOS	Not enrolled

You have the apps shown in the following table.

Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the users.
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
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

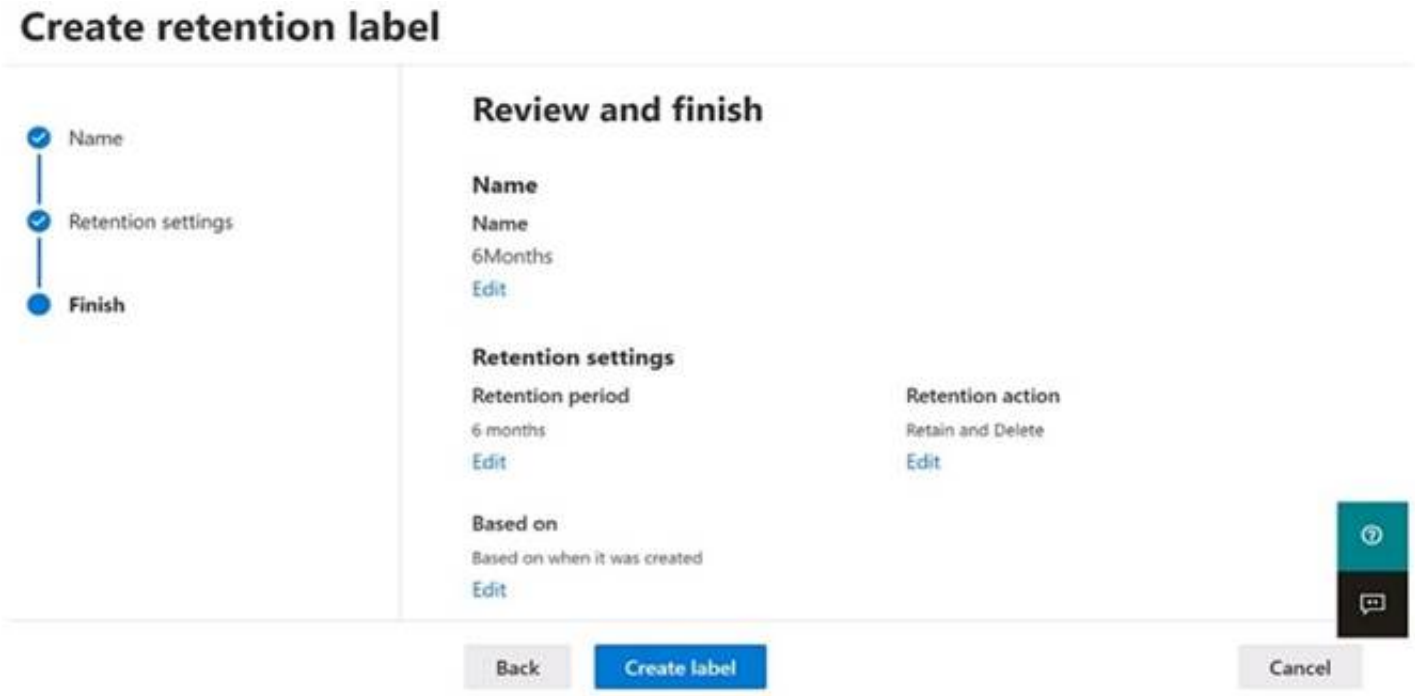
NEW QUESTION 267
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?

A. From the Cloud App Security admin center, select Users and accounts.
B. From the Microsoft 365 security center, view the Threat tracker.
C. From the Microsoft 365 admin center, view the Security & compliance report.
D. From the Azure Active Directory admin center, view the Risky sign-ins report.

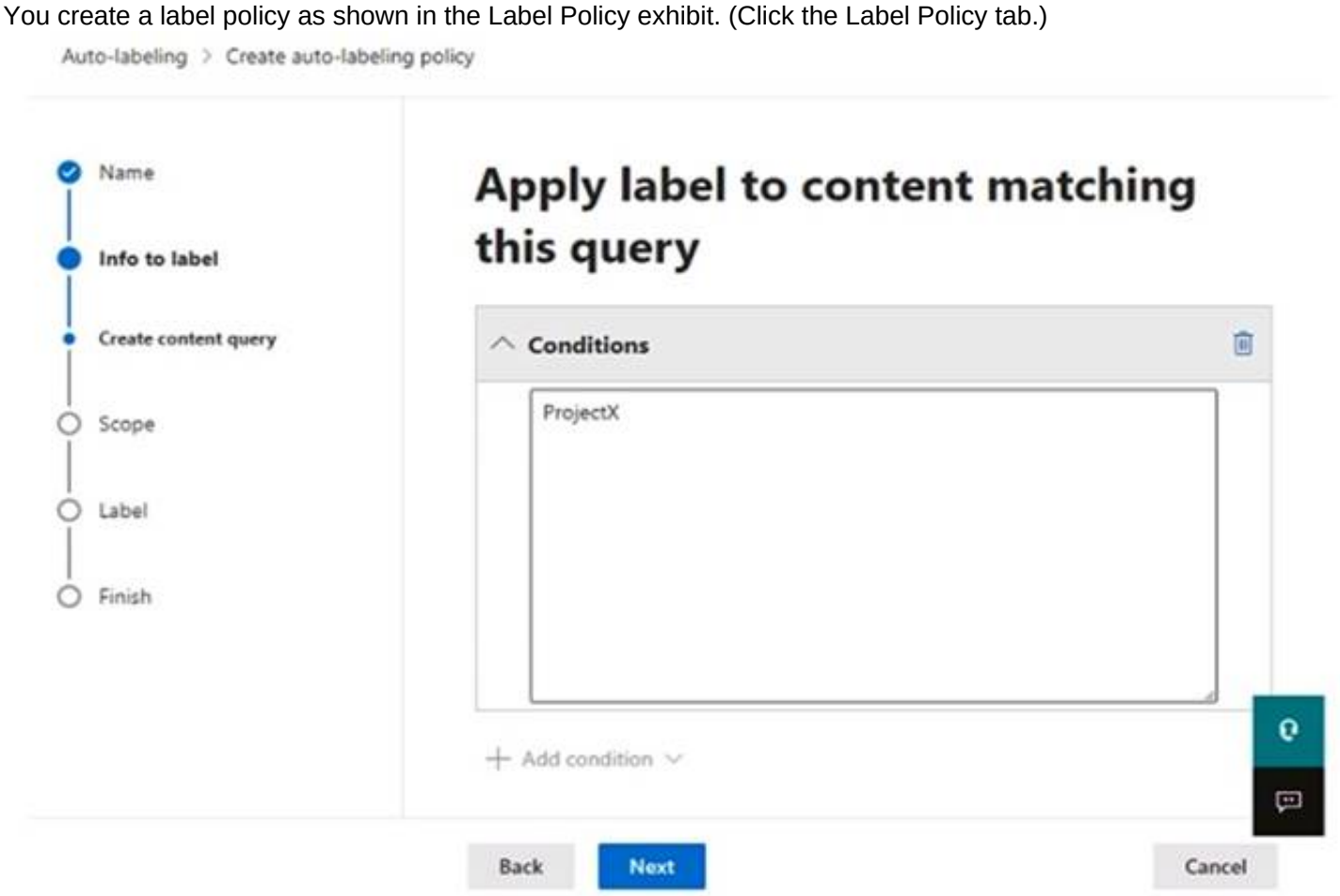
Answer: A

NEW QUESTION 269
HOTSPOT - (Topic 6)
HOTSPOT

You have a Microsoft 365 tenant.
You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)



You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)



The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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

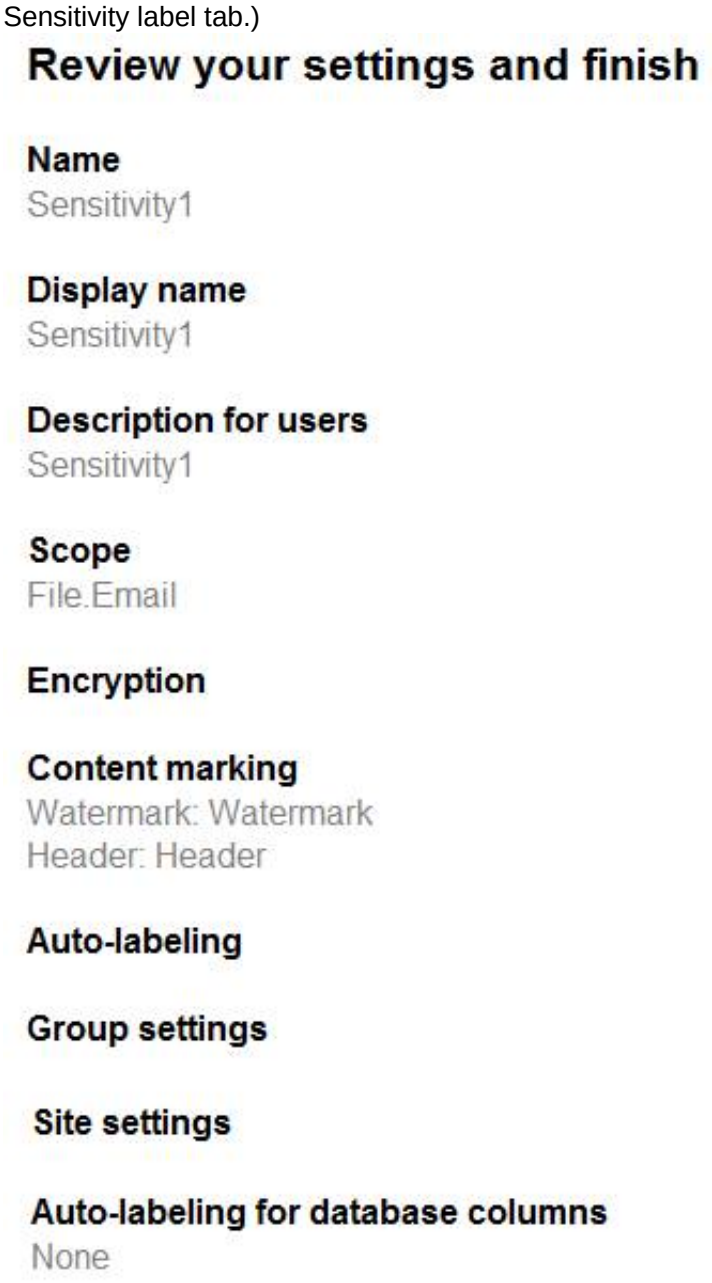
Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	○	○
Any sent email message that contains the word ProjectX will be retained for six months.	○	○
Users are required to manually apply a label to email messages that contain the word ProjectX.	○	○

A. Mastered
B. Not Mastered

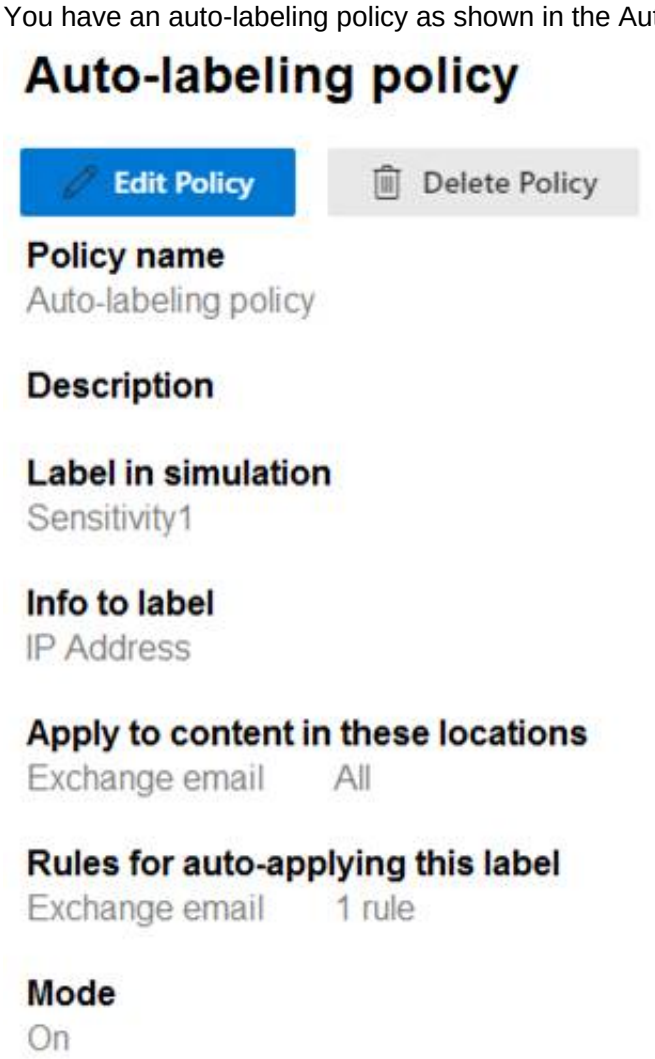
Answer: A

Explanation:
Box 1: No
Box 2: Yes
Box 3: No

NEW QUESTION 274
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant.
You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)



You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)



A user sends an email that contains the components shown in the following table.

Type	File	Includes IP address
Mail body	**Not applicable**	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

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
Sensitivity1 is applied to the email.	○	○
A watermark is added to File1.docx.	○	○
A header is added to File2.xml.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Sensitivity1 is applied to the email.	○	○
A watermark is added to File1.docx.	○	○
A header is added to File2.xml.	○	○

NEW QUESTION 275
DRAG DROP - (Topic 6)
DRAG DROP
Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD). The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2016	File Server Resource Manager (FSRM)
Server2	Windows Server 2016	*None*

You use Azure Information Protection.
You need to ensure that you can apply Azure Information Protection labels to the file stores on Server1.
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

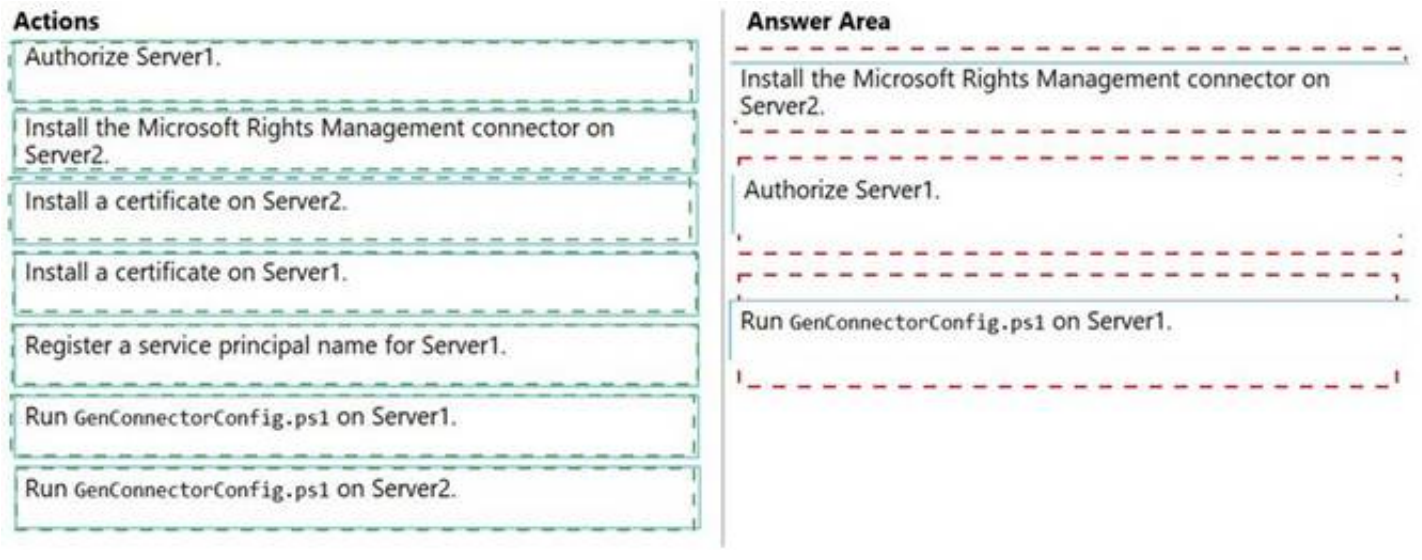
- Authorize Server1.
- Install the Microsoft Rights Management connector on Server2.
- Install a certificate on Server2.
- Install a certificate on Server1.
- Register a service principal name for Server1.
- Run `GenConnectorConfig.ps1` on Server1.
- Run `GenConnectorConfig.ps1` on Server2.

Answer Area

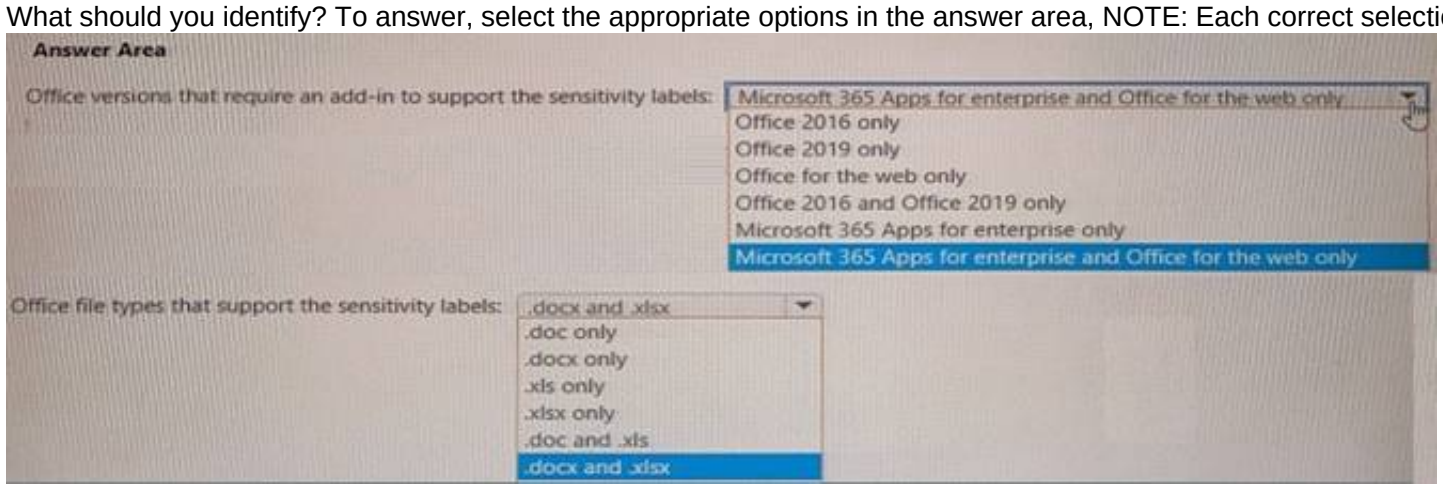
A. Mastered
B. Not Mastered

Answer: A

Explanation:



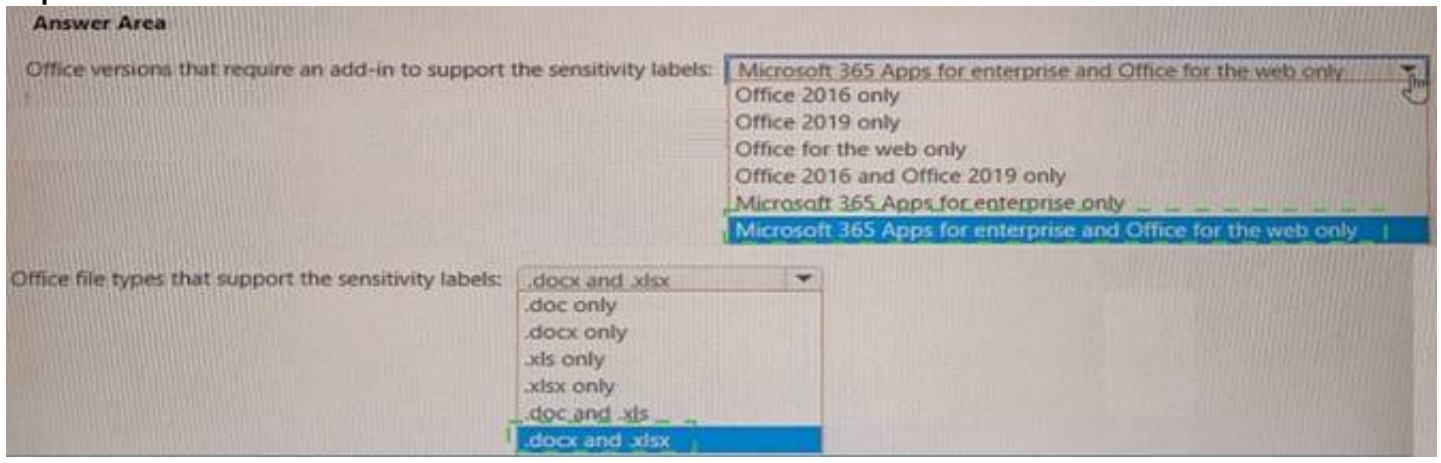
NEW QUESTION 277
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 E5 tenant.
Users at the company use the following versions of Microsoft Office:
• Microsoft 365 Apps for enterprise
• Office for the web
• Office 2016
• Office 2019
The company currently uses the following Office file types:
• .docx
• .xlsx
• .doc
• xls
You plan to use sensitivity labels. You need to identify the following:
• Which versions of Office require an add-in to support the sensitivity labels.
• Which file types support the sensitivity labels.
What should you identify? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

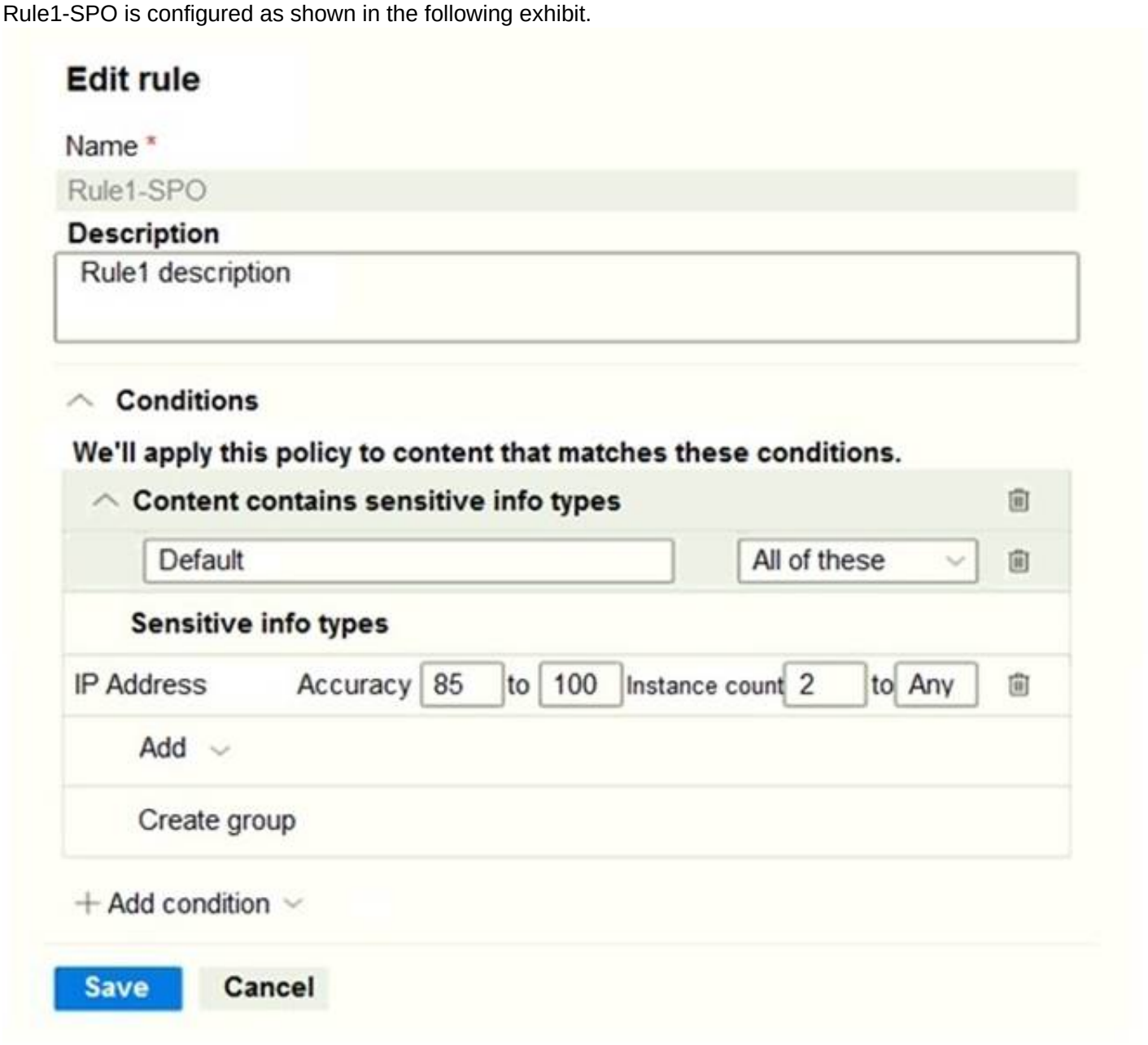
Explanation:



NEW QUESTION 282
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	5

You create a sensitivity label named Sensitivity1 and an auto-label policy that has the following configurations:
? Name: AutoLabel1
? Label to auto-apply: Sensitivity1
? Rules for SharePoint Online sites: Rule1-SPO
? Choose locations where you want to apply the label: Site1
Rule1-SPO is configured as shown in the following exhibit.



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

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	○	○
Sensitivity1 is applied to File2.txt.	○	○
Sensitivity1 is applied to File3.xlsx.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	○	○
Sensitivity1 is applied to File2.txt.	○	○
Sensitivity1 is applied to File3.xlsx.	○	○

NEW QUESTION 287
HOTSPOT - (Topic 5)
You are evaluating the use of multi-factor authentication (MFA).
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
Users will have 14 days to register for MFA after they sign in for the first time.	○	○
Users must use the Microsoft Authenticator app to complete MFA.	○	○
After registering, users must use MFA for every sign-in.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	○	○
Users must use the Microsoft Authenticator app to complete MFA.	○	○
After registering, users must use MFA for every sign-in.	○	○

NEW QUESTION 292
HOTSPOT - (Topic 5)
You need to ensure that Admin4 can use SSPR.
Which tool should you use. and which action should you perform? To answer, select the appropriate options m the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

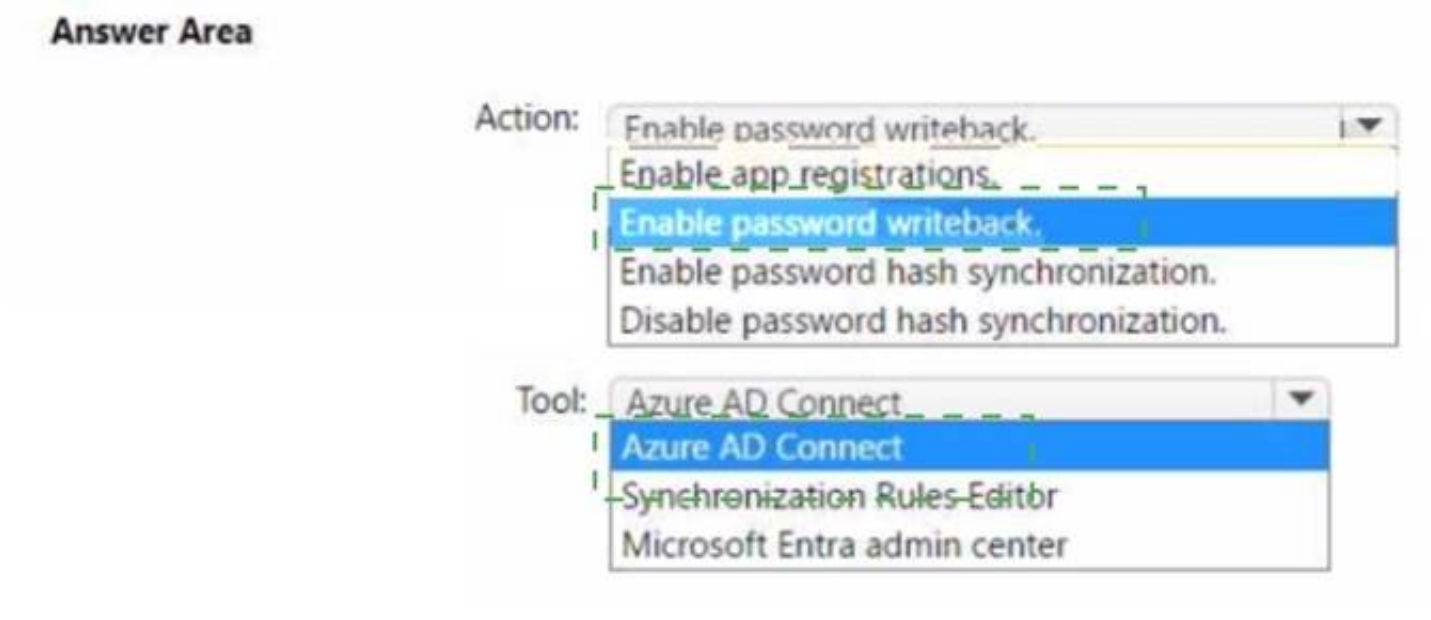
Action: Enable password writeback.
- Enable app registrations.
- Enable password writeback.
- Enable password hash synchronization.
- Disable password hash synchronization.

Tool: Azure AD Connect
- Azure AD Connect
- Synchronization Rules Editor
- Microsoft Entra admin center

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 297
HOTSPOT - (Topic 5)
You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.
Which users can review the incidents and advisories, and which blade should the users use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

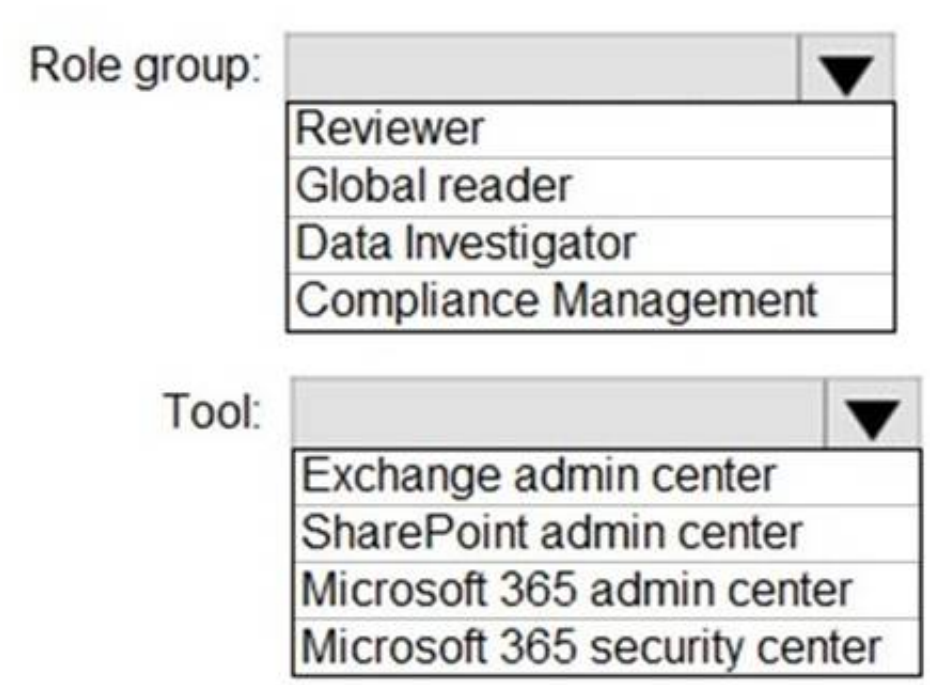
NEW QUESTION 302
- (Topic 4)
Which role should you assign to User1?
Available Choices (select all choices that are correct)

A. Hygiene Management
B. Security Reader
C. Security Administrator
D. Records Management

Answer: C

Explanation:
A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory- assign-admin-roles

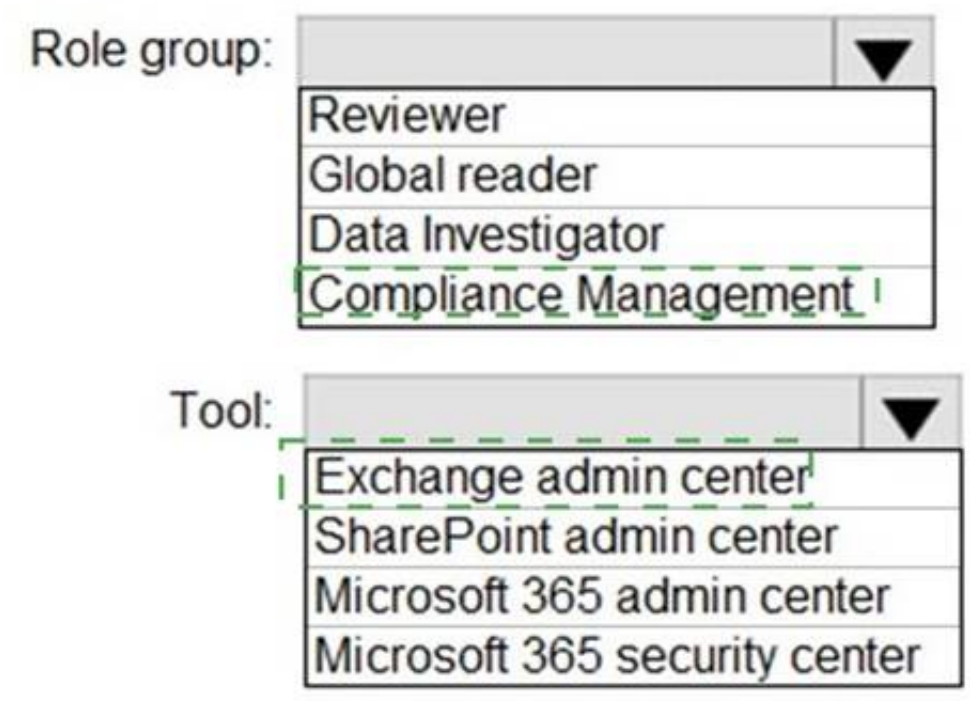
NEW QUESTION 306
HOTSPOT - (Topic 3)
You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements.
To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



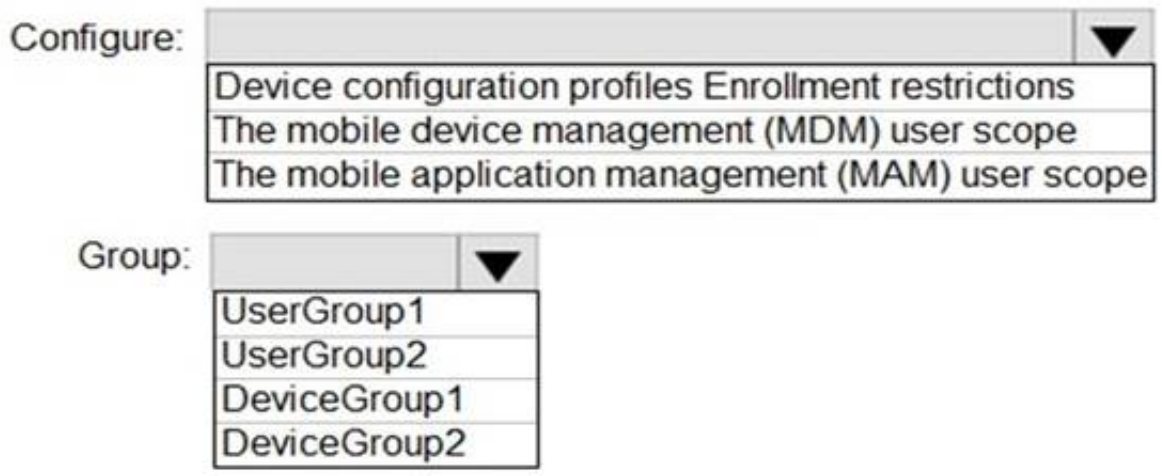
A. Mastered
B. Not Mastered

Answer: A

Explanation:



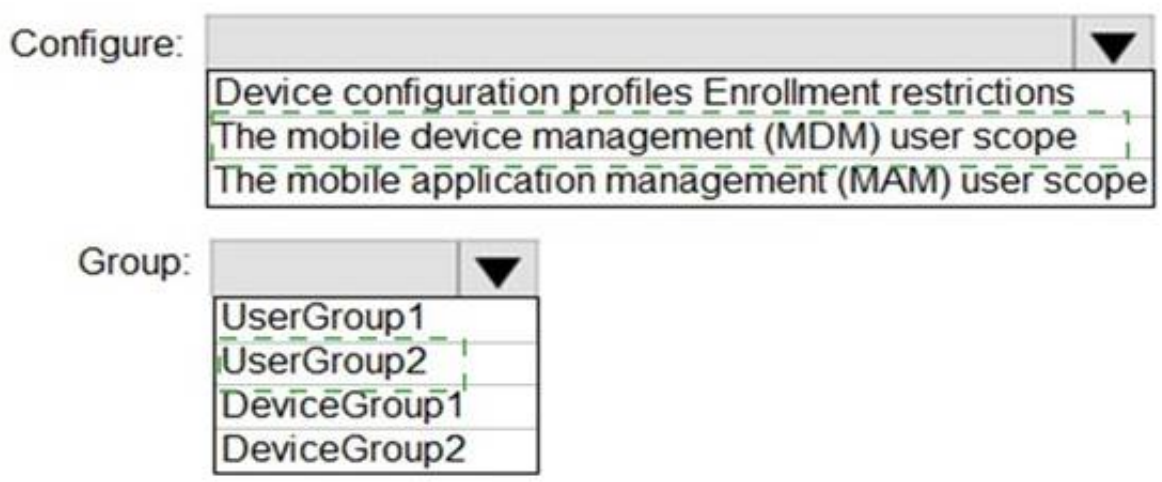
NEW QUESTION 307
HOTSPOT - (Topic 3)
You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.
What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 309
- (Topic 3)
You need to create the Safe Attachments policy to meet the technical requirements. Which option should you select?

A. Replace
B. Enable redirect
C. Block
D. Dynamic Delivery

Answer: D

Explanation:
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/safe-attachments.md

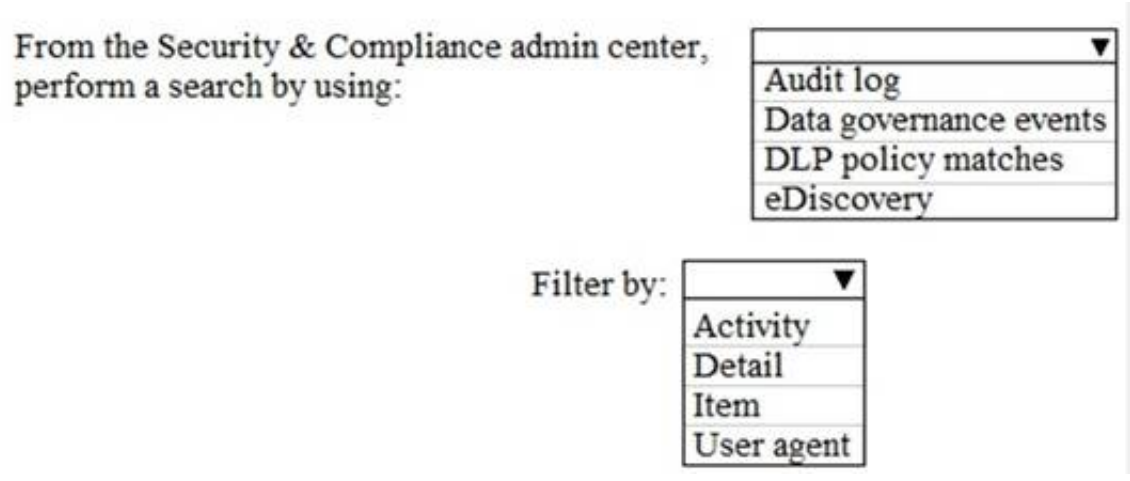
NEW QUESTION 311
- (Topic 3)
You need to configure the compliance settings to meet the technical requirements. What should you do in the Microsoft Endpoint Manager admin center?

A. From Compliance policies, modify the Notifications settings.
B. From Locations, create a new location for noncompliant devices.
C. From Retire Noncompliant Devices, select Clear All Devices Retire State.
D. Modify the Compliance policy settings.

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION 316
HOTSPOT - (Topic 2)
You need to meet the technical requirement for the SharePoint administrator. What should
you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



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#step-3-filter-the-search-results

NEW QUESTION 318
- (Topic 1)
On which server should you use the Defender for identity sensor?

A. Server1
B. Server2
C. Server3
D. Server4
E. Servers5

Answer: A

Explanation:
However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

NEW QUESTION 319
- (Topic 2)
Which report should the New York office auditors view?

A. DLP policy matches
B. DLP false positives and overrides
C. DLP incidents
D. Top Senders and Recipients

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention- policies
This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

NEW QUESTION 324
HOTSPOT - (Topic 1)
As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

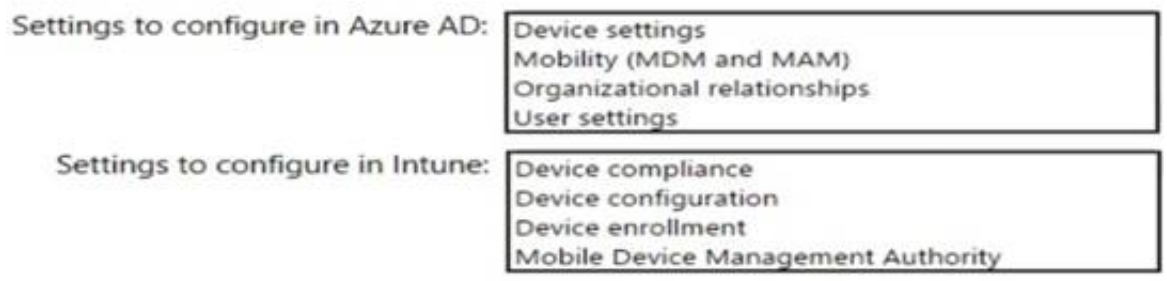
A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet March Feature Updates: Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date
References:
https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

NEW QUESTION 329
HOTSPOT - (Topic 1)
You need to meet the technical requirements and planned changes for Intune. What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

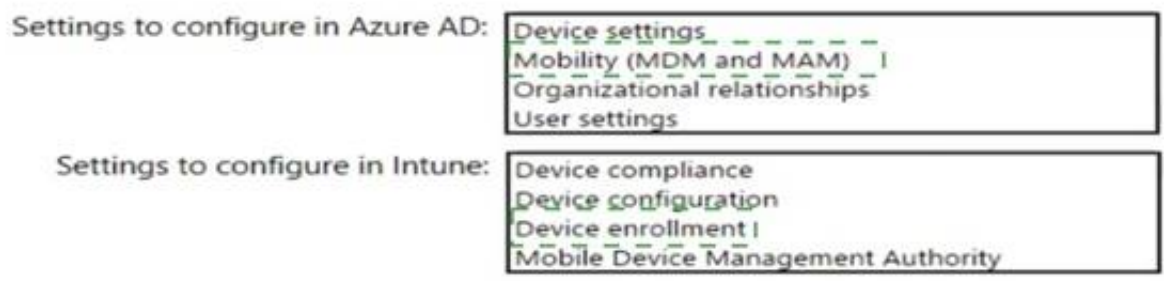


A. Mastered
B. Not Mastered

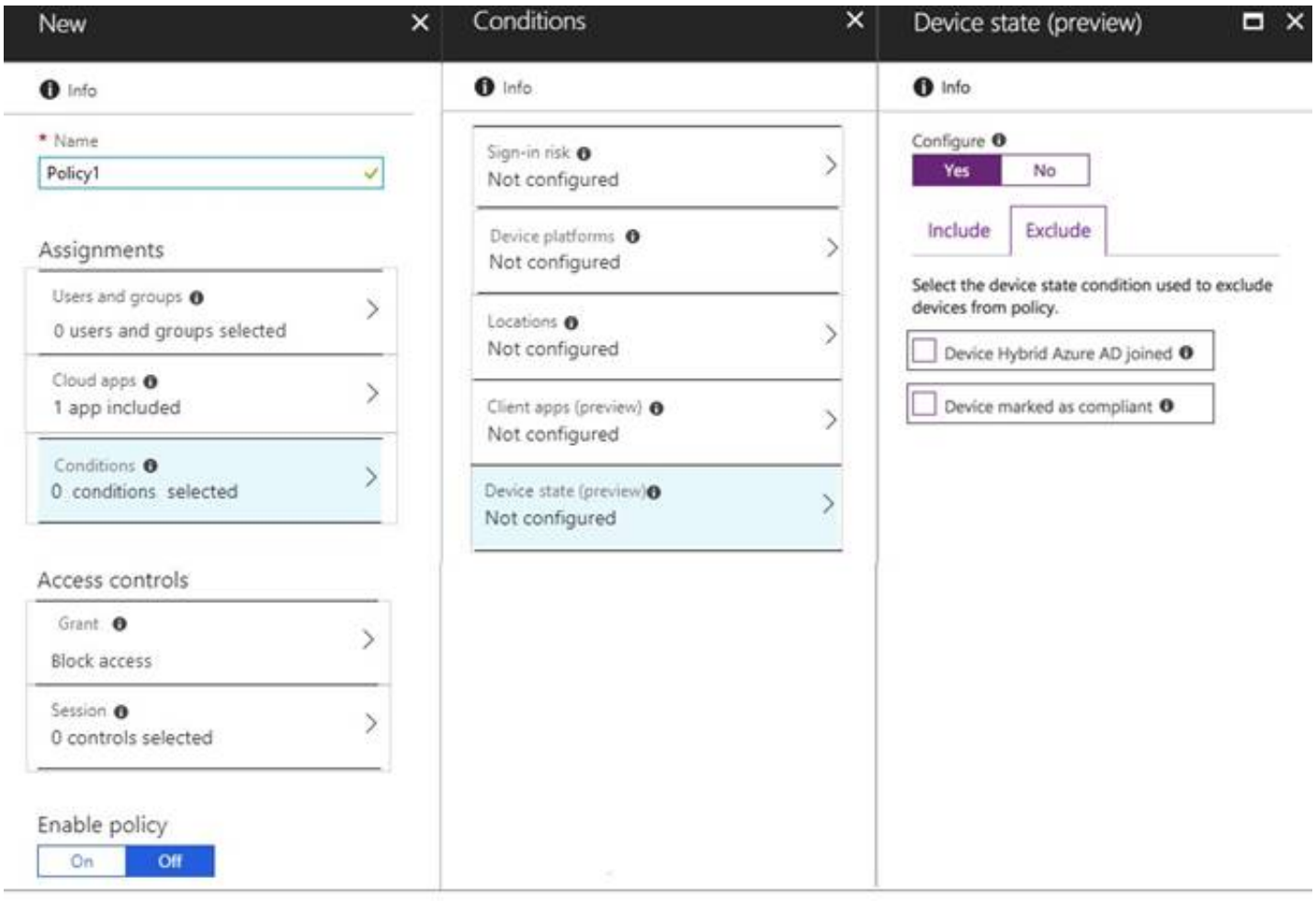
Answer: A

Explanation:

Answer Area



NEW QUESTION 334
HOTSPOT - (Topic 1)
You need to configure a conditional access policy to meet the compliance requirements. You add Exchange Online as a cloud app.
Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:https://docs.microsoft.com/en-us/intune/create-conditional-access-intune

NEW QUESTION 337
- (Topic 1)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.
Does this meet the goal?

A. Yes
B. NO

Answer: A

Explanation:
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune. Reference: https://docs.microsoft.com/en- us/configmgr/comanage/how-to-enable

NEW QUESTION 341
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to implement identity protection by configuring a sign-in risk policy and a user risk policy. Which type of risk is detected by each policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

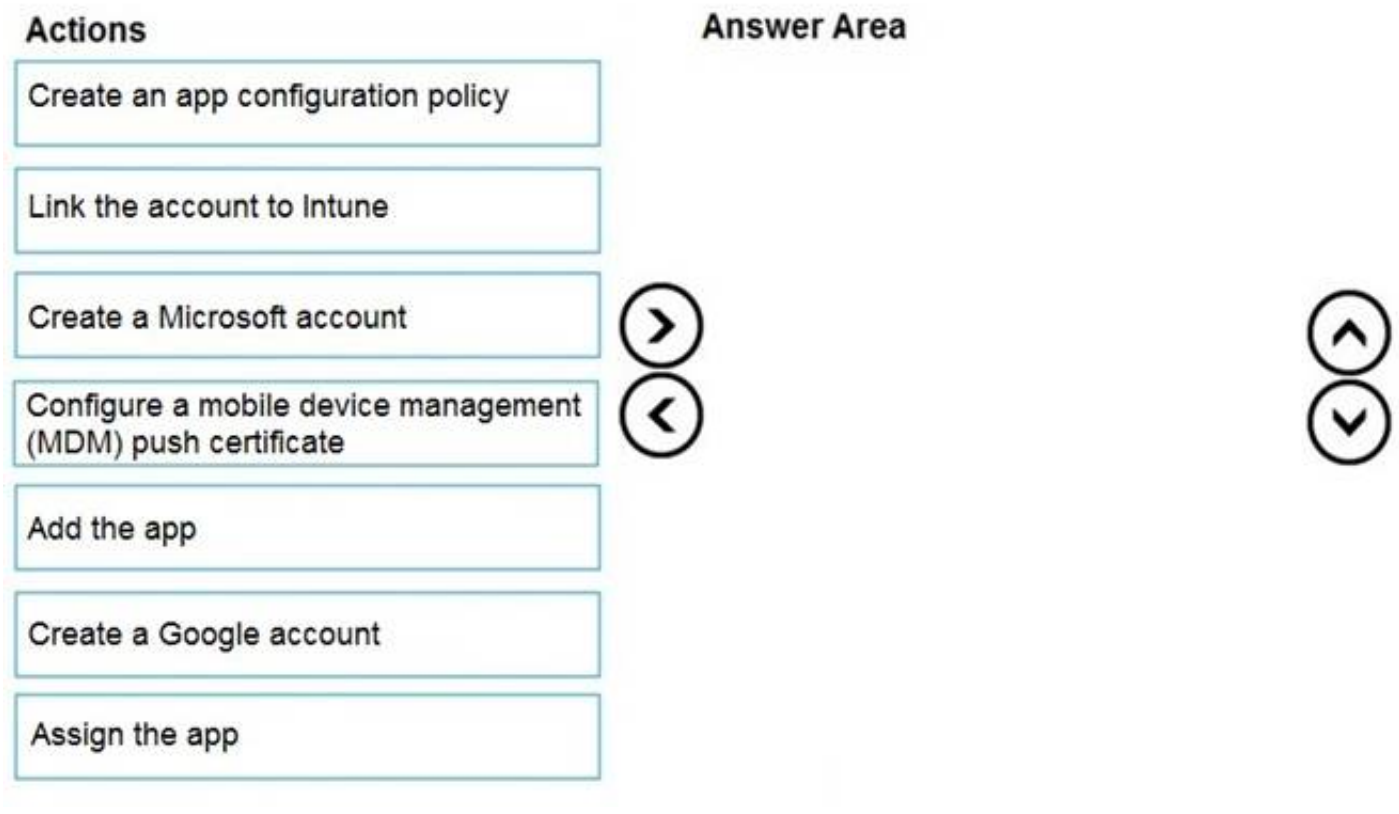
Explanation:

NEW QUESTION 343
- (Topic 6)
You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.
During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint.
You need to prevent the user from sharing the credit card information by using email and SharePoint.
What should you configure?

A. the status of the DLP policy
B. the user overrides of the DLP policy rule
C. the locations of the DLP policy
D. the conditions of the DLP policy rule

Answer: D

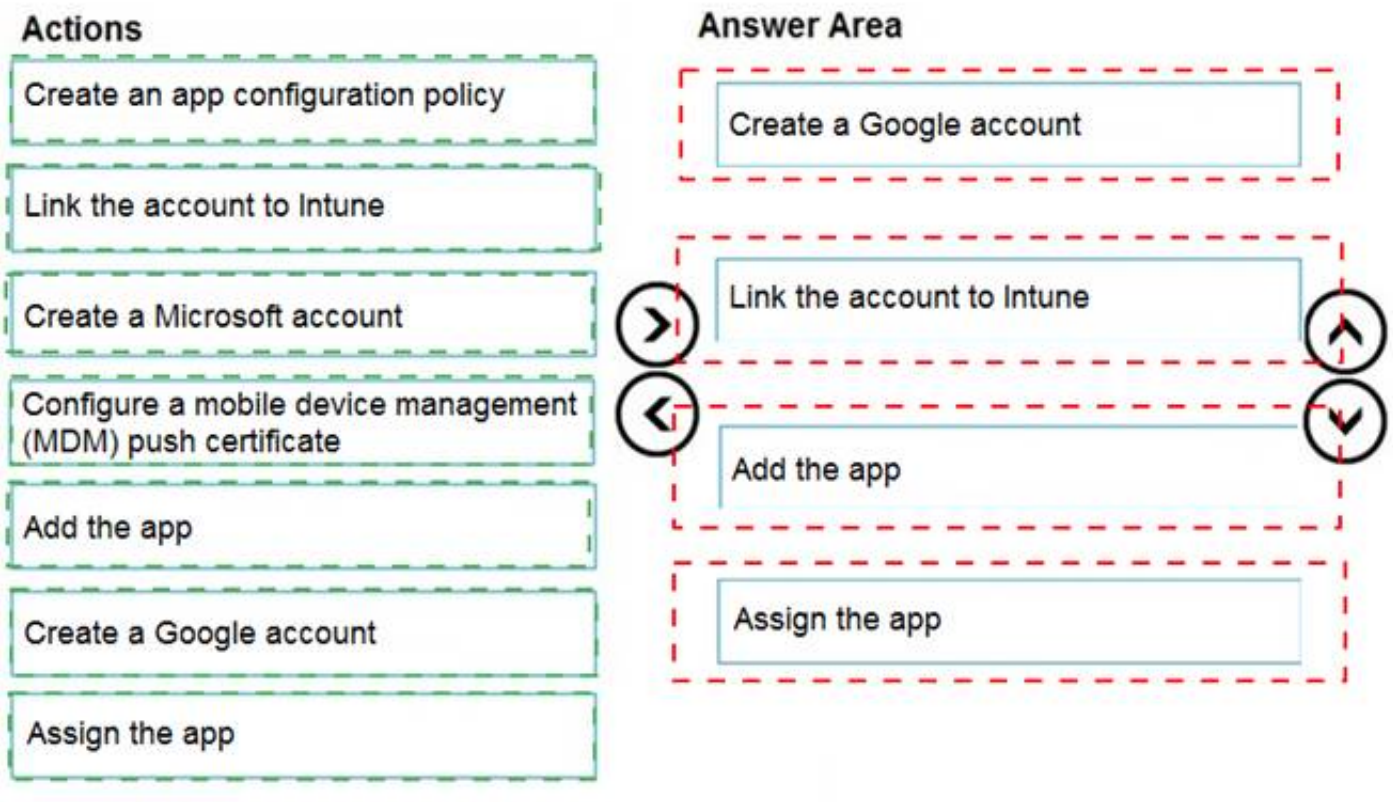
NEW QUESTION 345
DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune.
You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



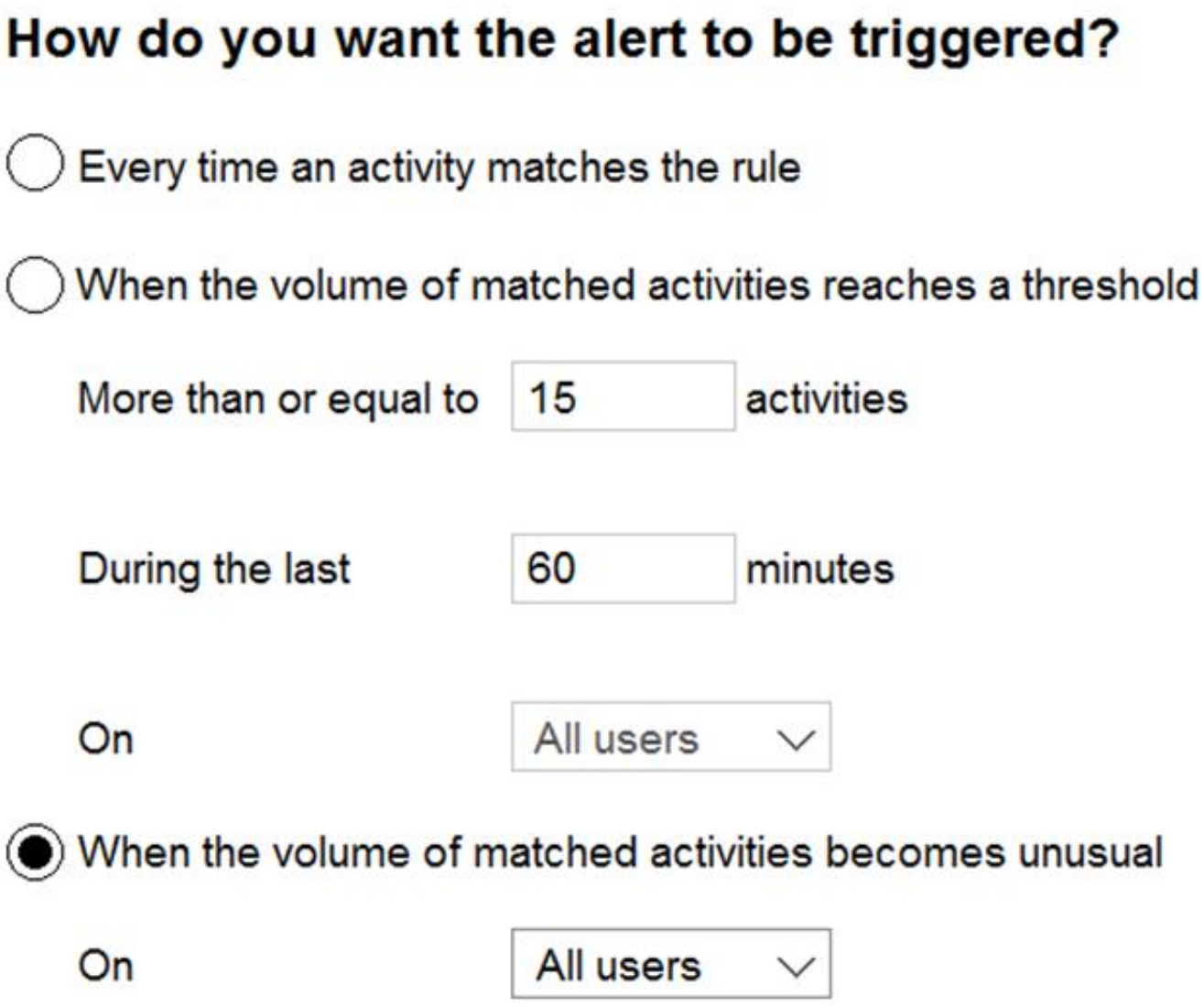
A. Mastered
B. Not Mastered

Answer: A

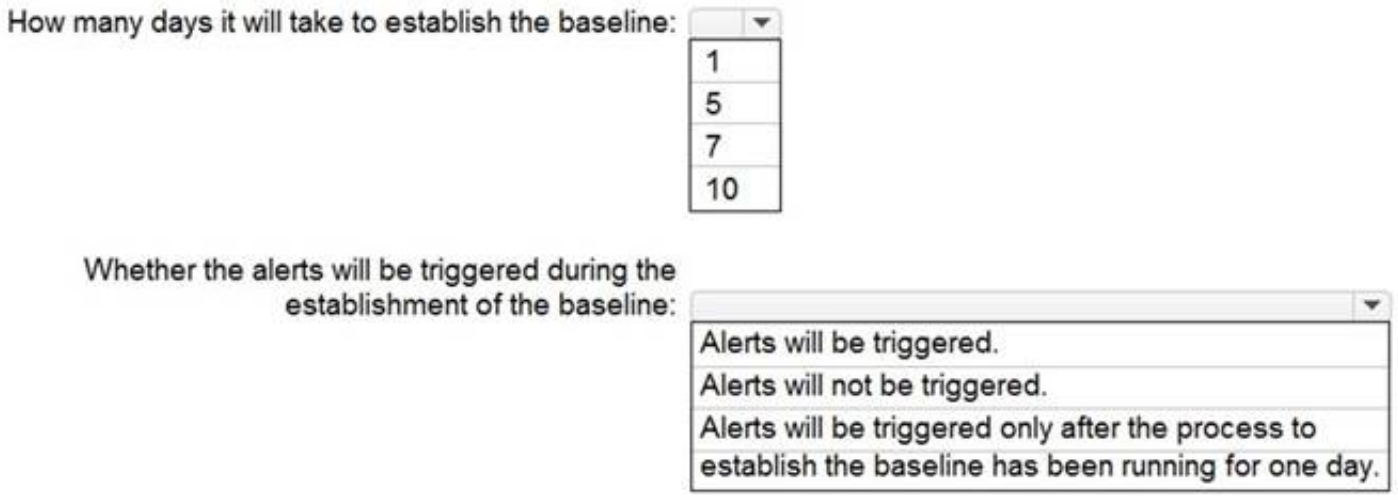
Explanation:



NEW QUESTION 348
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You configure a new alert policy as shown in the following exhibit.



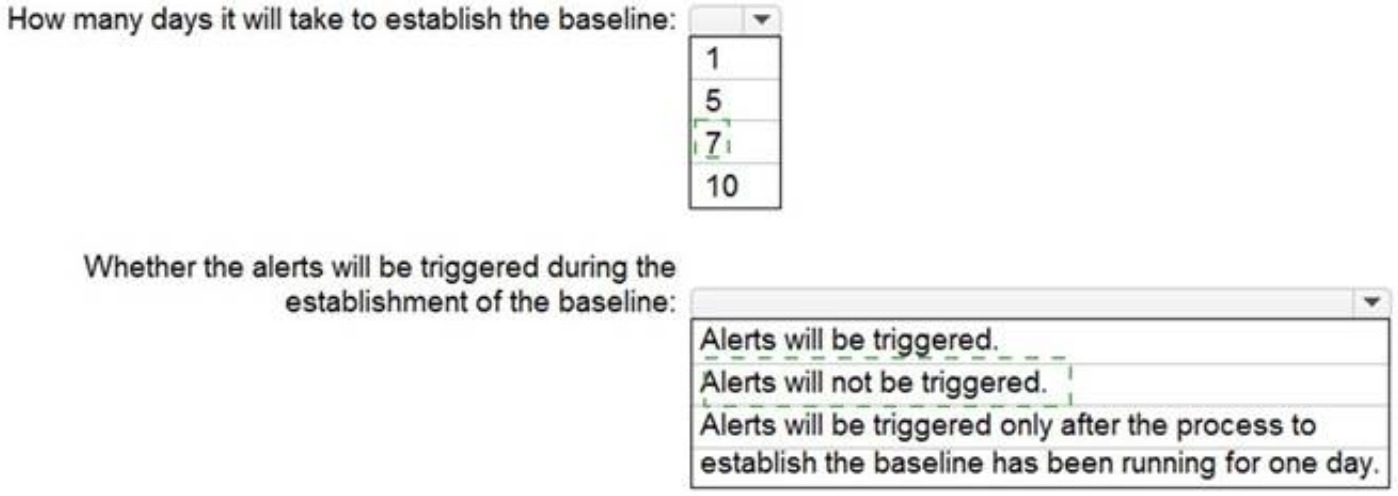
You need to identify the following:
? How many days it will take to establish a baseline for unusual activity.
? Whether alerts will be triggered during the establishment of the baseline.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

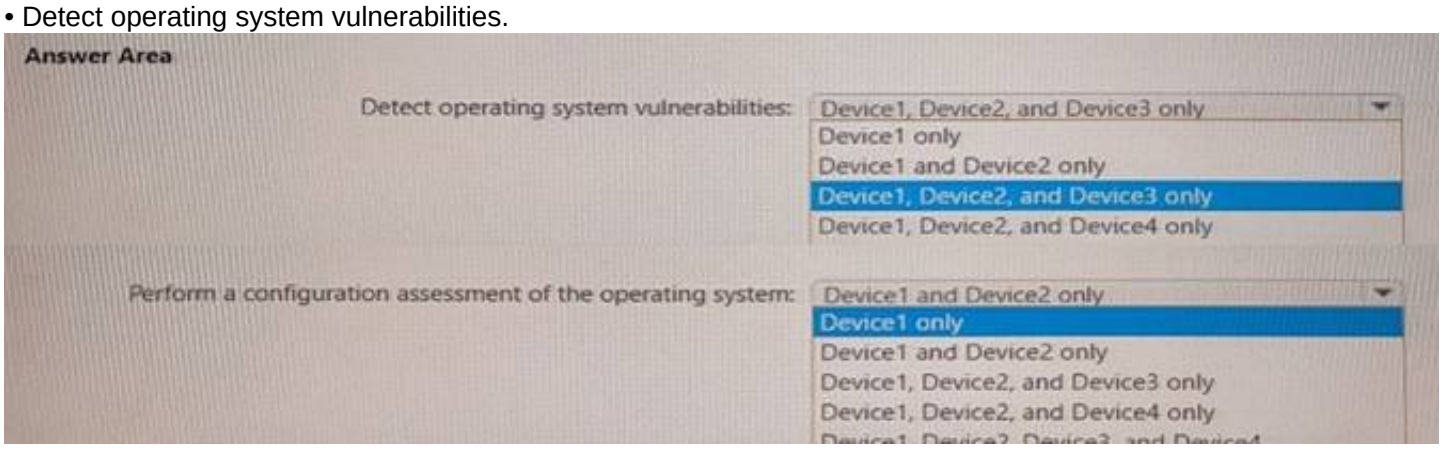
Explanation:



NEW QUESTION 350
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

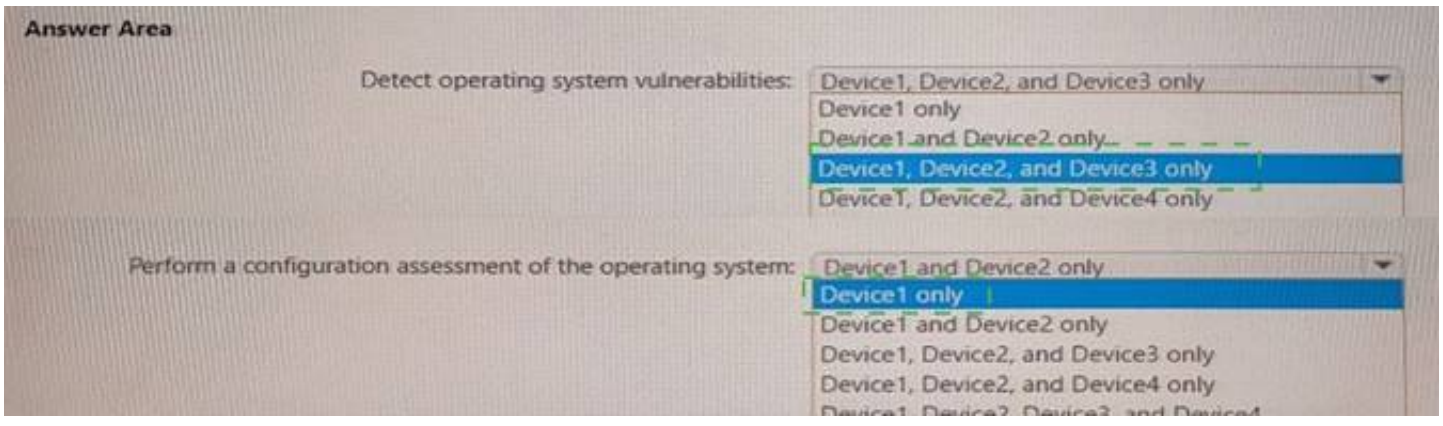
All the devices are onboarded To Microsoft Defender for Endpoint
You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:
• Detect operating system vulnerabilities.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 351
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.
You need to export the existing template.
Which file format should you use for the exported template?

A. CSV
B. XLSX
C. JSON
D. XML

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldwide#export-a-template

NEW QUESTION 352
- (Topic 6)
You have an Azure AD tenant that contains the users shown in the following table

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Exchange Administrator

You need to compare the permissions of each role. The solution must minimize administrative effort.
Which portal should you use?

A. the Microsoft Purview compliance portal
B. the Microsoft 365 admin center
C. the Microsoft 365 Defender portt1
D. the Microsoft Entra admin center

Answer: A

NEW QUESTION 354
- (Topic 6)
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 computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select System, and then you select About to view information about the system.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

NEW QUESTION 359
HOTSPOT - (Topic 6)
HOTSPOT
You have an Azure AD tenant that contains the administrative units shown in the following table.

Name	Members
AU1	User1, User2
AU2	User3

You have the following users:
? A user named User1 that is assigned the Password Administrator for AU1 and AU2.
? A user named User2 that is assigned the User Administrator for AU1.
? A user named User3 that is assigned the User Administrator for the tenant.
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
User1 can reset the password of User3.	○	○
User2 can update the display name of User1.	○	○
User1 can reset the password of User2.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
User1 is assigned the Password Administrator for AU1 and AU2. User3 is in AU2. User3 is User Adminstrator.
Password administrators cannot reset User Administrators passwords.
Note: Password Administrator
Users with this role have limited ability to manage passwords. This role does not grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user's password depends on the role the user is assigned.

Role that password can be reset	Password Admin	Helpdesk Admin	Auth Admin	User Admin	Privileged Auth Admin	Global Admin
User Admin				✔	✔	✔
Usage Summary Reports Reader		✔	✔	✔	✔	✔

Box 2: Yes
Box 3: No
User1 is assigned the Password Administrator for AU1 and AU2. User2 is in AU1. User2 is User Adminstrator.
Password administrators cannot reset User Administrators passwords.
Note: User Administrator
Can manage all aspects of users and groups, including resetting passwords for limited admins.

NEW QUESTION 361
- (Topic 6)
Your company has a Microsoft 365 subscription. you implement sensitivity Doris for your company.
You need to automatically protect email messages that contain the word Confidential m the subject line.
What should you create?

A. a sharing policy from the Exchange admin center
B. a mail flow rule from the Exchange admin center
C. a message Dace from the Microsoft 365 security center
D. a data loss prevention (DLP) policy from the Microsoft 365 compliance center

Answer: B

NEW QUESTION 362
- (Topic 6)
You plan to use Azure Sentinel and Microsoft Cloud App Security. You need to connect Cloud App Security to Azure Sentinel.
What should you do in the Cloud App Security admin center?

A. From Automatic log upload, add a log collector.
B. From Automatic log upload, add a data source.
C. From Connected apps, add an app connector.
D. From Security extension, add a SIEM agent.

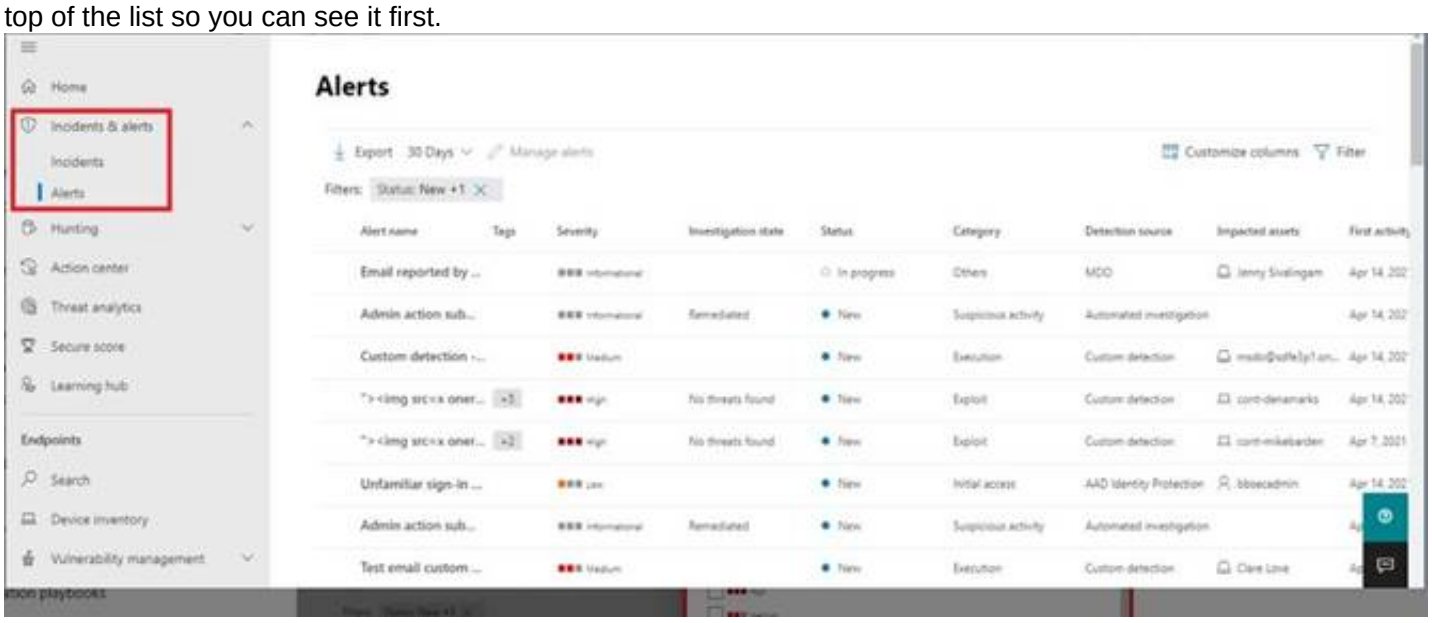
Answer: D

NEW QUESTION 366
- (Topic 6)
You are reviewing alerts in the Microsoft 365 Defender portal. How long are the alerts retained in the portal?

A. 30 days
B. 60 days
C. 3 months
D. 6 months
E. 12 months

Answer: C

Explanation:
Data retention information for Microsoft Defender for Office 365
By default, data across different features is retained for a maximum of 30 days. However, for some of the features, you can specify the retention period based on policy. See the following table for the different retention periods for each feature.
Defender for Office 365 Plan 1
* Alert metadata details (Microsoft Defender for Office alerts) 90 days.
Note: By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the top of the list so you can see it first.



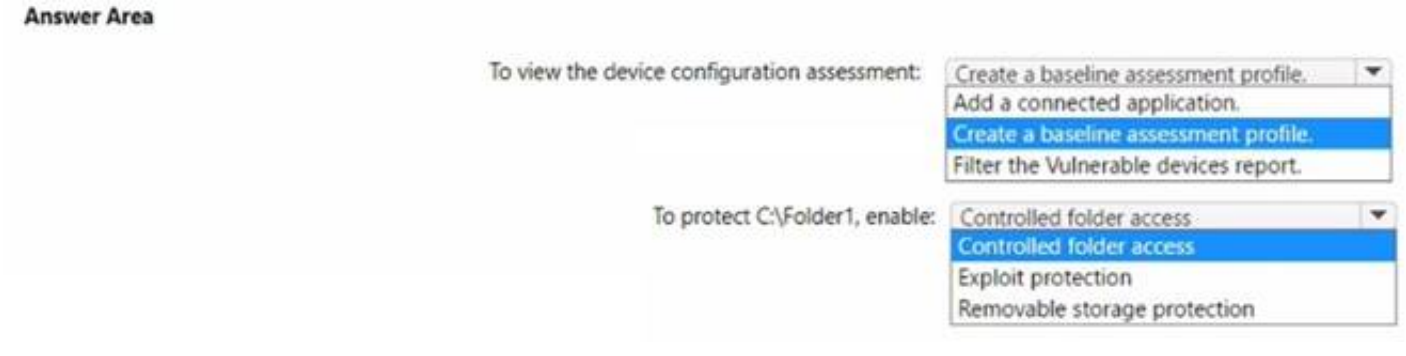
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data- retention

NEW QUESTION 369
- (Topic 6)
You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User1. you need to preserve a copy of all the email messages that contain the word ProjectX.
What should you do first?

A. From the Exchange admin center create a mail flow rule.
B. From Microsoft 365 Defender, start a message trace.
C. From Microsoft Defender for Cloud Apps, create an activity policy.
D. From the Microsoft Purview compliance portal, create a label and a label policy.

Answer: D

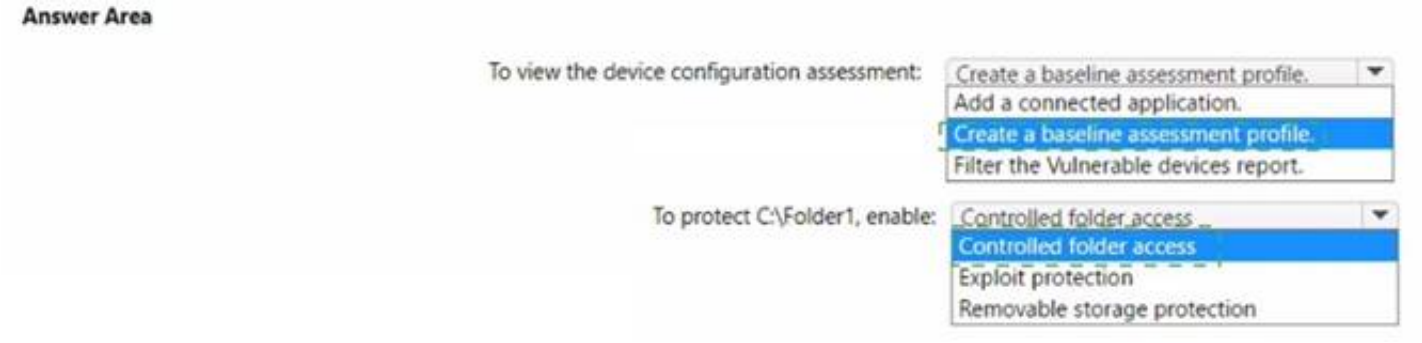
NEW QUESTION 372
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
All corporate Windows 11 devices are managed by using Microsoft Intune and onboarded to Microsoft Defender for Endpoint.
You need to meet the following requirements:
* View an assessment of the device configurations against the Center for Internet Security (CIS) vl.0.0 benchmark.
• Protect a folder named C:\Folder1 from being accessed by untrusted applications on the devices.
What should you do? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 377
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps. You configure a session control policy to block downloads from SharePoint Online sites. Users report that they can still download files from SharePoint Online sites.
You need to ensure that file download is blocked while still allowing users to browse SharePoint Online sites.
What should you configure?

A. an access policy
B. a data loss prevention (DLP) policy
C. an activity policy
D. a Conditional Access policy

Answer: A

NEW QUESTION 378
- (Topic 6)
You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

A. only the settings of Policy!
B. only the settings of Policy2
C. only the settings of Policy3
D. no settings

Answer: C

NEW QUESTION 381
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to implement records management and enable users to designate documents as regulatory records.
You need to ensure that the option to mark content as a regulatory record is visible when you create retention labels.
What should you do first?

A. Configure custom detection rules.
B. Create an Exact Data Match (EDM) schema.
C. Run the Sec-RegulacoryComplianceUI cmdlet.
D. Run the Sec-LabelPolicy cmdlet.

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365- worldwide

NEW QUESTION 386
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

MS-102 Practice Exam Features:

* MS-102 Questions and Answers Updated Frequently

* MS-102 Practice Questions Verified by Expert Senior Certified Staff

* MS-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* MS-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year