Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.
You need to remove User1 from the Restricted entities list. What should you use?

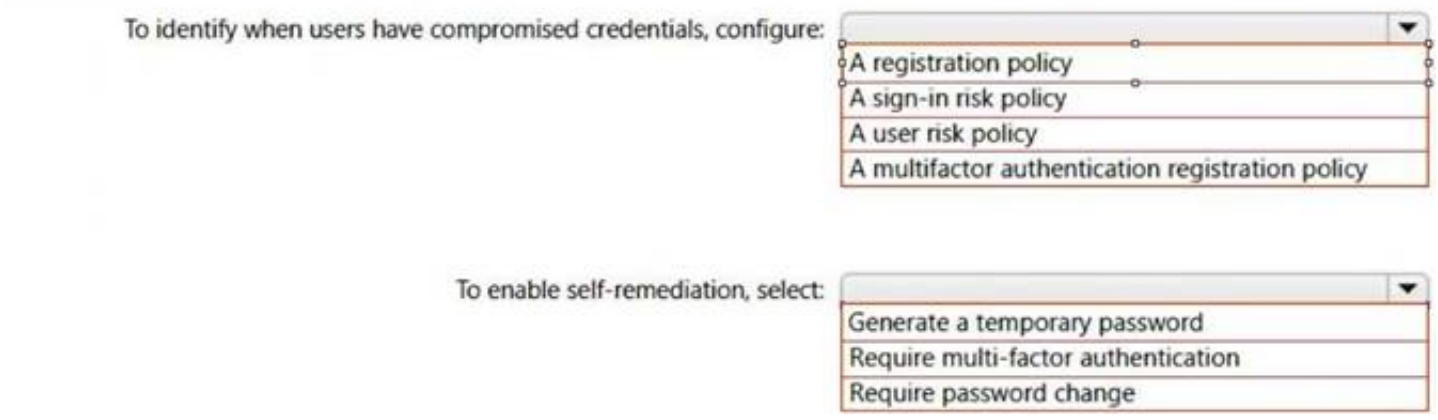
A. the Exchange admin center
B. the Microsoft Purview compliance portal
C. the Microsoft 365 admin center
D. the Microsoft 365 Defender portal
E. the Microsoft Entra admin center

Answer: D

Explanation:
Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.
Remove a user from the Restricted entities page in the Microsoft 365 Defender portal In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use https://security.microsoft.com/restrictedentities.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam

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



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)
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 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 4
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You plan to deploy 1.000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.
You need to recommend a Microsoft Intune enrollment option that meets the following requirements:
• Minimizes user interaction
• Minimizes administrative effort
• Automatically installs corporate apps What should you recommend?

A. Automated Device Enrollment (ADE)
B. bring your own device (BYOD) user and device enrollment
C. Apple Configurator enrollment

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll

NEW QUESTION 5
- (Topic 6)
You have a Microsoft 365 subscription.
You discover that some external users accessed center for a Microsoft SharePoint site. You modify the sharePoint sharing policy to prevent sharing, outside your organization. You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the Security $ Compliance admin center you create a threat management
policy.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 6
- (Topic 6)
Your company has a Microsoft 365 E5 tenant that contains a user named User1. You review the company's compliance score.
You need to assign the following improvement action to User1:Enable self-service password reset.
What should you do first?

A. From Compliance Manager, turn off automated testing.
B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

NEW QUESTION 7
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to configure a group naming policy.
Which portal should you use, and to which types of groups will the policy apply? 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:

NEW QUESTION 8
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Configuration
Group1	Global security group
User1	Enabled user account
User2	Disabled user account

You configure Azure AD Connect to sync contoso.com to Azure AD.
Which objects will sync to Azure AD?

A. Group1 only
B. User1 and User2 only
C. Group1 and User1 only
D. Group1, User1, and User2

Answer: D

Explanation:
Disabled accounts
Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.
The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts

NEW QUESTION 9
HOTSPOT - (Topic 6)
You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (default)	Device2	Group2

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 10
- (Topic 6)
You have a Microsoft 365 tenant that contains 500 Windows 10 devices and a Microsoft Endpoint Manager device compliance policy.
You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps.
Which policy type should you configure?

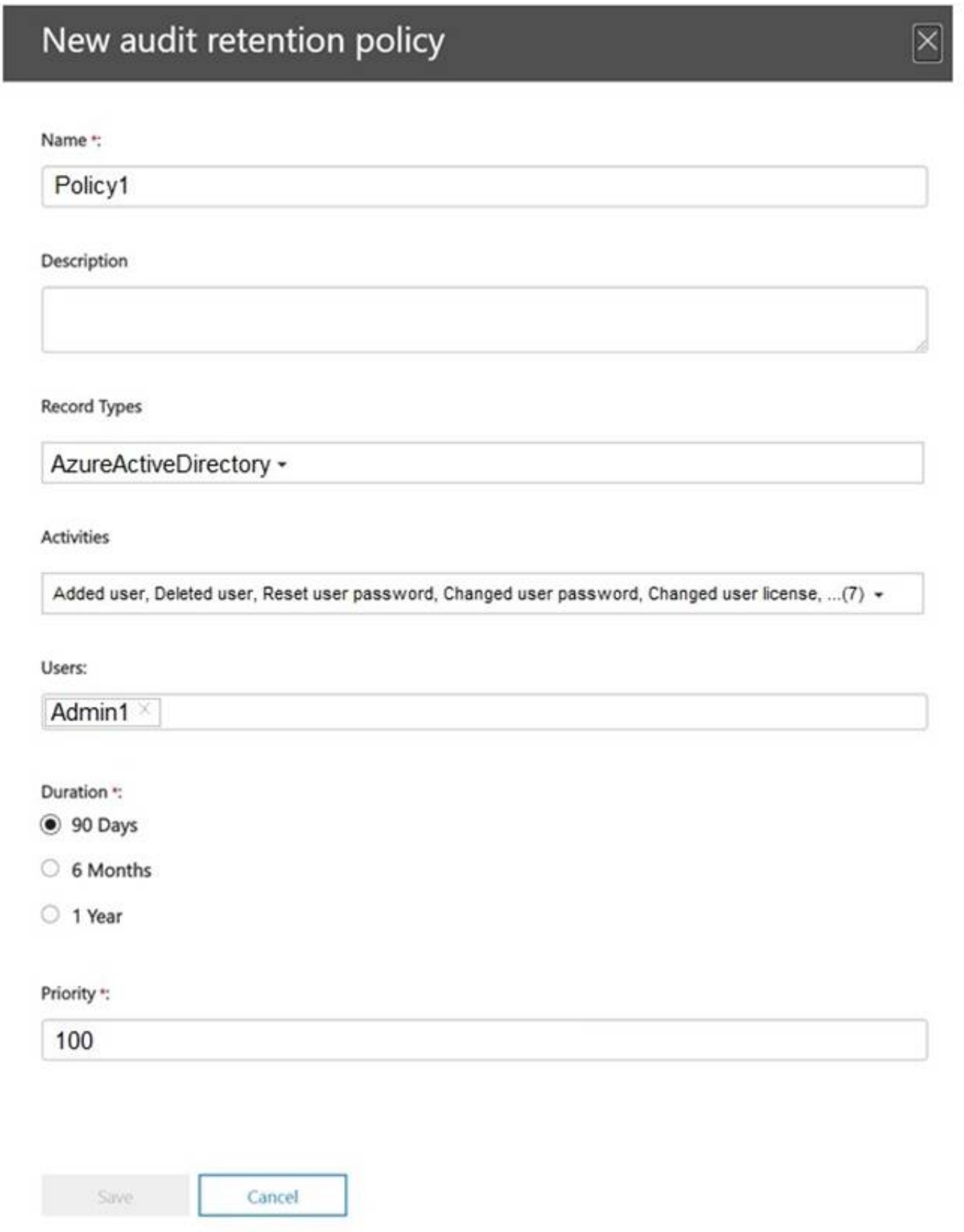
A. conditional access
B. account protection
C. attack surface reduction (ASR)
D. Endpoint detection and response

Answer: A

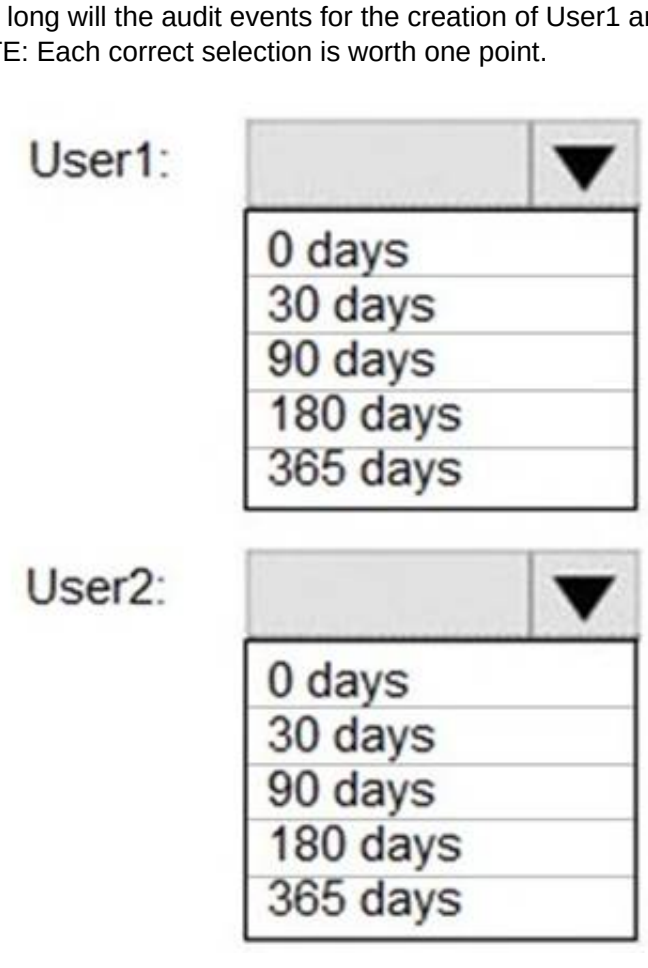
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION 10
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.)



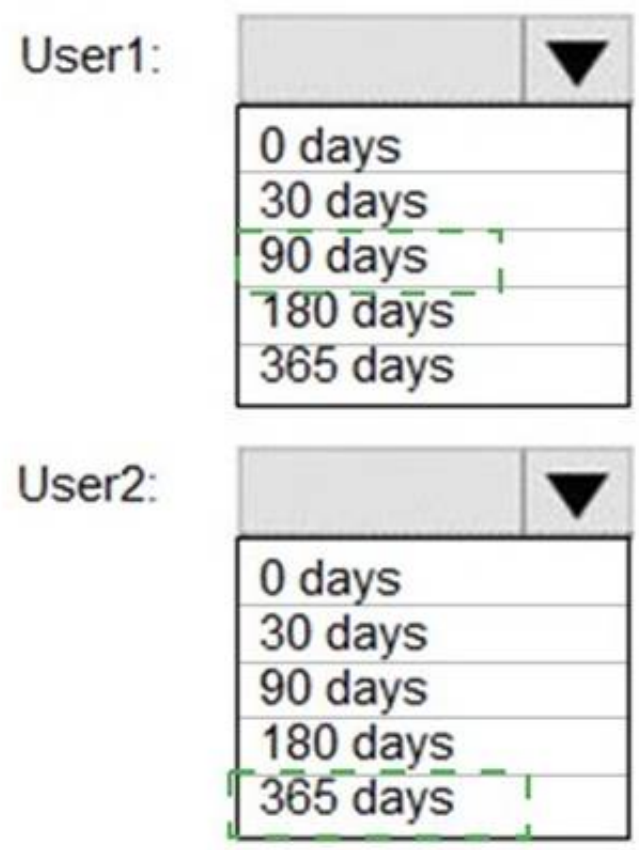
After Policy1 is created, the following actions are performed:
? Admin1 creates a user named User1.
? Admin2 creates a user named User2.
How long will the audit events for the creation of User1 and User2 be retained? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection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



A. Mastered
B. Not Mastered

Answer: A

Explanation:

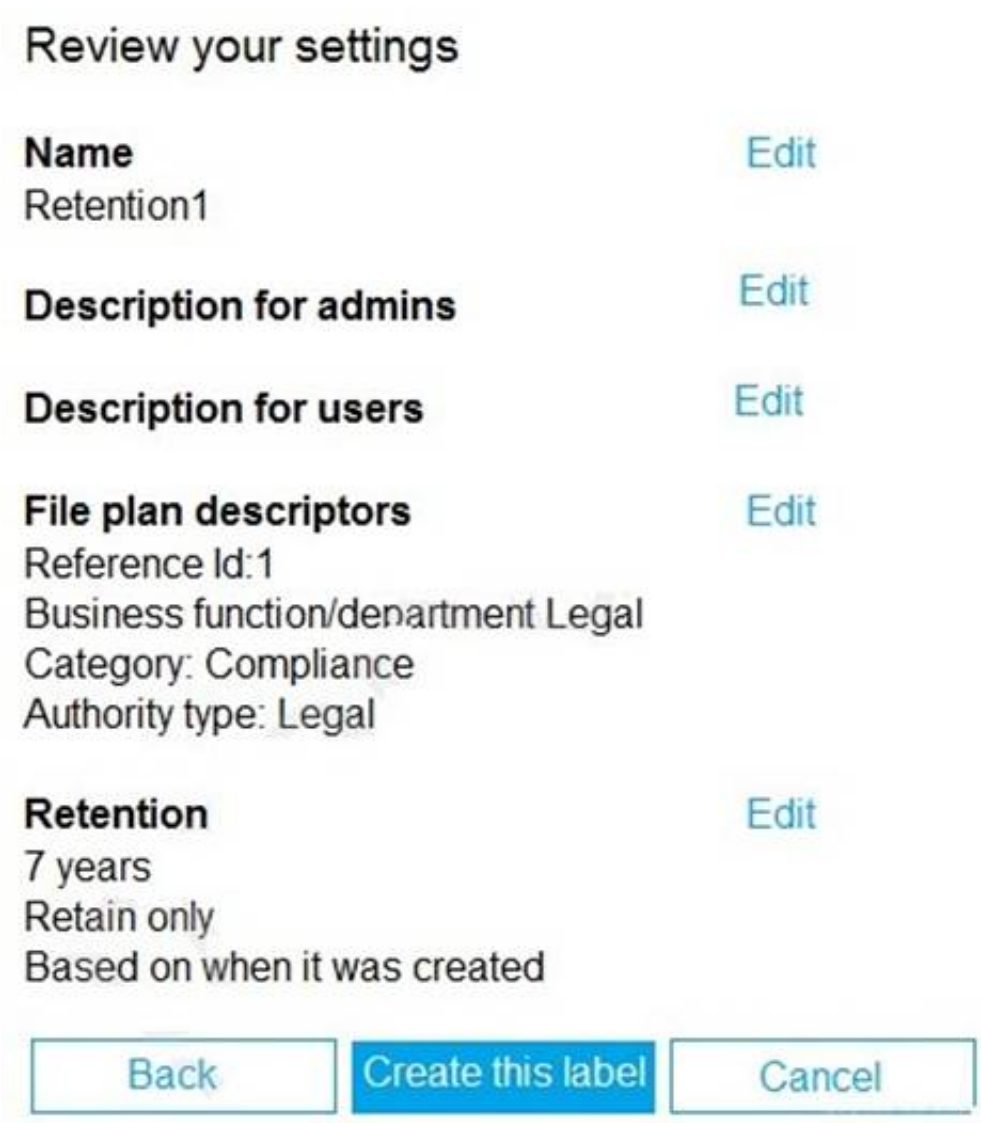


NEW QUESTION 11
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You define a retention label that has the following settings:
• Retention period 7 years
• Start the retention period bated on: When items were created
You need to prevent the removal of the label once the label K applied to a lie What should you select in the retention label settings?

A. Retain items even If users delete
B. Mark items as a record
C. Mark items as a regulatory record
D. Retain items forever

Answer: B

NEW QUESTION 12
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You create a retention label named Retention1 as shown in the following exhibit.



When users attempt to apply Retention1, the label is unavailable. You need to ensure that Retention1 is available to all the users. What should you do?

A. Create a new label policy
B. Modify the Authority type setting for Retention!
C. Modify the Business function/department setting for Retention 1.
D. Use a file plan CSV template to import Retention1.

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

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 19
- (Topic 6)
Your company has multiple offices.
You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.
You need to ensure that the local administrators can manage only the devices in their respective office.
What should you use?

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

Answer: A

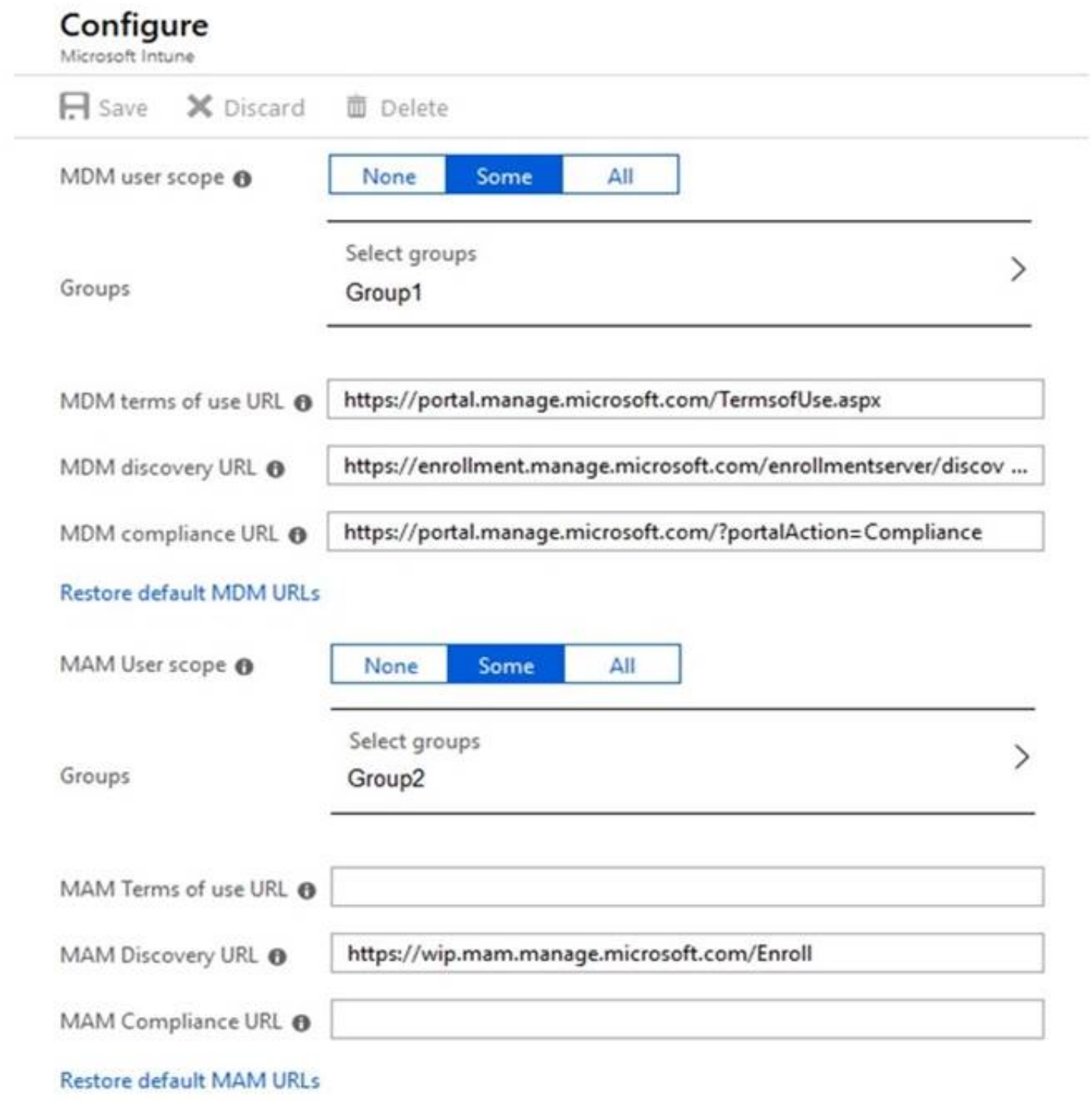
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

NEW QUESTION 21
HOTSPOT - (Topic 6)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.



You purchase a Windows 10 device named Device1.
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
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

NEW QUESTION 26
- (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

The policies are assigned to Device1.
Which policy settings will be applied to Device1?

A. only the settings of Policy1
B. only the settings of Policy2
C. only the settings of Policy3
D. no settings

Answer: D

NEW QUESTION 28
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 subscription that contains the users shown in the following table.

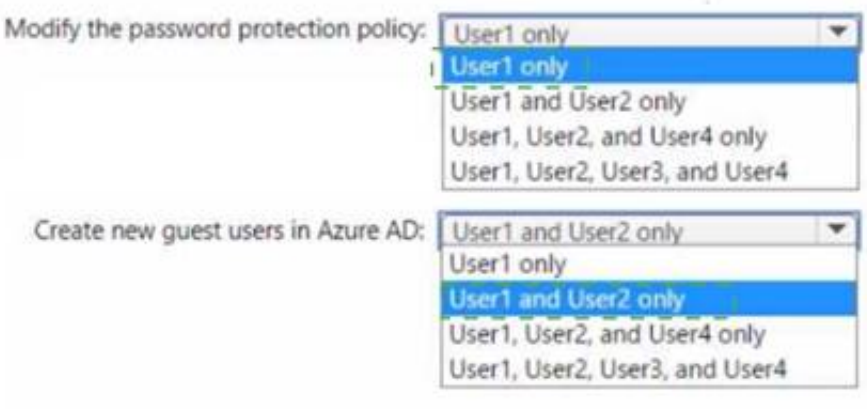
Name	Role
User1	Global Administrator
User2	Security Administrator, Guest Inviter
User3	None
User4	Password Administrator

External collaboration settings have default configuration.
You need to identify which users can perform the following administrative tasks:
• Modify the password protection policy.
• Create guest user accounts.
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.
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 31
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

A. Android
B. CentOS Linux
C. iOS
D. Window 10

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

NEW QUESTION 34
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

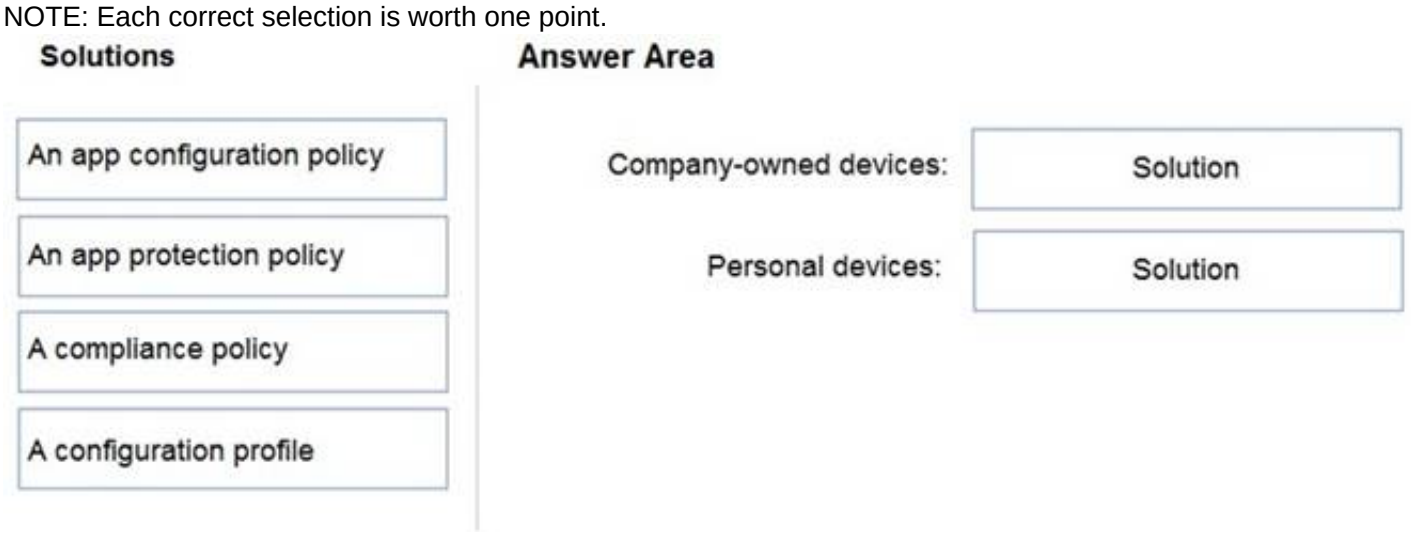
Explanation:
Box 1: will lose the role after eight hours
From exhibit: Activation, Activation maximum duration (hours): 8 hour(s)
Box 2: for up to three months
We see from exhibit: Assignment, Expire eligible assignment after: 3 month(s)

NEW QUESTION 35
- (Topic 6)
Your network contains an Active Directory forest named Contoso. Local. You have a Microsoft 365 subscription.
You plan to implement a directory synchronization solution that will use password hash synchronization.
From the Microsoft 365 admin center, you successfully verify the contoso.com domain name.
You need to prepare the environment for the planned directory synchronization solution. What should you do first?

A. From Active Directory Domains and Trusts, add contoso.com as a UPN suffix.
B. From the Microsoft 365 admin center verify the Contos
C. Local domain name.
D. From the public DNS zone of contoso.com, add a new mail exchanger (MX) record.
E. From Active Directory Users and Computers, modify the UPN suffix for all users.

Answer: A

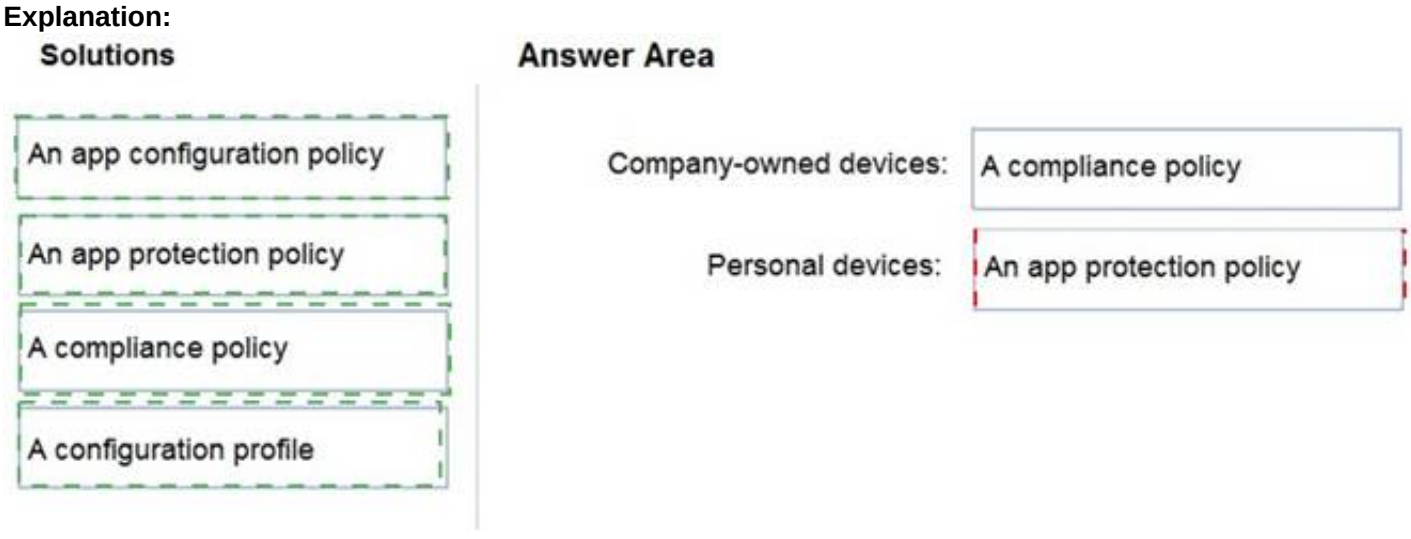
NEW QUESTION 38
DRAG DROP - (Topic 6)
Your company has a Microsoft 365 E5 tenant.
Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.
You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.
What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component 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:



NEW QUESTION 40
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.
You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for
10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.
You plan to onboard all the devices to Microsoft Defender for Endpoint. You need to store the Microsoft Defender for Endpoint data in Europe. What should you do first?

A. Delete the workspace.
B. Create a workspace.
C. Onboard a new device.
D. Offboard the test devices.

Answer: B

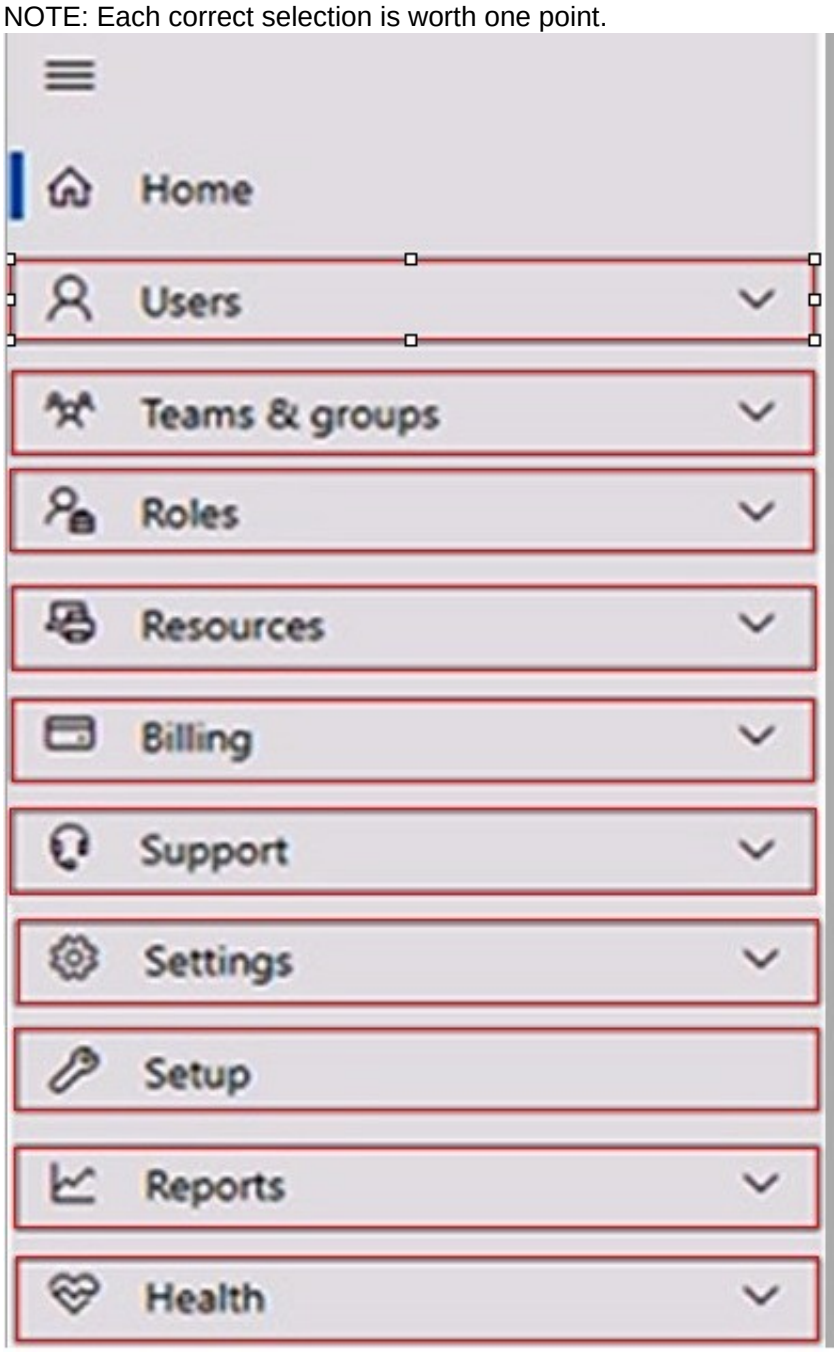
Explanation:
Storage locations
Understand where Defender for Cloud stores data and how you can work with your data:
* Machine information
- Stored in a Log Analytics workspace.
- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data- workspace

NEW QUESTION 41
- (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 47
- (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 49
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Role
User1	Global admin
User2	*None*
User3	*None*

You provision the private store in Microsoft Store for Business.
You assign Microsoft Store for Business roles to the users as shown in the following table.

Name	Role
User1	*None*
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.
Which users 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:

Can add apps to the private store:

- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

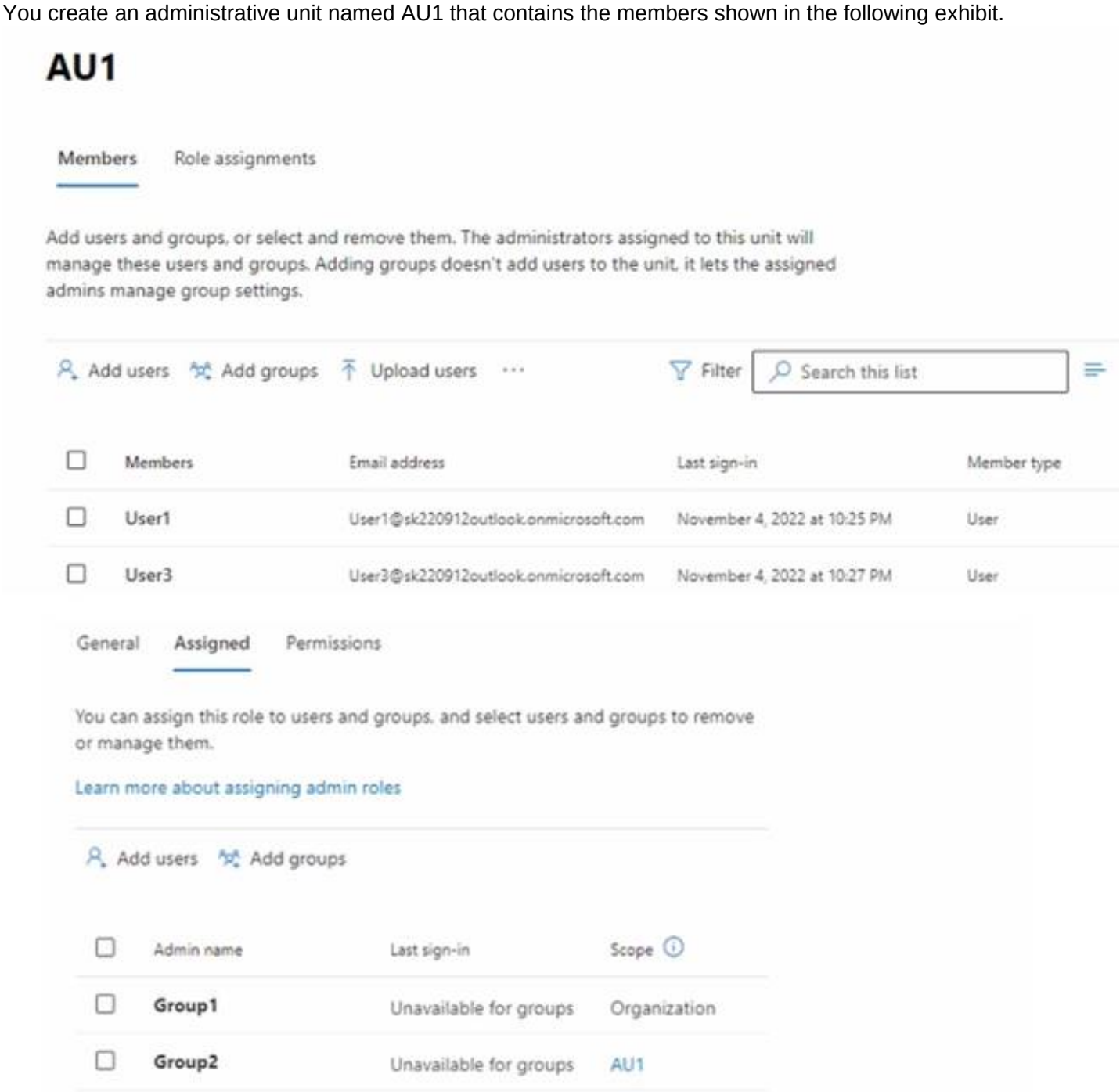
Can assign apps from Microsoft Store for Business:

- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

NEW QUESTION 50
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	None

You create an administrative unit named AU1 that contains the members 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.

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	○	○
User2 can reset the password of User3.	○	○
User2 can reset the password of User1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	○	
User2 can reset the password of User3.	○	
User2 can reset the password of User1.	○	

NEW QUESTION 54
- (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 57
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You onboard all devices to Microsoft Defender for Endpoint
You need to use Defender for Endpoint to block access to a malicious website at www.contoso.com.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

A. Create a web content filtering policy.
B. Configure an enforcement scope.
C. Enable Custom network indicators.
D. Create an indicator.
E. Enable automated investigation.

Answer: AC

NEW QUESTION 58
- (Topic 6)
You need to notify the manager of the human resources department when a user in the department shares a file or folder from the departments Microsoft

SharePoint Online site. What should you do?

A. From the SharePoint Online site, create an alert.
B. From the SharePoint Online admin center, modify the sharing settings.
C. From the Microsoft 365 Defender portal, create an alert policy.
D. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.

Answer: D

NEW QUESTION 62
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

Defender for Endpoint has the device groups shown in the following table.

Rank	Name	Matching rule
1	Group1	Tag Contains Inventory And OS in Android
2	Group2	Name Starts with Device And Tag Contains Inventory
Last	Ungrouped devices (default)	*Not applicable*

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@contoso.com

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
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	○
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	○
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.
Box 2: No
Computer1 does not belong to either Group1 or Group2
Box 3: Yes
Device3 belongs to both Group1 and Group2.
Note: Understanding alert severity
Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.
The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

NEW QUESTION 66
- (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 forest. You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
• Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
• User passwords must be 10 characters or more.
Solution: implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 71
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Group	MFA Status
User1	Group1	Enabled
User2	Group1, Group2	Enforced

You have the named locations shown in the following table.

Named location	IP range
Montreal	133.107.0.0/16
Toronto	193.77.10.0/24

You create a conditional access policy that has the following configurations:
• Users or workload identities: o Include: Group1
o Exclude: Group2
• Cloud apps or actions: Include all cloud apps
• Conditions:
o Include: Any location o Exclude: Montreal
• Access control: Grant access, Require multi-factor authentication User1 is on the multi-factor authentication (MFA) blocked users list.
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 Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	○	○
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	○	○
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	○	○
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	○	○
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	○	○

NEW QUESTION 73
- (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 78
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

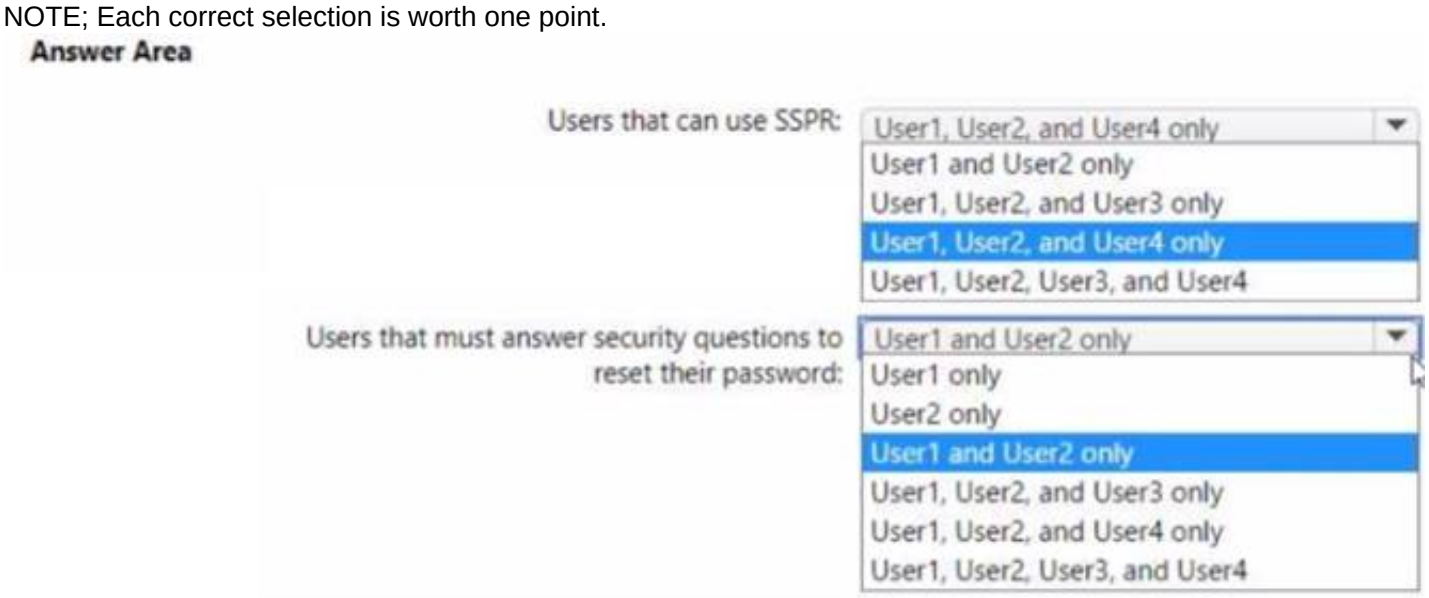
Explanation:

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 81
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Role
User1	Group1	User Administrator
User2	Group1	None
User3	Group2	None
User4	None	Global Administrator

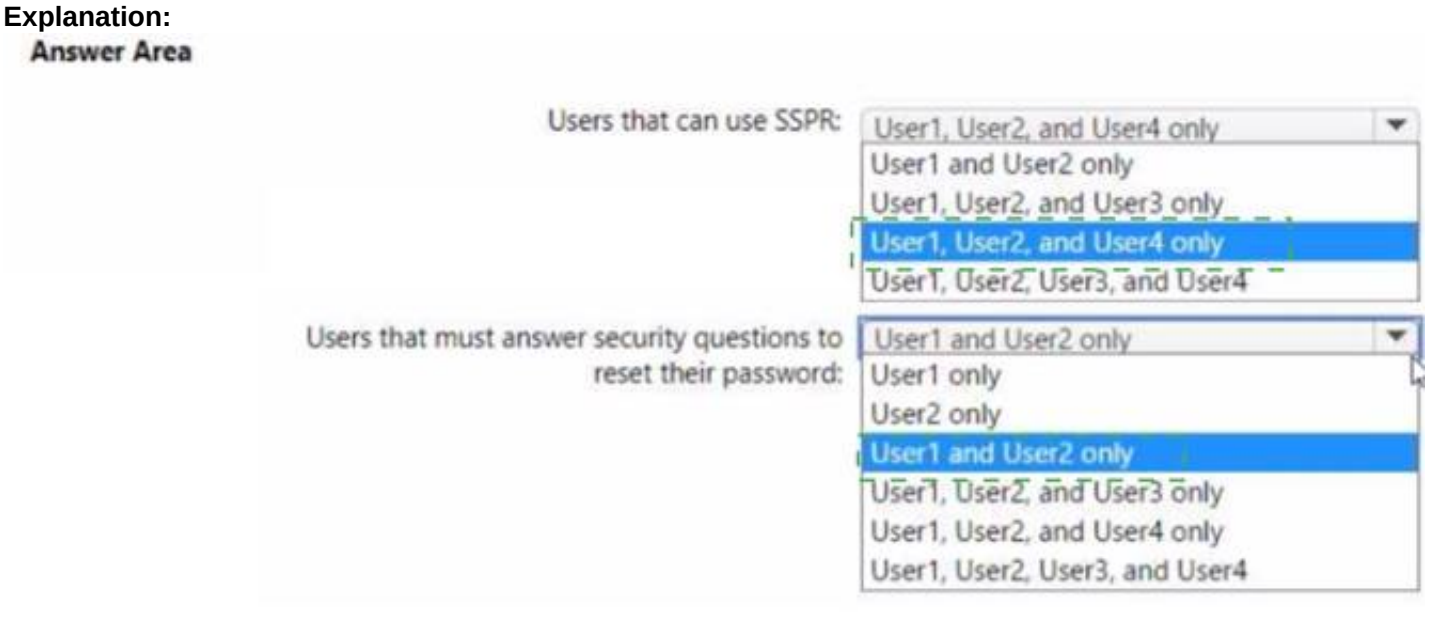
You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.
Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.
NOTE; Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 85
- (Topic 6)
Your on-premises network contains an Active Directory domain. You have a Microsoft 365 E5 subscription.
You plan to implement a hybrid configuration that has the following requirements:
• Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources
• Supports the use of Azure AD Identity Protection
You need to configure Azure AD Connect to support the planned implementation. Which two options should you select? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Password Hash Synchronization
B. Password writeback
C. Directory extension attribute sync
D. Enable single sign-on
E. Pass-through authentication

Answer: AB

NEW QUESTION 90

- (Topic 6)
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.
Where can you store data from the LinkedIn connector?

A. a Microsoft OneDrive for Business folder
B. a Microsoft SharePoint Online document library
C. a Microsoft 365 mailbox
D. Azure Files

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin- data?view=o365-worldwide

NEW QUESTION 94
- (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 95
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 98
- (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 99
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

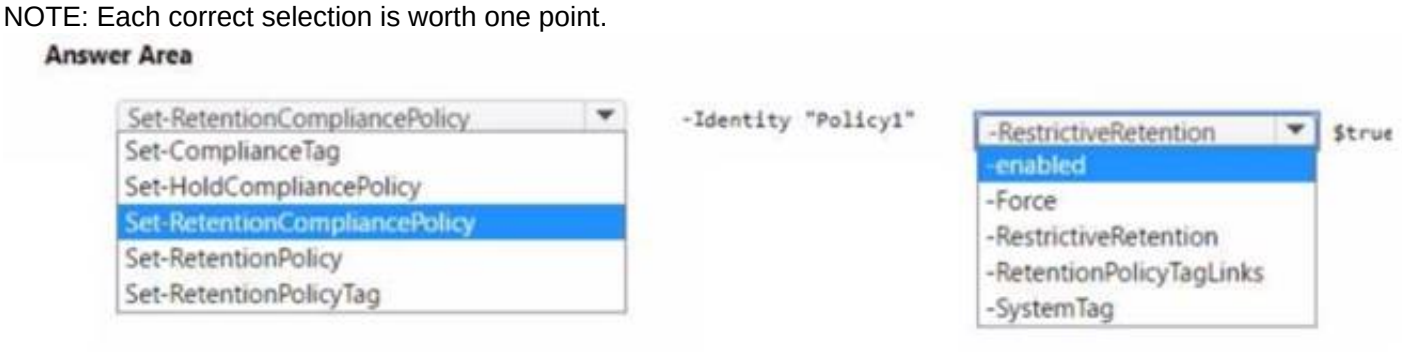
Answer: A

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 104
HOTSPOT - (Topic 6)
From the Microsoft Purview compliance portal, you create a retention policy named Policy 1.
You need to prevent all users from disabling the policy or reducing the retention period. How should you configure the Azure PowerShell command? 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:

NEW QUESTION 108
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription.
You are planning a threat management solution for your organization.
You need to minimize the likelihood that users will be affected by the following threats:
? Opening files in Microsoft SharePoint that contain malicious content
? Impersonation and spoofing attacks in email messages
Which policies should you create in Microsoft 365 Defender? 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 109
- (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 Azure Active Directory admin center, you assign SecAdmin1 the
Security administrator role.

Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 111
- (Topic 6)
You have a Microsoft 365 E5 subscription. You need to create a mail-enabled contact. Which portal should you use?

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

Answer: A

NEW QUESTION 115
- (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 116
- (Topic 6)
You have a Microsoft 365 subscription.
You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.
What is the maximum number of onmicrosoft.com domains the subscription can contain?

A. 1
B. 2
C. 5
D. 10

Answer: C

Explanation:
You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to create a new one.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq

NEW QUESTION 118
- (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 122
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 123
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains four devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager. To which devices can you deploy Microsoft 365 Apps for enterprise?

A. Device1 only
B. Device1 and Device3 only
C. Device2 and Device4 only
D. Device1, Device2. and Device3 only
E. Device1, Device2, Device3, and Device4

Answer: B

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

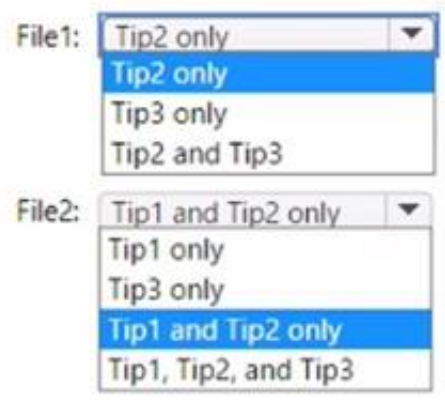
NEW QUESTION 128
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. Site! contains the files shown in the following table.

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

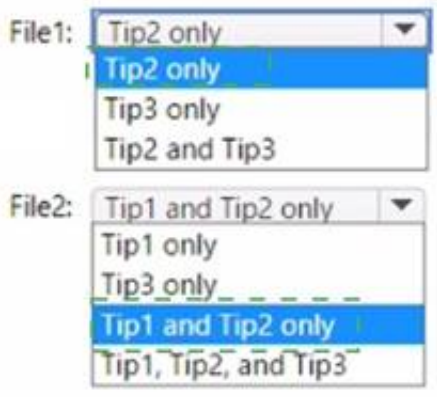


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 133
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.

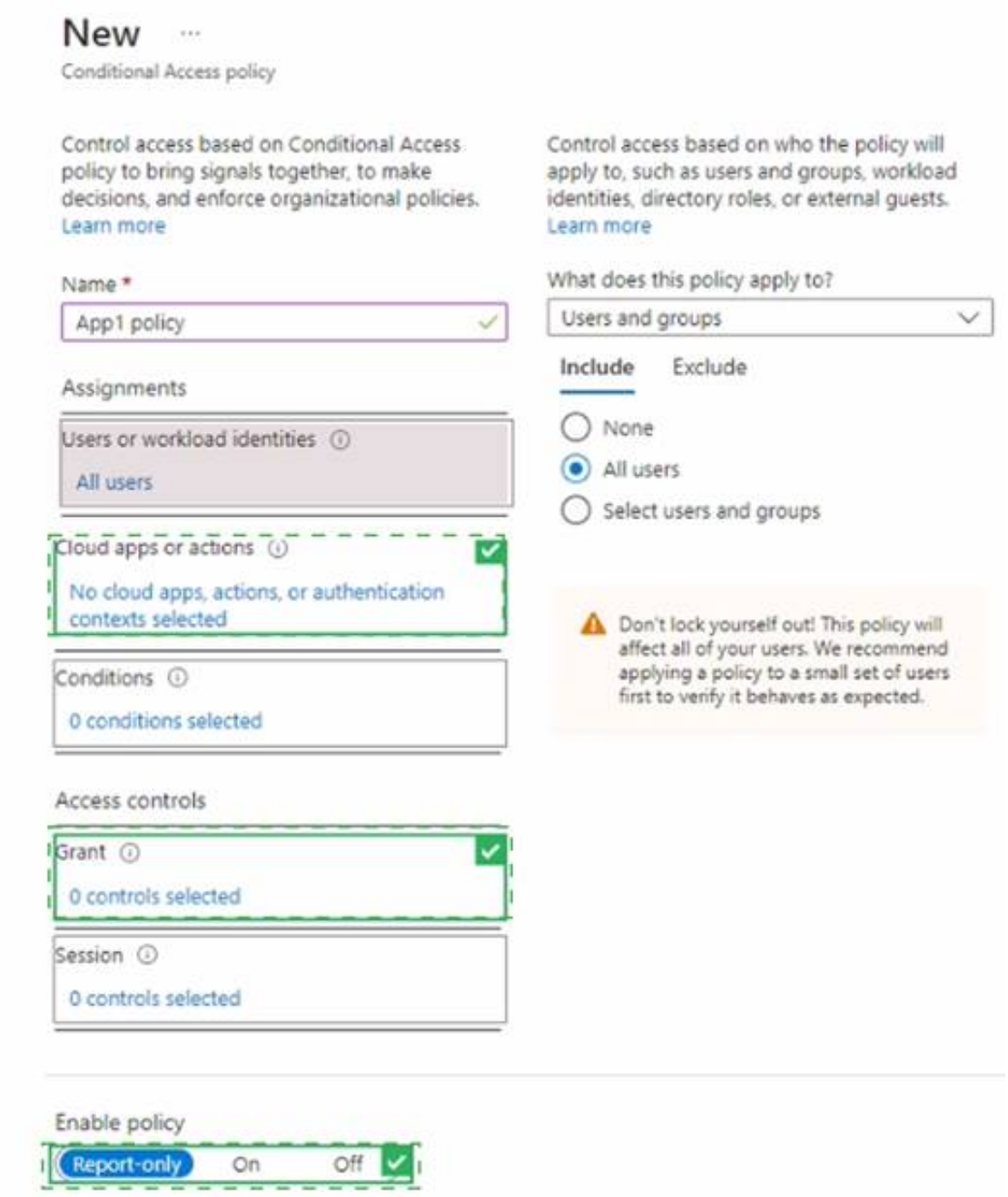
Answer Area

A. Mastered
B. Not Mastered

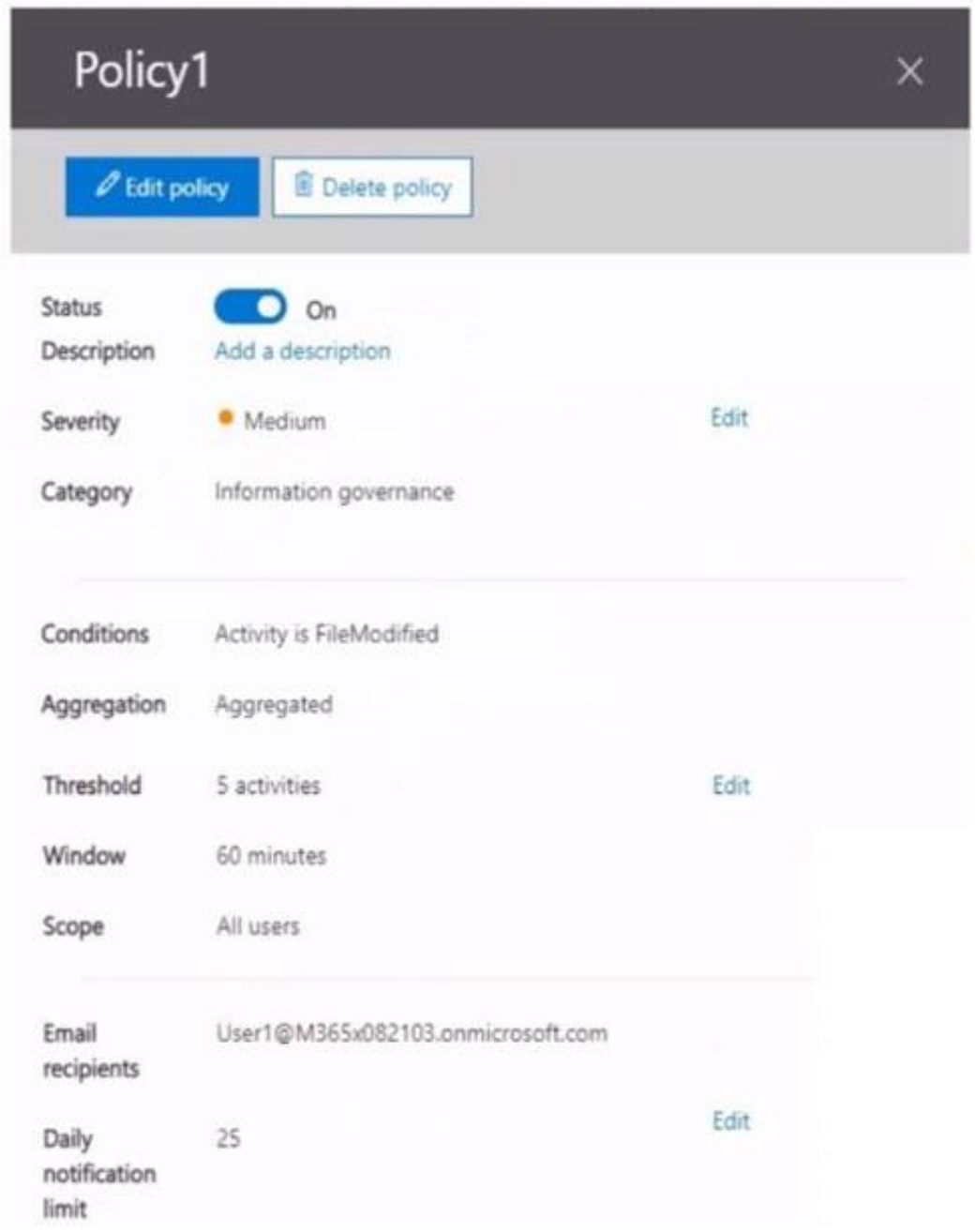
Answer: A

Explanation:

Answer Area



NEW QUESTION 138
- (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

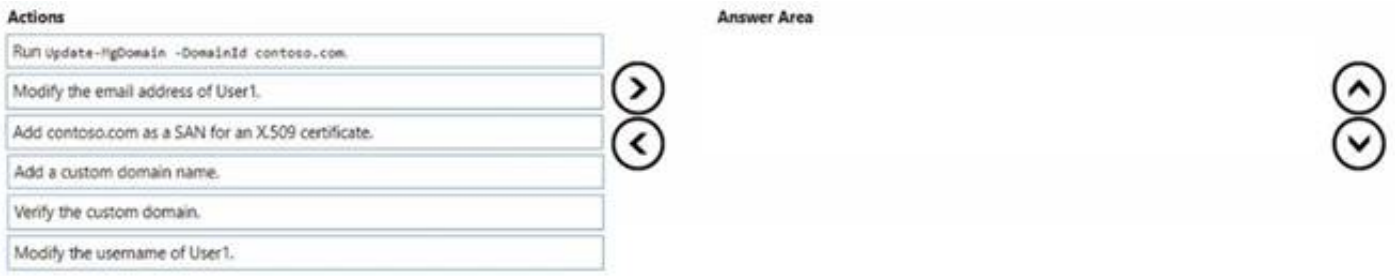
Answer: D

NEW QUESTION 140
- (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

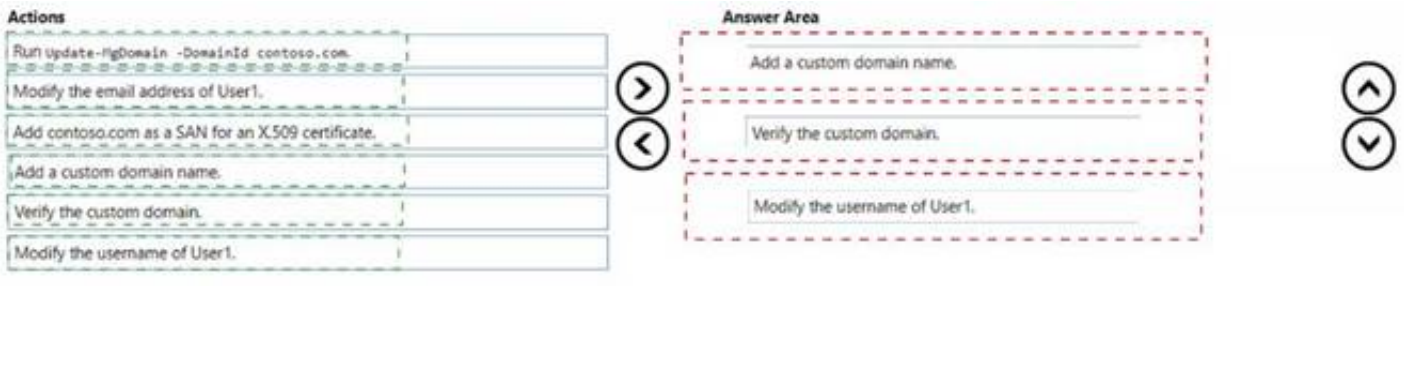
NEW QUESTION 145
DRAG DROP - (Topic 6)
Your company has an Azure AD tenant named contoso.onmicrosoft.com.
You purchase a domain named contoso.com from a registrar and add all the required DNS records.
You create a user account named User1. User1 is configured to sign in as userl@contoso.onmicrosoft.com.
You need to configure User1 to sign in as user1@contoso.com.
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 149
- (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 forest. You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
• Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
• User passwords must be 10 characters or more.
Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 151
- (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

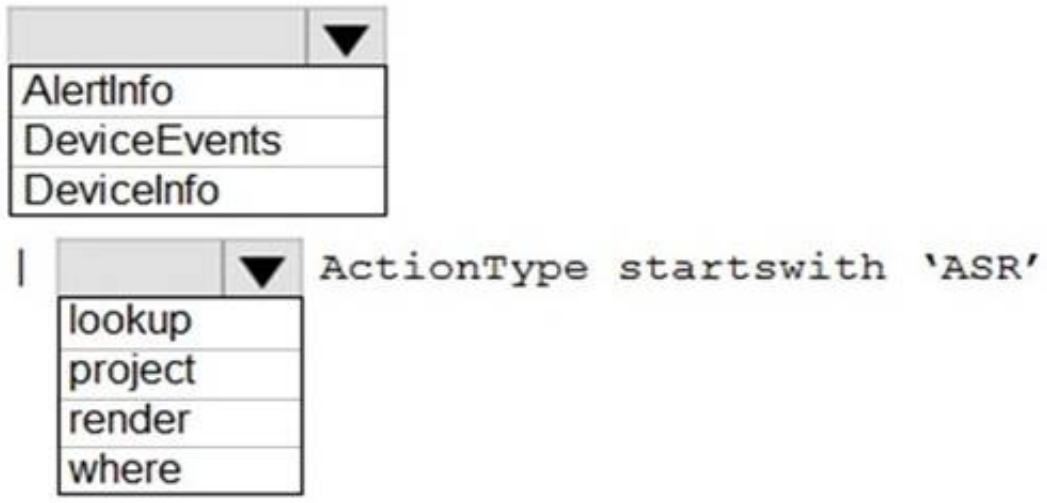
Explanation:
You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

NEW QUESTION 156
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.
You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory.
What should you configure in the profile?

A. Microsoft Defender Credential Guard
B. BitLocker Drive Encryption (BitLocker)
C. Microsoft Defender
D. Microsoft Defender Exploit Guard

Answer: A

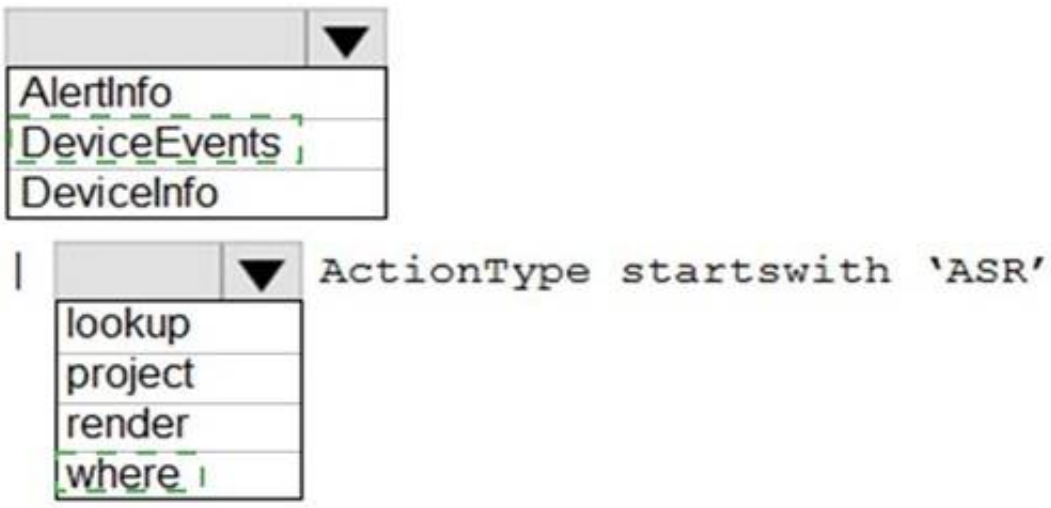
NEW QUESTION 157
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices. You plan to attack surface reduction (ASR) rules for the Windows 10 devices.
You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.
You need to find the ASR rules that match the activities on the devices.
How should you complete the Kusto query? 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 158
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.
What should you use to onboard each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

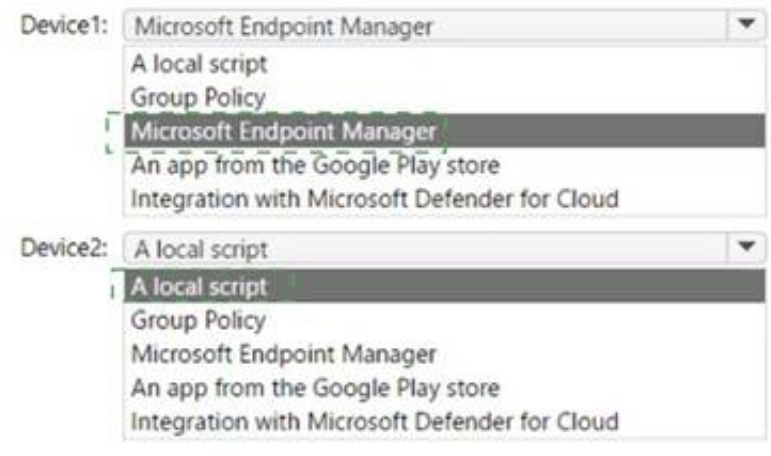
Answer Area

A. Mastered
B. Not Mastered

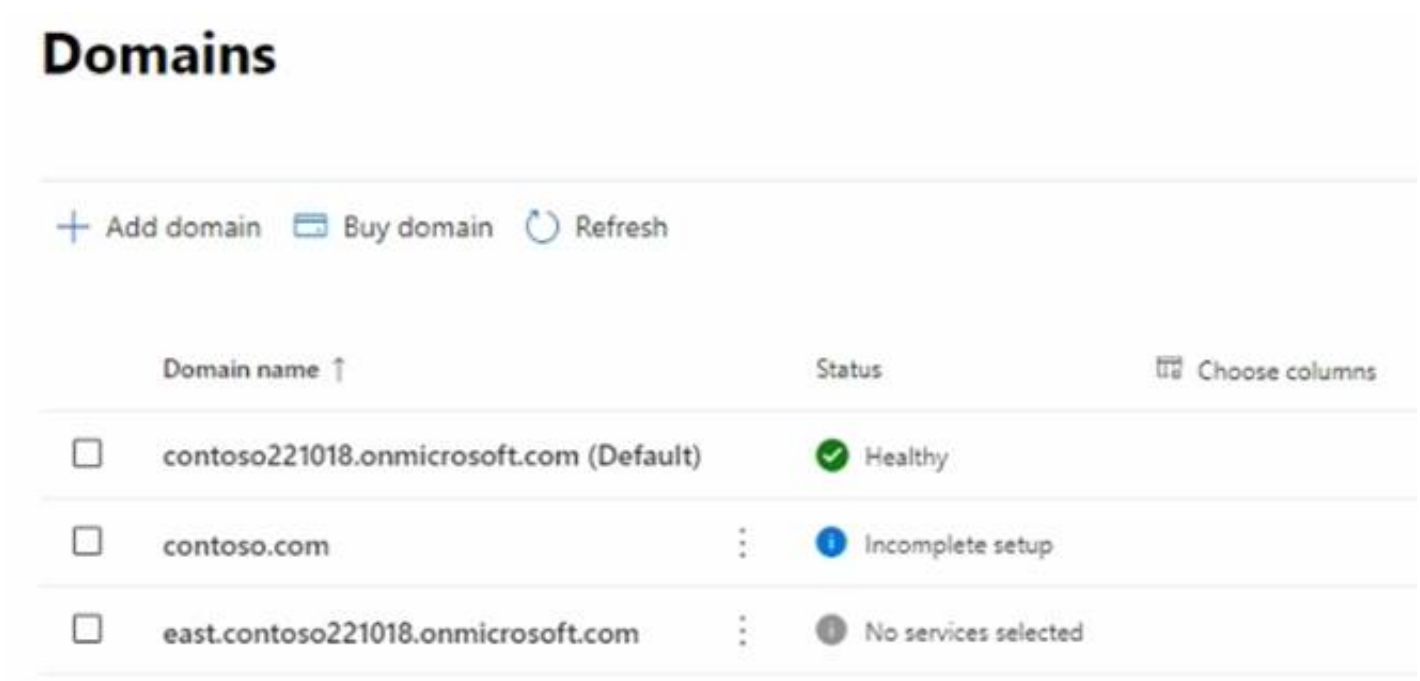
Answer: A

Explanation:

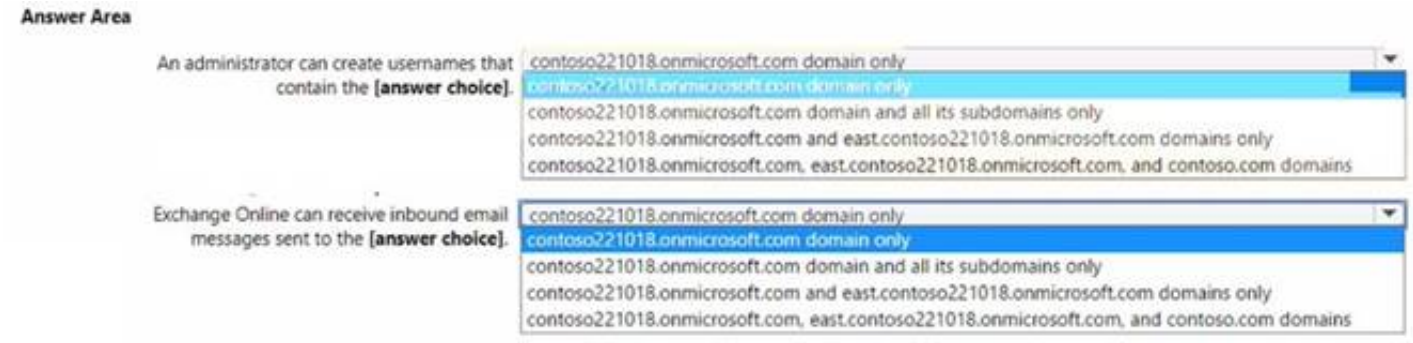
Answer Area



NEW QUESTION 159
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 subscription That contains the domains shown in the following exhibit.



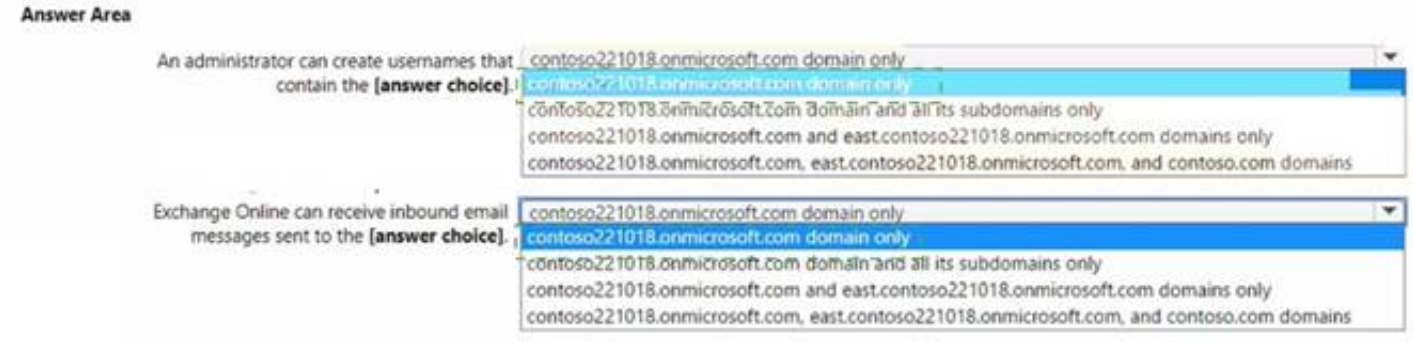
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE; Each correct selection is worth one point.



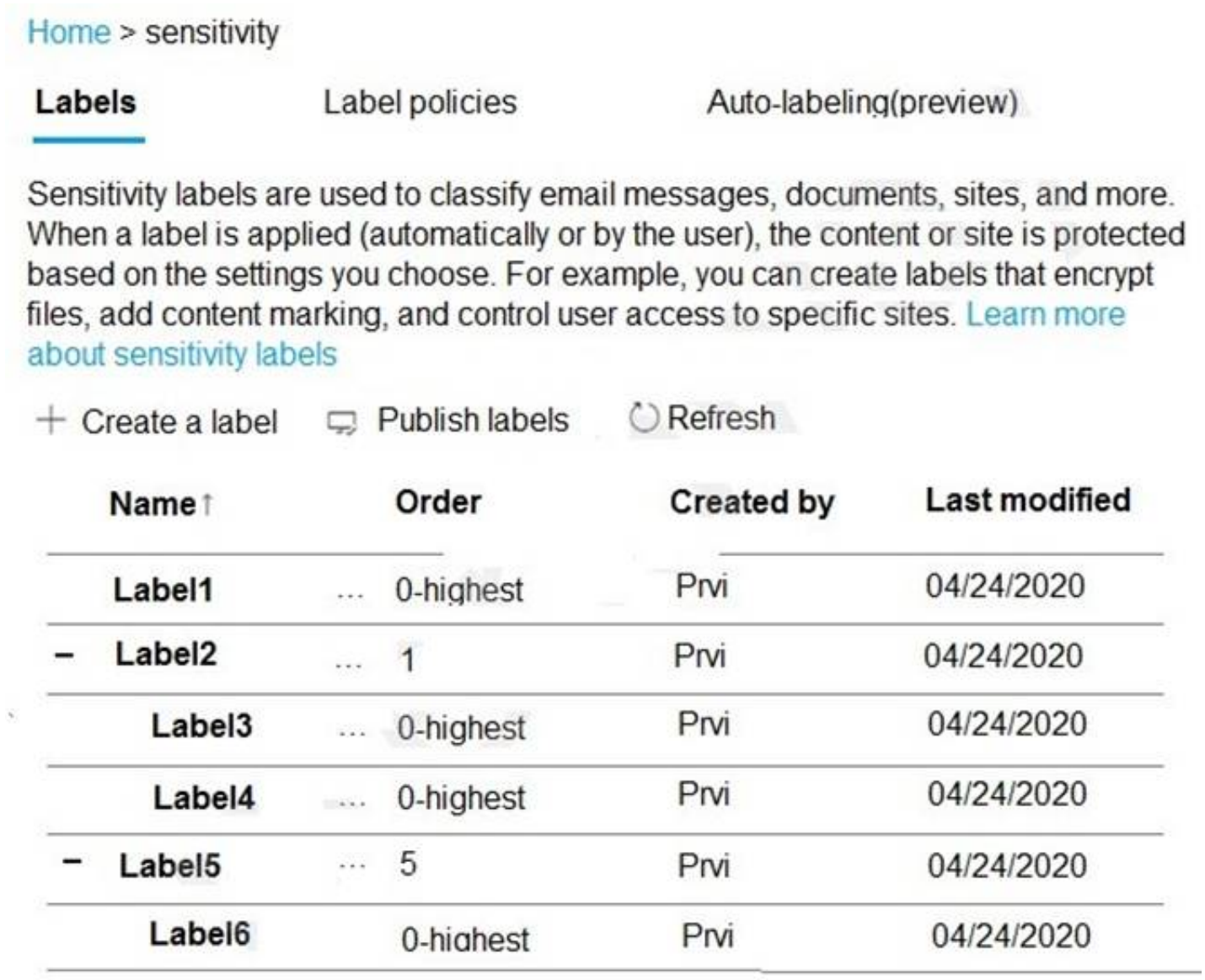
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 162
- (Topic 6)
You have the sensitivity labels shown in the following exhibit.



Which labels can users apply to content?

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

Answer: D

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

NEW QUESTION 164
- (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 Device Manager, you view the computer properties. Does this meet the goal?

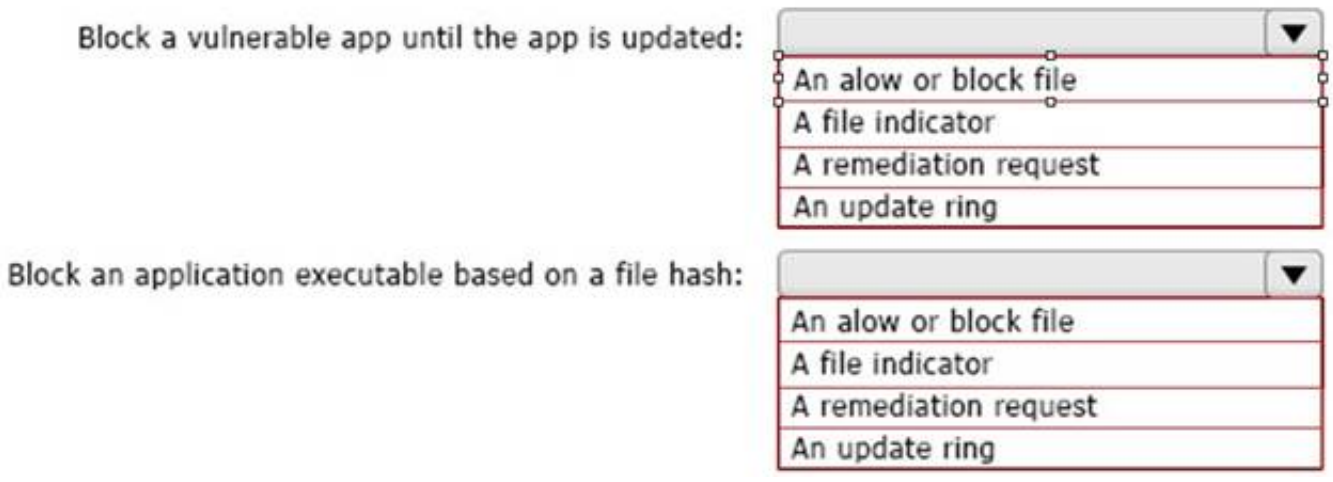
A. Yes
B. No

Answer: B

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 168
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 170
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.

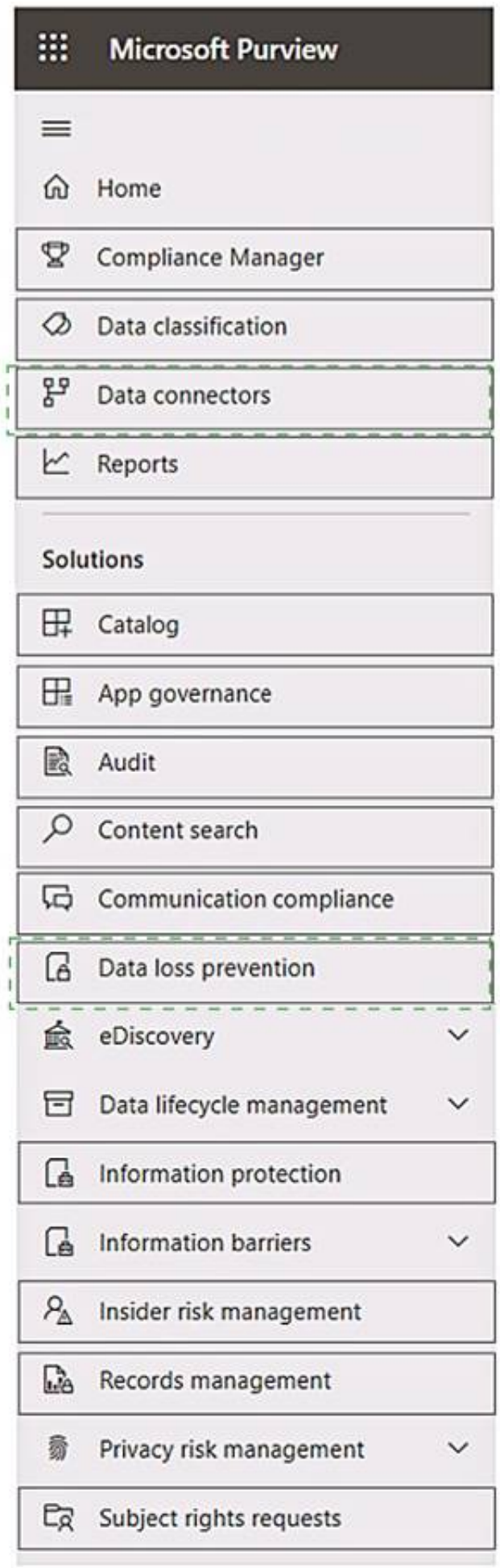
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 175
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.
From Azure AD Identity Protection, you enable a sign-in risk policy.
Users report that when they use the VDI solution, they are regularly blocked when they attempt to access Microsoft 365.
What should you configure?

A. the Tenant restrictions settings in Azure AD
B. a trusted location
C. a Conditional Access policy exclusion
D. the Microsoft 365 network connectivity settings

Answer: B

Explanation:
There are two types of risk policies in Azure Active Directory (Azure AD) Conditional Access you can set up to automate the response to risks and allow users to self-remediate when risk is detected:
Sign-in risk policy User risk policy
Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.
Reference:

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity- protection-configure-risk-policies
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location- condition

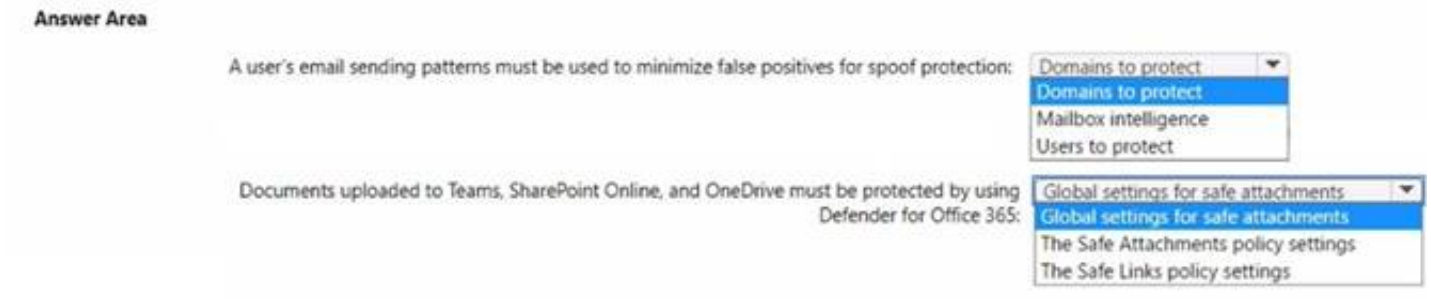
NEW QUESTION 177
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 179
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to configure Microsoft Defender for Office 365 to meet the following requirements:
• A user's email sending patterns must be used to minimize false positives for spoof protection.
• Documents uploaded to Microsoft Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365.
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 184
- (Topic 6)
Your company has a Microsoft E5 tenant.
The company must meet the requirements of the ISO/IEC 27001:2013 standard. You need to assess the company's current state of compliance.
What should you use?

A. eDiscovery
B. Information governance
C. Compliance Manager
D. Data Subject Requests (DSRs)

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

NEW QUESTION 188
- (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 189
- (Topic 6)
You have a Microsoft 365 E5 tenant. Users store data in the following locations:
? Microsoft Teams
? Microsoft OneDrive
? Microsoft Exchange Online
? Microsoft SharePoint Online
You need to retain Microsoft 365 data for two years.
What is the minimum number of retention policies that you should create?

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

Answer: C

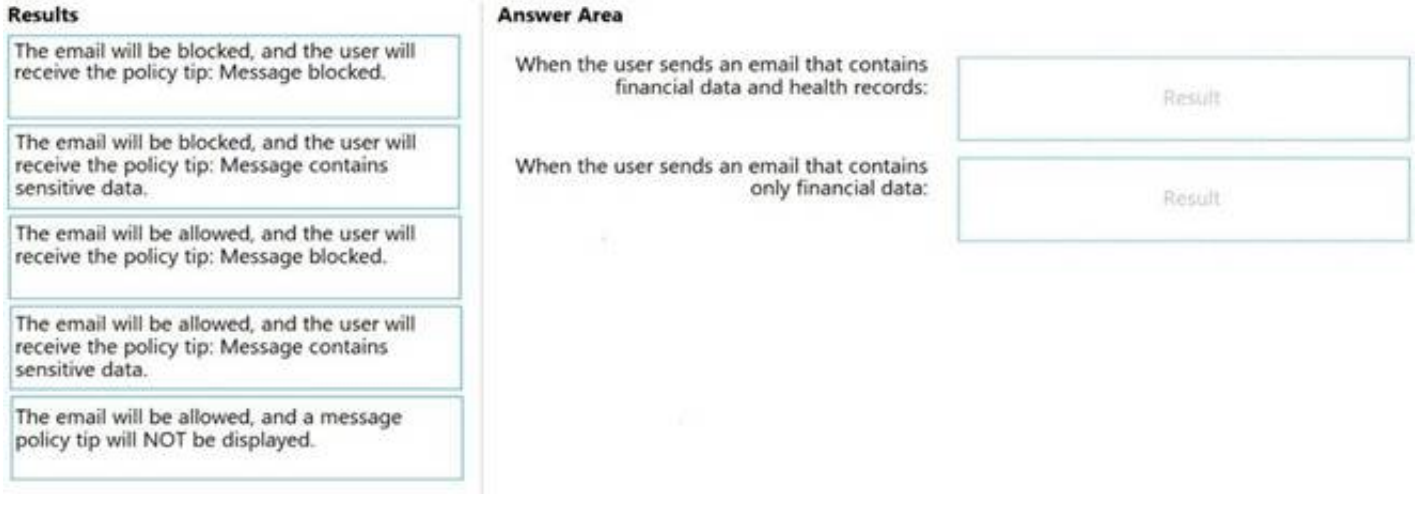
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide

NEW QUESTION 192
- (Topic 6)
You have a Microsoft 365 E5 tenant. You configure sensitivity labels.
Users report that the Sensitivity button is unavailability in Microsoft Word for the web. The sensitivity button is available in Word for Microsoft 365.
You need to ensure that the users can apply the sensitivity labels when they use Word for the web.
What should you do?

A. Copy policies from Azure information Protection to the Microsoft 365 Compliance center
B. Publish the sensitivity labels.
C. Create an auto-labeling policy
D. Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive.

Answer: B

NEW QUESTION 193
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.

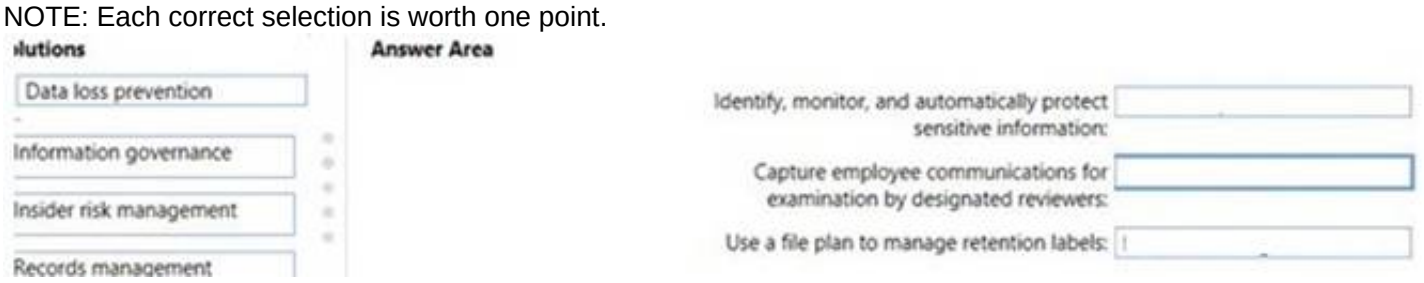
NEW QUESTION 196
- (Topic 6)
Your on-premises network contains an Active Directory domain.
You have a Microsoft 365 subscription.
You need to sync the domain with the subscription. The solution must meet the following requirements:
On-premises Active Directory password complexity policies must be enforced. Users must be able to use self-service password reset (SSPR) in Azure AD. What should you use?

A. password hash synchronization
B. Azure AD Identity Protection
C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
D. pass-through authentication

Answer: D

Explanation:
Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.
This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations
wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.
Note: Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time by using either Azure AD Connect or Azure AD Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.
Password writeback is supported in environments that use the following hybrid identity models:
Password hash synchronization Pass-through authentication
Active Directory Federation Services
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback

NEW QUESTION 200
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 E5 tenant.
You need to implement compliance solutions that meet the following requirements:
• Use a file plan to manage retention labels.
• Identify, monitor, and automatically protect sensitive information.
• Capture employee communications for examination by designated reviewers.
Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 201
- (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?

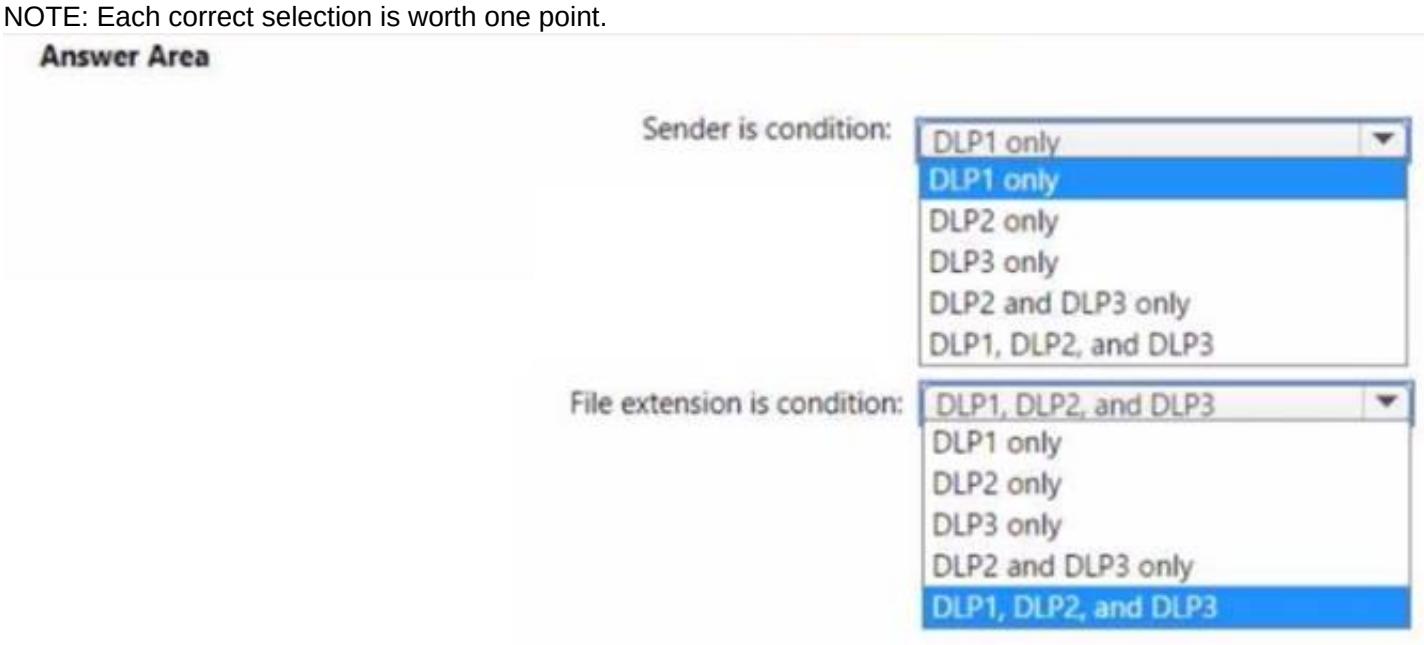
A. the policy rule exceptions
B. the DLP policy locations
C. the policy rule conditions
D. the policy rule actions

Answer: C

NEW QUESTION 204
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to create the data loss prevention (DLP) policies shown in the following table.

Name	Apply to location
DLP1	Exchange email
DLP2	SharePoint sites
DLP3	OneDrive accounts

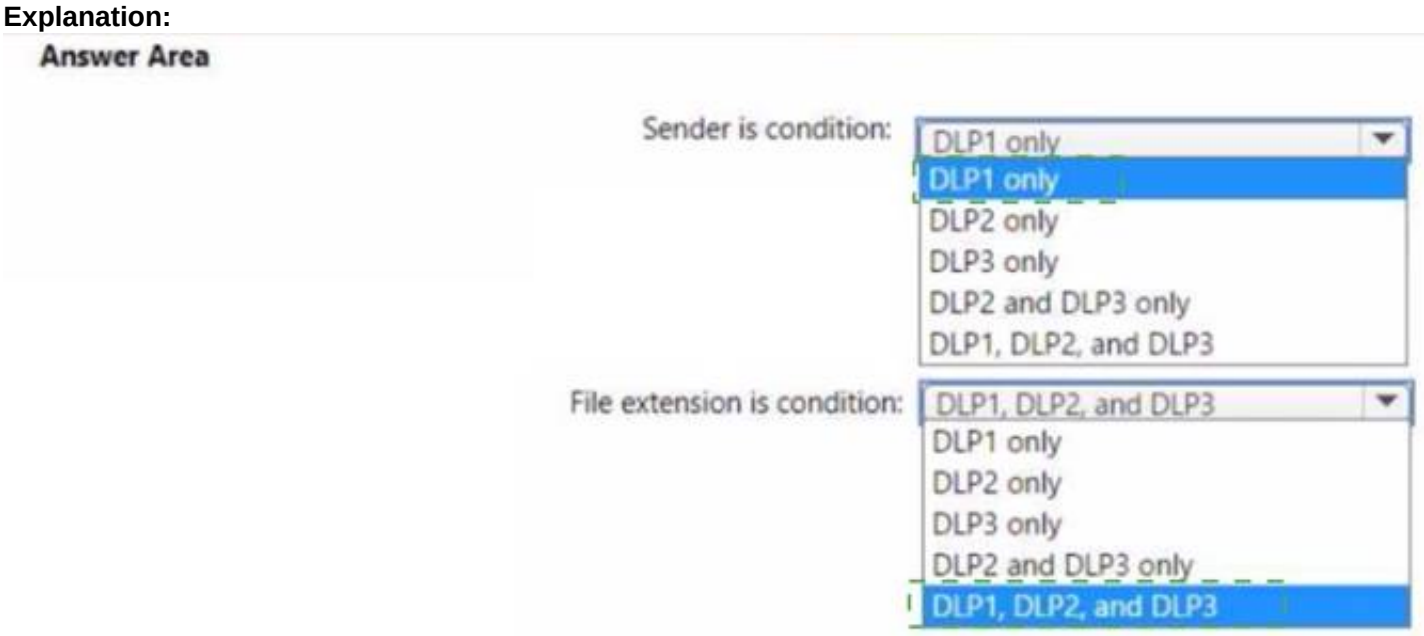
You need to create DLP rules for each policy.
Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



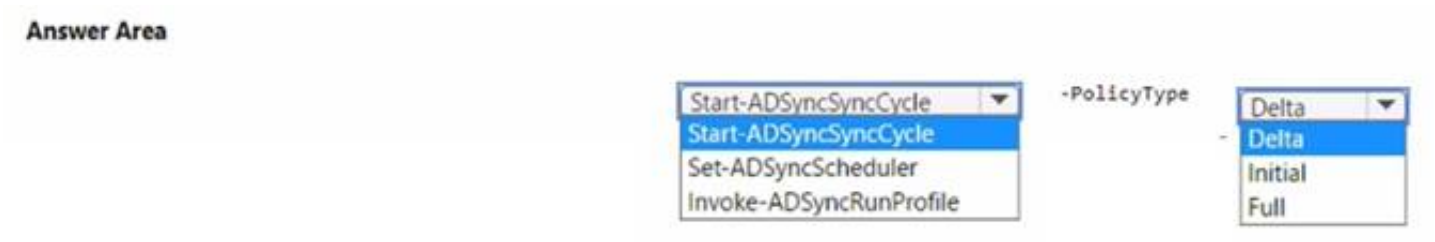
A. Mastered
B. Not Mastered

Answer: A

Explanation:



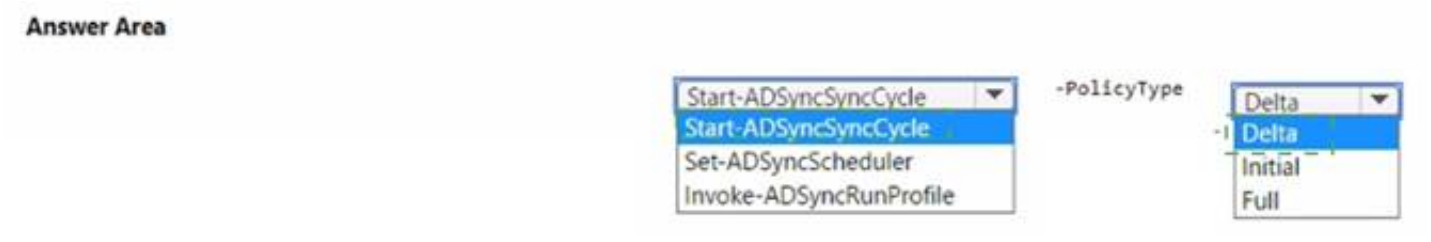
NEW QUESTION 207
HOTSPOT - (Topic 6)
Your network contains an Active Directory domain and an Azure AD tenant.
You implement directory synchronization for all 10.000 users in the organization. You automate the creation of 100 new user accounts.
You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.
Which command should you run? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 208
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft intune.
in the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices,
You enable device clean-up rules
What can you configure as the minimum number of days before a device a removed automatically?

A. 10
B. 30
C. 45
D. 90

Answer: D

NEW QUESTION 209
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:
• Support KQL for querying data.
• Retain report data for at least one year.
What should you include in the recommendation?

A. a security report in Microsoft 365 Defender
B. End point analytics
C. Microsoft 365 usage analytics
D. Azure Monitor workbooks

Answer: D

NEW QUESTION 210
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 213
HOTSPOT - (Topic 6)
Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD) Password hash synchronization is disabled.
You plan to implement co-management.
You need to configure Azure AD Connect and the domain to support co-management. 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 configure Azure AD Connect:
- Configure hybrid Azure AD join.
- Enable device writeback.
- Enable password hash synchronization.

To configure the domain:
- Add an alternative UPN suffix.
- Register a service connection point.
- Register a service principal name (SPN).

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

To configure Azure AD Connect:
- Configure hybrid Azure AD join.
- Enable device writeback.
- Enable password hash synchronization.

To configure the domain:
- Add an alternative UPN suffix.
- Register a service connection point.
- Register a service principal name (SPN).

NEW QUESTION 216
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.
You need to implement passwordless authentication. The solution must support all the devices.
Which authentication method should you use?

A. Windows Hello
B. FID02 compliant security keys
C. Microsoft Authenticator app

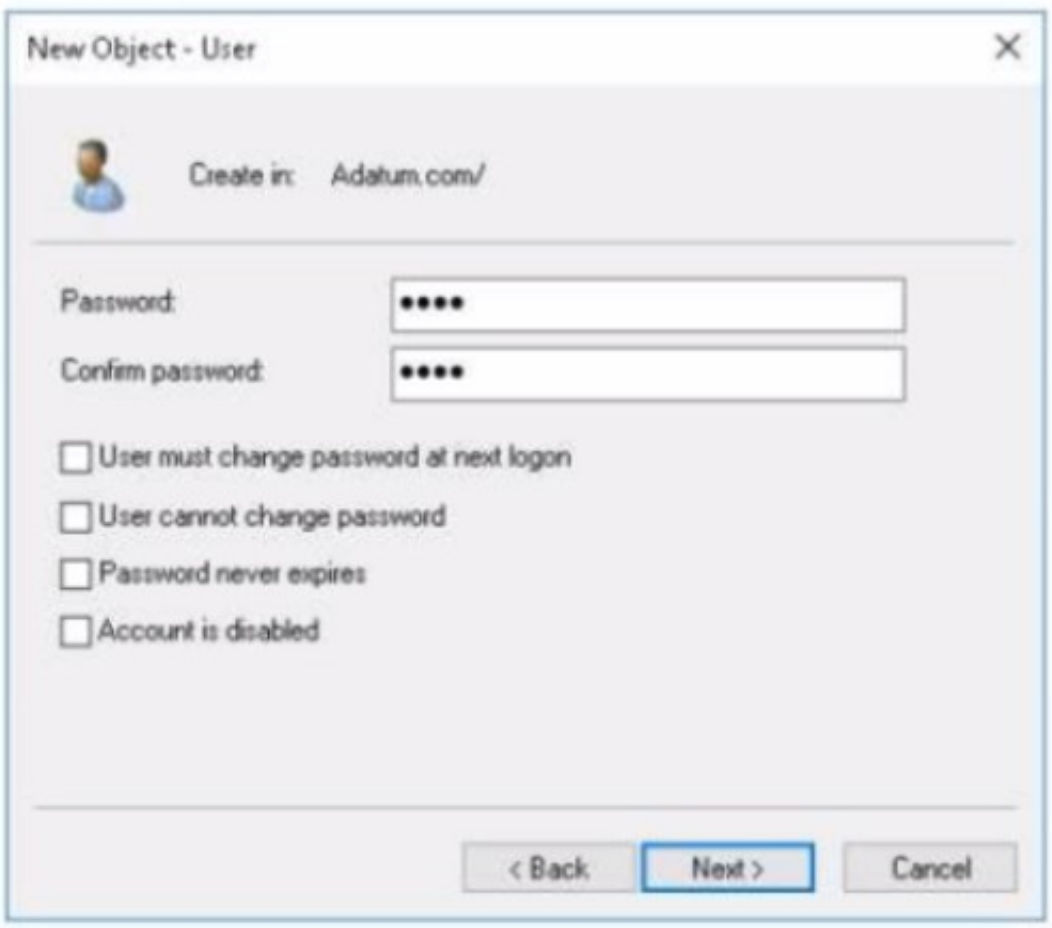
Answer: C

NEW QUESTION 217
- (Topic 6)
You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that Used can place a hold on all mailbox content. What permission should you assign to User1?

A. the Information Protection administrator ide from the Azure Active Directory admin center.
B. the eDiscovery Manager tote from the Microsoft 365 compliance center.
C. the Compliance Management role from the Exchange admin center.
D. the User management administrator role from the Microsoft 365 admin center.

Answer: B

NEW QUESTION 221
HOTSPOT - (Topic 6)
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure AD by using the Azure AD Connect Express Settings. Password write back is disabled.
You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.



The Azure AD password policy is configured as shown in the following exhibit. Password policy
Set the password policy for all users in your organization. Days before passwords expire 90
Days before a user is notified about 14 expiration
You confirm that User1 is synced to Azure AD.
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 Azure AD.	○	○
User1 can change the password immediately by using the My Apps portal.	○	○
From Azure AD, User1 must change the password every 90 days.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can sign in to Azure AD.	○	○
User1 can change the password immediately by using the My Apps portal.	○	○
From Azure AD, User1 must change the password every 90 days.	○	○

NEW QUESTION 222
HOTSPOT - (Topic 6)
You work at a company named Contoso, Ltd.
Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.
Contoso purchases a company named Fabrikam, Inc.
Contoso plans to add the following domains to the Microsoft 365 subscription:
• fabrikam.com
• east.fabrikam.com
• west.contoso.com
You need to ensure that the devices in the new domains can register by using Autodiscover.
How many domains should you verify, and what is the minimum number of enterprise registration DNS records you should add? 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 226
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.	○	○

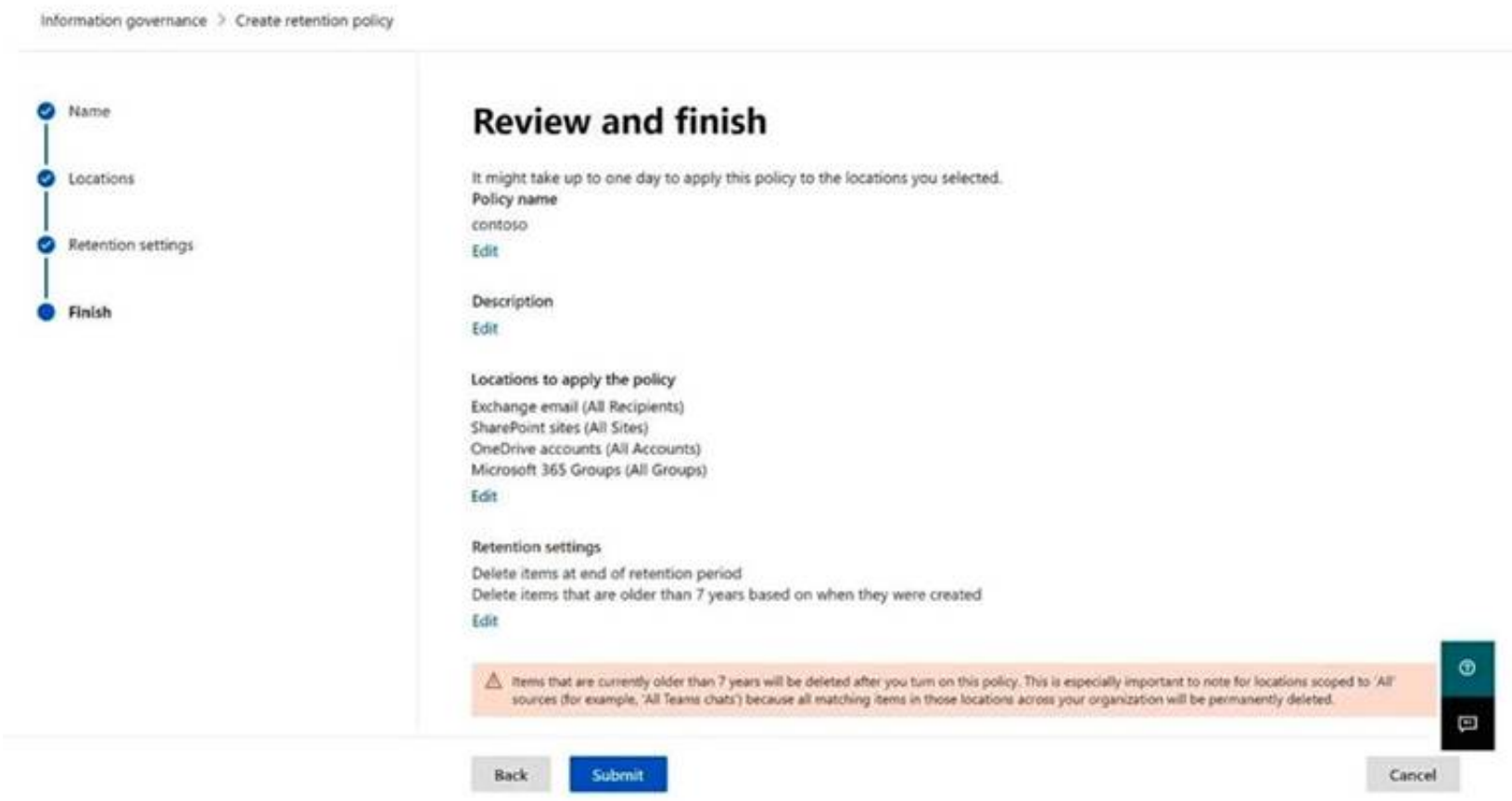
A. Mastered
B. Not Mastered

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 229
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 tenant.
You plan to create a retention policy as 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

Microsoft SharePoint files that are affected by the policy will be **[answer choice]**.
- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, **[answer choice]**.
- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Deleted seven years after they were created. From the exhibit:
The retention policy applies to SharePoint sites.
Delete items that are older than 7 years based on when they were created.
Box 2: data will retained for a minimum of seven years
The longest retention period wins. If content is subject to multiple retention settings that retain content for different periods of time, the content will be retained until the end of the longest retention period for the item.
Note: Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email).
For example, if all documents in a SharePoint site should be retained for 5 years, it's more efficient to do this with a retention policy than apply the same retention label to all documents in that site. However, if some documents in that site should be retained for 5
years and others retained for 10 years, a retention policy wouldn't be able to do this. When you need to specify retention settings at the item level, use retention labels.

NEW QUESTION 230
- (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 232
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	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

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

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

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

Name	Assigned to
Policy1	Group3
Policy2	Group2

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

Answer Area

Statements	Yes	No
Device1 is compliant.	○	○
Device2 is compliant.	○	○
Device3 is compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device1 is compliant.	○	○
Device2 is compliant.	○	○
Device3 is compliant.	○	○

NEW QUESTION 233
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro
Device3	Windows 10 Enterprise
Device4	Ubuntu 18.04 LTS

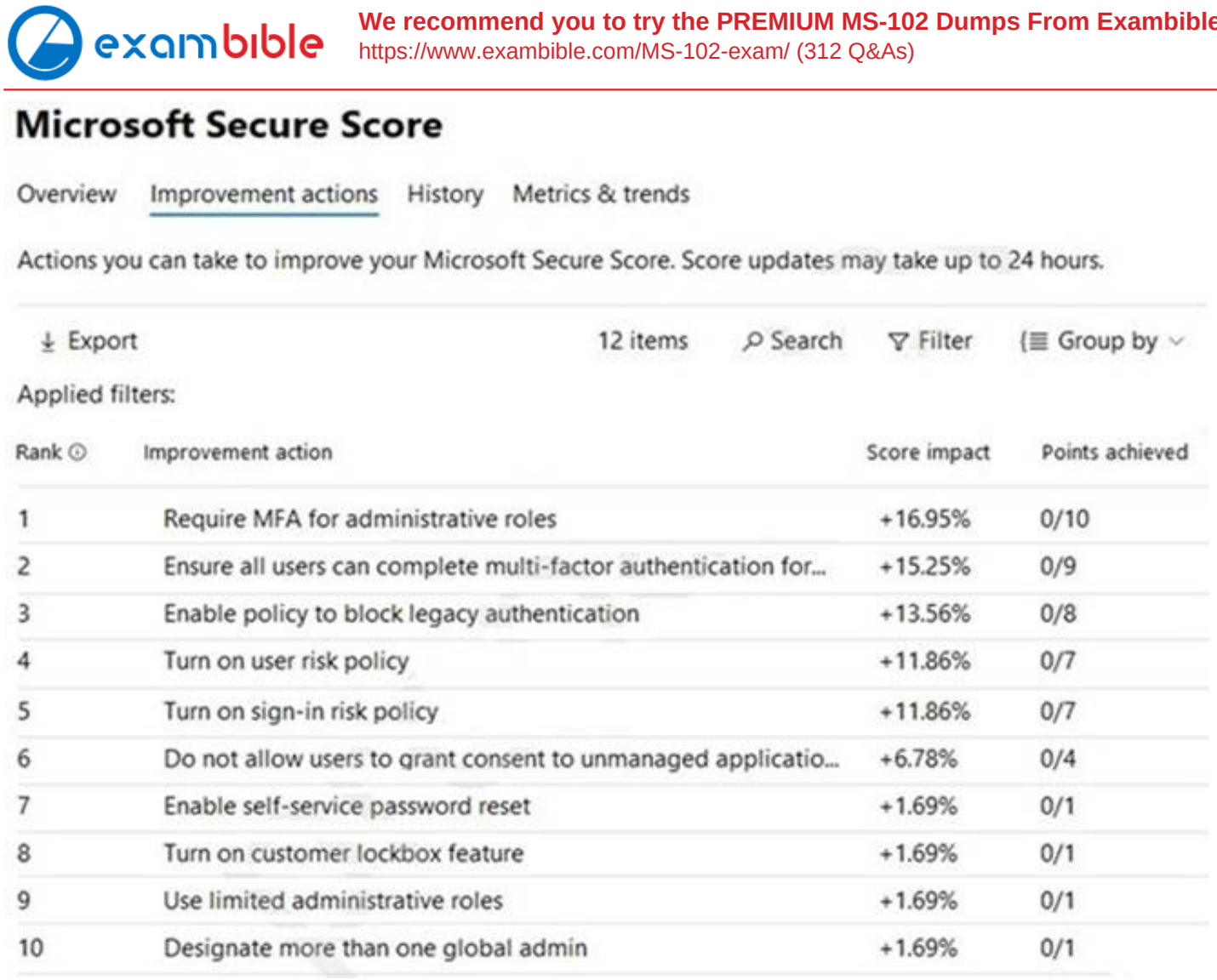
You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?

A. Device 1, Device2, and Device3 only
B. Device3 only
C. Device2 and Device3 only
D. Device1, Device2, Devices and Device4

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements

NEW QUESTION 236
- (Topic 6)
You have a Microsoft 365 E5 tenant.
The Microsoft Secure Score for the tenant is shown in the following exhibit.



You plan to enable Security defaults for Azure Active Directory (Azure AD). Which three improvement actions will this affect?

A. Require MFA for administrative roles.
B. Ensure all users can complete multi-factor authentication for secure access
C. Enable policy to block legacy authentication
D. Enable self-service password reset
E. Use limited administrative roles

Answer: ABC

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

NEW QUESTION 238
- (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 243
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform	Azure Active Directory (Azure AD)
Device1	Windows 10	Joined
Device2	Windows 10	Registered
Device3	Windows 10	Not joined or registered
Device4	Android	Registered

You plan to review device startup performance issues by using Endpoint analytics. Which devices can you monitor by using Endpoint analytics?

A. Device1 only
B. Device1 and Device2 only
C. Device1, Device2, and Device3 only
D. Device1, Device2, and Device4 only
E. Device1, Device2, Device3, and Device4

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/analytics/overview

NEW QUESTION 247
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.

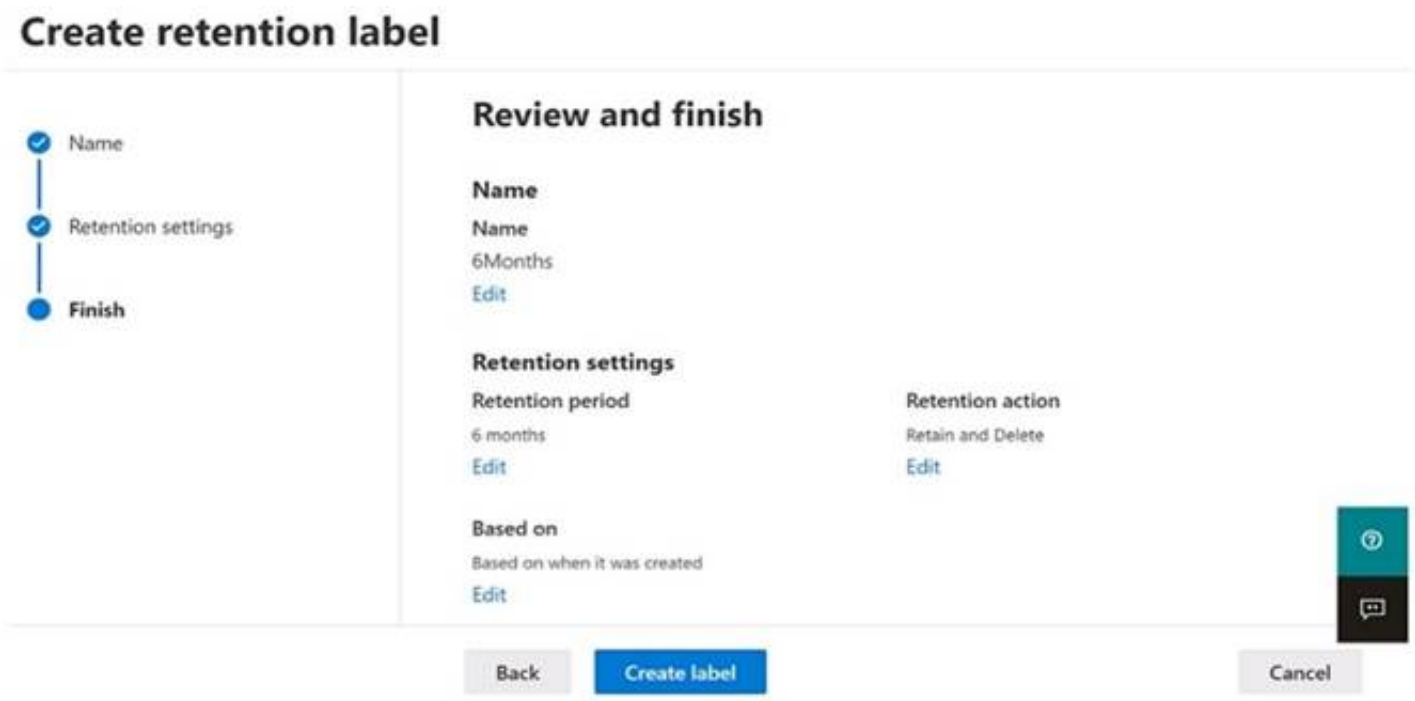
Statements	Yes	No
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

A. Mastered
B. Not Mastered
Answer: A

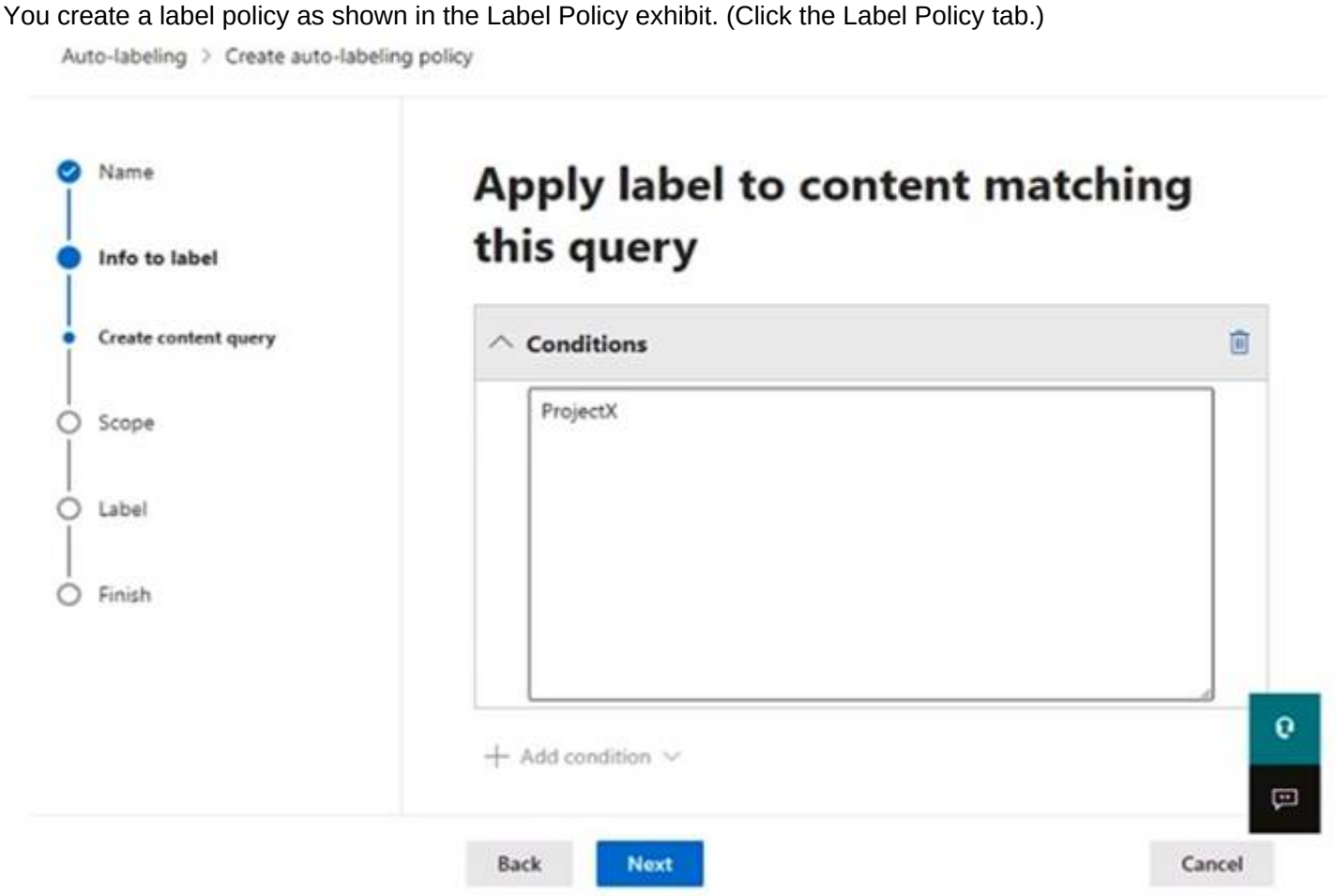
Explanation:

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 249
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.	○	○

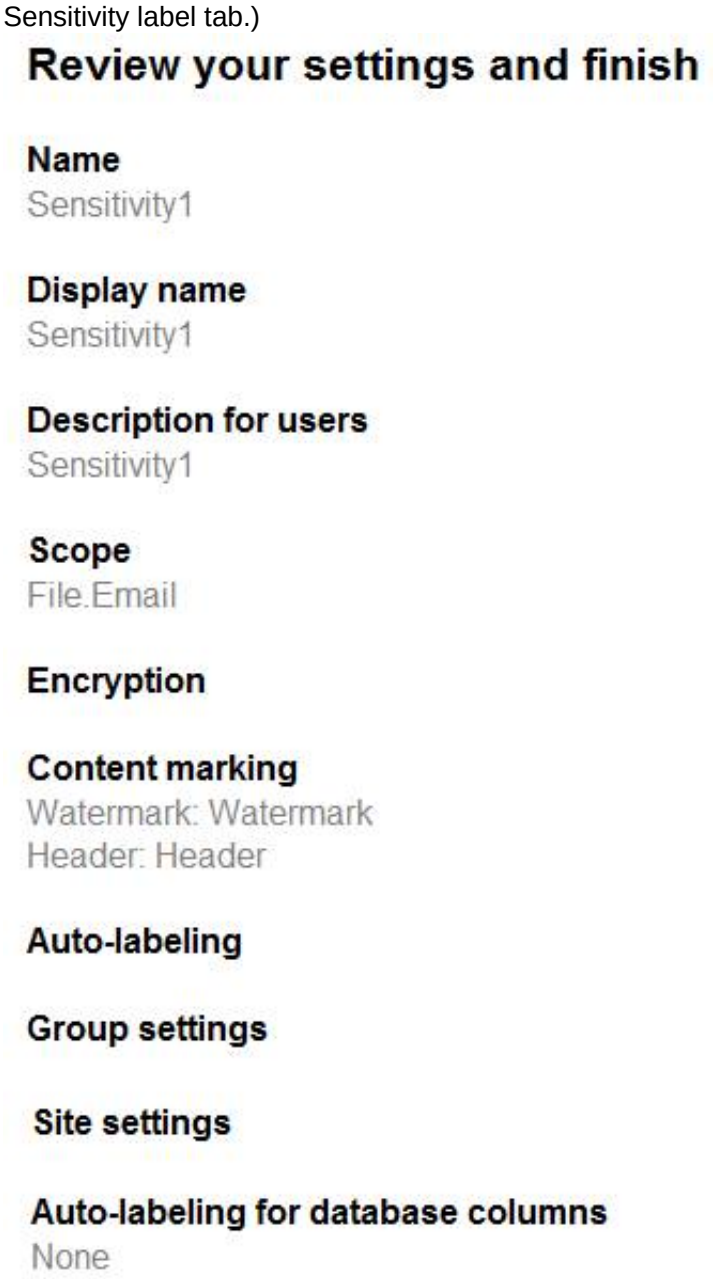
A. Mastered
B. Not Mastered

Answer: A

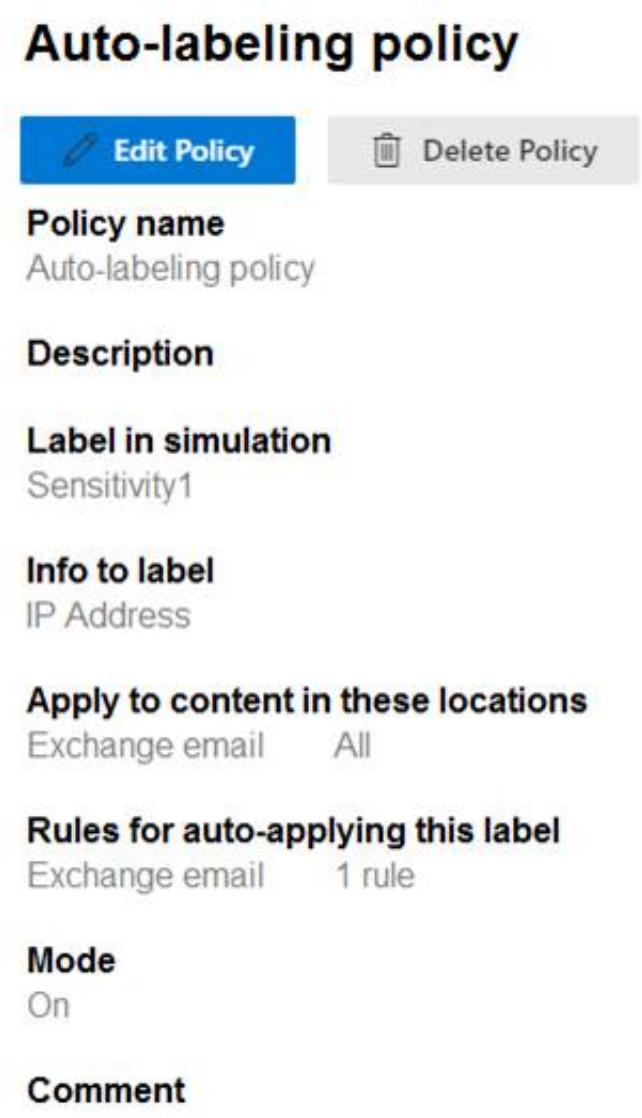
Explanation:
Box 1: No
Box 2: Yes
Box 3: No

NEW QUESTION 252
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

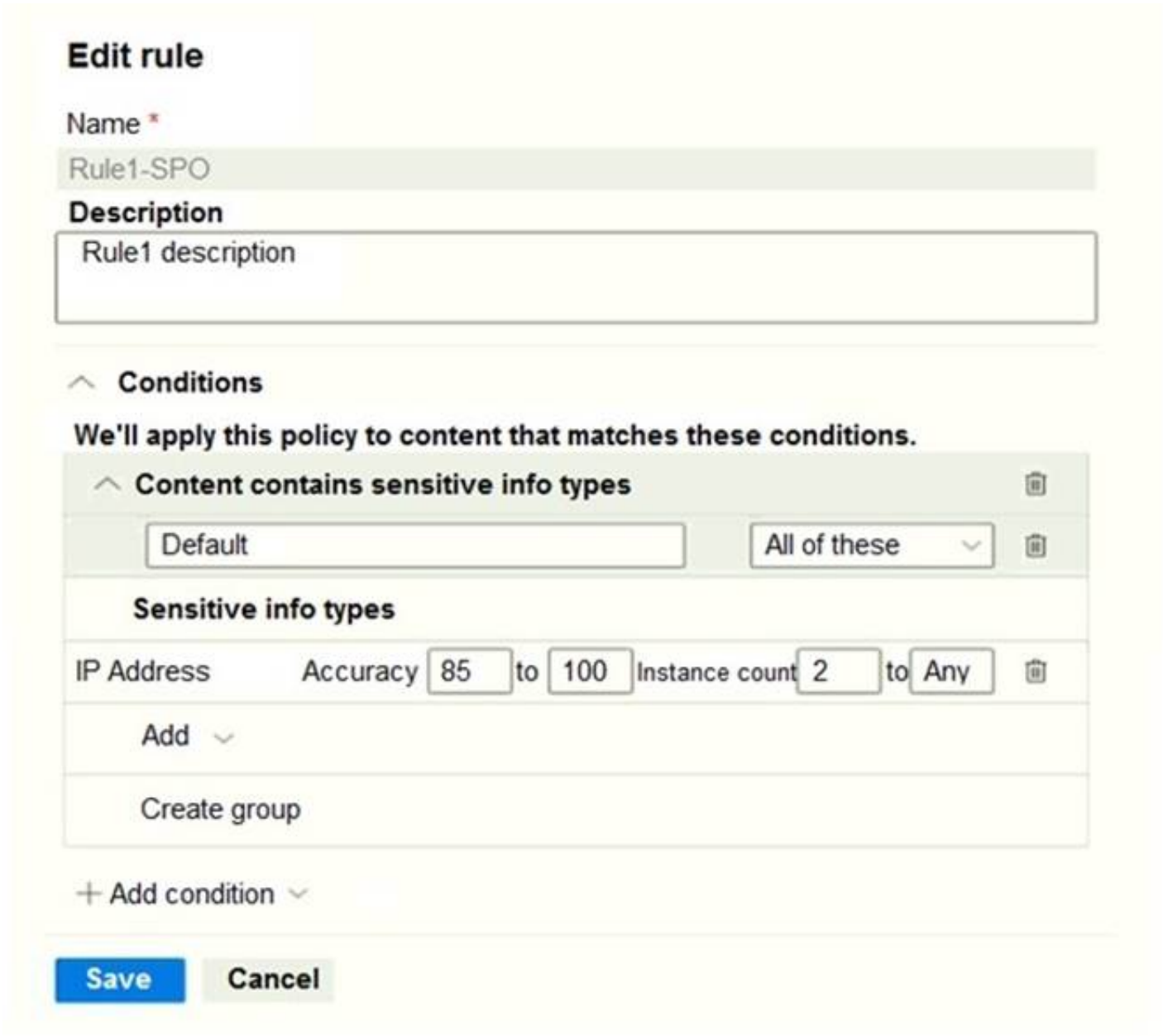
Explanation:

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 257
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

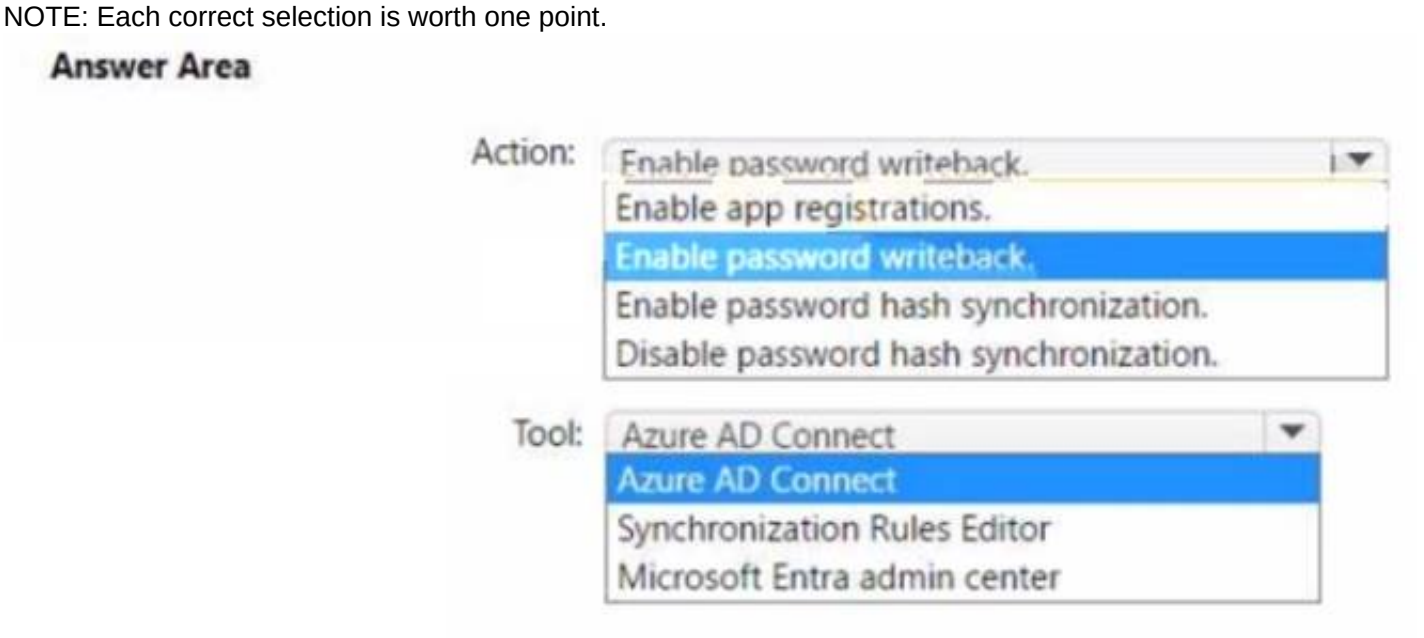
Answer: A

Explanation:

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

NEW QUESTION 259
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.

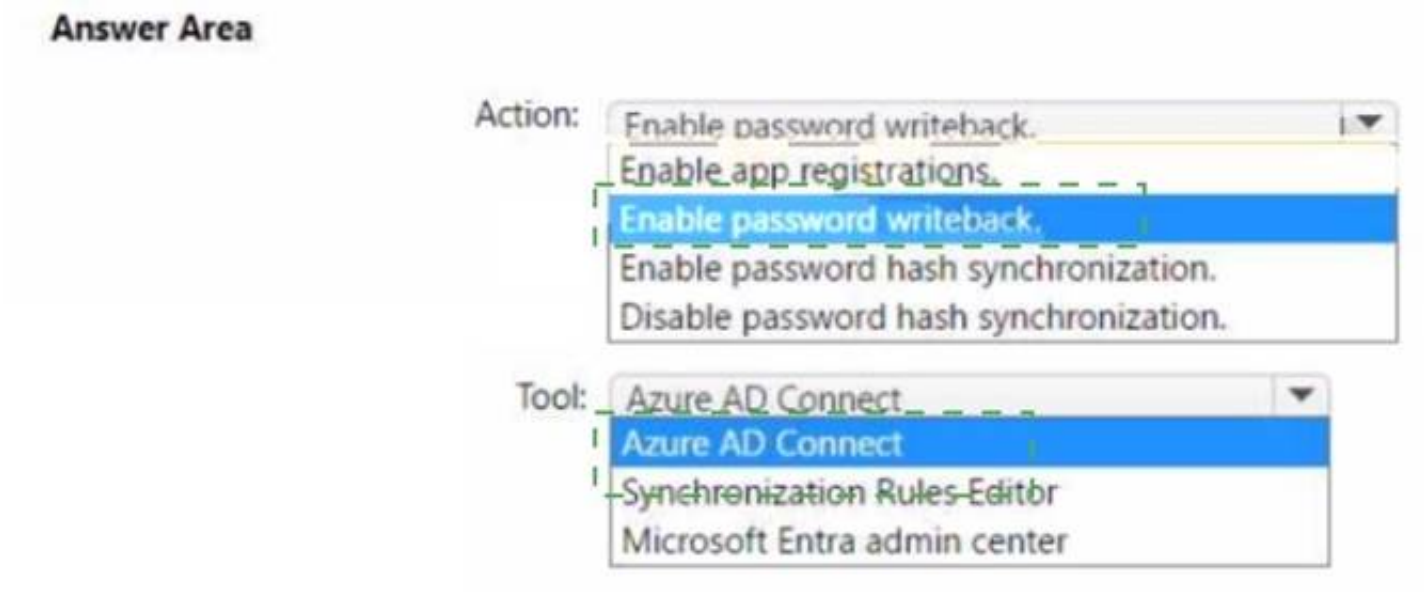
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 262
- (Topic 3)
You create the planned DLP policies.
You need to configure notifications to meet the technical requirements. What should you do?

A. From the Microsoft 365 security center, configure an alert policy.
B. From the Microsoft Endpoint Manager admin center, configure a custom notification.
C. From the Microsoft 365 admin center, configure a Briefing email.
D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

Answer: D

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

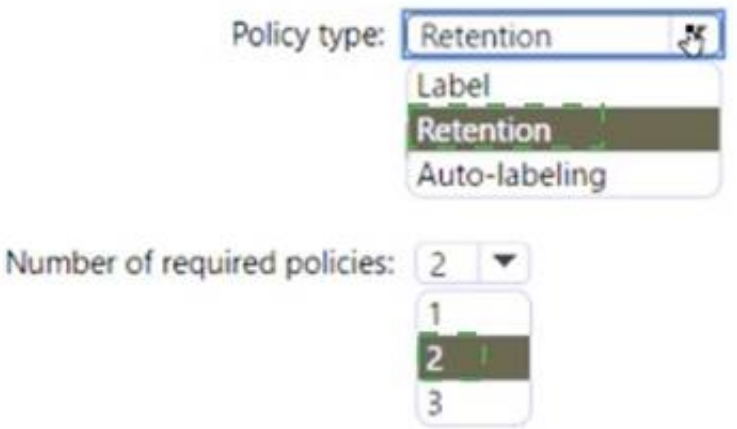
NEW QUESTION 266
HOTSPOT - (Topic 3)
You need to configure the information governance settings to meet the technical requirements.
Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

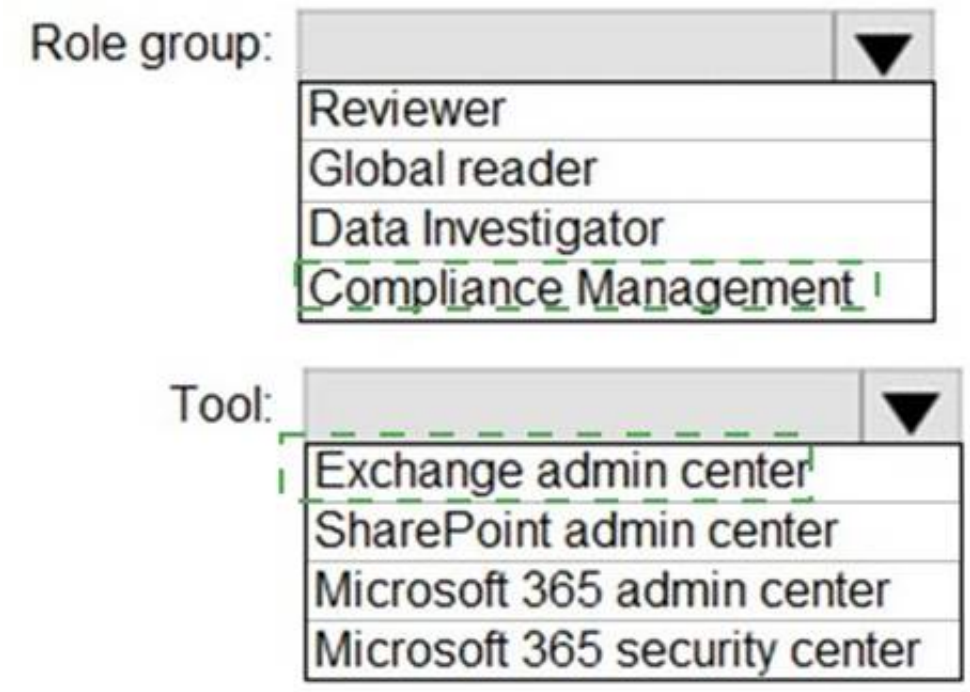


NEW QUESTION 269
HOTSPOT - (Topic 3)
You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements.
To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



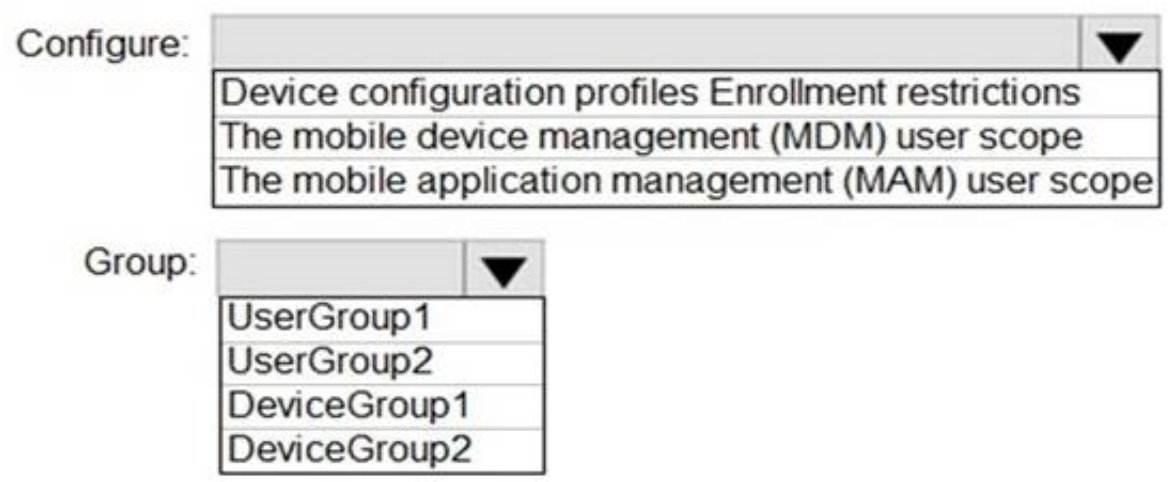
NEW QUESTION 272
- (Topic 3)
You need to configure Office on the web to meet the technical requirements. What should you do?

A. Assign the Global reader role to User1.
B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.
C. Configure an auto-labeling policy to apply the sensitivity labels.
D. Assign the Office apps admin role to User1.

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide

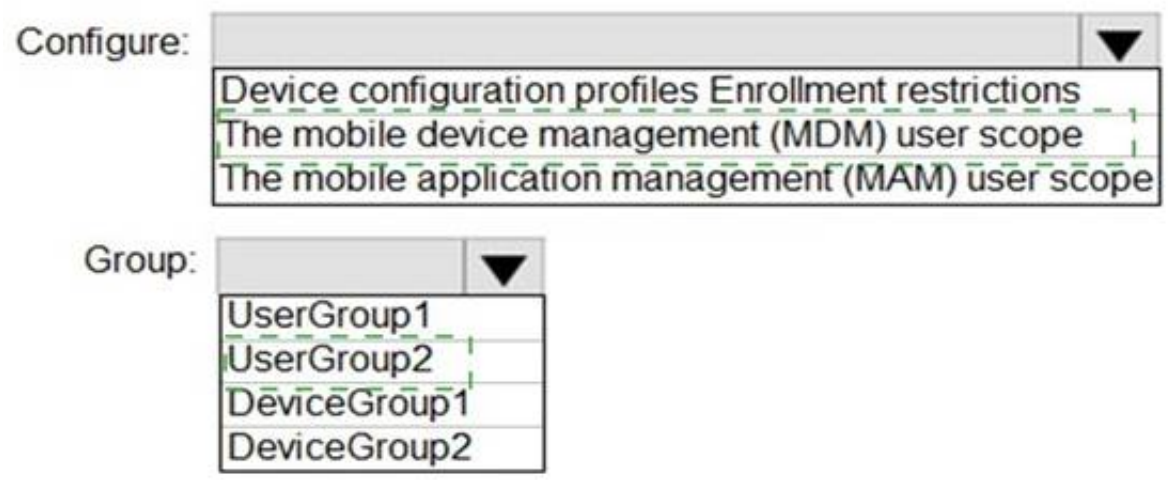
NEW QUESTION 275
HOTSPOT - (Topic 3)
You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.
What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



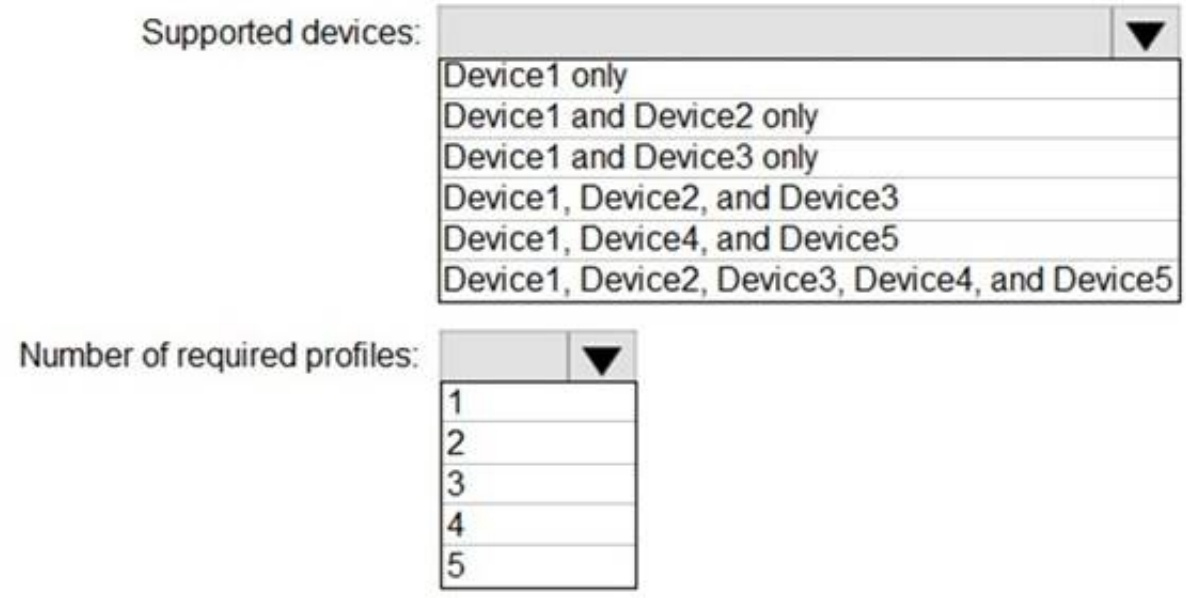
NEW QUESTION 279
- (Topic 3)
You need to create the DLP policy to meet the technical requirements. What should you configure first?

A. sensitive info types
B. the Insider risk management settings
C. the event types
D. the sensitivity labels

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

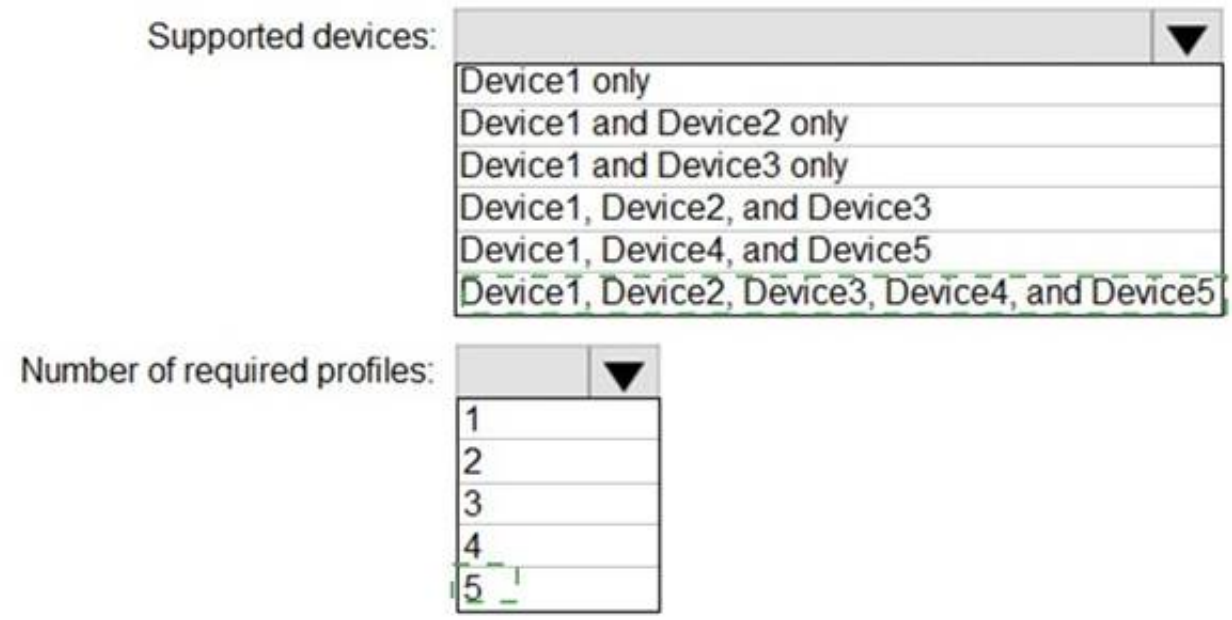
NEW QUESTION 281
HOTSPOT - (Topic 3)
You plan to implement the endpoint protection device configuration profiles to support the planned changes.
You need to identify which devices will be supported, and how many profiles you should implement.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 283
- (Topic 1)
You need to create the Microsoft Store for Business. Which user can create the store?

A. User2
B. User3
C. User4
D. User5

Answer: C

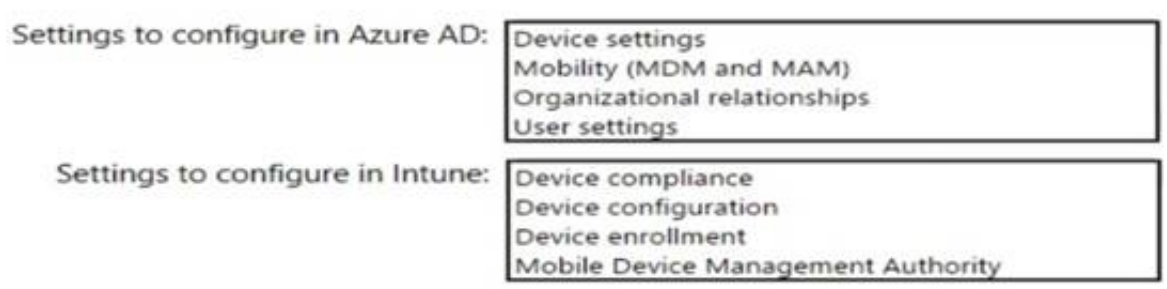
Explanation:
References:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for- business

NEW QUESTION 286
- (Topic 2)
You need to protect the U.S. PII data to meet the technical requirements. What should you create?

A. a data loss prevention (DLP) policy that contains a domain exception
B. a Security & Compliance retention policy that detects content containing sensitive data
C. a Security & Compliance alert policy that contains an activity
D. a data loss prevention (DLP) policy that contains a user override

Answer: A

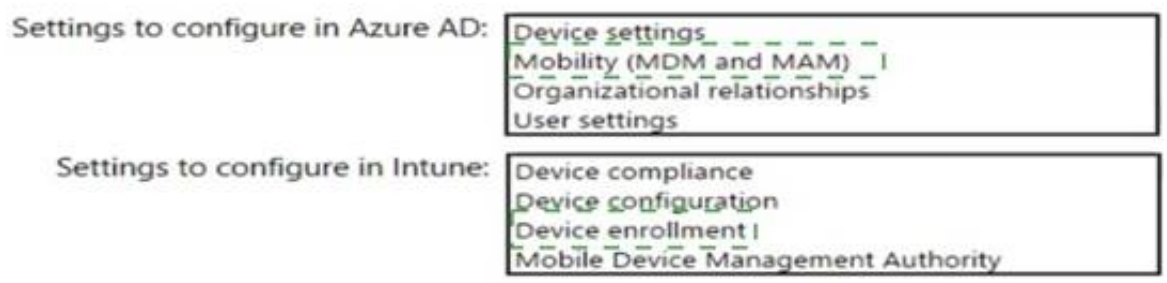
NEW QUESTION 289
HOTSPOT - (Topic 1)
You need to meet the technical requirements and planned changes for Intune. What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 290
- (Topic 1)
You need to meet the compliance requirements for the Windows 10 devices. What should you create from the Intune admin center?

A. a device compliance policy
B. a device configuration profile
C. an application policy
D. an app configuration policy

Answer: C

NEW QUESTION 295
- (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 298
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 299
- (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 302
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named site1. You need to ensure that site1 meets the following requirements:
• Retains all data for 10 years
• Prevents the sharing of data outside the organization
Which two items should you create and apply to site1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. a retention policy
B. a sensitive info type
C. a data loss prevention (DLP) policy
D. a sensitivity label
E. a retention label
F. a retention label policy

Answer: CE

NEW QUESTION 303
- (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 User4 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 304
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant.
You configure a device compliance policy as shown in the following exhibit.

Compliance settings Edit

Microsoft Defender ATP

Require the device to be at or under the machine risk score:	Low

Device Health

Rooted devices	Block
Require the device to be at or under the Device Threat Level	

System Security

Require a password to unlock mobile devices	Require
Required password type	Device default
Encryption of data storage on device.	Require
Block apps from unknown sources	Block

Actions for noncompliance Edit

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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.

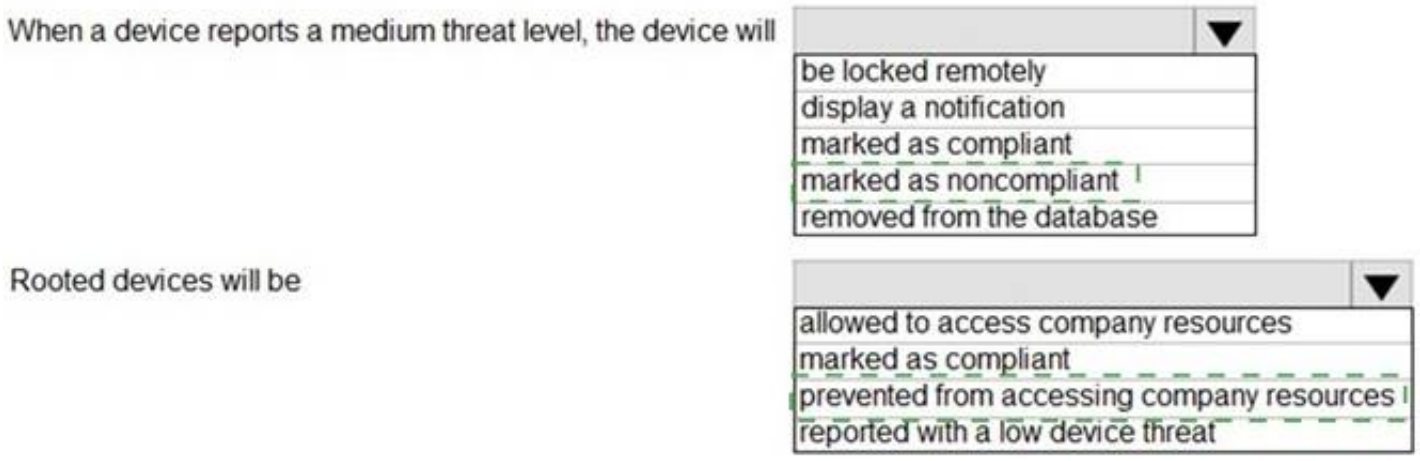
When a device reports a medium threat level, the device will
- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

Rooted devices will be
- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 306
- (Topic 6)
You have a Microsoft 365 subscription that contains a user named User1. User1 requires admin access to perform the following tasks:
Manage Microsoft Exchange Online settings. Create Microsoft 365 groups.
You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.
What should you use?

A. zure AD Identity Protection
B. Microsoft Entra Verified ID
C. Conditional Access
D. Azure AD Privileged Identity Management (PJM)

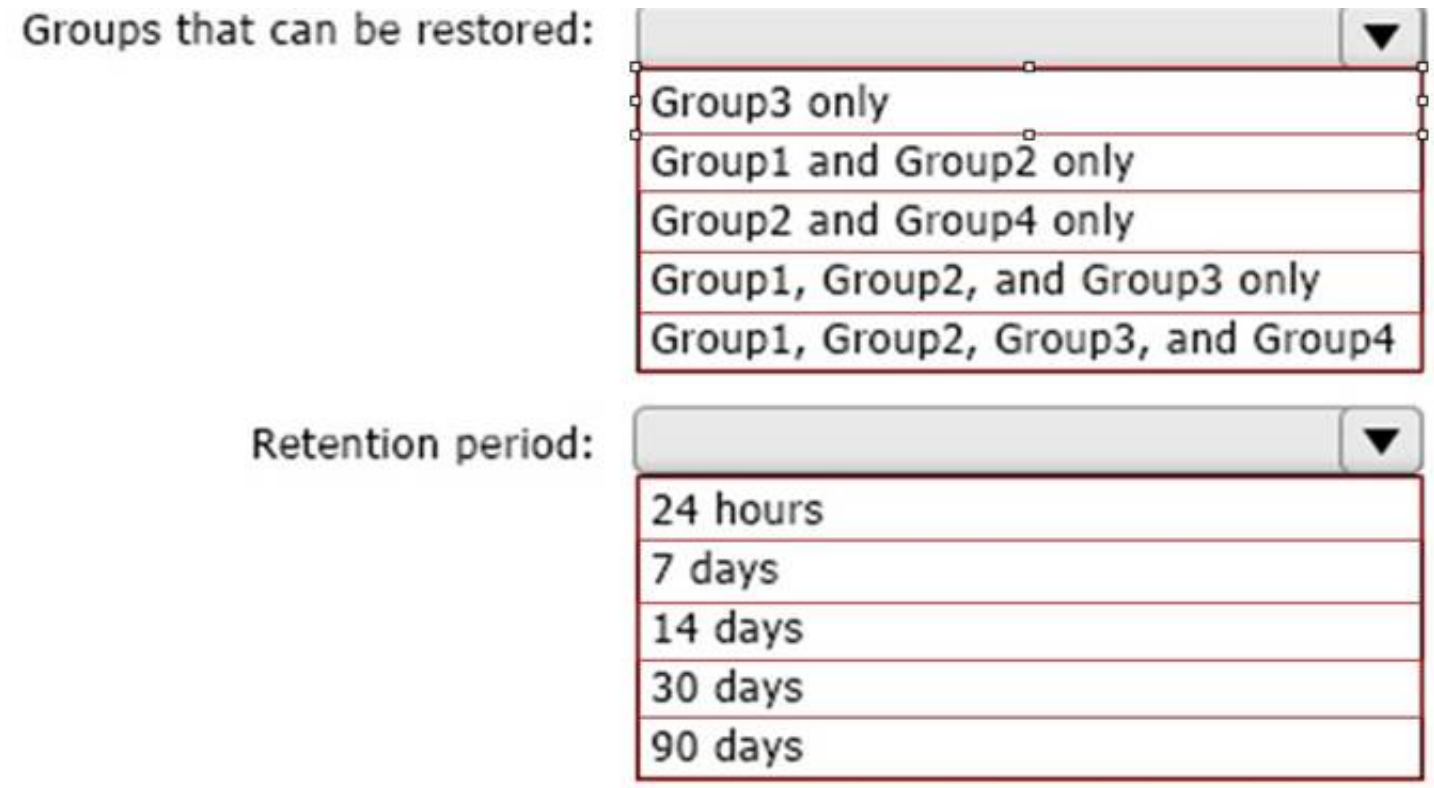
Answer: D

Explanation:
Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:
Provide just-in-time privileged access to Azure AD and Azure resources Assign time-bound access to resources using start and end dates Require approval to activate privileged roles
Enforce multi-factor authentication to activate any role Use justification to understand why users activate
Get notifications when privileged roles are activated Conduct access reviews to ensure users still need roles Download audit history for internal or external audit
Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity- management/pim-configure

NEW QUESTION 309
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

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

All the groups are deleted.
Which groups can be restored, and what is the retention period? 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: Group3 only
Box 2: 30 days
If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a "soft-delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

NEW QUESTION 314
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365 and contains a user named User1.
User1 emails a product catalog in the PDF format to 300 vendors. Only 200 vendors receive the email message, and User1 is blocked from sending email until the next day.
You need to prevent this issue from reoccurring. What should you configure?

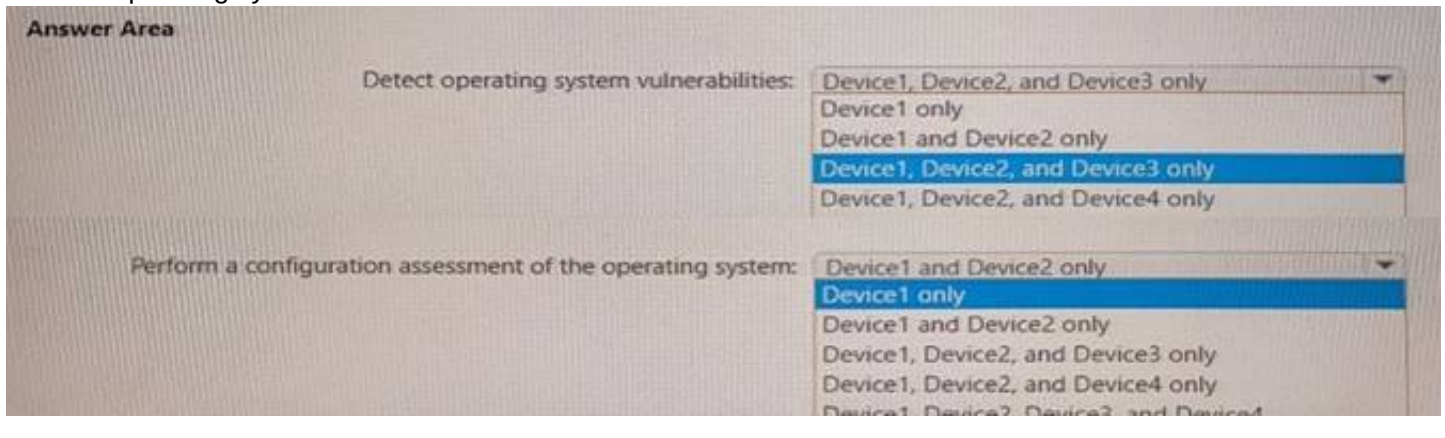
A. anti-spam policies
B. Safe Attachments policies
C. anti-phishing policies
D. anti-malware policies

Answer: A

NEW QUESTION 316
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

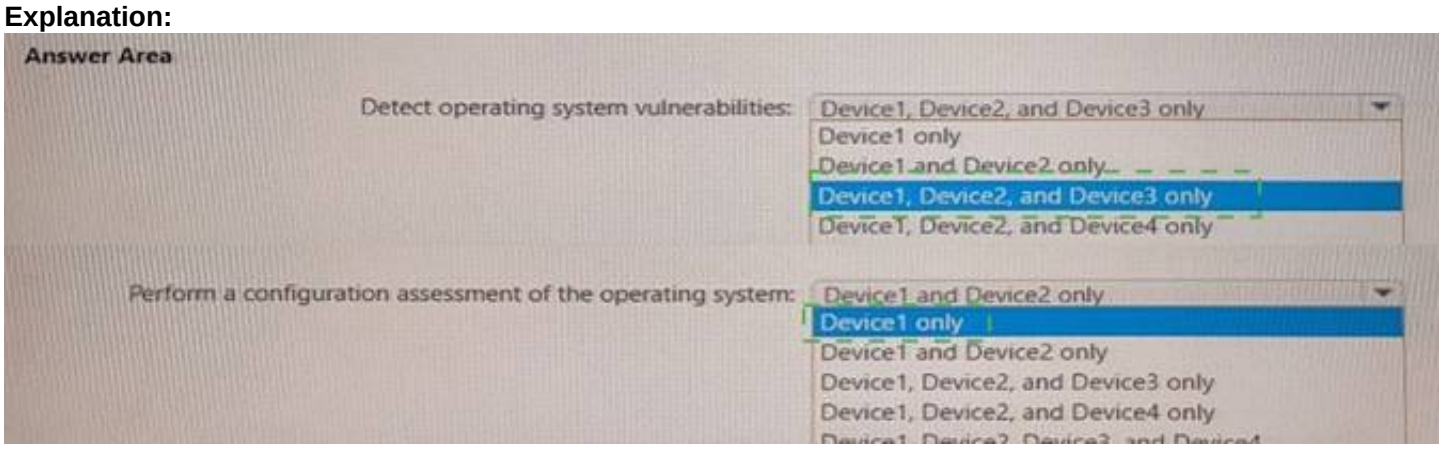
All the devices are onboarded To Microsoft Defender for Endpoint
You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:
• Detect operating system vulnerabilities.



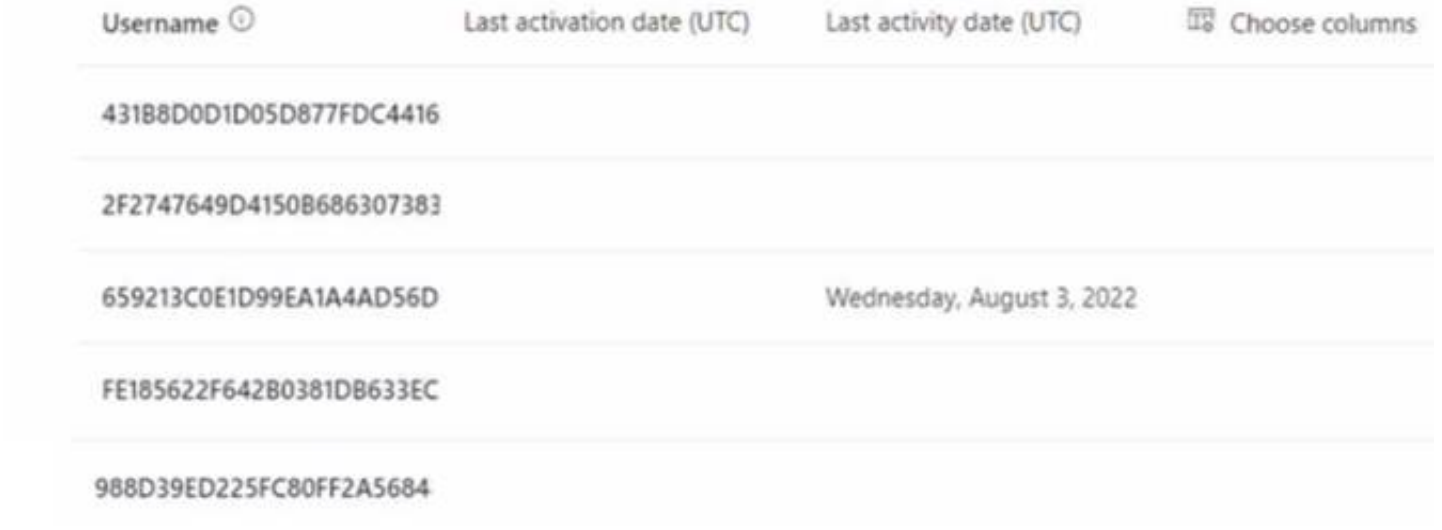
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 318
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription.
From the Microsoft 365 admin center, you open the Microsoft 365 Apps usage report as shown in the following exhibit.



You need ensure that the report meets the following requirements:
• The Username column must display the actual name of each user.
• Usage of the Microsoft Teams mobile app must be displayed.
What should you modify for each requirement? 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 322
- (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 326
- (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

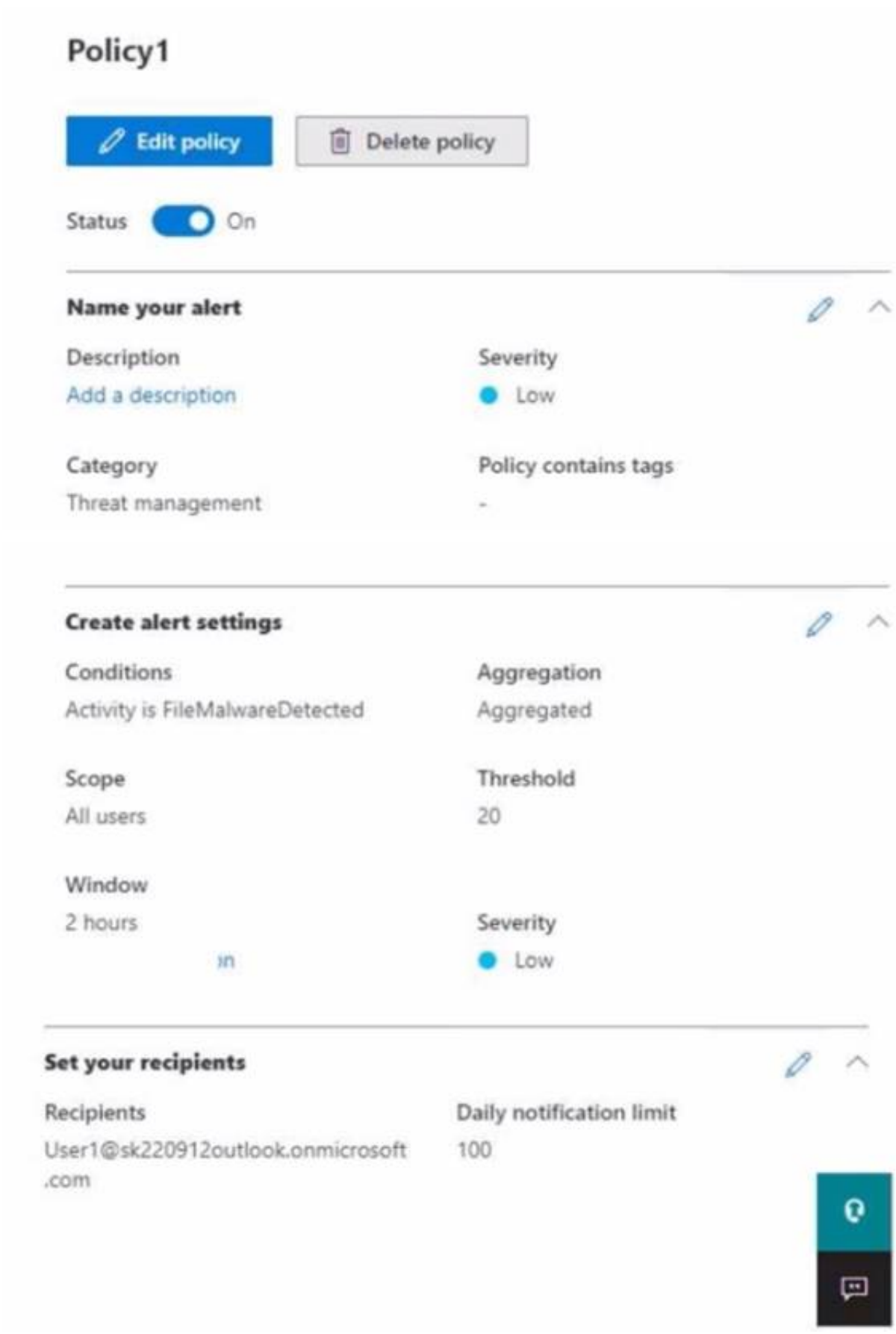
Explanation:
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

NEW QUESTION 331
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to be alerted when Microsoft 365 Defender detects high-severity incidents. What should you use?

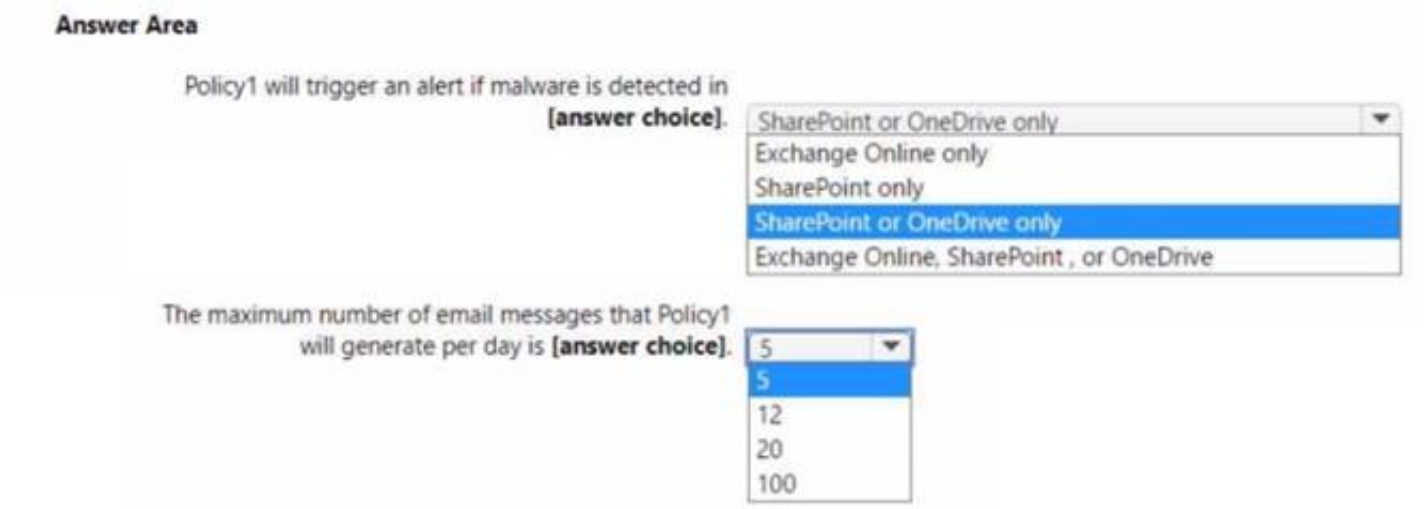
A. a custom detection rule
B. a threat policy
C. an alert policy
D. a notification rule

Answer: C

NEW QUESTION 332
HOTSPOT - (Topic 6)
You have Microsoft 365 subscription.
You create an alert policy as shown in the following exhibit.



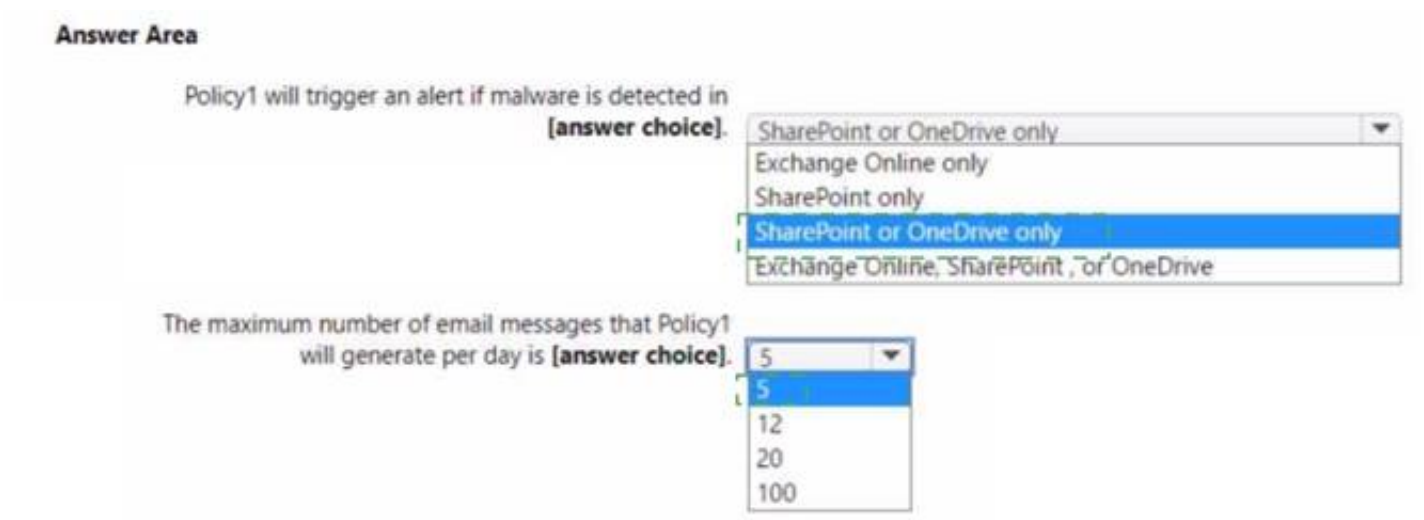
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 336
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.

A. Mastered
B. Not Mastered

Answer: A

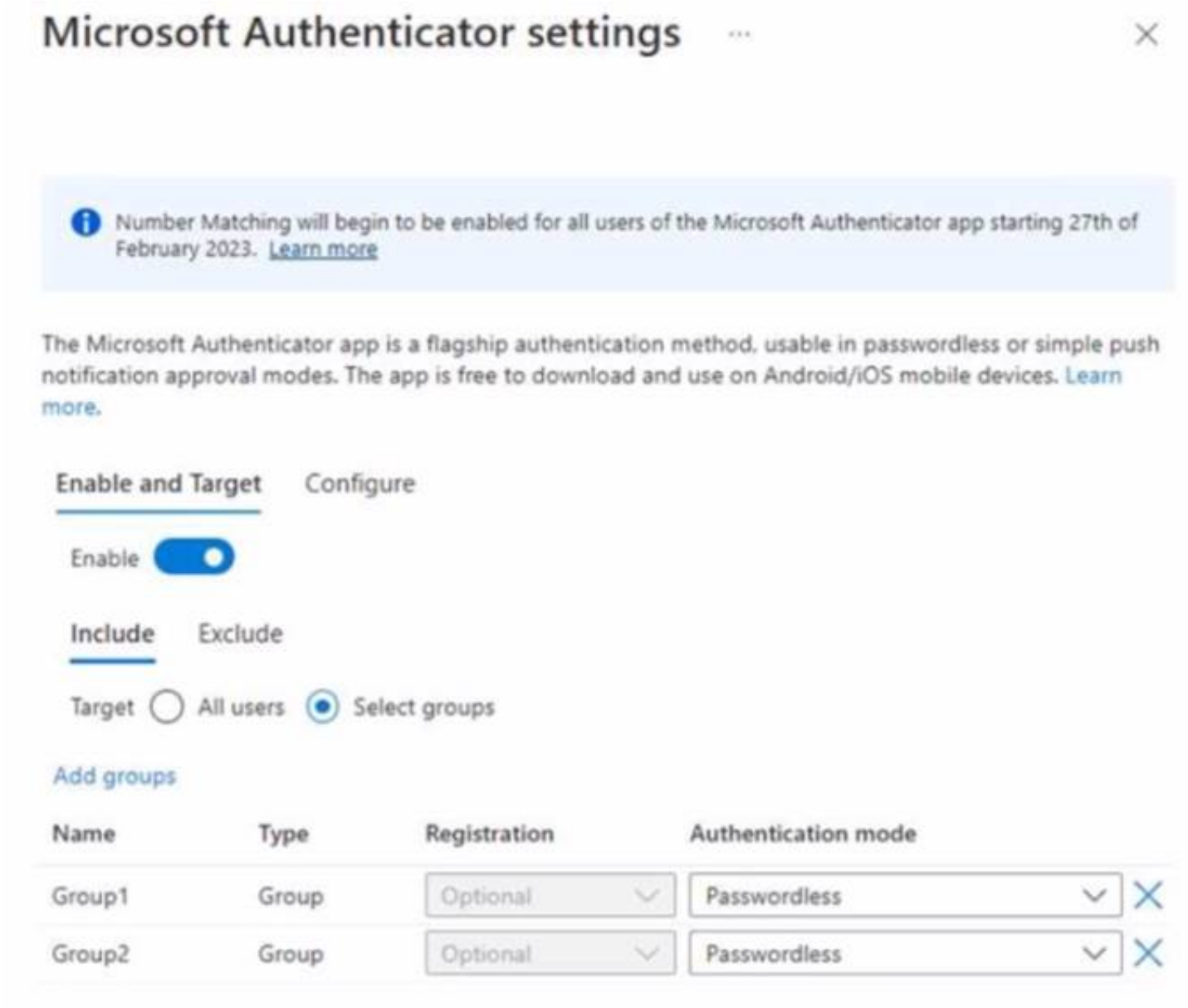
Explanation:
Box 1: No
User1 is assigned the Password Administrator for AU1 and AU2. User3 is in AU2. User3 is User Adminstrator.
Password administrators cannot reset User Administrators passwords.
Note: Password Administrator
Users with this role have limited ability to manage passwords. This role does 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		✔	✔	✔	✔	✔

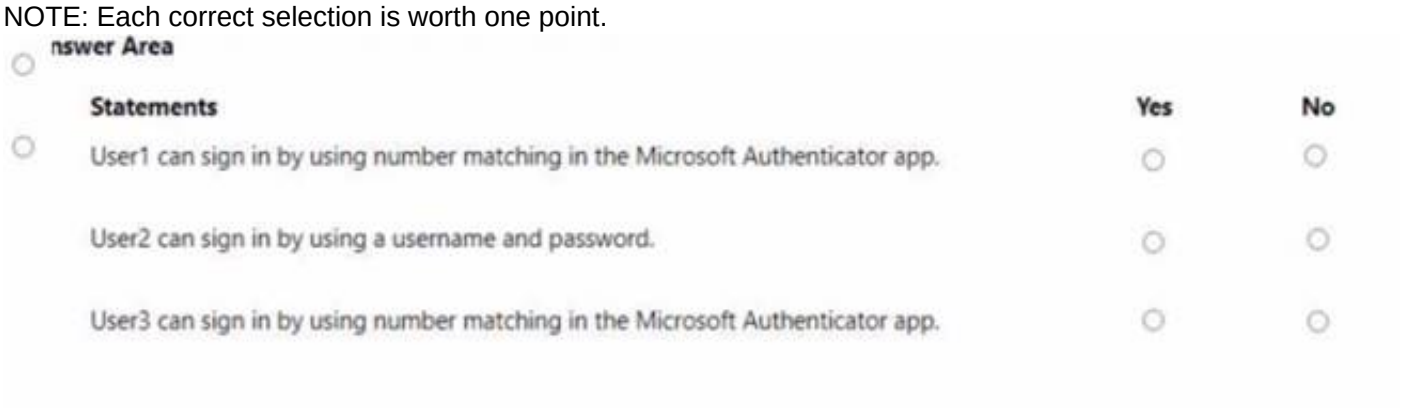
Box 2: Yes
Box 3: No
User1 is assigned the Password Administrator for AU1 and AU2. User2 is in AU1. User2 is User Adminstrator.
Password administrators cannot reset User Administrators passwords.
Note: User Administrator
Can manage all aspects of users and groups, including resetting passwords for limited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

NEW QUESTION 338

HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.
Each user has an Android device with the Microsoft Authenticator app installed and has set up phone sign-in.
The subscription has the following Conditional Access policy:
• Name: Policy1
• Assignments
o Users and groups: Group1, Group2 o Cloud apps or actions: All cloud apps
• Access controls
o Grant Require multi-factor authentication
• Enable policy: On
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.



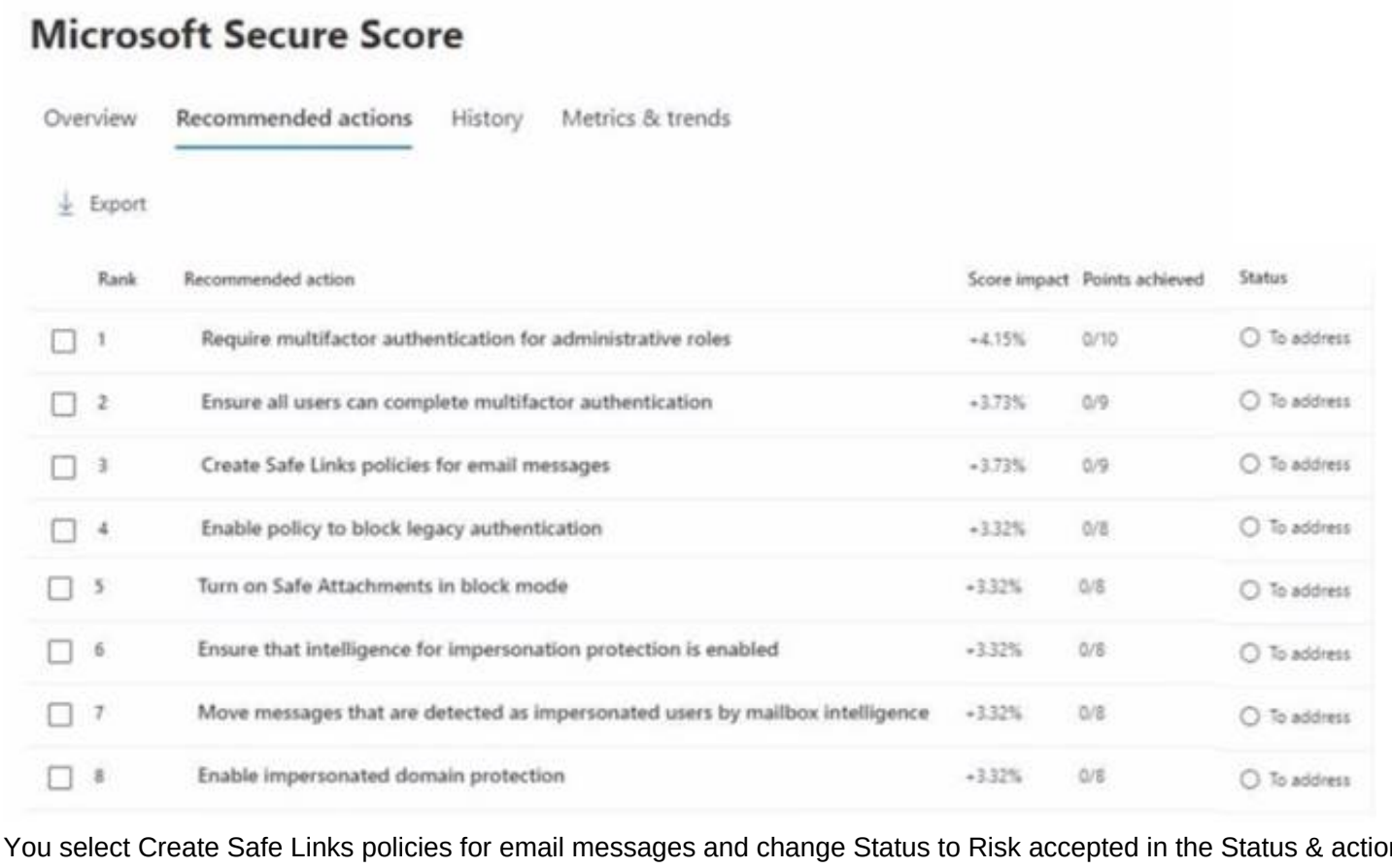
A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 339
- (Topic 6)

You have a Microsoft 365 E5 subscription.
Your company s Microsoft Secure Score recommends the actions shown in the following exhibit.



You select Create Safe Links policies for email messages and change Status to Risk accepted in the Status & action plan settings.
How does the change affect the Secure Score?

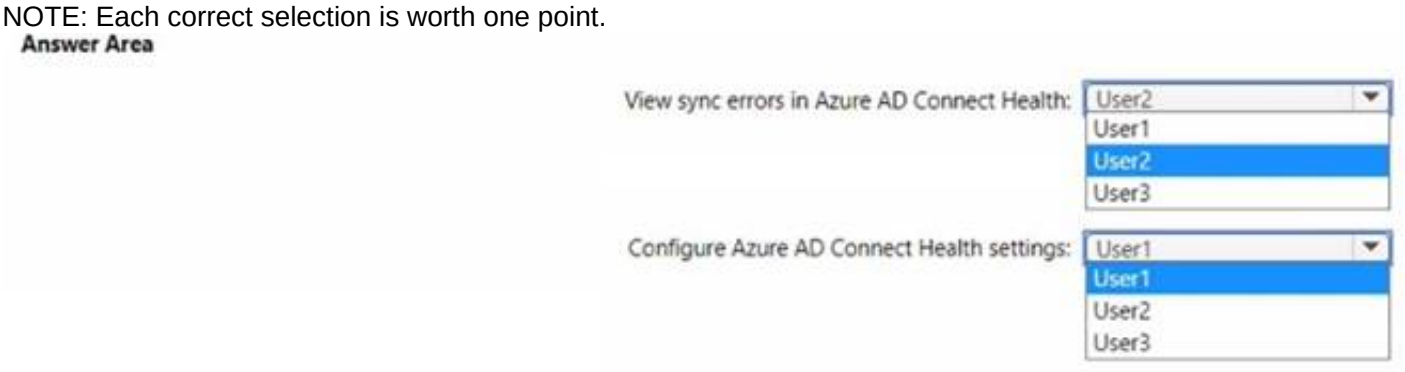
A. remains the same
B. increases by 1 point
C. increases by 9 points
D. decreases by 1 point
E. decreases by 9 points

Answer: A

NEW QUESTION 343
HOTSPOT - (Topic 6)
You have a hybrid deployment of Azure AD that contains the users shown in the following table.

Name	Description
User1	Azure AD Connect sync account
User2	Contributor for Azure AD Connect Health
User3	Application administrator in Azure AD

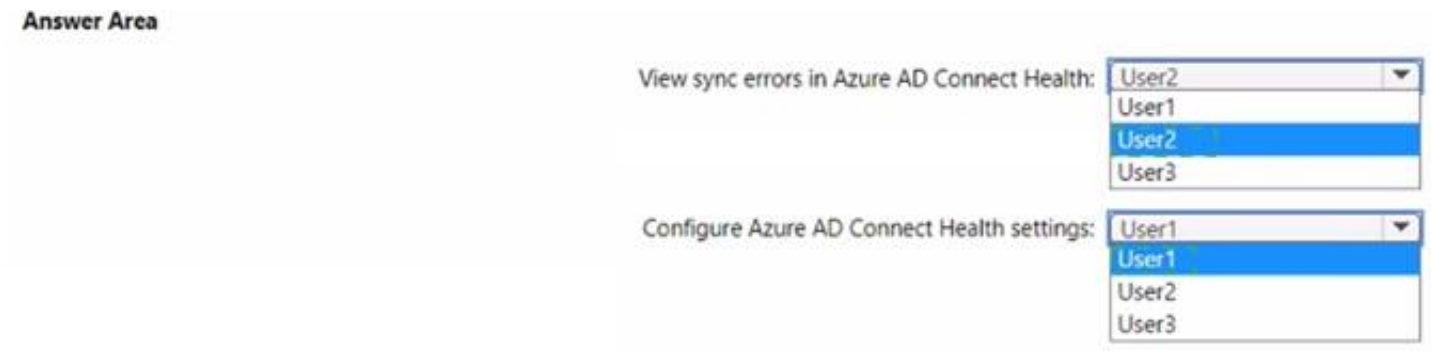
You need to identify which users can perform the following tasks:
• View sync errors in Azure AD Connect Health.
• Configure Azure AD Connect Health settings.
Which user should you identify for each task? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

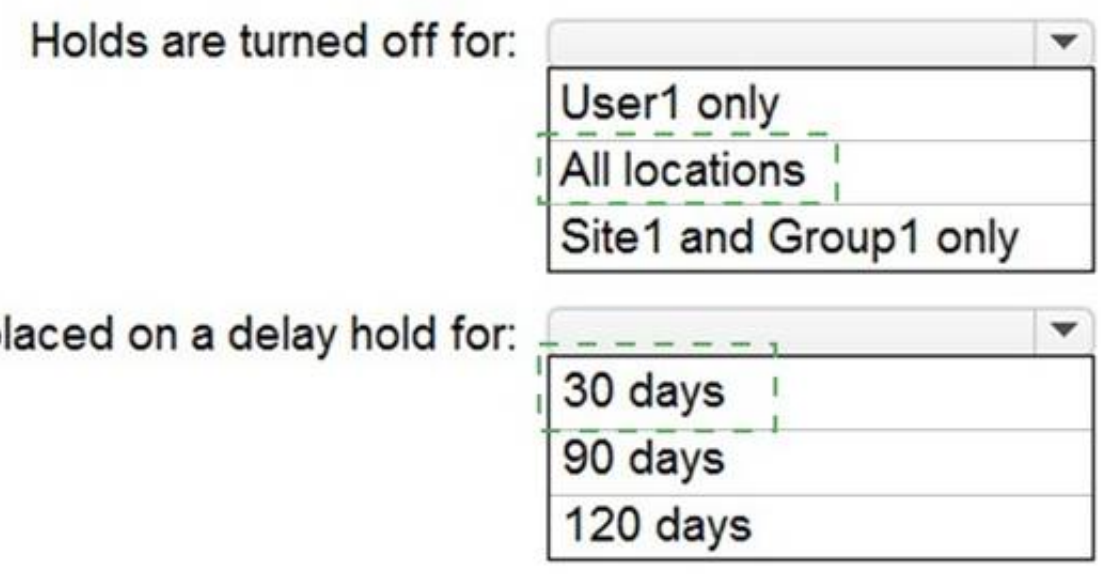


NEW QUESTION 348
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:
? Name: Case1
? Included content: Group1, User1, Site1
? Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders
The investigation for Case1 completes, and you close the case.
What occurs after you close Case1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

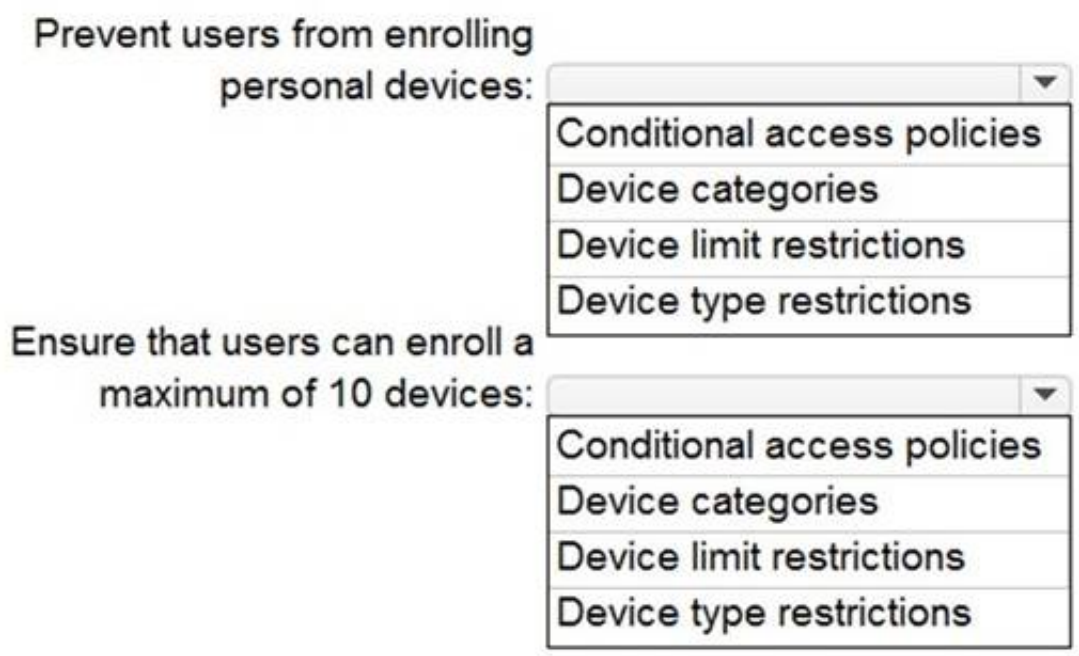
A. Mastered
B. Not Mastered

Answer: A

Explanation:



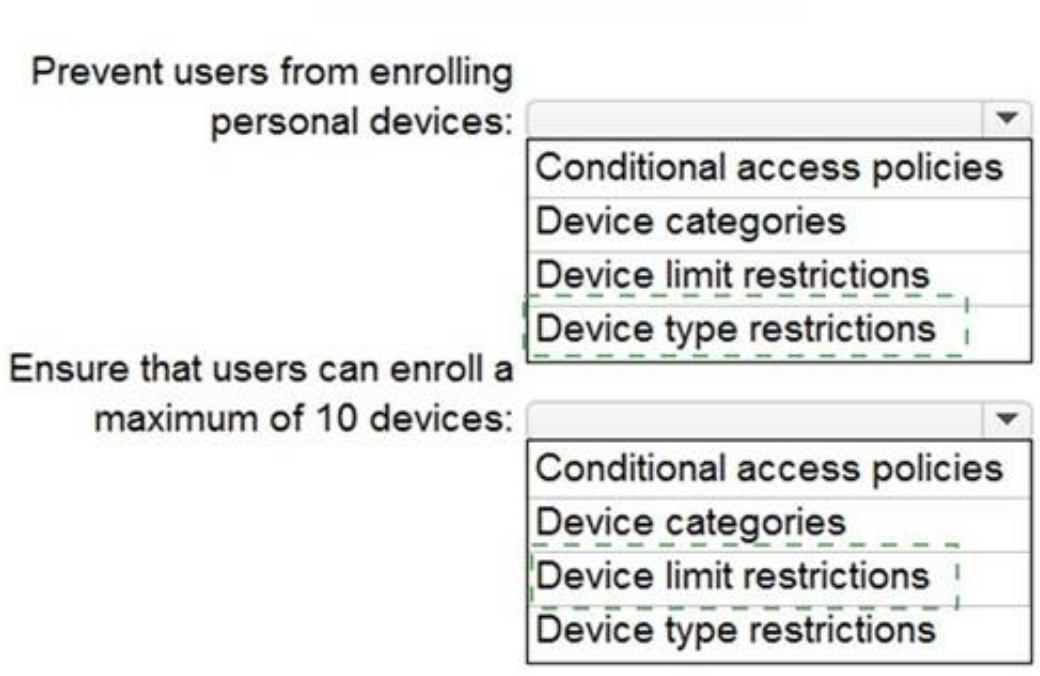
NEW QUESTION 349
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that uses Microsoft Intune. You need to configure Intune to meet the following requirements:
? Prevent users from enrolling personal devices.
? Ensure that users can enroll a maximum of 10 devices.
What should you use for each requirement? 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 352
- (Topic 6)
Your network contains an Active Directory forest named contoso.local. You purchase a Microsoft 365 subscription.
You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months.
You need to prepare for the planned move to Microsoft 365.
What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

A. Purchase a third-party X.509 certificate.
B. Create an external forest trust.
C. Rename the Active Directory forest.
D. Purchase a custom domain name.

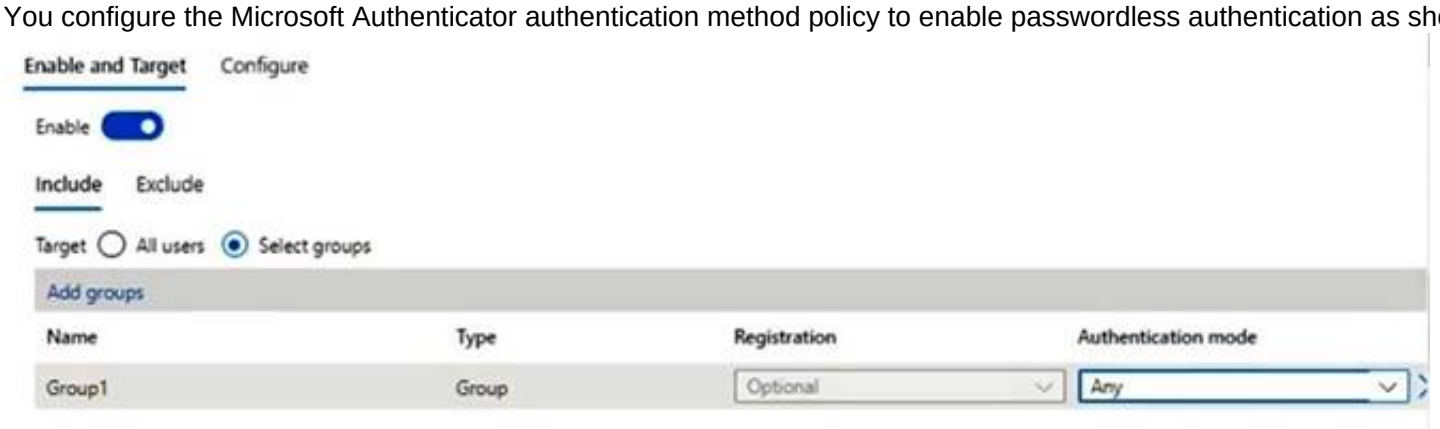
Answer: D

Explanation:
The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on- premise Active Directory if it's a routable domain name, for example, contoso.com.
If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active Directory.
Incorrect:
Not C: No need to rename the Active Directory forest. As we use a non-routable domain name contoso.local, we just need to add the routable domain name as a UPN suffix in Active Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization

NEW QUESTION 355
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

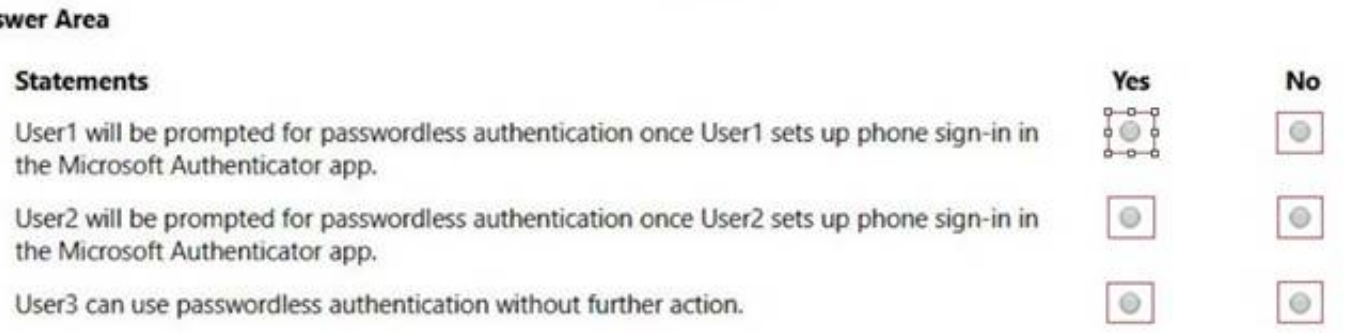
Name	Member of	Multi-factor authentication (MFA) method registered
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1	*None*

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.



Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.
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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
User1 is member of Group1.
User1 has MFA registered method of Microsoft Authenticater app (push notification) The Microsoft Authenticator authentication method policy is configured for Group1, registration is optional, authentication method is any.
Note: Microsoft Authenticator can be used to sign in to any Azure AD account without using a password. Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology.
This authentication technology can be used on any device platform, including mobile. This technology can also be used with any app or website that integrates with Microsoft Authentication Libraries.
Box 2: No
User2 is member of Group2.
The Microsoft Authenticator authentication method policy is configured for Group1, not for Group2.
Box 3: No
User3 is member of Group1.
User3 has no MFA method registered.
User3 must choose an authentication method.
Note: Enable passwordless phone sign-in authentication methods
Azure AD lets you choose which authentication methods can be used during the sign-in process. Users then register for the methods they'd like to use.

NEW QUESTION 357
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profile?

A. Ubuntu Linux
B. macOS
C. iOS
D. Android

Answer: B

Explanation:
Intune device configuration profiles can be applied to Windows 10 devices and macOS devices
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
? Windows 10
? macOS
Other incorrect answer options you may see on the exam include the following:
? Android Enterprise
? Windows 8.1

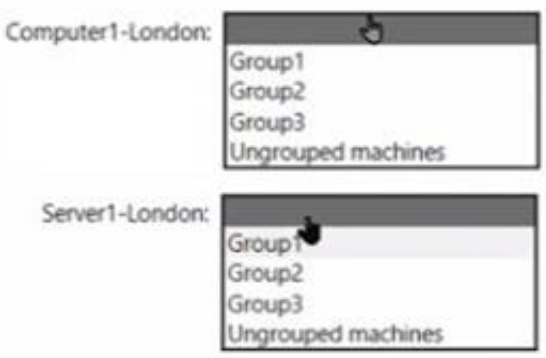
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

NEW QUESTION 361
HOTSPOT - (Topic 6)
You use Microsoft Defender for Endpoint.
You have the Microsoft Defender for Endpoint device groups shown in the following table

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	*Not applicable*

You plan to onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

NEW QUESTION 363
- (Topic 6)
You have a Microsoft 365 subscription that contains a user named User1.
You need to ensure that User1 can search the Microsoft 365 audit logs from the Security & Compliance admin center.
Which role should you assign to User1?

A. View-Only Audit Logs in the Security & Compliance admin center
B. View-Only Audit Logs in the Exchange admin center
C. Security reader in the Azure Active Directory admin center
D. Security Reader in the Security & Compliance admin center

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

NEW QUESTION 367
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Windows 10 edition	Azure Active Directory (Azure AD)	Mobile device management (MDM) enrollment
Device1	Windows 10 Pro	Registered	Microsoft Intune
Device2	Windows 10 Enterprise	Joined	Microsoft Intune
Device3	Windows 10 Pro	Joined	Not enrolled
Device4	Windows 10 Enterprise	Registered	Microsoft Intune
Device5	Windows 10 Enterprise	Joined	Not enrolled

You add custom apps to the private store in Microsoft Store Business.
You plan to create a policy to show only the private store in Microsoft Store for Business. To which devices can the policy be applied?

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

Answer: C

NEW QUESTION 371
- (Topic 6)
You have a Microsoft 365 subscription.
You need to identify which administrative users performed eDiscovery searches during the past week.
What should you do from the Security & Compliance admin center?

A. Perform a content search
B. Create a supervision policy
C. Create an eDiscovery case
D. Perform an audit log search

Answer: D

NEW QUESTION 373
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the labels shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

You have the items shown in the following table.

Name	Stored in	Description
File1	Microsoft SharePoint	File document that has Label1 applied
File2	Microsoft Teams channel	File document that has Label2 applied
Mail1	Microsoft Exchange Online	Email message that has Label1 applied
Mail2	Microsoft Exchange Online	Email message that has Label2 applied

Which items can you view in Content explorer?

A. File1 only
B. File1 and File2 only
C. File1 and Mail! only
D. File2 and Mail2 only
E. File1, File2, Mail1, and Mail2

Answer: C

NEW QUESTION 375
.....

Relate Links

100% Pass Your MS-102 Exam with Exambible Prep Materials

https://www.exambible.com/MS-102-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/