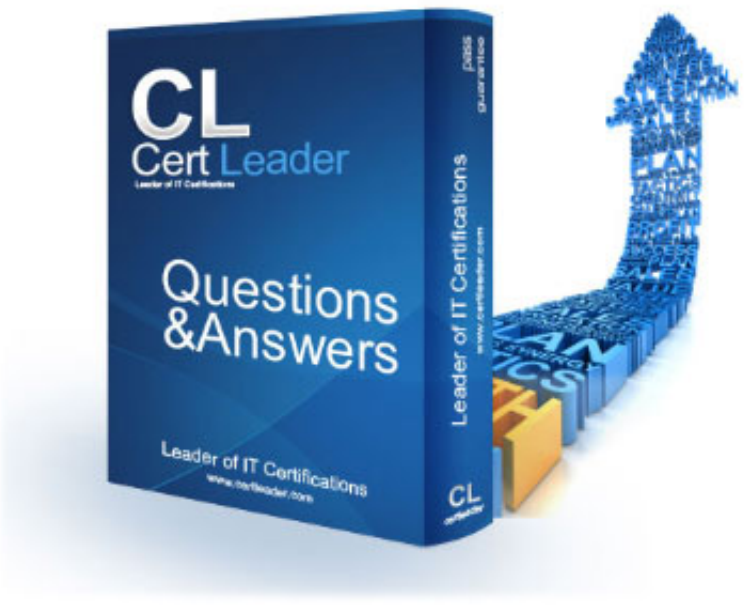
MS-102 Dumps

Microsoft 365 Administrator Exam

https://www.certleader.com/MS-102-dumps.html



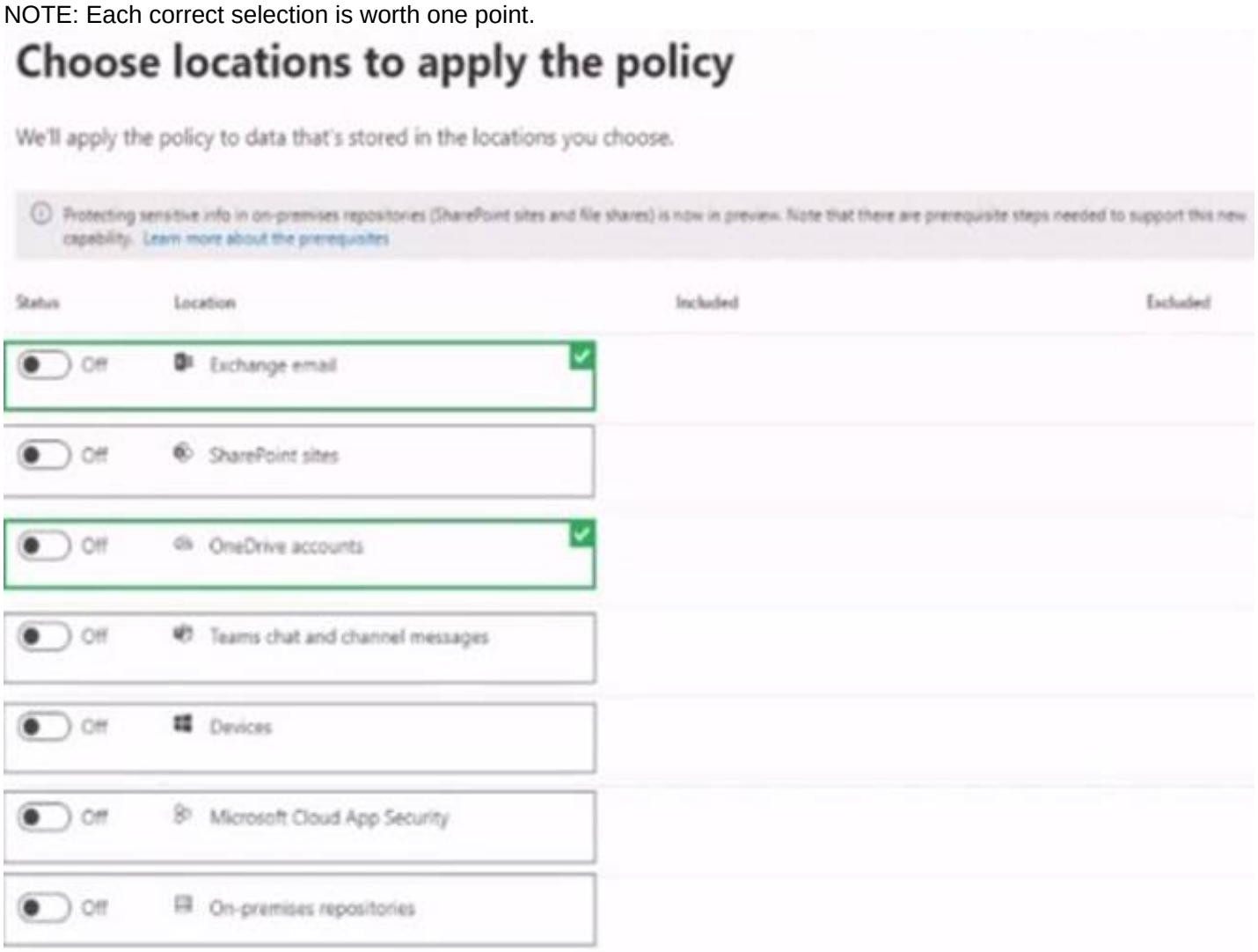
NEW QUESTION 1
- (Topic 6)
You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1. You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:
• Assign licenses to users.
• Procure apps from Microsoft Store.
• Manage private store availability for all items.
The solution must use the principle of least privilege.
Which Microsoft Store for Business role should you assign to User1?

A. Basic Purchaser
B. Device Guard signer
C. Admin
D. Purchaser

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

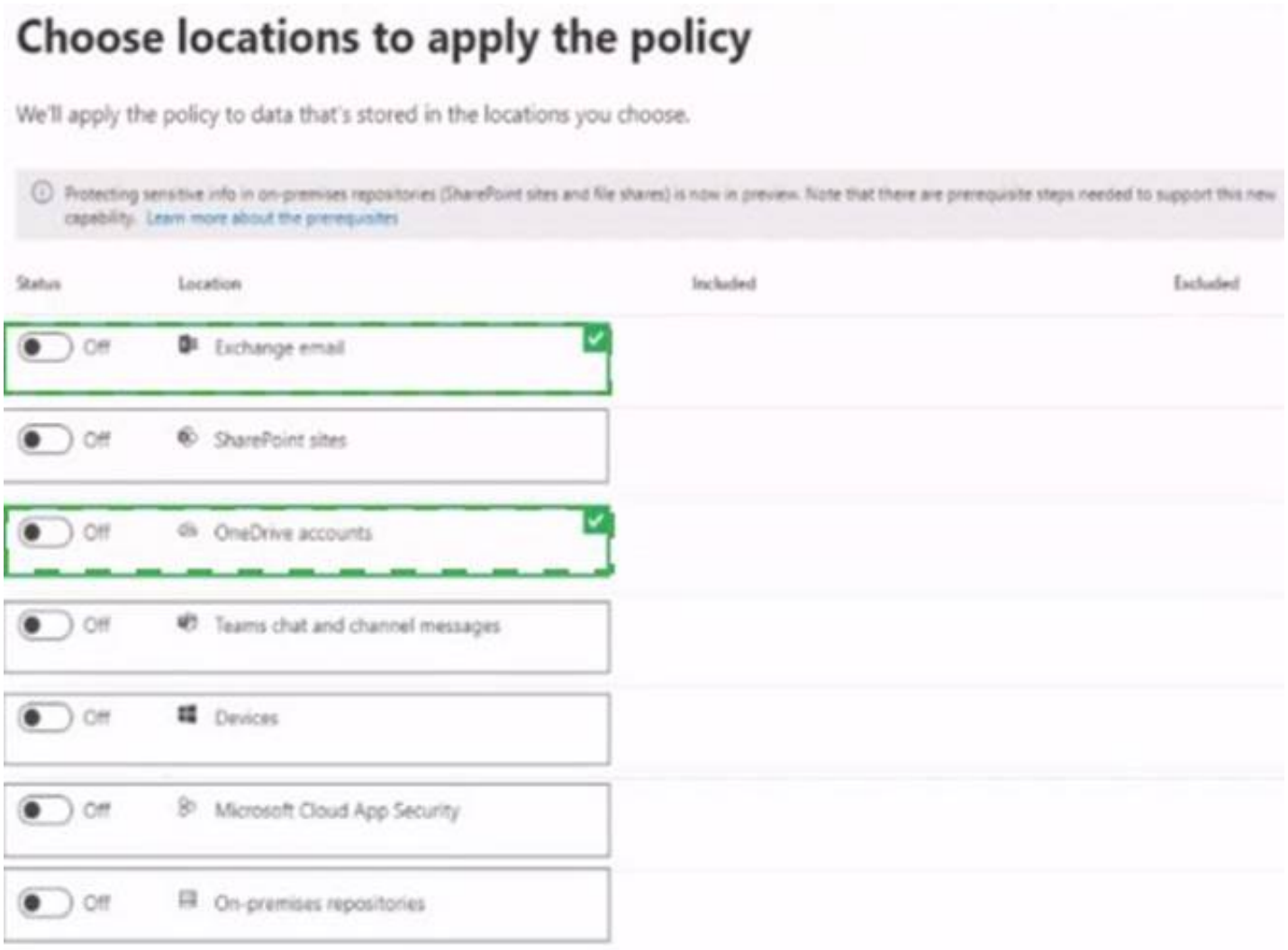
NEW QUESTION 2
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant
You create a data toss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.
To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 3
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
You need to implement identity protection. The solution must meet the following requirements:
? Identify when a user's credentials are compromised and shared on the dark web.
? Provide users that have compromised credentials with the ability to self-remediate.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: A user risk policy
Identify when a user's credentials are compromised and shared on the dark web.
User risk-based Conditional Access policy
Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:
Block access
Allow access but require a secure password change.
A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.
Box 2: Require password change
Provide users that have compromised credentials with the ability to self-remediate.
A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators

NEW QUESTION 4
- (Topic 6)
Your company has offices in five cities. The company has a Microsoft 365 tenant.
Each office is managed by a local administrator. You plan to deploy Microsoft Intune.

You need to recommend a solution to manage resources in intune that meets the following requirements:
? Local administrators must be able to manage only the resources in their respective office.
? Local administrators must be prevented from managing resources in other offices.
? Administrative effort must be minimized.
What should you include in the recommendation?

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

Answer: B

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

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

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

Answer: B

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

NEW QUESTION 6
- (Topic 6)
Your company has 10,000 users who access all applications from an on-premises data center.
You plan to create a Microsoft 365 subscription and to migrate data to the cloud. You plan to implement directory synchronization.
User accounts and group accounts must sync to Azure AD successfully. You discover that several user accounts fail to sync to Azure AD.
You need to resolve the issue as quickly as possible. What should you do?

A. From Active Directory Administrative Center, search for all the users, and then modify the properties of the user accounts.
B. Run idfix.exe, and then click Edit.
C. From Windows PowerShell, run the start-AdSyncSyncCycle -PolicyType Delta command.
D. Run idfix.exe, and then click Complete.

Answer: B

Explanation:
IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for- synch-with-idfix

NEW QUESTION 7
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.
What should you use?

A. an attack surface reduction (ASR) policy
B. an app configuration policy
C. a device compliance policy
D. a device configuration profile

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

NEW QUESTION 8
- (Topic 6)
You have a Microsoft 365 E5 subscription.
On Monday, you create a new user named User1.
On Tuesday, User1 signs in for the first time and perform the following actions:

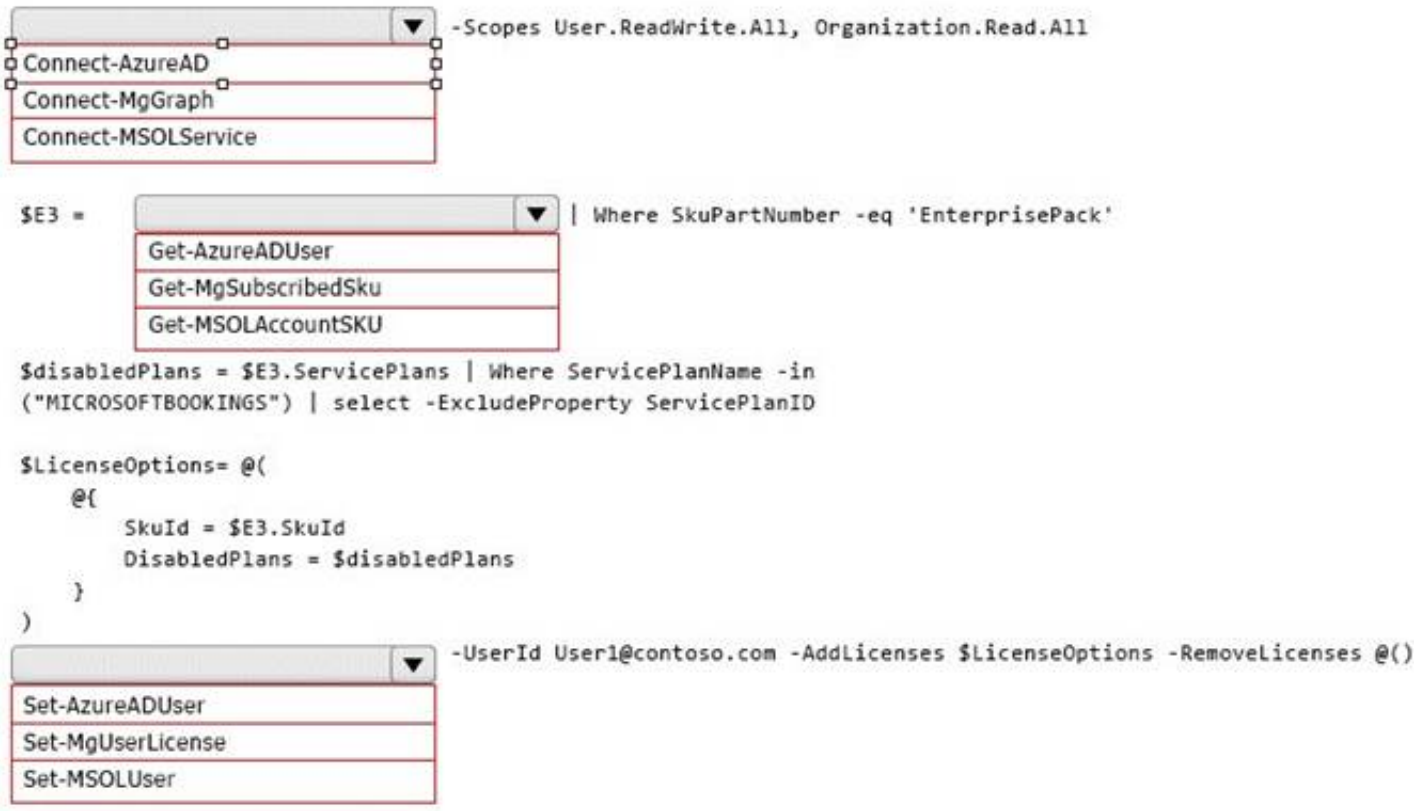
• Signs in to Microsoft Exchange Online from an anonymous IP address
• Signs in to Microsoft SharePoint Online from a device in New York City.
• Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections
Which types of sign-in risks will Azure AD Identity Protection detect for User1?

A. anonymous IP address only
B. anonymous IP address and atypical travel
C. anonymous IP address, atypical travel, and unfamiliar sign-in properties
D. unfamiliar sign-in properties and atypical travel only
E. anonymous IP address and unfamiliar sign-in properties only

Answer: C

NEW QUESTION 9
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription.
A user named user1@contoso.com was recently provisioned.
You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.
How should you complete the 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:
Box 1: Connect-MgGraph
Assign Microsoft 365 licenses to user accounts with PowerShell Use the Microsoft Graph PowerShell SDK
First, connect to your Microsoft 365 tenant.
Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the 'Assign license' Microsoft Graph API reference page.
The Organization.Read.All permission scope is required to read the licenses available in the tenant.
Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All Box 2: Get-MgSubscribedSku
Run the Get-MgSubscribedSku command to view the available licensing plans and the
number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.
Box 3: Set-MgUserLicense Assigning licenses to user accounts
To assign a license to a user, use the following command in PowerShell.
Set-MgUserLicense -UserId $userUPN -AddLicenses @{SkuId = "<SkuId>"} - RemoveLicenses @()
This example assigns a license from the SPE_E5 (Microsoft 365 E5) licensing plan to the unlicensed user belindan@litwareinc.com:
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId =
$e5Sku.SkuId} -RemoveLicenses @()

NEW QUESTION 10
- (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

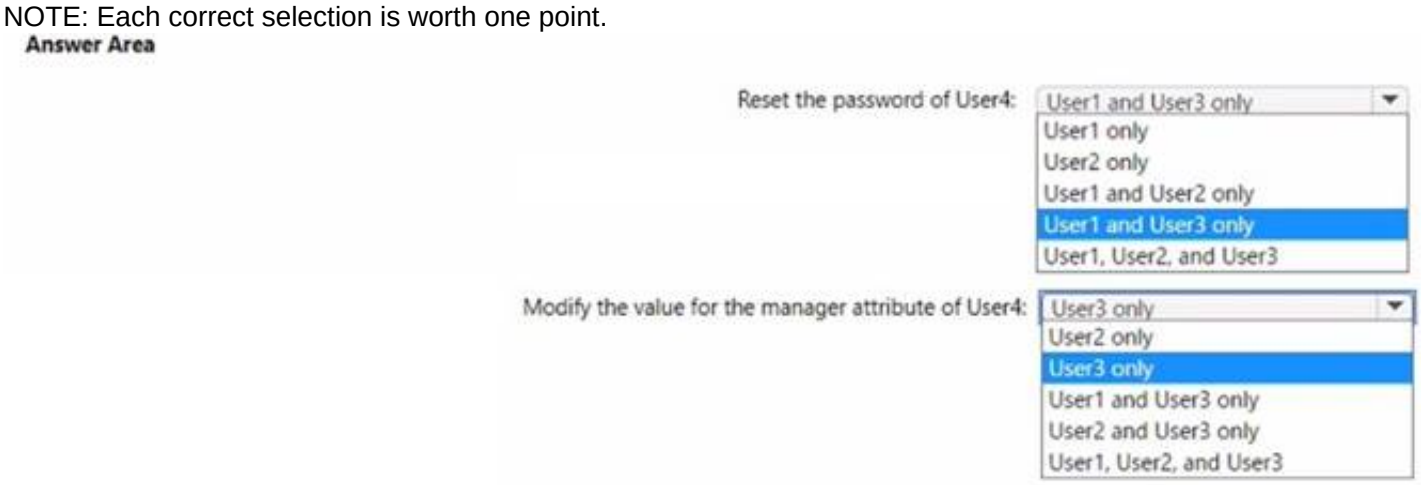
D. Anti-spam
E. Safe Links

Answer: CE

NEW QUESTION 10
HOTSPOT - (Topic 6)
Your company has a Azure AD tenant named comoso.onmicrosoft.com that contains the users shown in the following table.

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

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

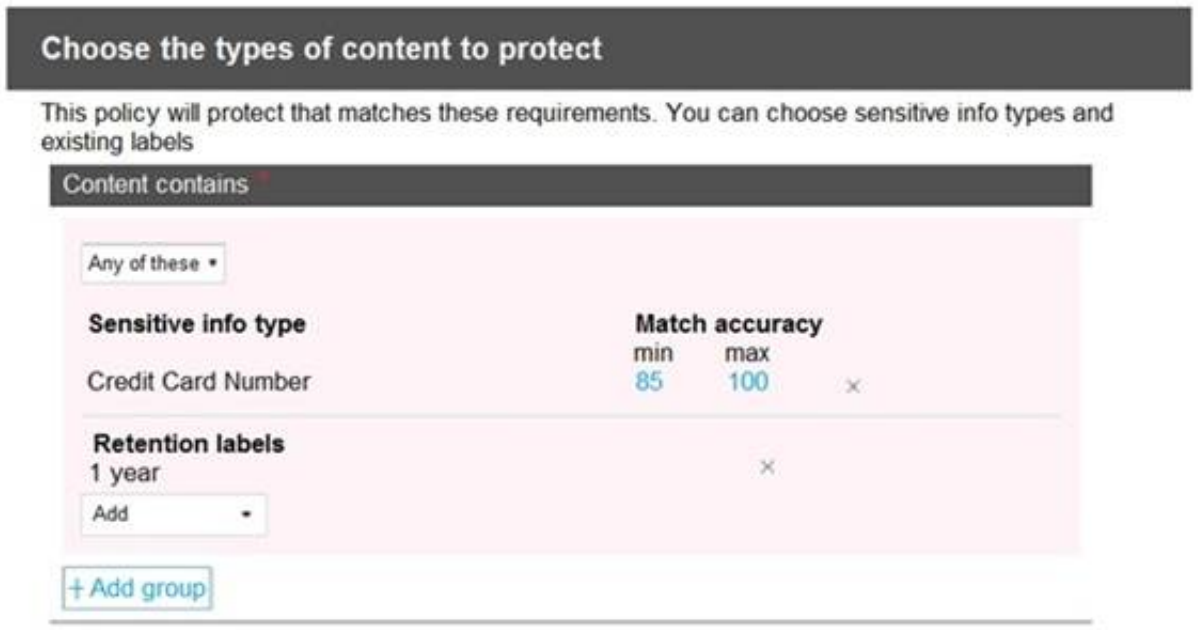


A. Mastered
B. Not Mastered

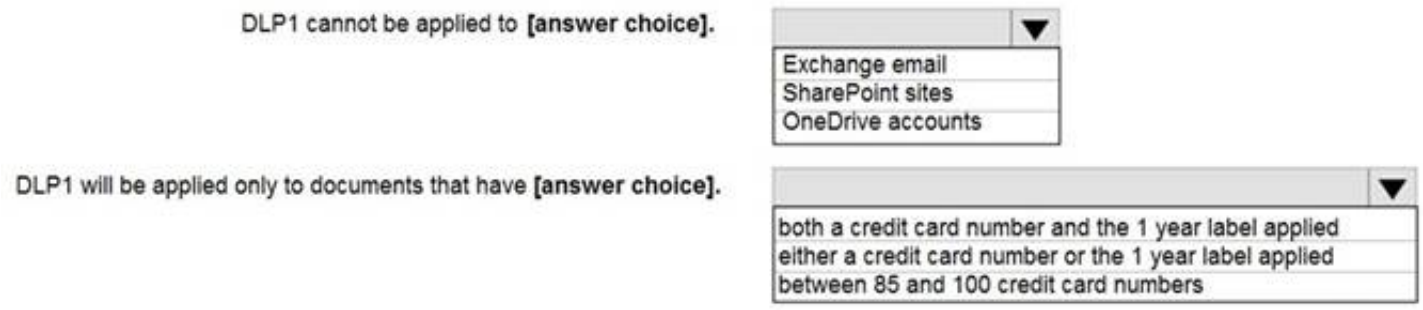
Answer: A

Explanation:

NEW QUESTION 12
HOTSPOT - (Topic 6)
You configure a data loss prevention (DLP) policy named DLP1 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:
Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

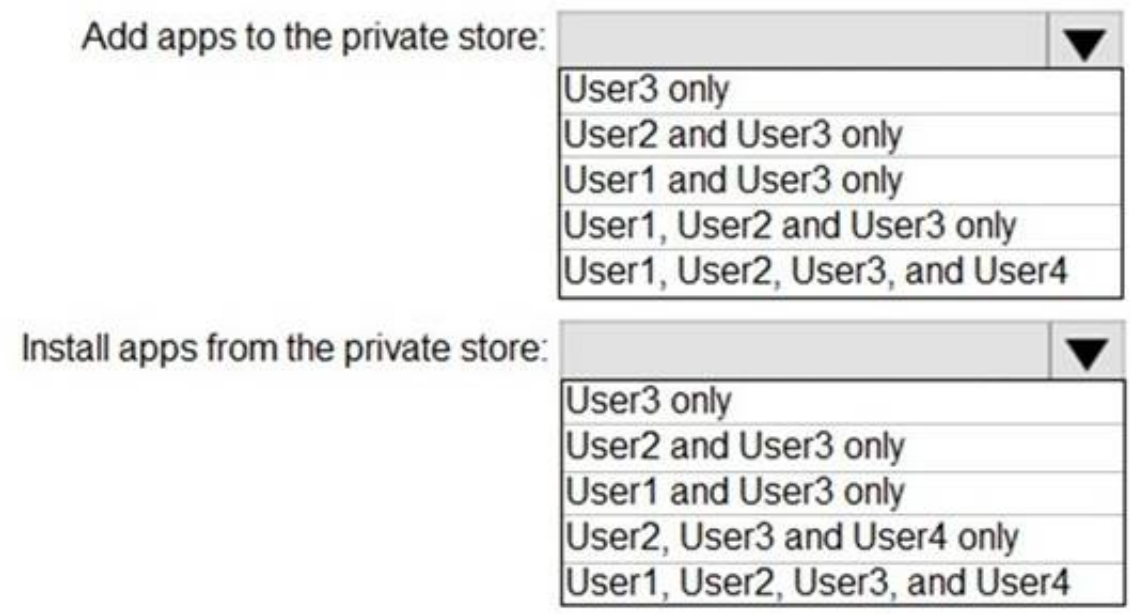
NEW QUESTION 16
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	**None**

Users are assigned Microsoft Store for Business roles as shown in the following table.

User	Role
User1	**None**
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

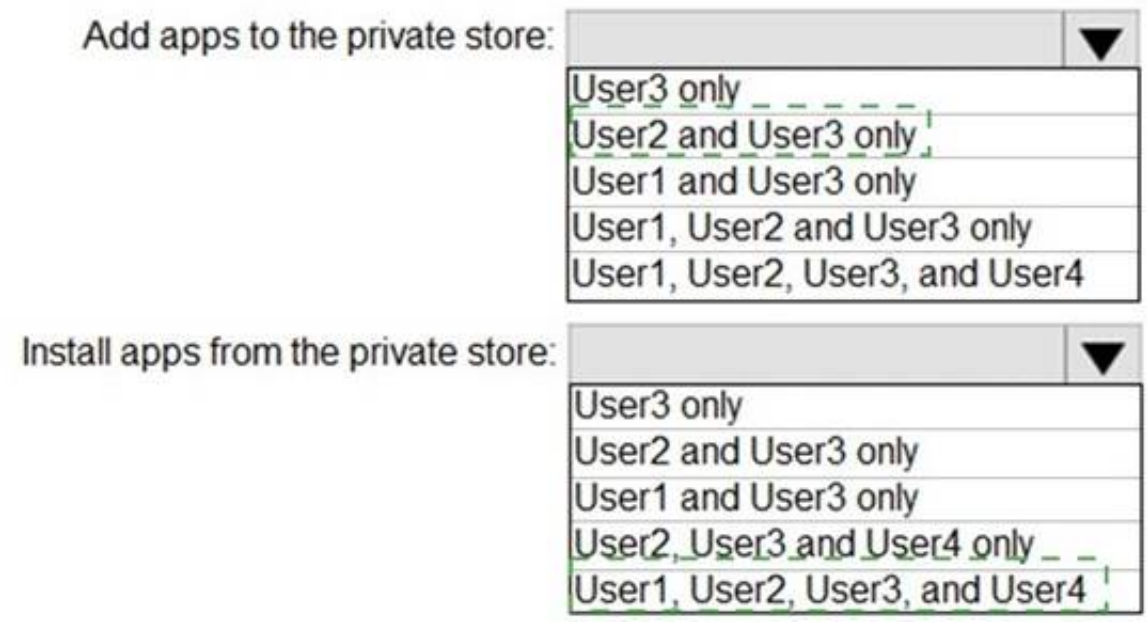
Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 20
- (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.

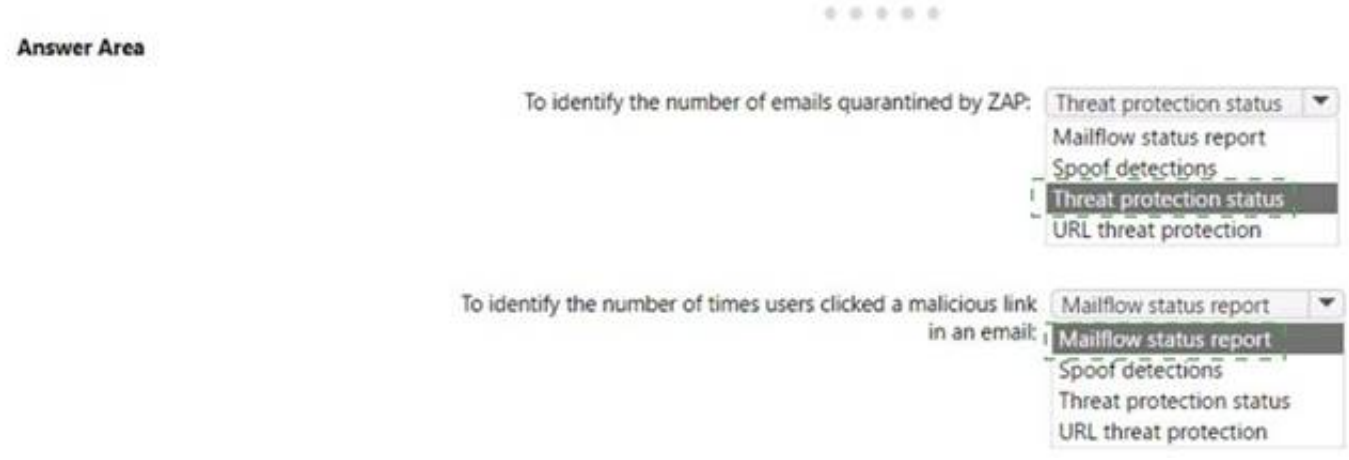
Answer: C

NEW QUESTION 23
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.
The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.
You need to identify the following information:
• The number of email messages quarantined by zero-hour auto purge (ZAP)
• The number of times users clicked a malicious link in an email message
Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

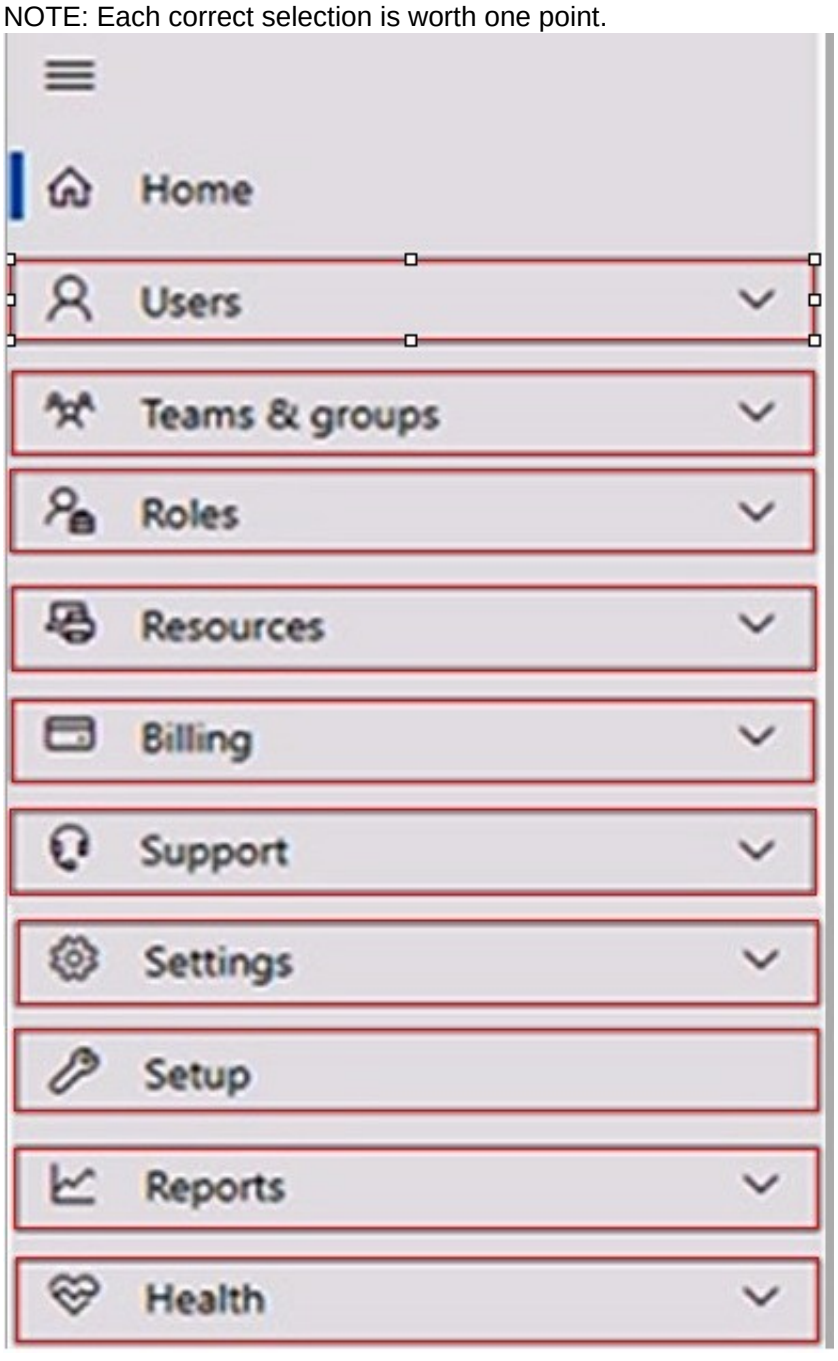
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 24
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 28
- (Topic 6)
You have a Microsoft 365 subscription.
You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.
To which location can the policy be applied?

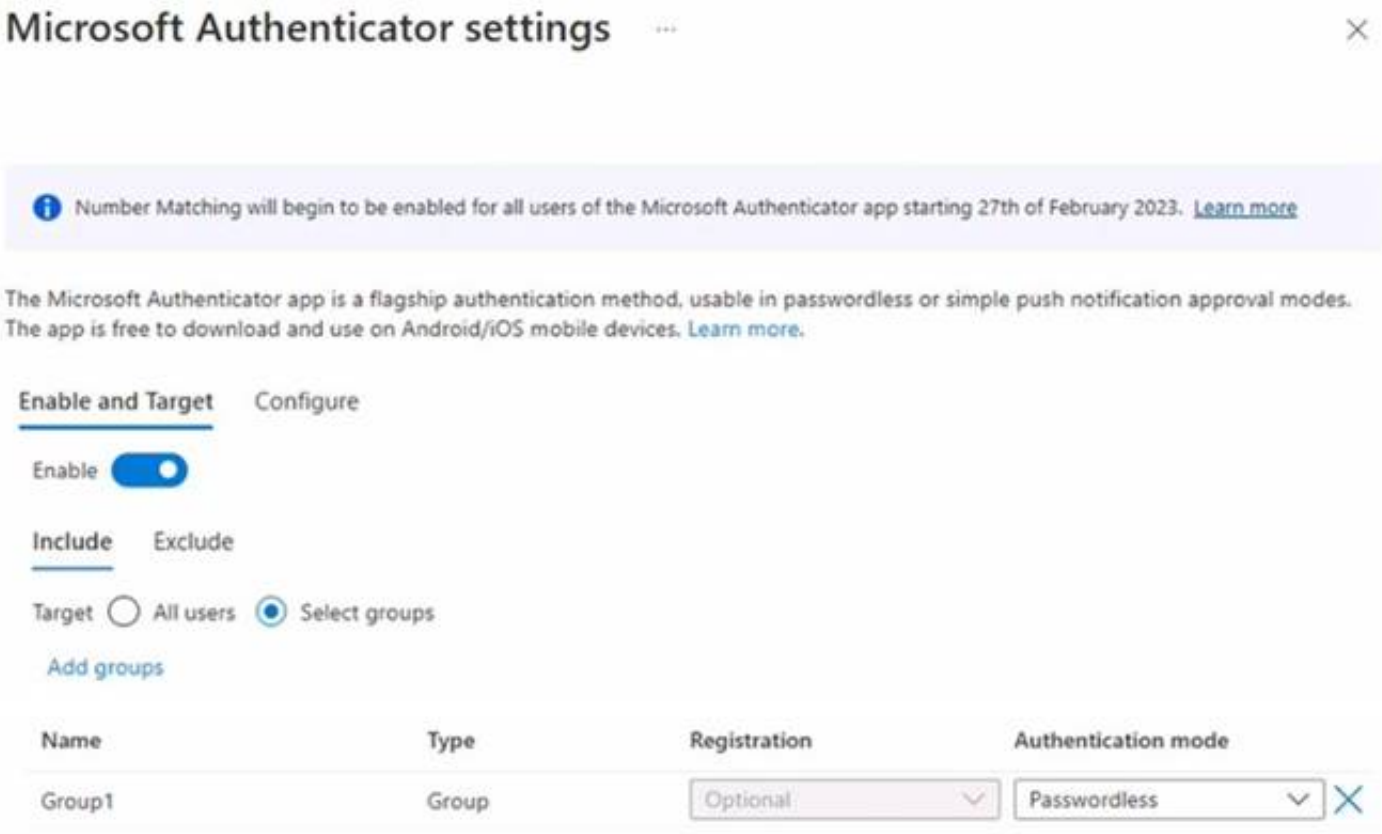
A. OneDrive accounts
B. Exchange email
C. Teams chat and channel messages
D. SharePoint sites

Answer: B

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

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

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



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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 37
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You have the devices shown in the following table.

Name	TPM version	Operating system	BIOS/UEFI	BitLocker Drive Encryption (BitLocker)
Device1	TPM 1.2	Windows 10 Pro	BIOS	Enabled
Device2	TPM 2	Windows 10 Home	BIOS	**Not applicable**
Device3	TPM 2	Windows 8.1 Pro	UEFI	Enabled

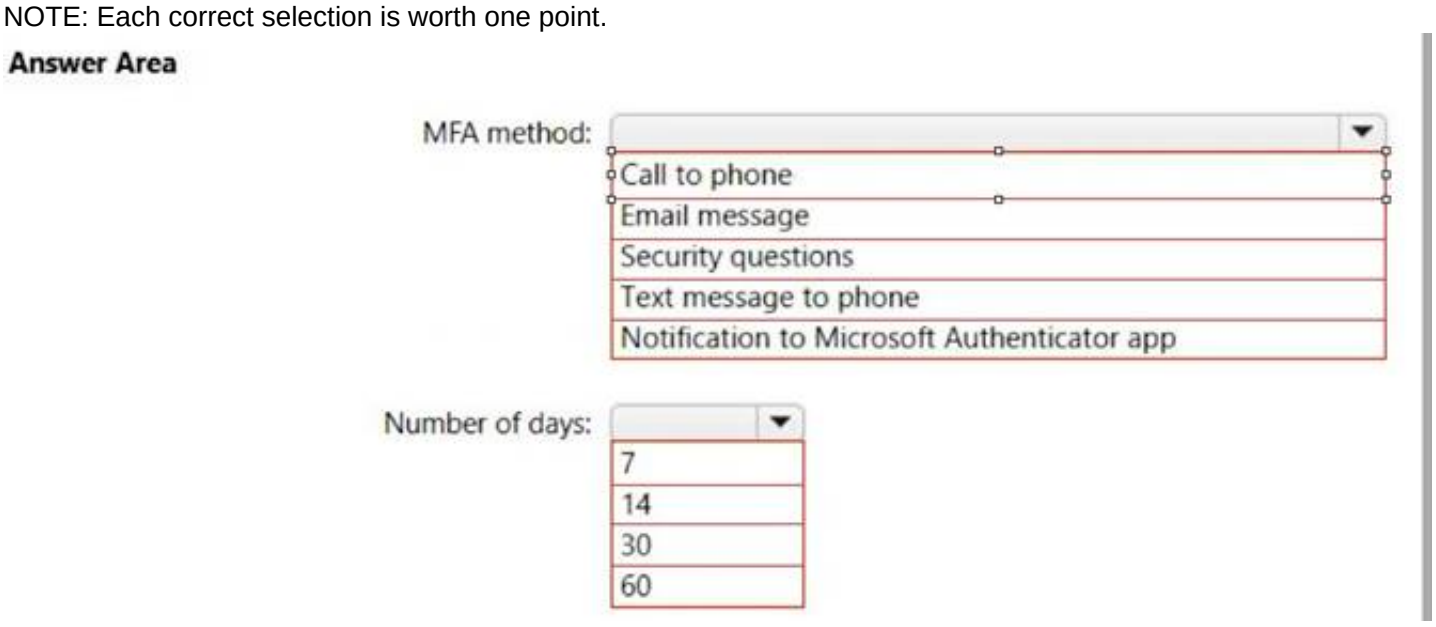
You plan to join the devices to Azure Active Directory (Azure AD)
What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, of not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 38
HOTSPOT - (Topic 6)
HOTSPOT
You have a new Microsoft 365 E5 tenant. Enable Security defaults is set to Yes.
A user signs in to the tenant for the first time.
Which multi-factor authentication (MFA) method can the user use, and how many days does the user have to register for MFA? 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: Notification to Microsoft Authenticator app
Do users have 14 days to register for Azure AD Multi-Factor Authentication?
Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won't be able to sign in until MFA registration is completed.
Box 2: 14
Azure AD Identity Protection will prompt your users to register the next time they sign in interactively and they'll have 14 days to complete registration. During this 14-day period, they can bypass registration if MFA isn't required as a condition, but at the end of the period they'll be required to register before they can complete the sign-in process.

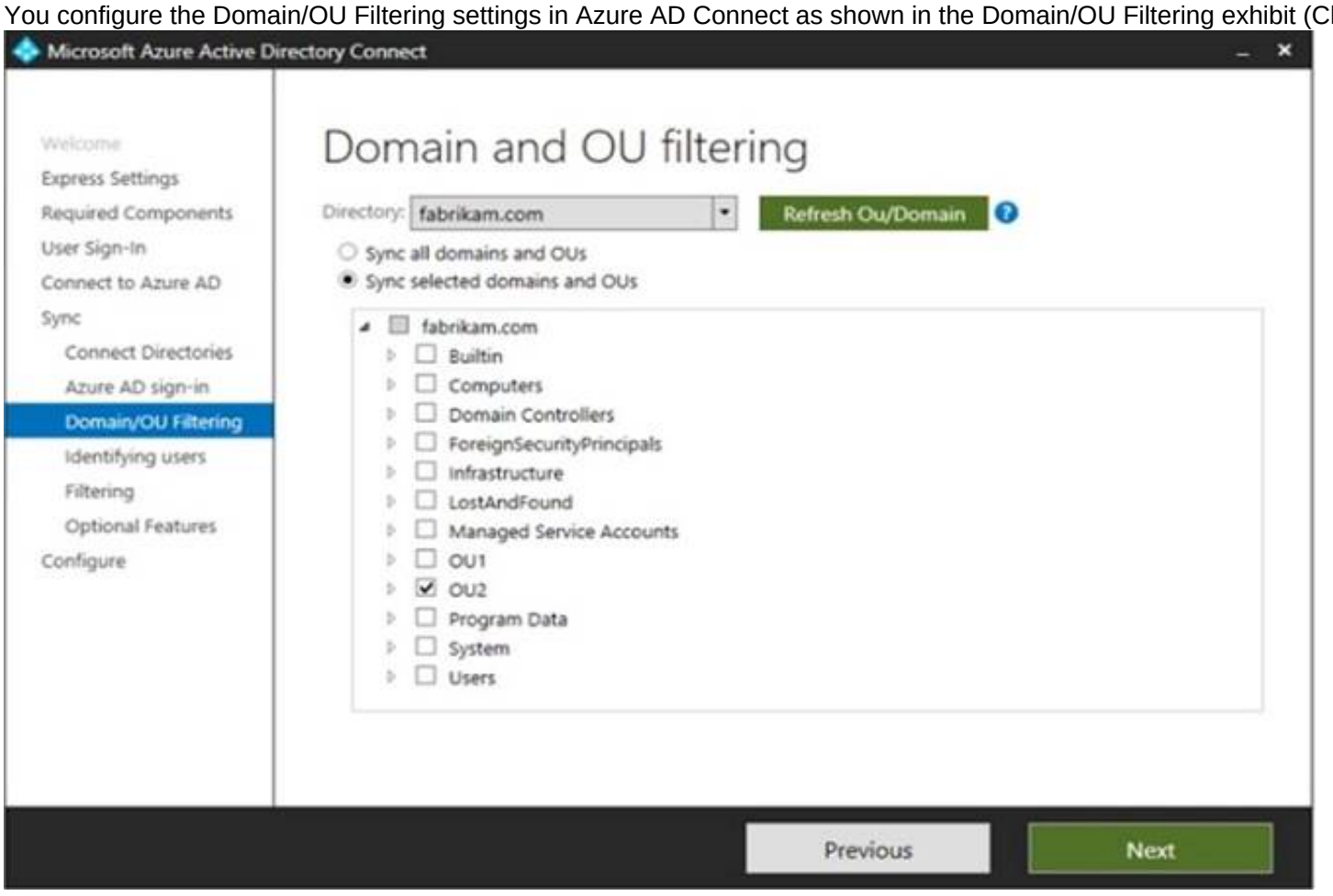
NEW QUESTION 42
HOTSPOT - (Topic 6)
HOTSPOT
Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

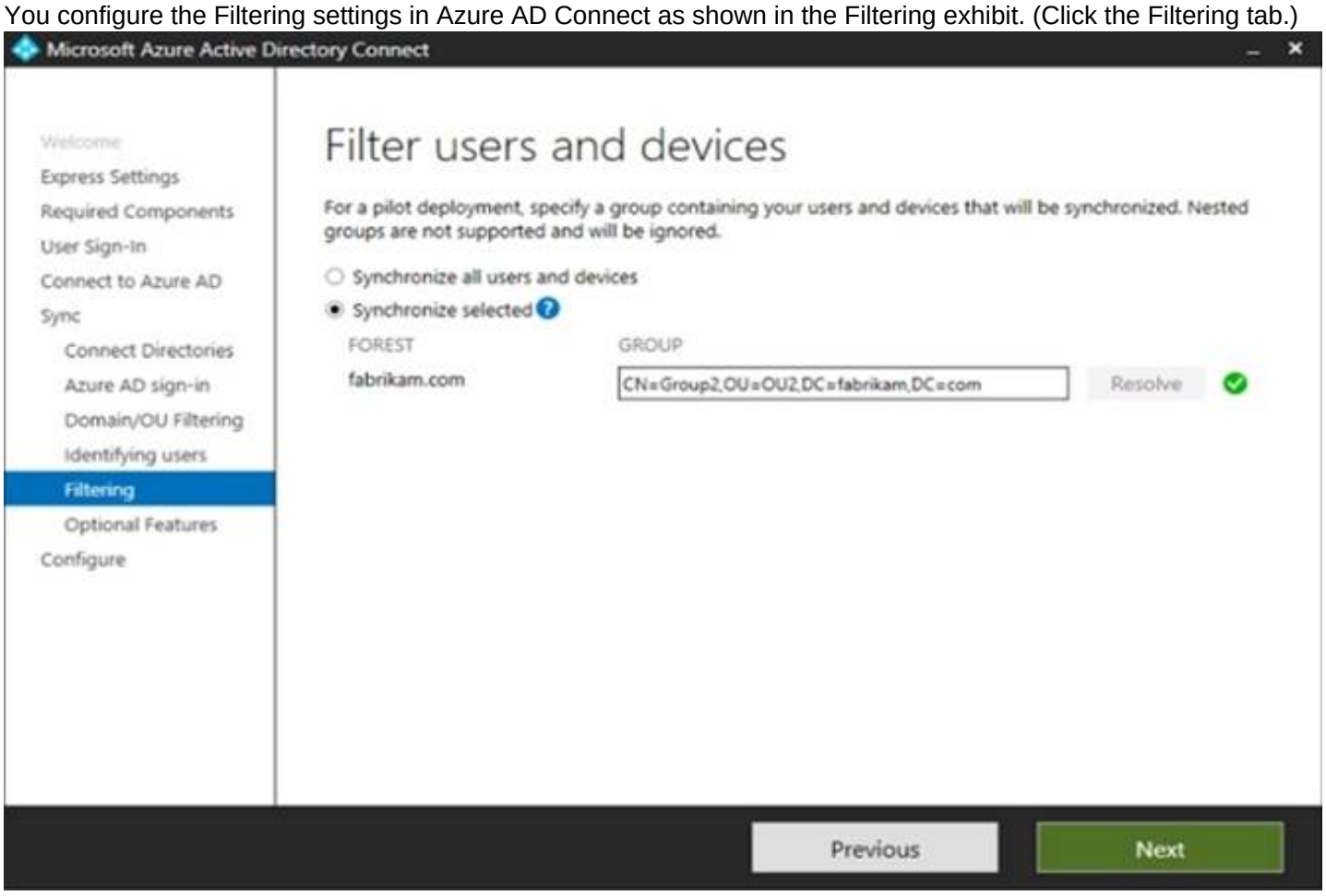
The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.
You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)



You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)



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

Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	○	○
Group2 will synchronize to Azure AD.	○	○
User3 will synchronize to Azure AD.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.
User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD.
Box 2: Yes
Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.
Box 3: Yes
User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD.

NEW QUESTION 47
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 48
- (Topic 6)
You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.
Devices are onboarded by using Microsoft Defender for Endpoint.
You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.
What should you create first?

A. a device configuration policy
B. a device compliance policy
C. a conditional access policy
D. an endpoint detection and response policy

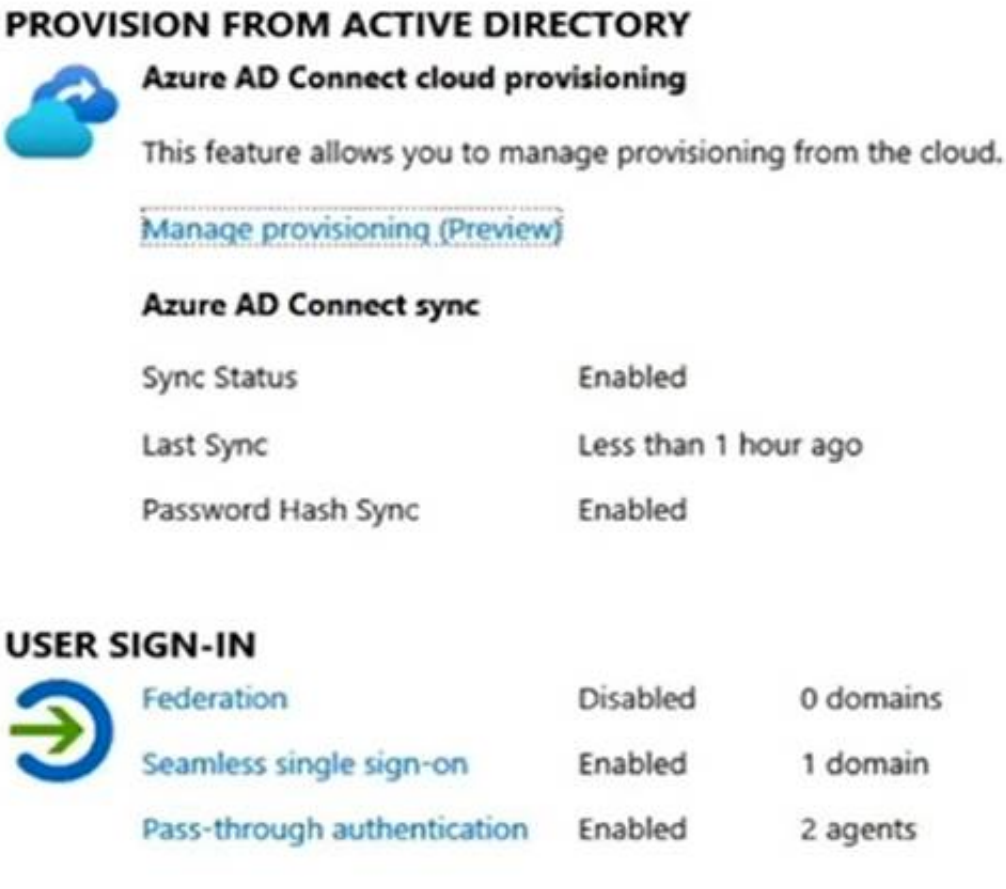
Answer: B

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

NEW QUESTION 52
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet the goal?

A. Yes
B. No

Answer: A

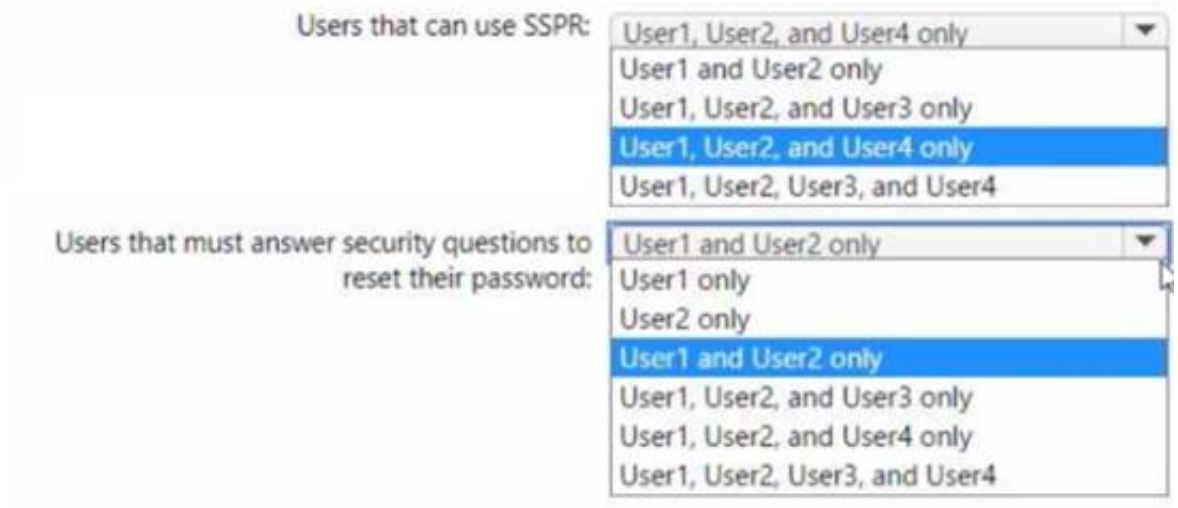
Explanation:
The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

NEW QUESTION 55
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.

Answer Area

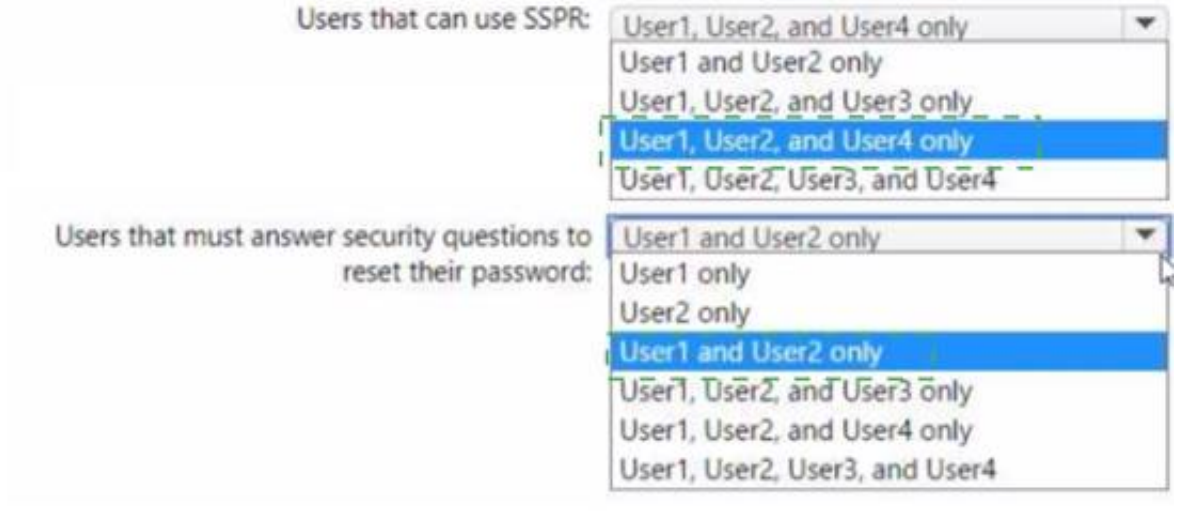


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 60
- (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 64
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it as a result, these questions will not appear in the review screen.

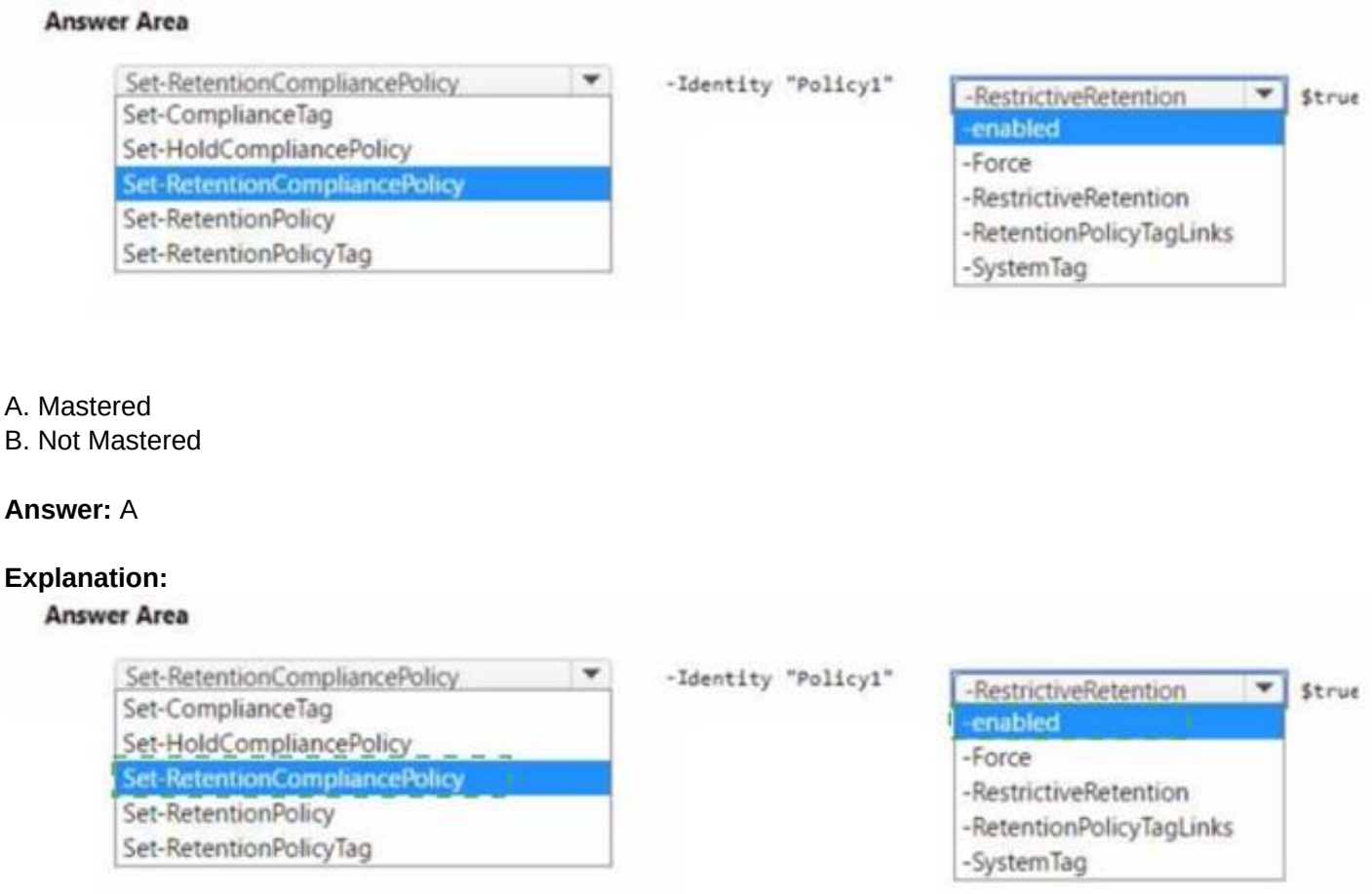
Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the filtering settings.
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 66
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 70
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.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Opening files in SharePoint that contain malicious content: Safe Attachments

Impersonation and spoofing attacks in email messages: Anti-Phishing

NEW QUESTION 71
- (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 74
HOTSPOT - (Topic 6)
Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Member
1	Group1	Name starts with Comp
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped devices (default)	Not applicable

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

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer! and Computed members? To answer, select the appropriate options in The answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Computer1: Group1 only

Computer2: Group1 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 75
- (Topic 6)
You have a Microsoft 365 subscription.
You plan to implement Microsoft Purview Privileged Access Management. Which Microsoft Office 365 workloads support privileged access?

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

Answer: A

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

NEW QUESTION 78
- (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

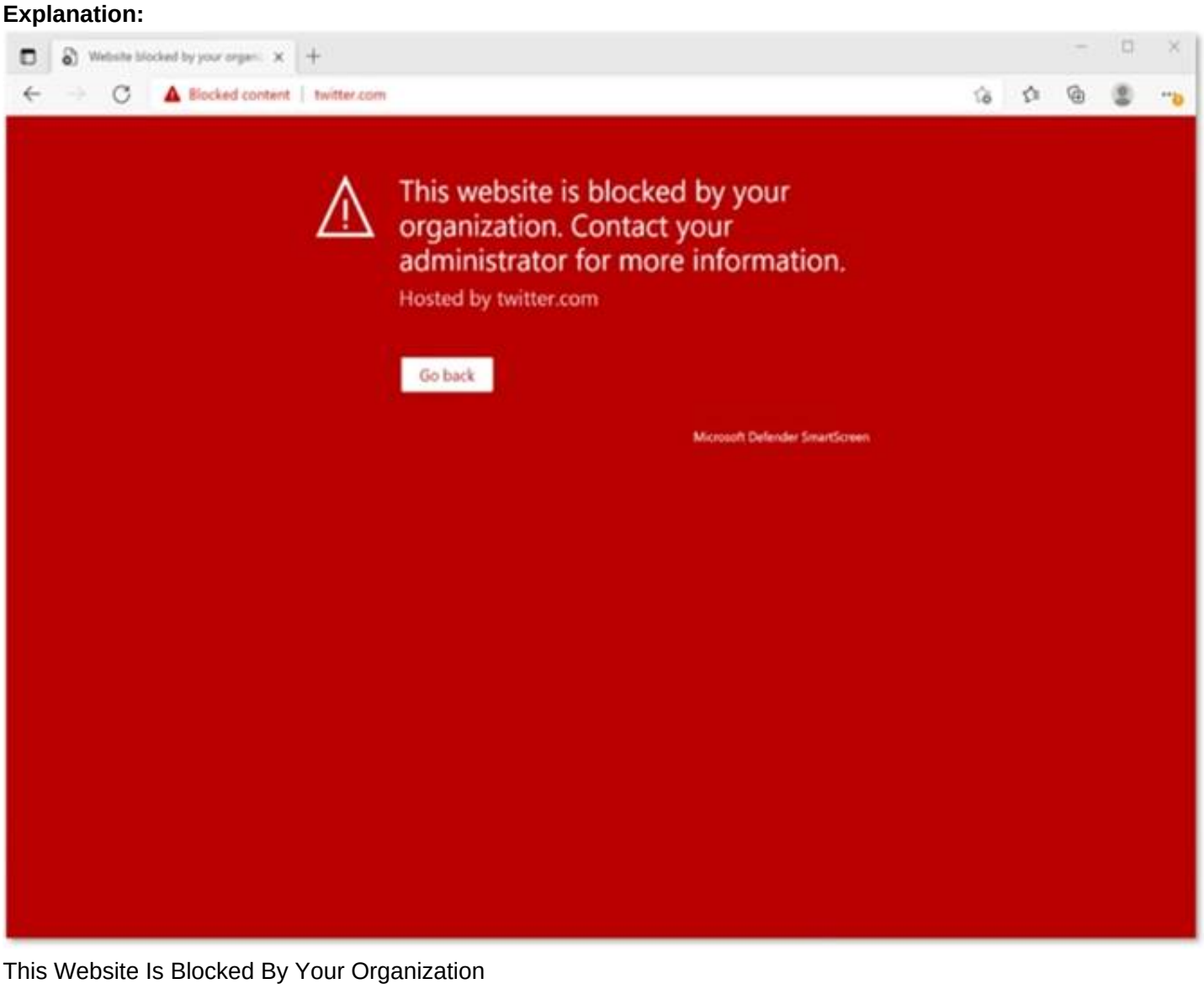
NEW QUESTION 82
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

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

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

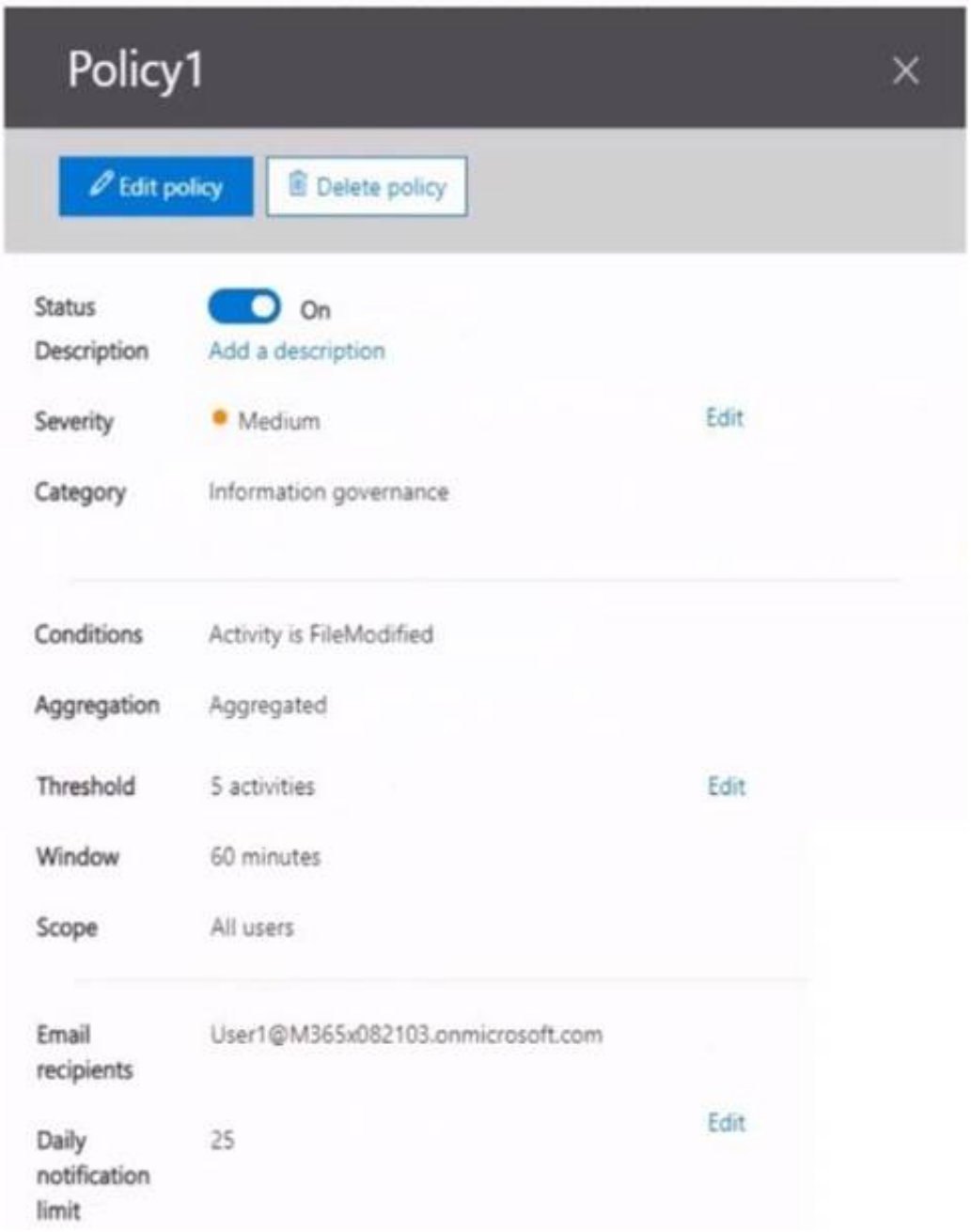
Answer: E

Explanation:



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

NEW QUESTION 86
- (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 87
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

At 08:00. you create an incident notification rule that has the following configurations:
• Name: Notification!
• Notification settings
o Notify on alert seventy: Low o Device group scope: All (3)
o Details: First notification per incident
• Recipients: Userl@contoso.com, User2@contoso.com
At 08:02. you create an incident notification rule that has the following configurations:
• Name: Notification
• Notification settings
o Notify on alert severity: Low. Medium
o Device group scope: DevtceGroup1, DeviceGroup2
• Recipients: Userl@contoso.com
in Microsoft 365 Defender, alerts are logged as shown in the following table.

Time	Alert name	Severity	Impacted assets
08:05	Activity1	Low	Device1
08:07	Activity1	Low	Device1
08:08	Activity1	Medium	Device1
08:15	Activity2	Medium	Device2
08:16	Activity2	Medium	Device2
08:20	Activity1	High	Device1
08:30	Activity3	Medium	Device2
08:35	Activity2	High	Device2

For each of the following statements, select Yes if the statement is true. Otherwise, select No1.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	○	○
User2@contoso.com will receive an incident notification email for the alert at 08:07.	○	○
User1@contoso.com will receive an incident notification email for the alert at 08:20.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	○	○
User2@contoso.com will receive an incident notification email for the alert at 08:07.	○	○
User1@contoso.com will receive an incident notification email for the alert at 08:20.	○	○

NEW QUESTION 90
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:
? Scope type: Directory
? Selected members: Group1
? Assignment type: Active
? Assignment starts: Mar 15, 2023
? Assignment ends: Aug 15, 2023
You add the following assignment for the Exchange Administrator role:
? Scope type: Directory
? Selected members: Group2
? Assignment type: Eligible
? Assignment starts: Jun 15, 2023
? Assignment ends: Oct 15, 2023
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
On July 15, 2023, Admin1 can reset the password of a user.	○	○
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	○	○
On May 1, 2023, Admin3 can reset the password of a user.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
Admin1 is member of Group1.
The User Administrator role assignment has Group1 as a member. The assignment type: Active
July 15, 2023 is with the assignment period.
A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.
Box 2: No
Admin2 is member of Group2.
The Exchange Administrator role assignment has Group2 as a member. The assignment type: Eligible
June 20, 2023 is with the assignment period. The assignment must be approved.
Note: Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.
Box 3: Yes
Admin3 is member of Gropu1 and Group2.
The User Administrator role assignment has Group1 as a member. The assignment type: Active
May 1, 2023 is with the assignment period.

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

Name	Member of Microsoft 365 role group
Admin1	Content Explorer List viewer Content Explorer Content viewer
Admin2	Security Administrator Content Explorer List Viewer

You have labels in Microsoft 365 as shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

The content in Microsoft 365 is assigned labels as shown in the following table.

Name	Type	Label
File1	File in SharePoint Online	Label1
Mail1	Email message in Exchange Online	Label2

You have labels In Microsoft 365 as shown in the following table.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

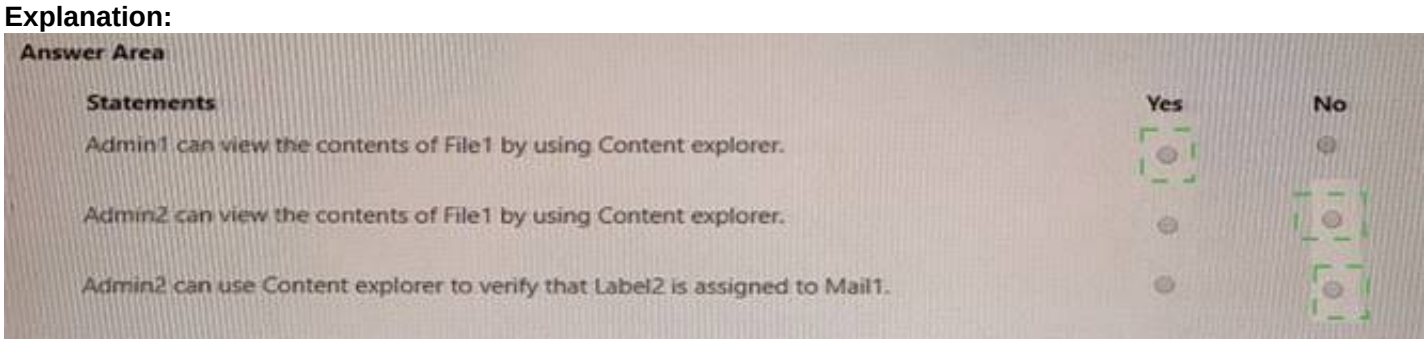
Answer Area

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	○	○
Admin2 can view the contents of File1 by using Content explorer.	○	○
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 96
- (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

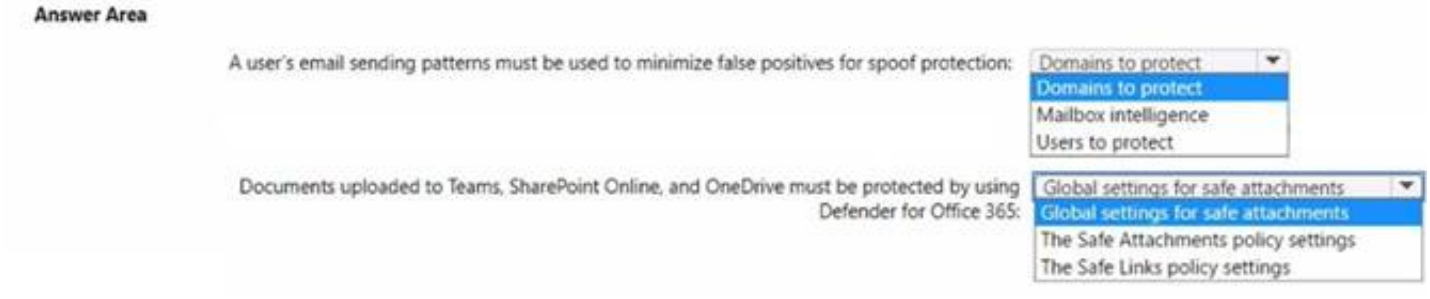
NEW QUESTION 101
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.
From Azure AD Identity Protection, you enable a sign-in risk policy.
Users report that when they use the VDI solution, 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

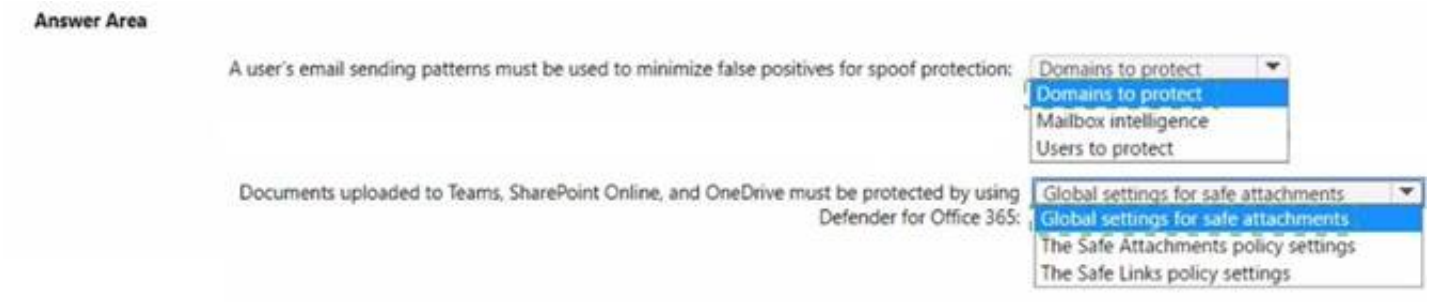
NEW QUESTION 106
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to configure Microsoft Defender for Office 365 to meet the following requirements:
• A user's email sending patterns must be used to minimize false positives for spoof protection.
• Documents uploaded to Microsoft 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 111
- (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 114
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.
You deploy a third-party antivirus solution to the devices.
You need to ensure that the devices are marked as compliant.
Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

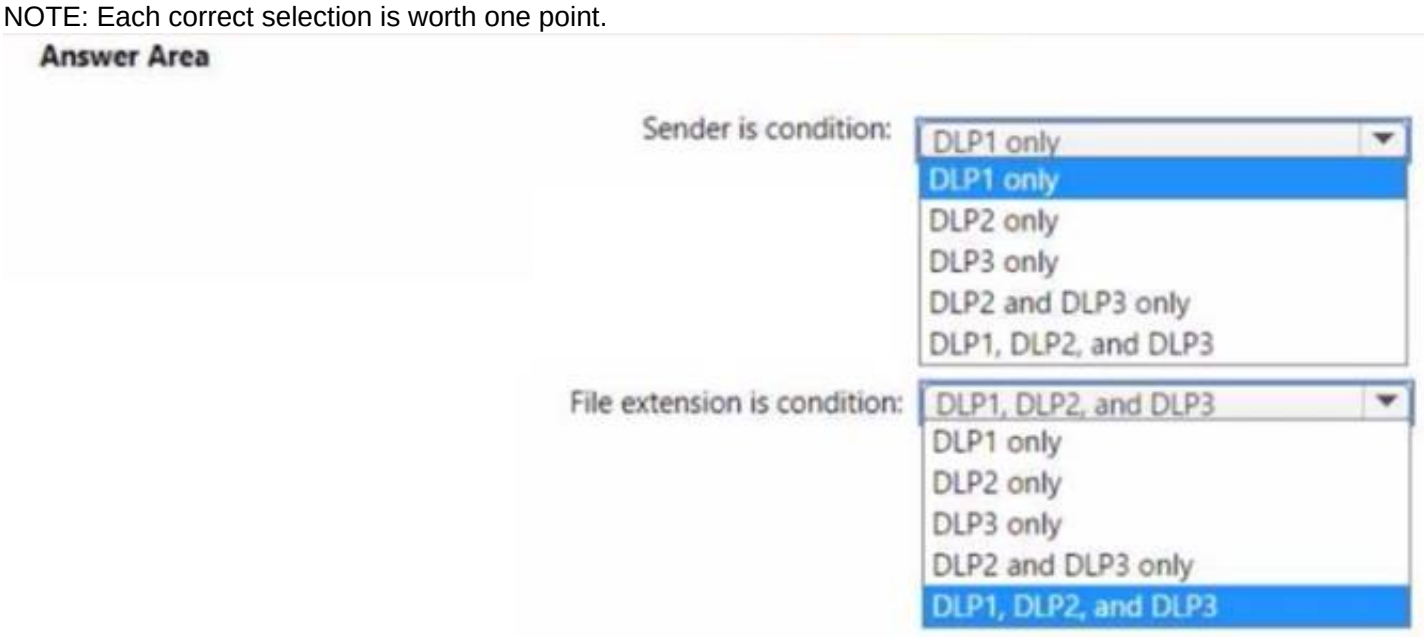
Explanation:

Answer Area

NEW QUESTION 116
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

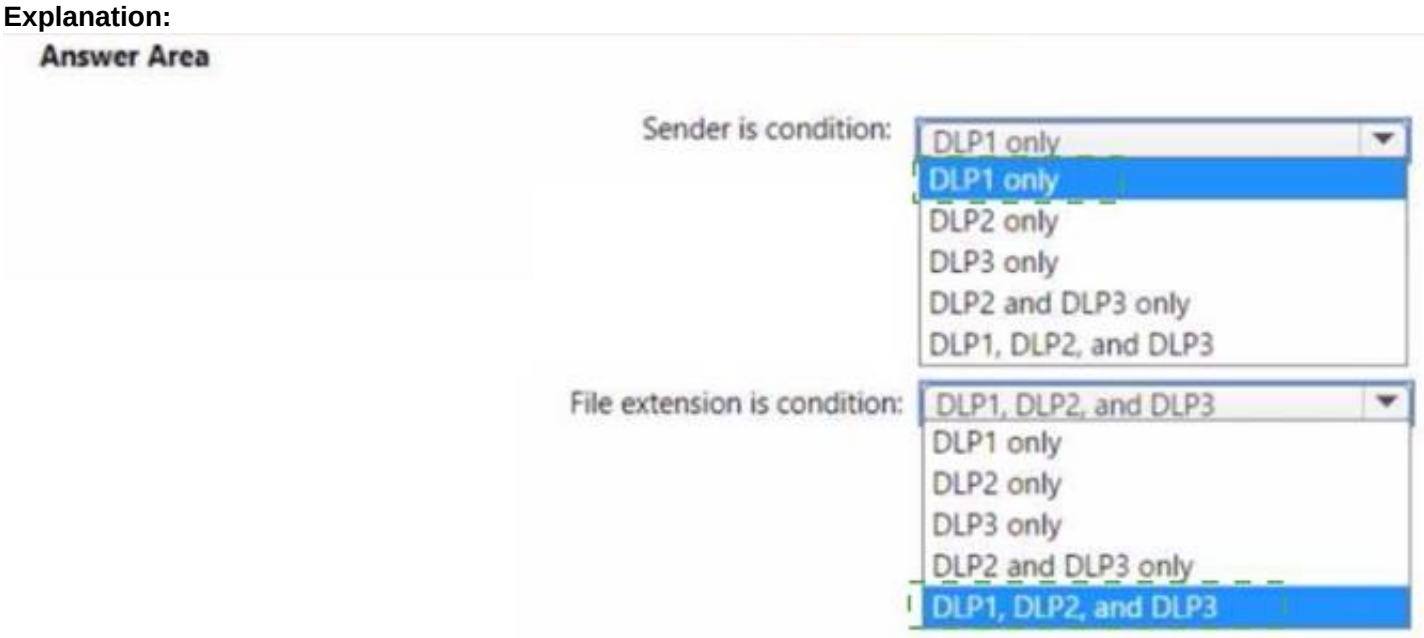
You need to create DLP rules for each policy.
Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



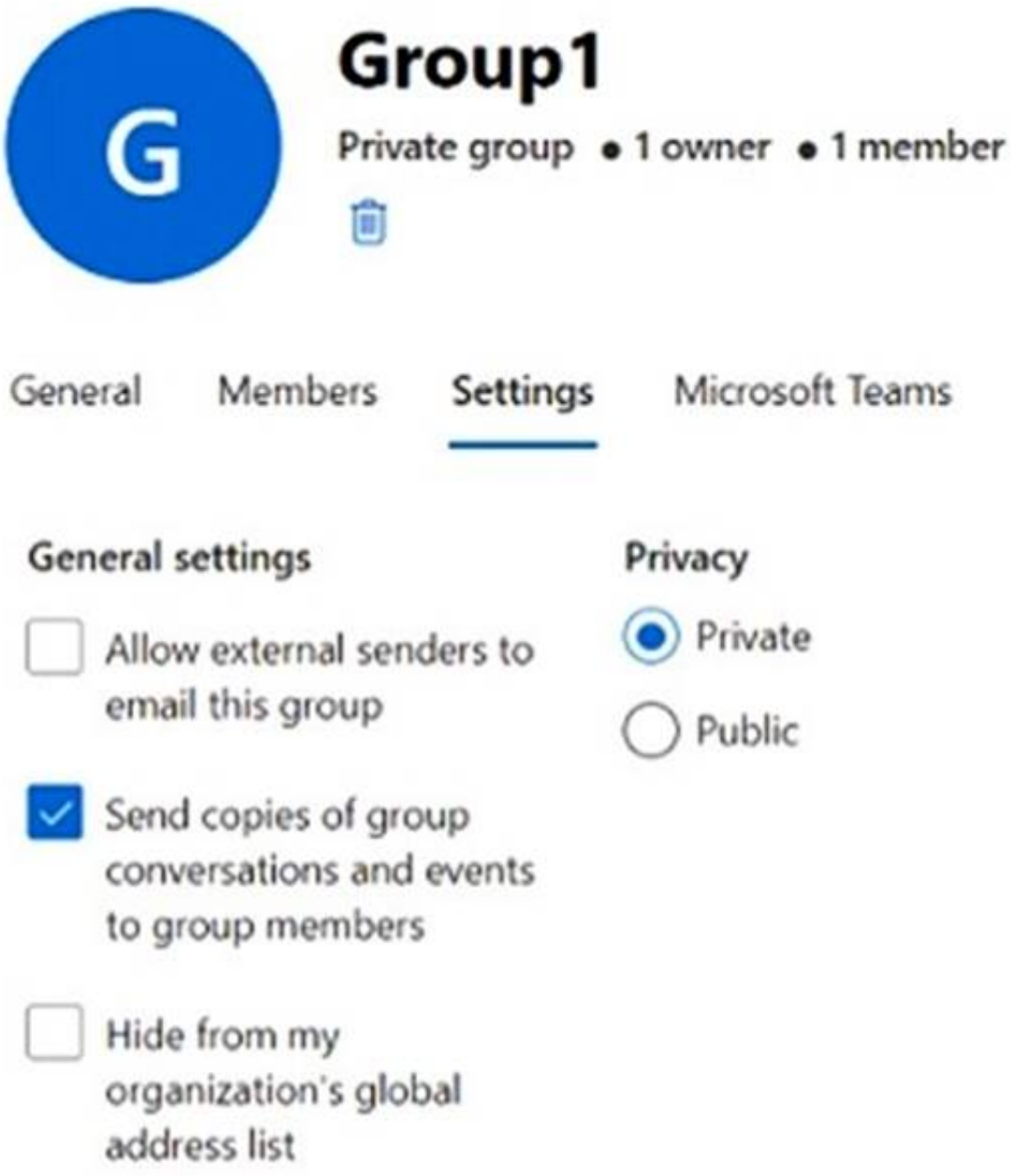
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 121
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



An external user named User1 has an email address of user1@outlook.com. You need to add User1 to Group1.
What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Action:
- Add User1 to the subscription as an active user.
- For Group1, change the Privacy setting to Public.
- For Group1, select Allow external senders to email this group.
- Invite User1 to collaborate with your organization as a guest.

Portal:
- The Microsoft Entra admin center
- The Exchange admin center
- The Microsoft 365 admin center
- The Microsoft Purview compliance portal

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Invite User1 to collaborate with your organization as a guest.
To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.
Navigate with your Web browser to https://admin.microsoft.com. On the left pane, click on “Users”, then click “Guest Users”.
On the “Guest Users” page, to create a new guest user, click on either the “Add a guest user” link on the top of the page or click on “Go to Azure Active Directory to add guest users” link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at https://aad.portal.azure.com.
On the “New user” page in the Microsoft Azure portal, you must choose to either “Create user” or “Invite user”. If you choose the “Create user” option, this will create a new user in your organization, which will have a login address with format username@tenantdomain,dot,com. If you choose the “Invite user” option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the “Invite user” option.
Box 2: The Microsoft Entra admin center
Microsoft Entra admin center unites Azure AD with family of identity and access products
Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.

Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).

NEW QUESTION 124
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

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

You create a retention label named Label 1 that has the following configurations:
• Retains content for five years
• Automatically deletes all content that is older than five years
You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:
• Applies to content that contains the word Merger
• Specifies the OneDrive accounts and SharePoint sites locations You run the following command.
Set-RetentionConpliancePolicy Policy1 -RestrictiveRetention Strue -Force
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 128
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.

Answer Area

Start-ADSyncSyncCycle -PolicyType Delta

Start-ADSyncSyncCycle
Set-ADSyncScheduler
Invoke-ADSyncRunProfile

Delta
Initial
Full

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 132
- (Topic 6)
You have a new Microsoft 365 E5 tenant.
You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.
What should you do first?

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

Answer: A

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

NEW QUESTION 134
- (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 135
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.	○	○

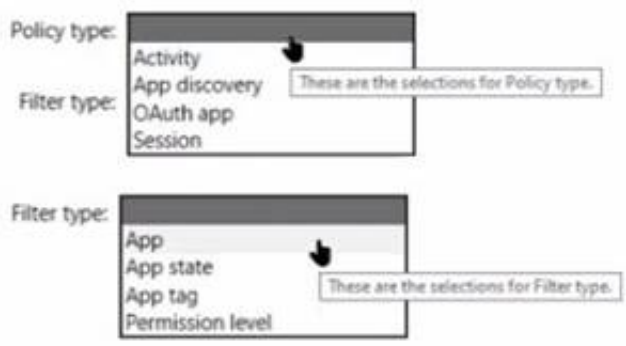
NEW QUESTION 138
- (Topic 6)
Your company has three main offices and one branch office. The branch office is used for research.
The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.
You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.
What should you include in the recommendation?

A. Azure AD password protection
B. a Microsoft Intune device configuration profile
C. a Microsoft Intune device compliance policy
D. Azure AD conditional access

Answer: D

NEW QUESTION 140
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to create a policy that will generate an email alert when a banned app is detected requesting permission to access user information or data in the subscription.
What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

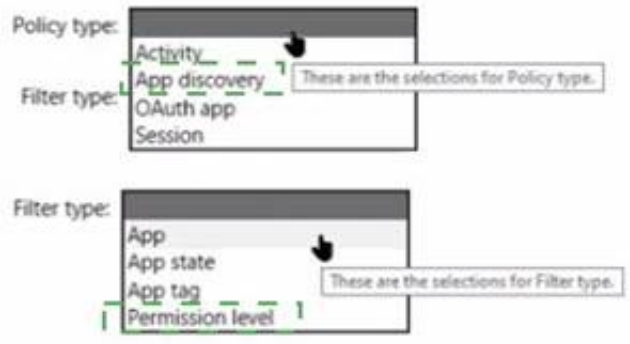


A. Mastered
B. Not Mastered

Answer: A

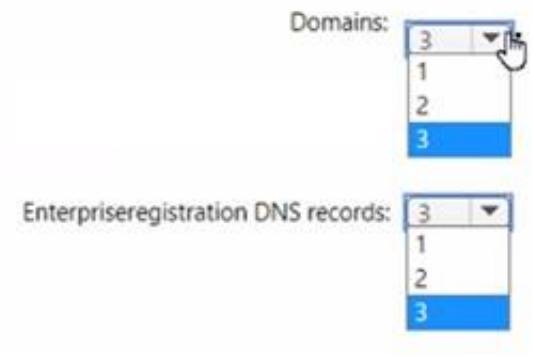
Explanation:

Answer Area



NEW QUESTION 143
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.

Answer Area

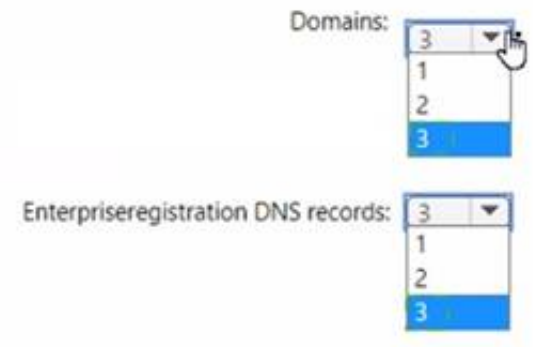


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

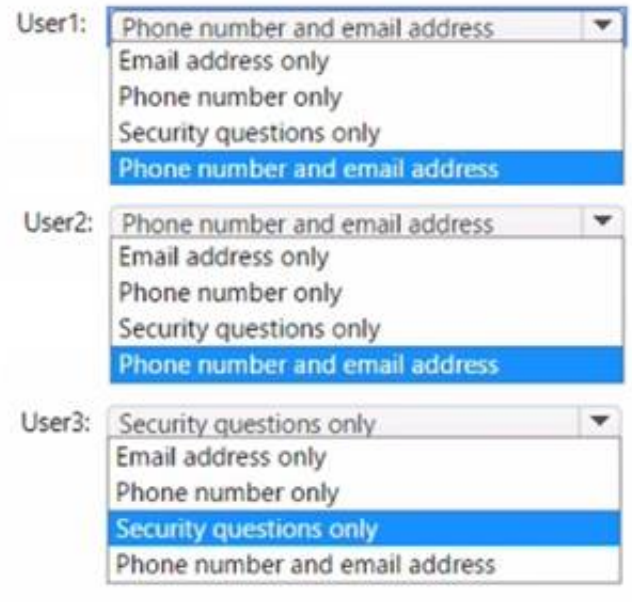


NEW QUESTION 145
HOTSPOT - (Topic 6)
You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	*None*

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.
What information must be configured for each user before the user can perform a self- service password reset? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

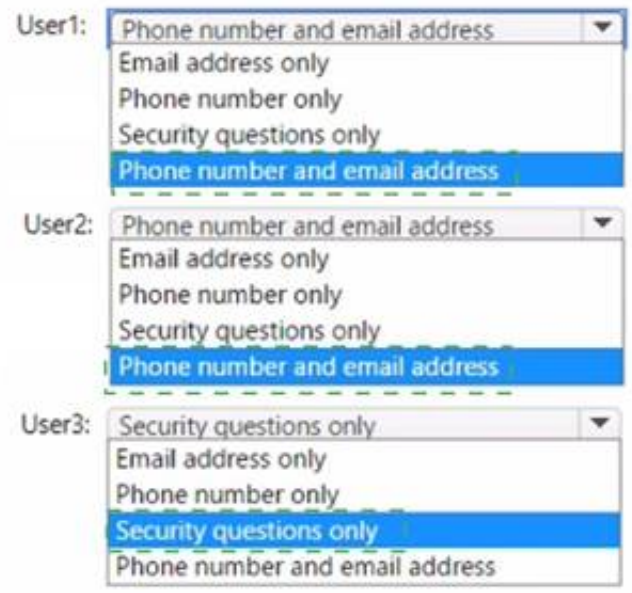


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

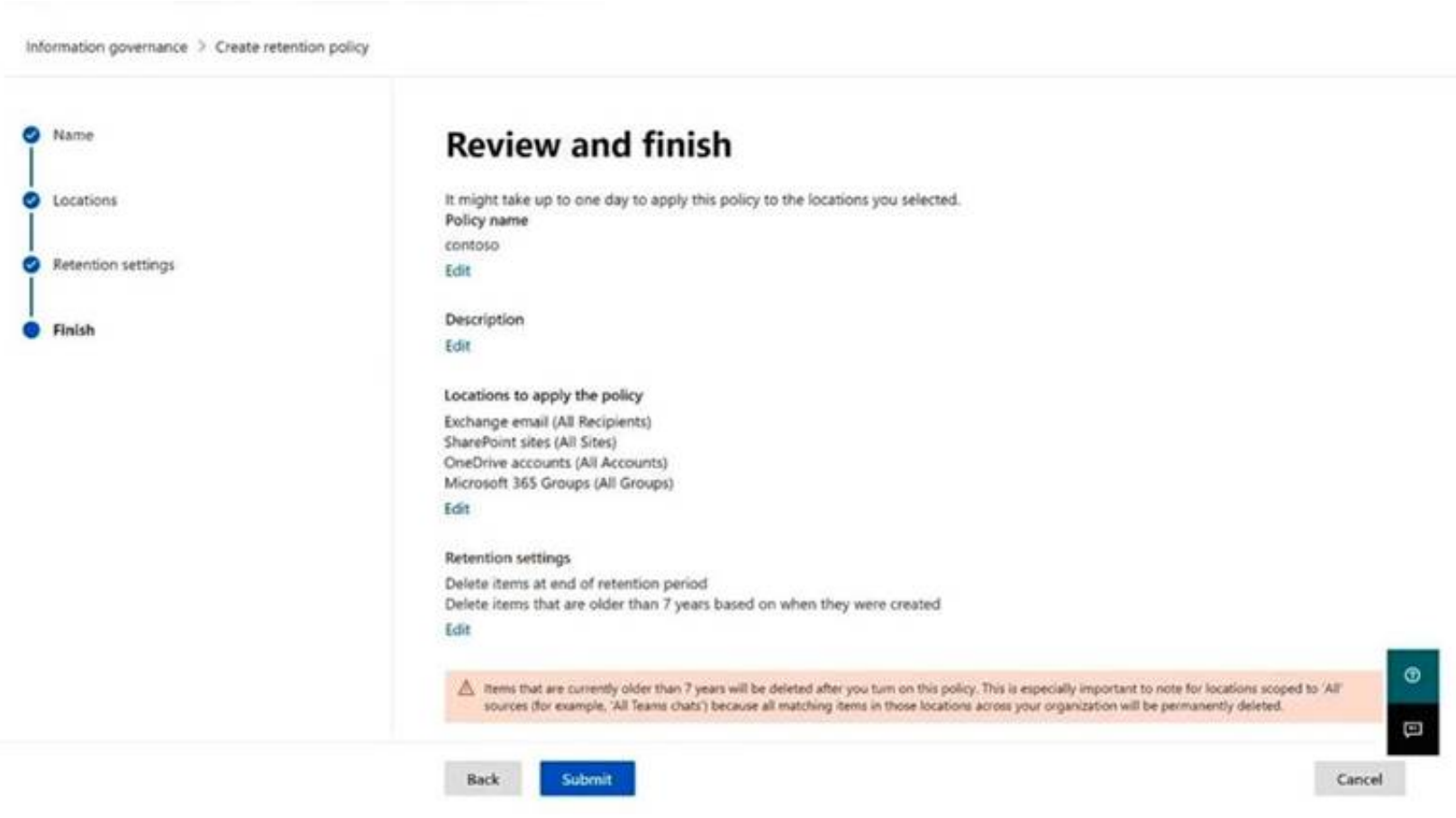


NEW QUESTION 149
- (Topic 6)
You purchase a new computer that has Windows 10, version 21H1 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

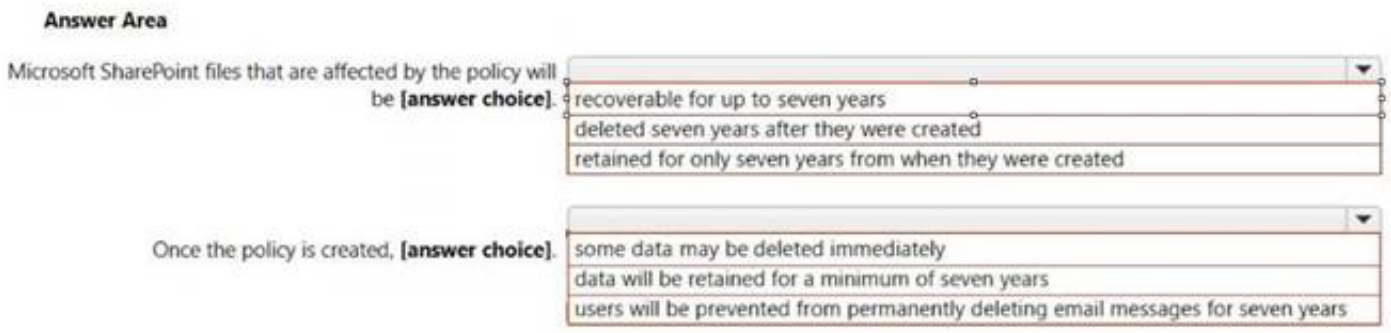
A. Install all the feature updates released since version 21H1 and the latest quality update only.
B. Install the latest feature update and all the quality updates released since version 21H1.
C. Install the latest feature update and the latest quality update only.
D. Install all the feature updates released since version 21H1 and all the quality updates released since version 21H1 only.

Answer: C

NEW QUESTION 150
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.



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 151
HOTSPOT - (Topic 6)
You have device compliance policies shown in the following table.

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 156
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You need to review reports to identify the following:
• The storage usage of files stored in Microsoft Teams
• The number of active users per team
Which report should you review for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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

Report
- The device usage report in Teams
- The OneDrive usage report
- The SharePoint site usage report
- The Teams usage report in Teams
- The User activity report in Teams

Requirements
- The storage usage of files stored in Microsoft Teams: [ ]
- Number of active users per Microsoft Team: [ ]

A. Mastered
B. Not Mastered

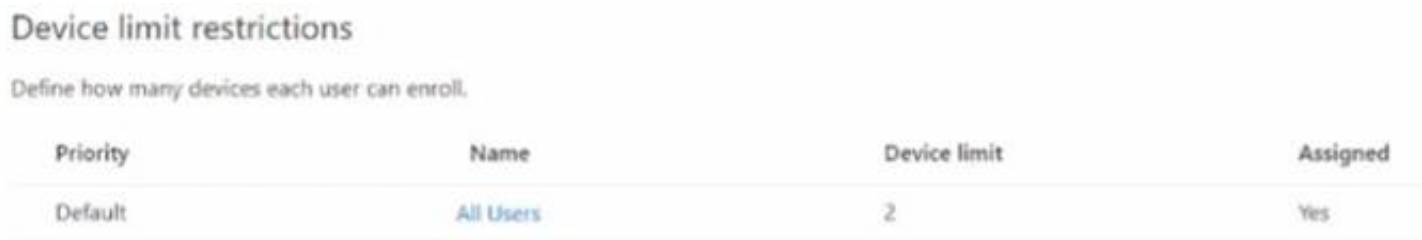
Answer: A

Explanation:

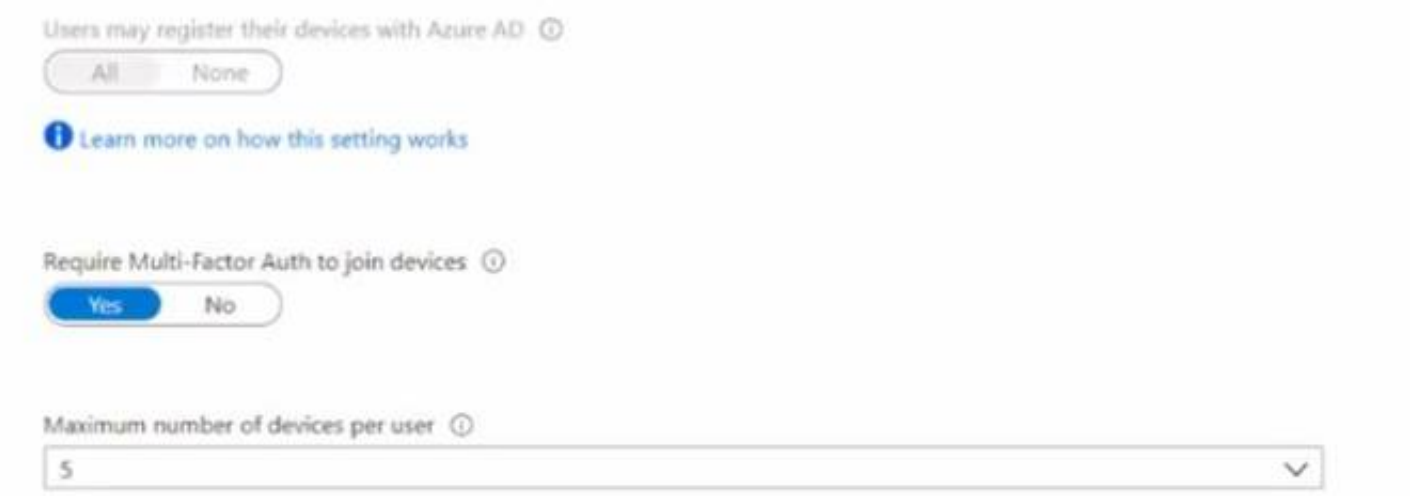
Report
- The device usage report in Teams
- The OneDrive usage report
- The SharePoint site usage report
- The Teams usage report in Teams
- The User activity report in Teams

Requirements
- The storage usage of files stored in Microsoft Teams: The SharePoint site usage report
- Number of active users per Microsoft Team: The Teams usage report in Teams

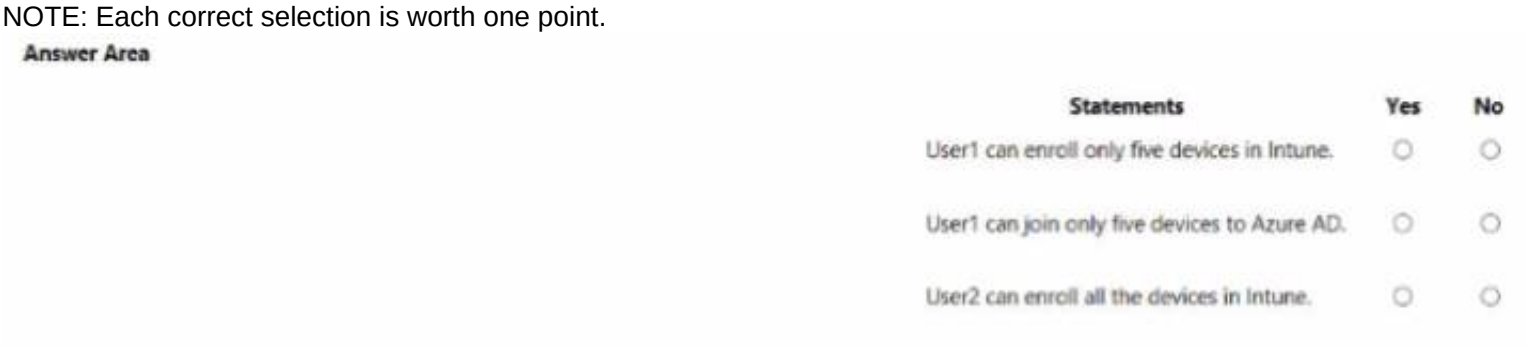
NEW QUESTION 159
HOTSPOT - (Topic 6)
You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.
In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.



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



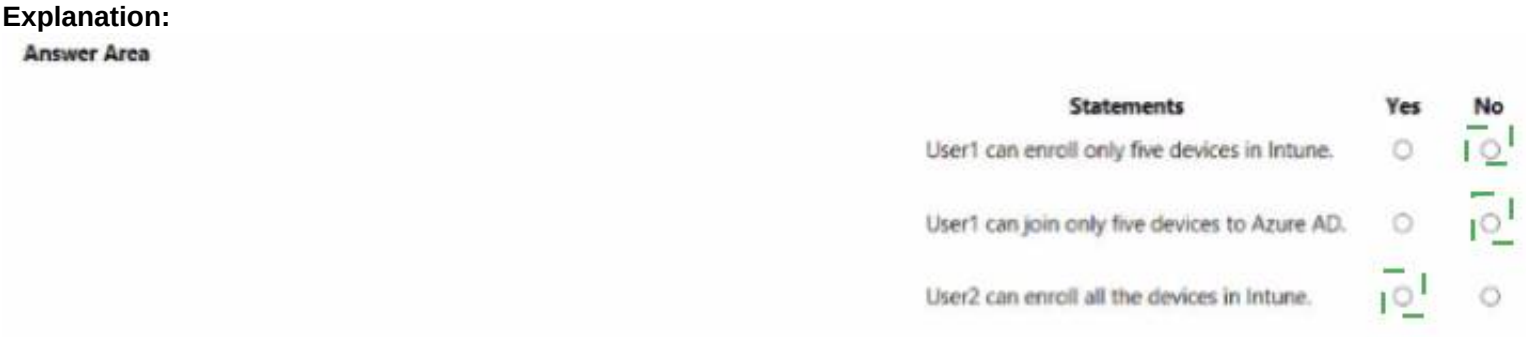
From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).
For each of the following statement, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 160
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.	O	O
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	O	O
App3 can be installed automatically for UserGroup1.	O	O

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 161
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.)

Review your settings and finish

Name
Sensitivity1

Display name
Sensitivity1

Description for users
Sensitivity1

Scope
File.Email

Encryption

Content marking
Watermark: Watermark
Header: Header

Auto-labeling

Group settings

Site settings

Auto-labeling for database columns
None

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

Auto-labeling policy

Edit Policy | Delete Policy

Policy name
Auto-labeling policy

Description

Label in simulation
Sensitivity1

Info to label
IP Address

Apply to content in these locations
Exchange email All

Rules for auto-applying this label
Exchange email 1 rule

Mode
On

Comment

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 162
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains the administrative units shown in the following table.

Name	Members
AU1	Group1, User2
AU2	Group2, User3, User4

The groups contain the members shown in the following table.

Name	Members
Group1	User1
Group2	User2, User4

The users are assigned the roles shown in the following table.

Name	Role	Scope
User1	*None*	*Not applicable*
User2	Password Administrator	AU1
User3	License Administrator	Organization
User4	*None*	*Not applicable*

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

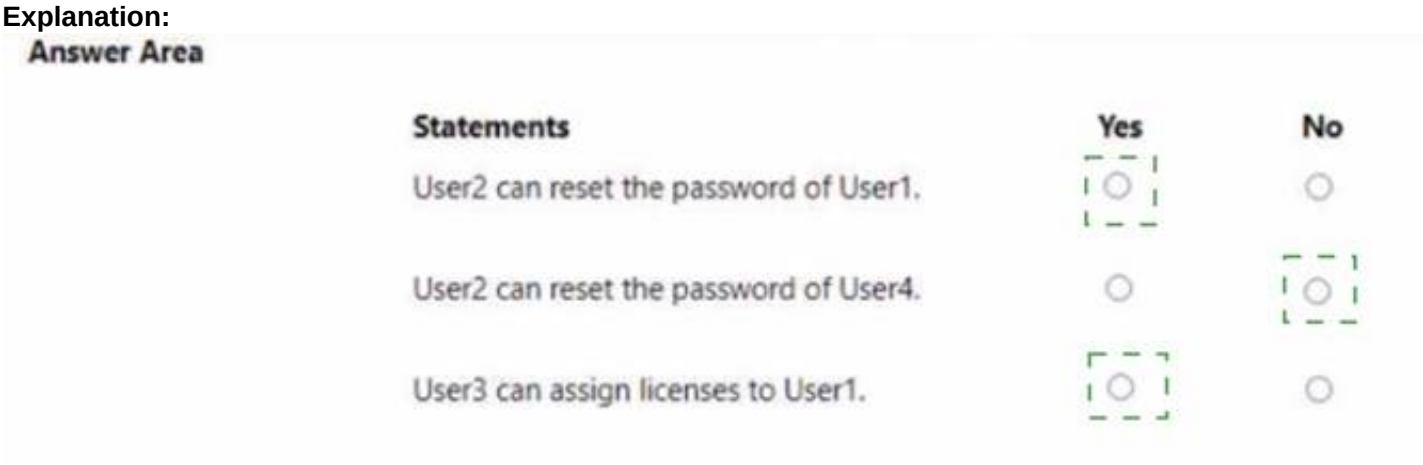
Answer Area

Statements	Yes	No
User2 can reset the password of User1.	○	○
User2 can reset the password of User4.	○	○
User3 can assign licenses to User1.	○	○

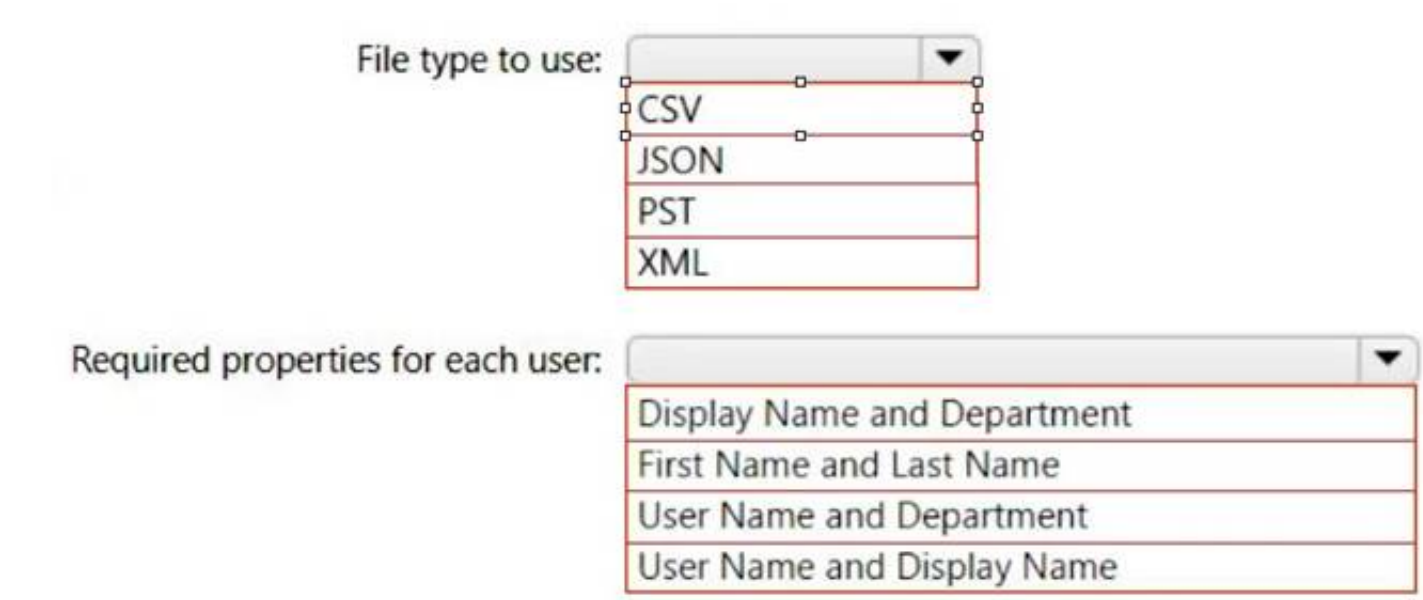
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 163
HOTSPOT - (Topic 6)
HOTSPOT
Your company uses a legacy on-premises LDAP directory that contains 100 users. The company purchases a Microsoft 365 subscription.
You need to import the 100 users into Microsoft 365 by using the Microsoft 365 admin center.
Which type of file should you use and which properties are required? 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: CSV
Add multiple users in the Microsoft 365 admin center
? Sign in to Microsoft 365 with your work or school account.
? In the admin center, choose Users > Active users.
? Select Add multiple users.
? On the Import multiple users panel, you can optionally download a sample CSV file with or without sample data filled in.
? Etc.
Note: More information about how to add users to Microsoft 365 Not sure what CSV format is?
A CSV file is a file with comma separated values. You can create or edit a file like this with any text editor or spreadsheet program, such as Excel.
Box 2: User Name and Display Name
What if I don't have all the information required for each user? The user name and display name are required, and you cannot add a new user without this information. If you don't have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.

NEW QUESTION 166
- (Topic 5)
You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs.
What should you do?

A. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.
B. From PowerShell, run the Add-ADSyncConnectorAttnbuteinclusion cmdlet.
C. From PowerShell, run the start-ADSyncSyncCycle cmdlet.
D. From the Microsoft Azure AD Connect wizard, select Manage federation.

Answer: A

NEW QUESTION 167
- (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 171
- (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

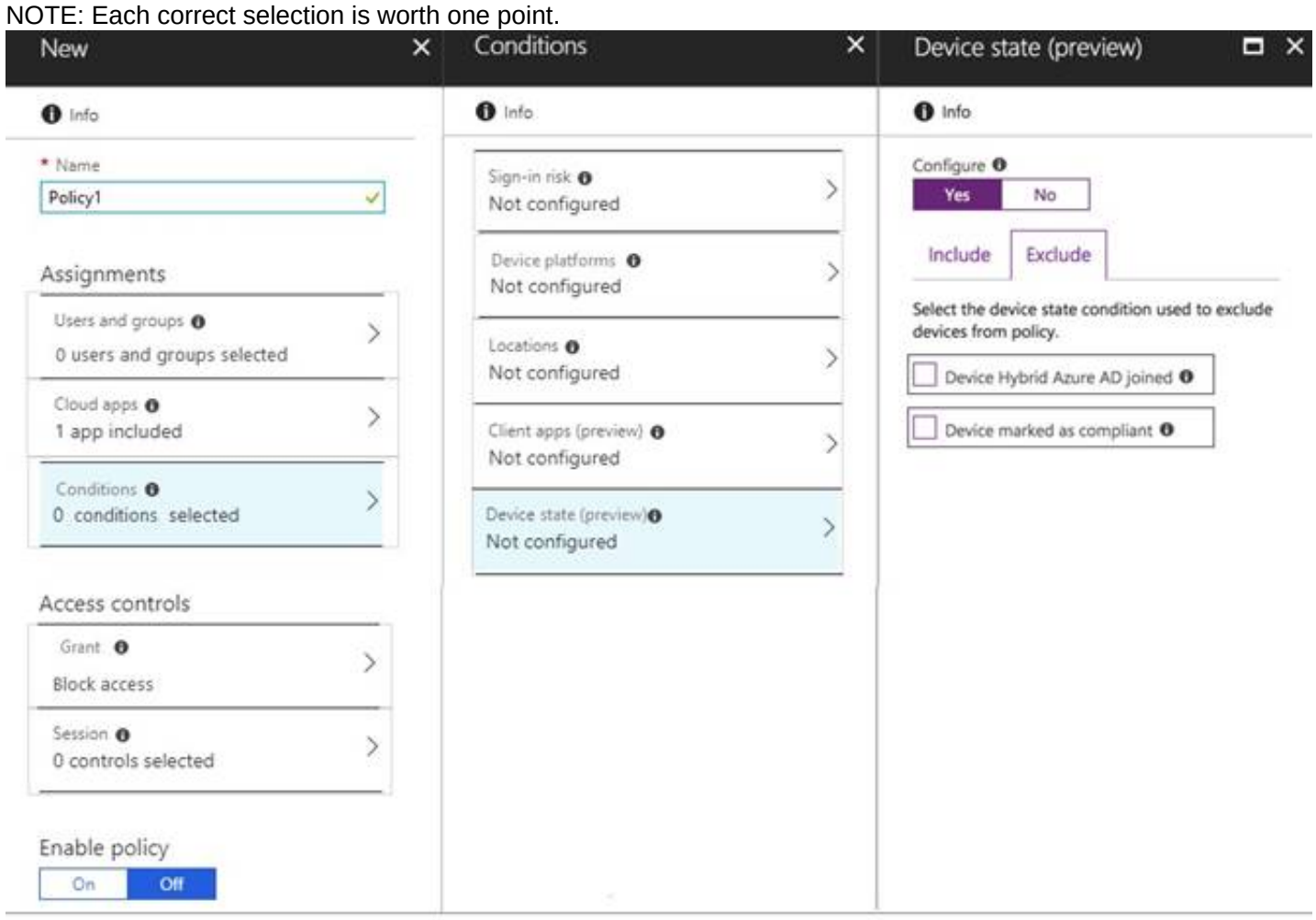
Explanation:
References:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for- business

NEW QUESTION 174
- (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 175
HOTSPOT - (Topic 1)
You need to configure a conditional access policy to meet the compliance requirements. You add Exchange Online as a cloud app.
Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 177
- (Topic 1)
You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?

A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator rote.
B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
C. From the Intune admin center, add User1 as a device enrollment manager.
D. From the Intune admin center, configure the Enrollment restrictions.

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

NEW QUESTION 179
- (Topic 1)
You need to meet the compliance requirements for the Windows 10 devices. What should you create from the Intune admin center?

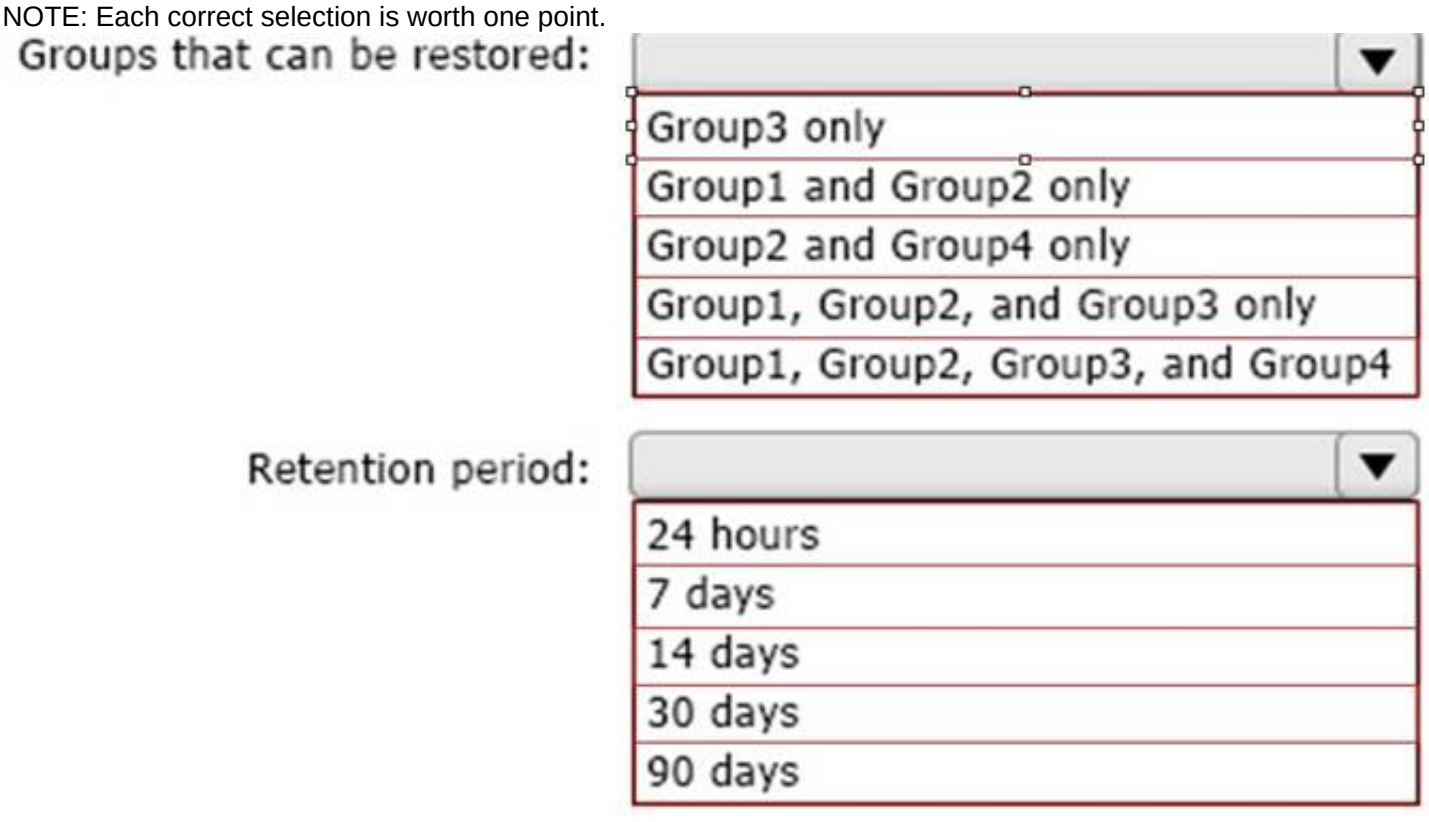
A. a device compliance policy
B. a device configuration profile
C. an application policy
D. an app configuration policy

Answer: C

NEW QUESTION 182
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.

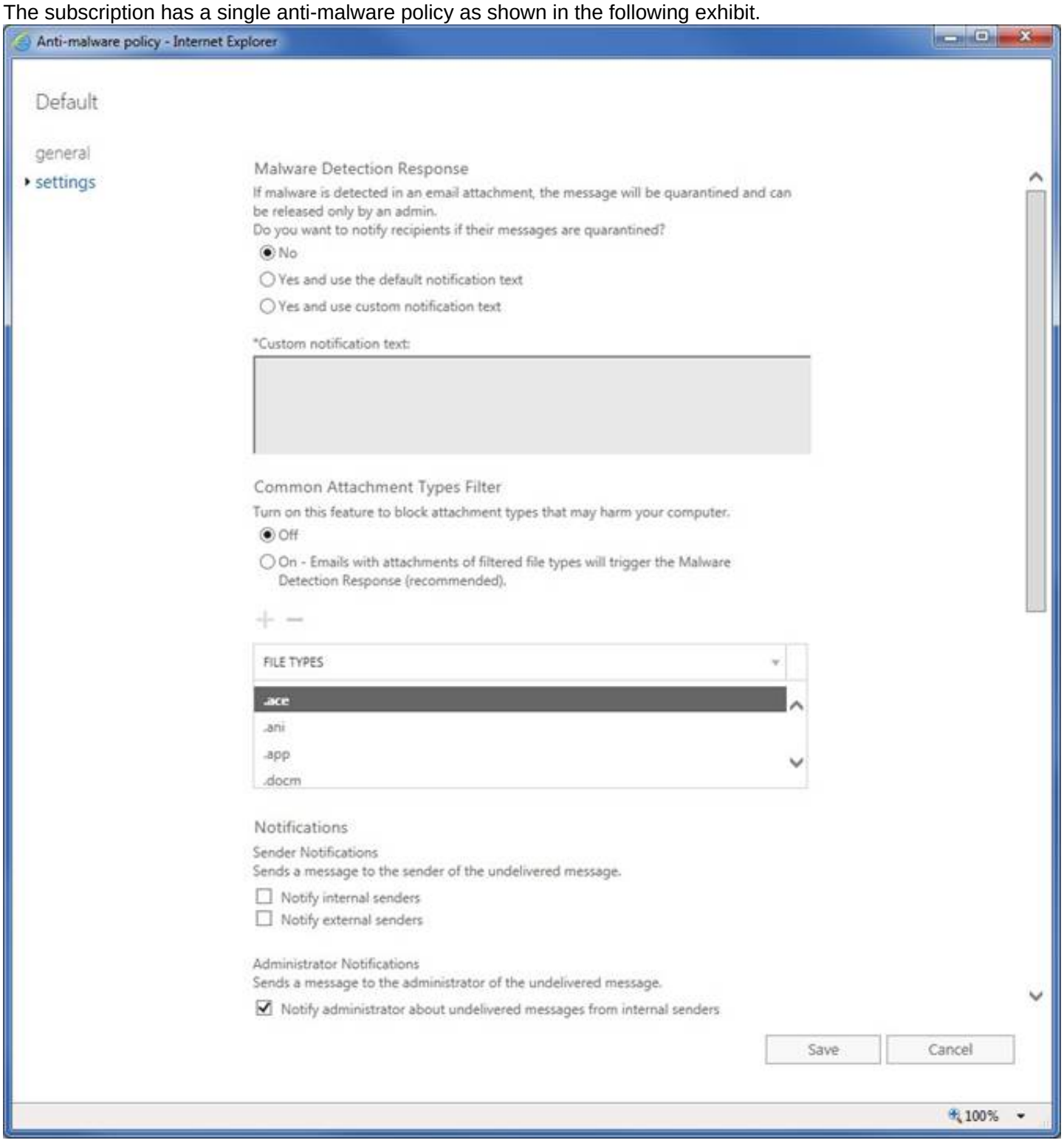


A. Mastered
B. Not Mastered

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 183
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1.
The subscription has a single anti-malware policy as shown in the following exhibit.



An email message that contains text and two attachments is sent to User1. One attachment is infected with malware.
How will the email message and the attachments be processed?

A. Both attachments will be remove
B. The email message will be quarantined, and Used will receive an email message without any attachments and an email message that includes the following text: 'Malware was removed.'
C. The email message will be quarantined, and the message will remain undelivered.
D. Both attachments will be remove
E. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: 'Malware was removed."
F. The malware-infected attachment will be remove
G. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies

NEW QUESTION 188
- (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 Defender for CloudUse the
B. Microsoft Purview
C. Azure Arc
D. Microsoft Defender for Identity

Answer: D

Explanation:

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

NEW QUESTION 190
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.
You need to export the existing template.
Which file format should you use for the exported template?

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

Answer: B

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

NEW QUESTION 194
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.

Username	Last activation date (UTC)	Last activity date (UTC)	Choose columns
431B8D0D1D05D877FDC4416			
2F2747649D4150B686307383			
659213C0E1D99EA1A4AD56D		Wednesday, August 3, 2022	
FE185622F642B0381DB633EC			
988D39ED225FC80FF2A5684			

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.
Answer Area

The Username column must display the actual name of each user: Reports in Org settings
- Privacy profile in Org settings
- Reports in Org settings
- The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed: Microsoft Teams in Org settings
- Microsoft Teams in Org settings
- The columns in the report
- The Teams license assignment

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

The Username column must display the actual name of each user: Reports in Org settings
- Privacy profile in Org settings
- Reports in Org settings
- The membership of the Reports Reader role

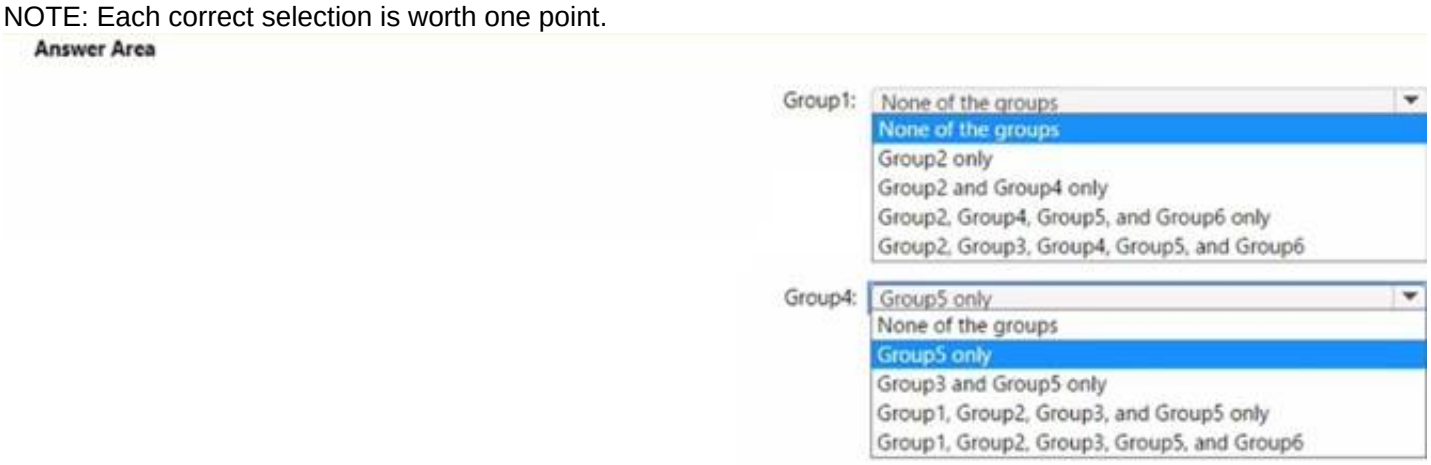
Usage of the Teams mobile app must be displayed: Microsoft Teams in Org settings
- Microsoft Teams in Org settings
- The columns in the report
- The Teams license assignment

NEW QUESTION 197
HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type	Security enabled	Role assignments allowed
Group1	Microsoft 365	No	No
Group2	Microsoft 365	No	No
Group3	Security	Yes	Yes
Group4	Security	Yes	No
Group5	Security	Yes	No
Group6	Distribution	No	No

Which groups can be members of Group1 and Group4? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

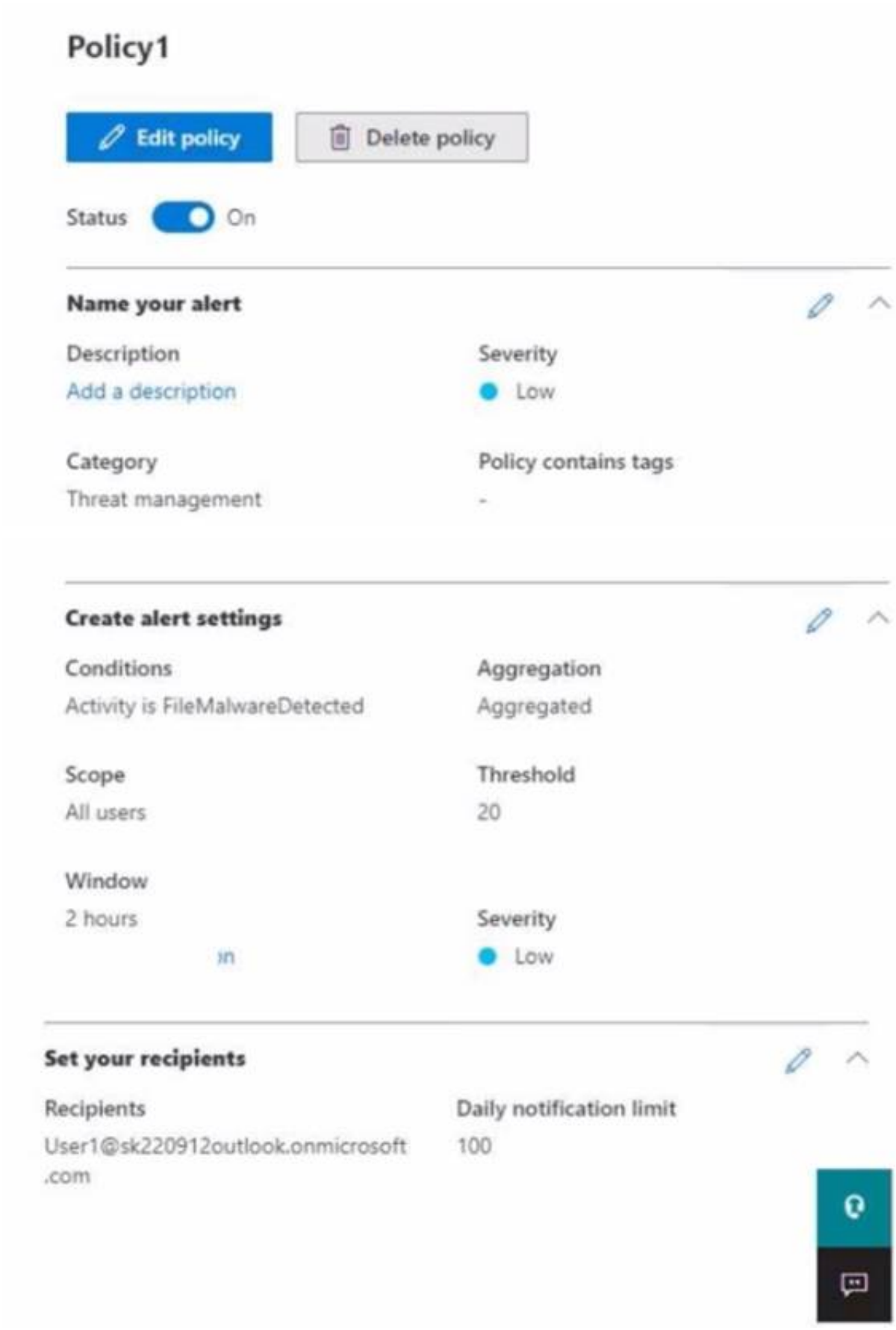


A. Mastered
B. Not Mastered

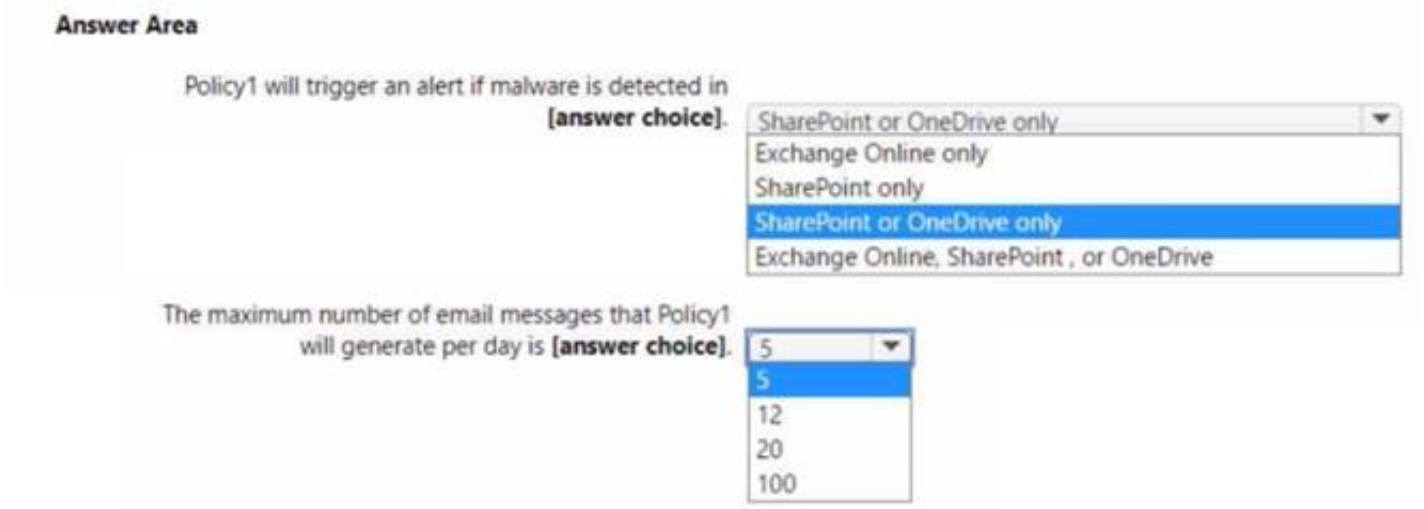
Answer: A

Explanation:

NEW QUESTION 198
HOTSPOT - (Topic 6)
You have Microsoft 365 subscription.
You create an alert policy as shown in the following exhibit.



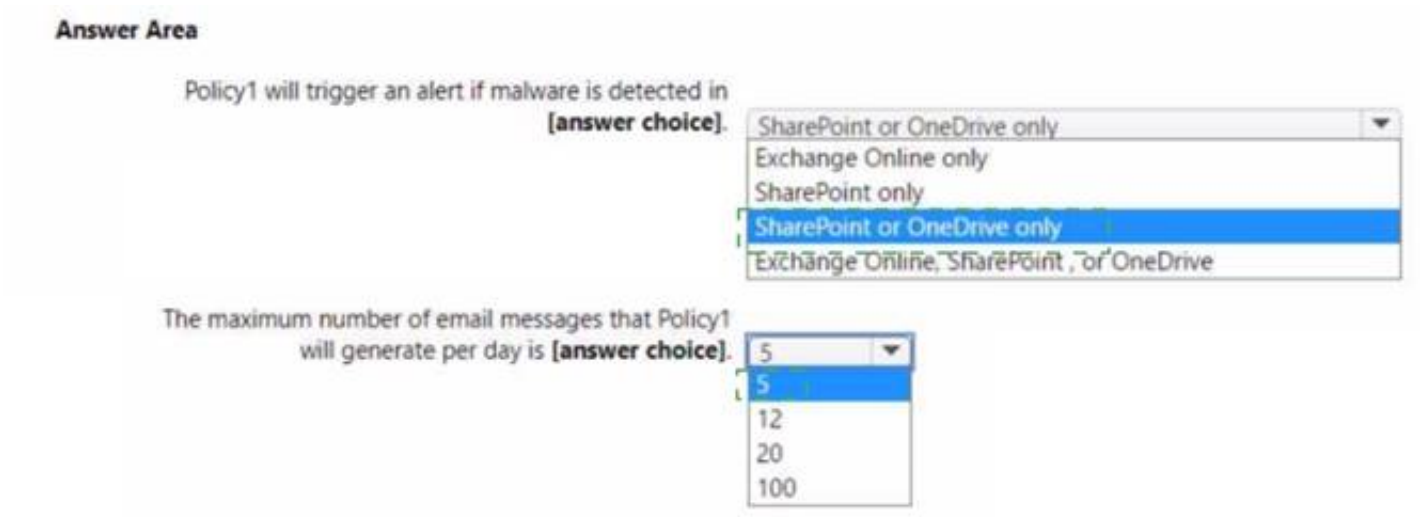
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 202
- (Topic 6)
Your company has an Azure AD tenant named contoso.com that includes the users shown in the following table.

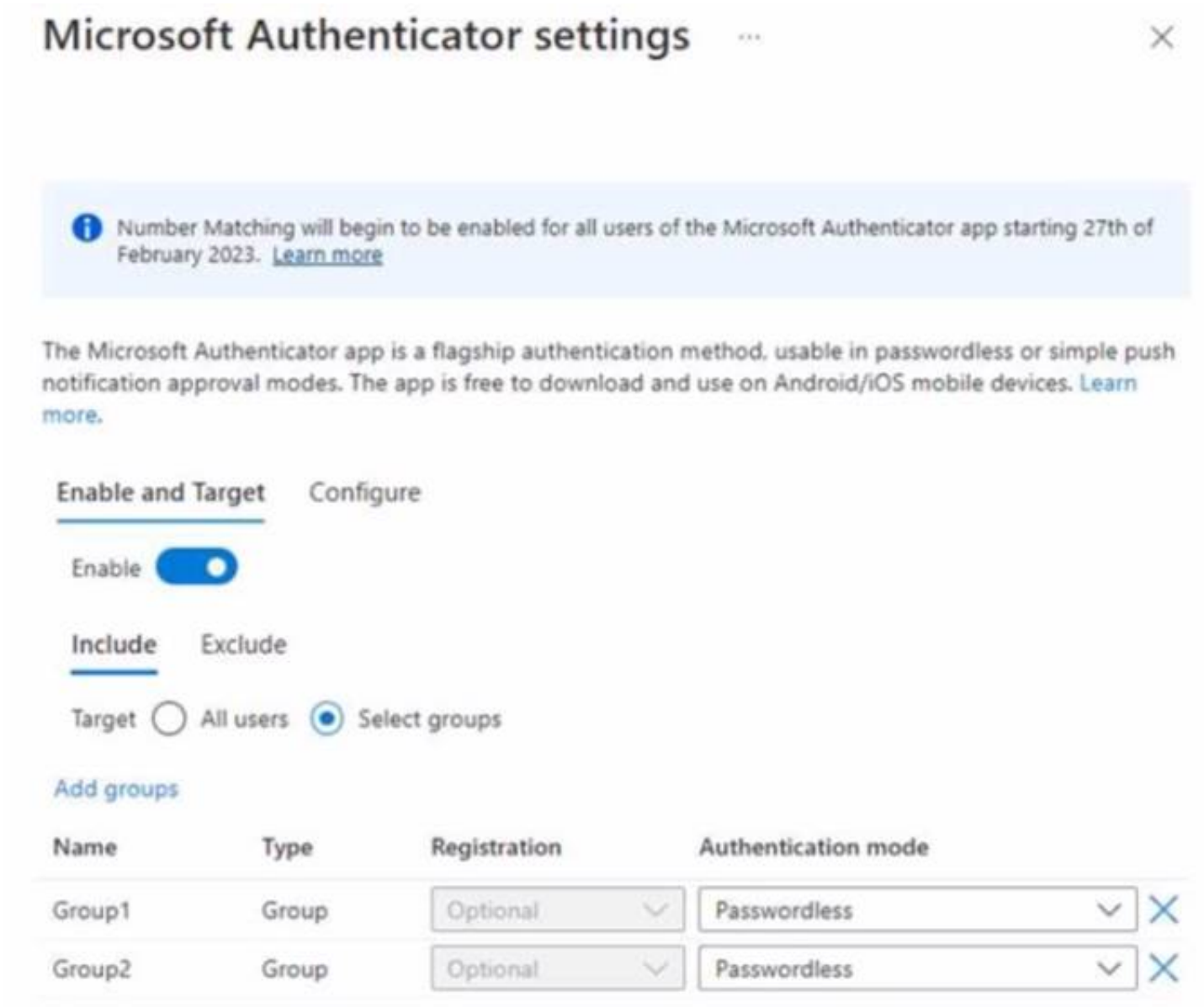
Name	Usage location	Membership
User1	United States	Group1, Group2
User2	*Not set*	Group2
User3	*Not set*	Group1
User4	Canada	Group1

Group2isa member of Group1.
You assign an Office 365 Enterprise E3 license to Group1. How many Office 365 E3 licenses are assigned?

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

Answer: C

NEW QUESTION 204
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.

nswer Area

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	○	○
User2 can sign in by using a username and password.	○	○
User3 can sign in by using number matching in the Microsoft Authenticator app.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

nswer Area

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	○	○
User2 can sign in by using a username and password.	○	○
User3 can sign in by using number matching in the Microsoft Authenticator app.	○	○

NEW QUESTION 209
- (Topic 6)
Your company has a Microsoft 365 subscription. you implement sensitivity Doris for your company.
You need to automatically protect email messages that contain the word Confidential m the subject line.
What should you create?

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

Answer: B

NEW QUESTION 212
- (Topic 6)
Your network contains an Active Directory domain named adatum.com that is synced to Azure AD.
The domain contains 100 user accounts.
The city attribute for all the users is set to the city where the user resides.
You need to modify the value of the city attribute to the three-letter airport code of each city.
What should you do?

A. From Windows PowerShell on a domain controller, run the Gec-ADUser and Sec- ADUser cmdlets.
B. From Azure Cloud Shell, run the Gec-ADUser and Sec-ADUser cmdlets.
C. From Windows PowerShell on a domain controller, run the Gec-MgUser and Updace- MgUser cmdlets.
D. From Azure Cloud Shell, run the Gec-MgUser and Update-MgUser cmdlets.

Answer: A

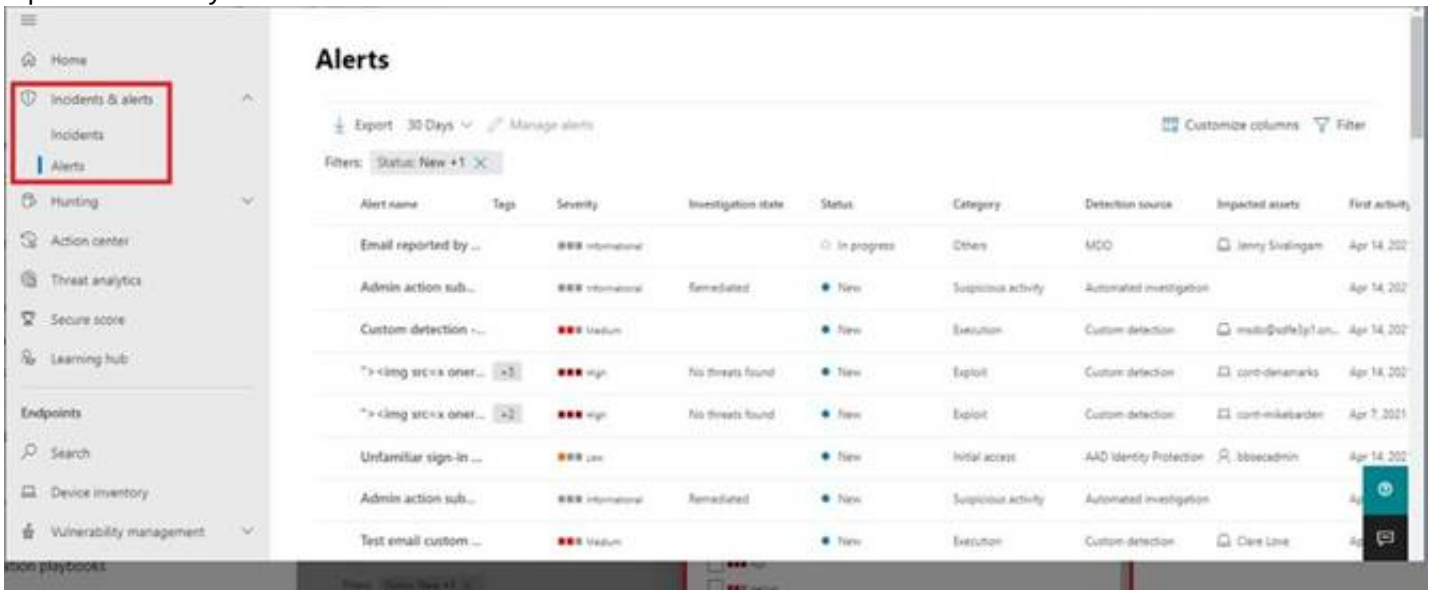
Explanation:
The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on- premise Active Directory.
You can use Windows PowerShell on a domain controller and run the Get-ADUser cmdlet to get the required users and pipe the results into Set-ADUser cmdlet to modify the city attribute.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
* 1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
* 2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.
Other incorrect answer options you may see on the exam include the following:
* 1. From the Azure portal, select all the Azure AD users, and then use the User settings blade.
* 2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set- AzureADUser cmdlets.
* 3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
* 4. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.
Reference:
https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser

NEW QUESTION 217
- (Topic 6)
You are reviewing alerts in the Microsoft 365 Defender portal. How long are the alerts retained in the portal?

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

Answer: C

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



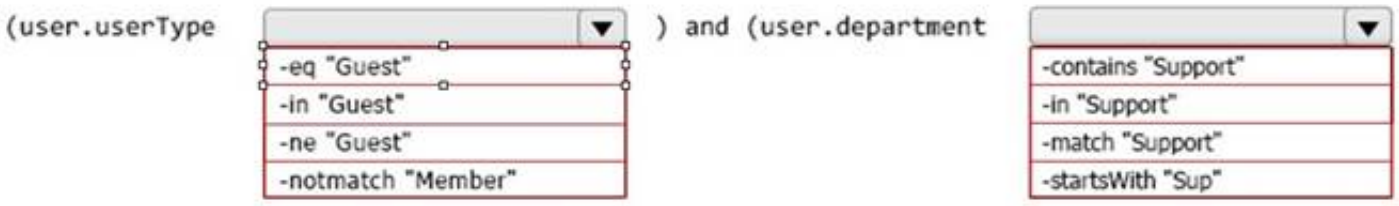
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data- retention

NEW QUESTION 218
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.
How should you complete the membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

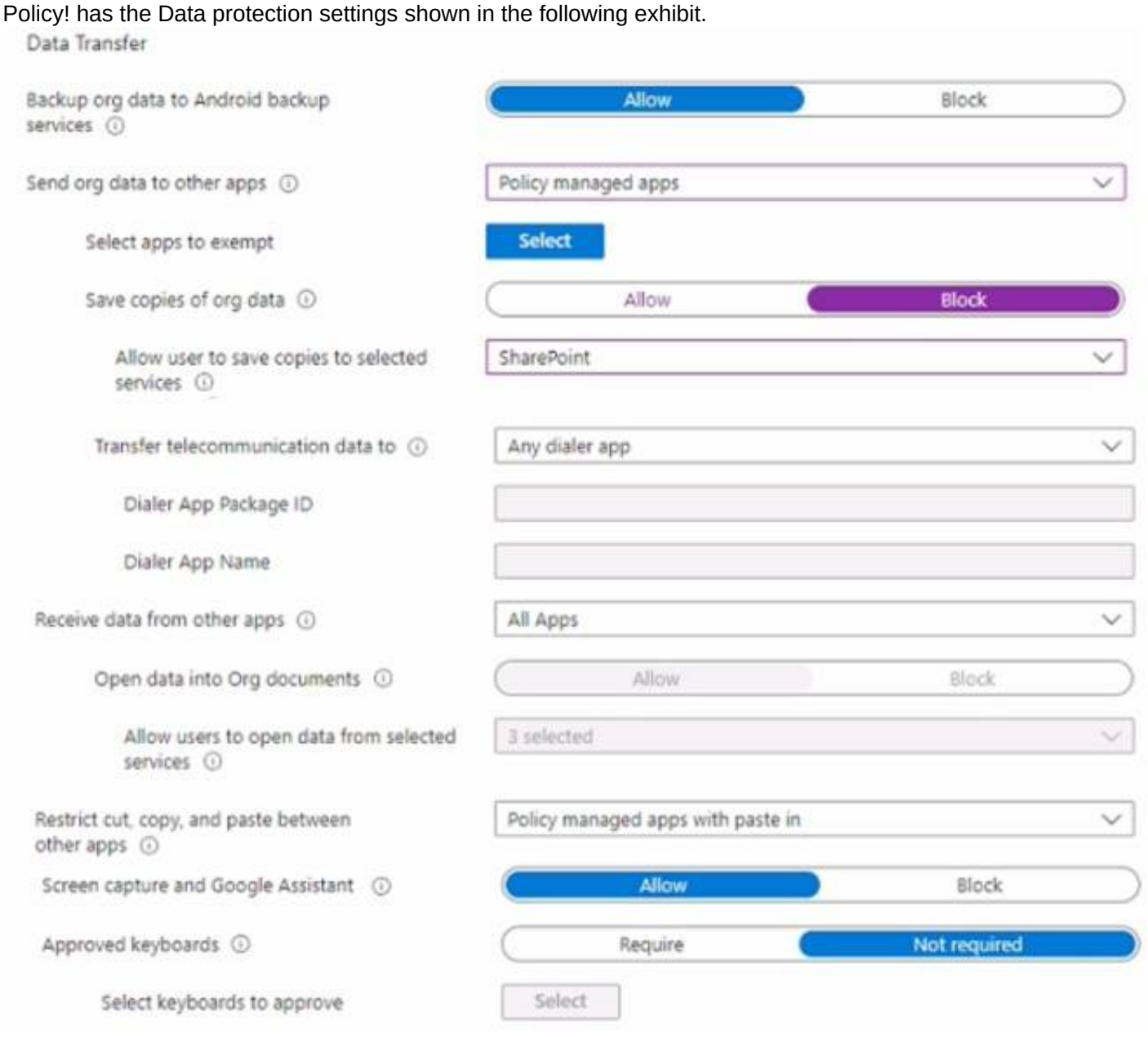


A. Mastered
B. Not Mastered

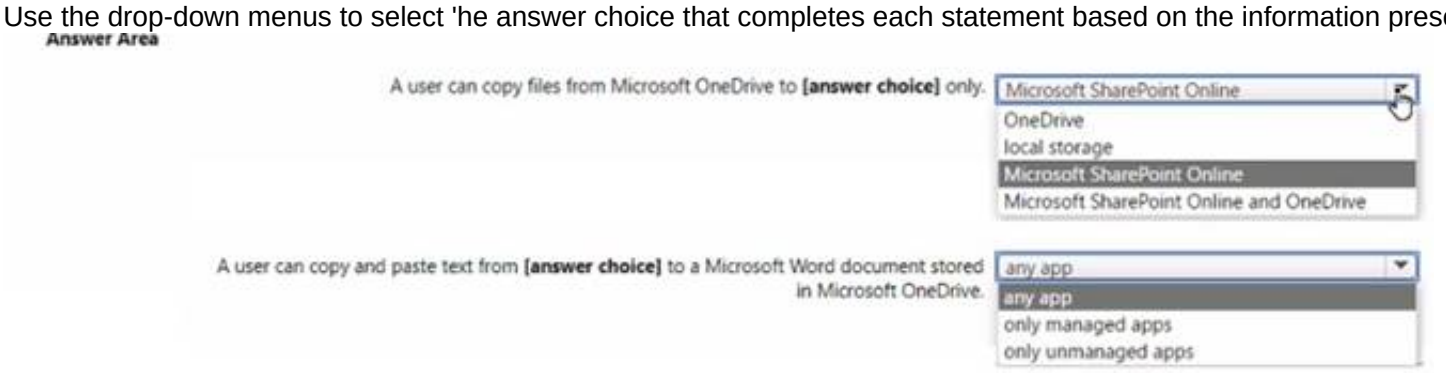
Answer: A

Explanation:
Box 1: -eq "Guest"
Dynamic membership rules for groups in Azure Active Directory
Supported expression operators
The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.
* Equals
-eq
* Contains
-contains
* Etc.
Box 2: -contains "Support" Incorrect:
* -in
If you want to compare the value of a user attribute against multiple values, you can use
the -in or -notIn operators.

NEW QUESTION 219
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains 200 Android devices enrolled in Microsoft Intune.
You create an Android app protection policy named Policy! that is targeted to all Microsoft apps and assigned to all users.
Policy! has the Data protection settings shown in the following exhibit.



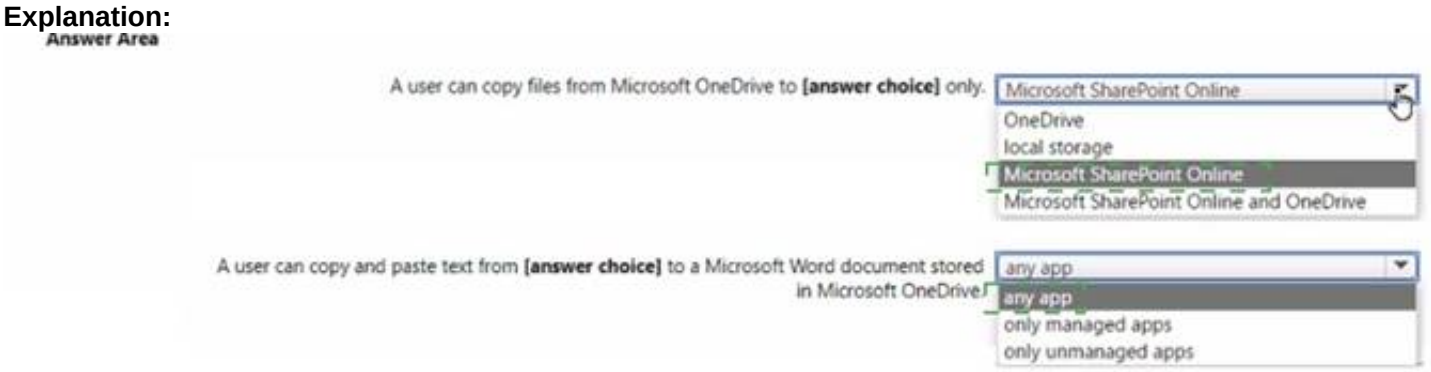
Use the drop-down menus to select 'he answer choice that completes each statement based on the information presented in the graphic.



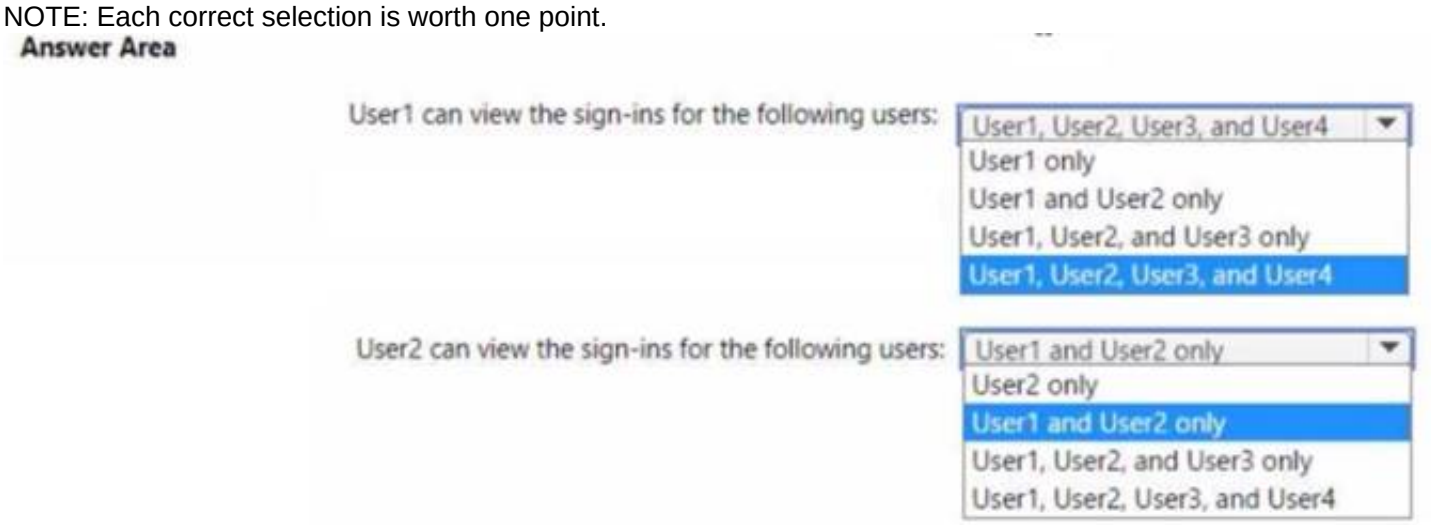
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 220
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.
From the Sign-ins blade of the Microsoft Entra admin center for which users can User1 and User2 view the sign-ins? 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 221
- (Topic 6)
Your company has a Microsoft 365 subscription.
You need to identify all the users in the subscription who are licensed for Office 365 through a group membership. The solution must include the name of the group

used to assign the license.
What should you use?

A. Active users in the Microsoft 365 admin center
B. Reports in Microsoft Purview compliance portal
C. the Licenses blade in the Microsoft Entra admin center
D. Reports in the Microsoft 365 admin center

Answer: D

Explanation:
Microsoft 365 Reports in the admin center
You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.
Which activity reports are available in the admin center
Depending on your subscription, here are the available reports in all environments.

Report	Public	GCC	GCC-High	DoD	Office 365 operated by 21Vianet
Microsoft browser usage	Yes	No[1]	No[1]	No[1]	No[1]
Email activity	Yes	Yes	Yes	Yes	Yes
Email apps usage	Yes	Yes	Yes	Yes	Yes
Mailbox usage	Yes	Yes	Yes	Yes	Yes
Office activations	Yes	Yes	Yes	Yes	Yes

Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports

NEW QUESTION 224
- (Topic 6)
You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

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

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

Answer: C

NEW QUESTION 228
- (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 231
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your MS-102 Exam with Our Prep Materials Via below:

https://www.certleader.com/MS-102-dumps.html