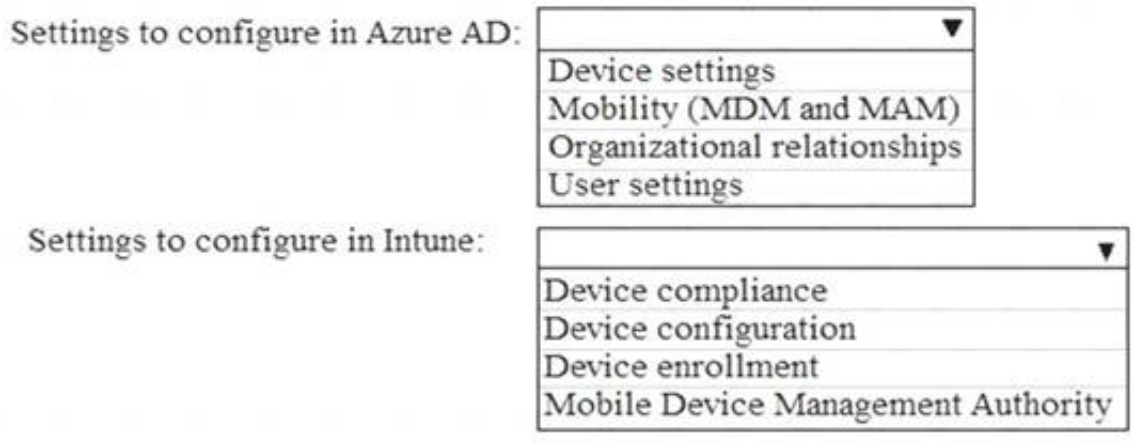
Exam Questions MS-102

Microsoft 365 Administrator Exam

https://www.2passeasy.com/dumps/MS-102/

NEW QUESTION 1
- (Exam Topic 1)
You need to meet the Intune requirements for the Windows 10 devices.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/intune/windows-enroll

NEW QUESTION 2
- (Exam 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 3
- (Exam Topic 1)
As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 4
- (Exam Topic 1)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current
Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager. Solution: You create a device configuration profile from the Device Management admin center.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
It looks like the given answer is correct. There is an on-premises Active Directory synced to Azure Active Directory (Azure AD) So the co-management path1 - Auto-enroll existing clients 1. Hybrid Azure AD 2. Client agent setting for hybrid Azure AD-join 3. Configure auto-enrollment of devices to Intune 4. Enable co-management in Configuration Manager
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-client

NEW QUESTION 5
- (Exam 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 6
- (Exam Topic 2)
Which report should the New York office auditors view?

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

Answer: C

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

NEW QUESTION 7
- (Exam Topic 3)
You need to create the DLP policy to meet the technical requirements. What should you configure first?

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

Answer: A

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

NEW QUESTION 8
- (Exam Topic 3)
You need to configure the compliance settings to meet the technical requirements. What should you do in the Microsoft Endpoint Manager admin center?

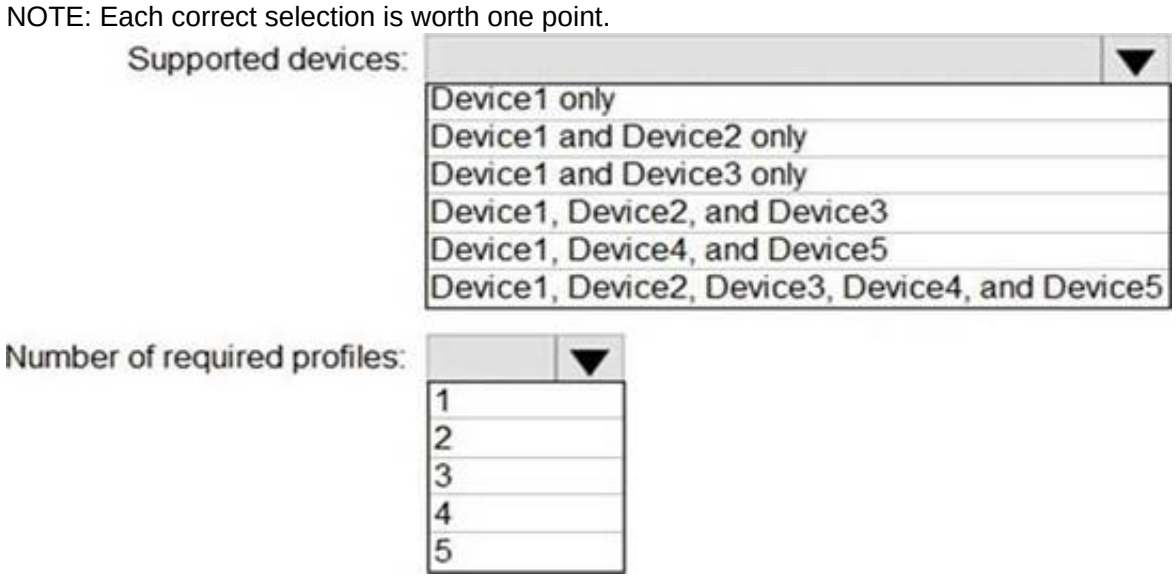
A. From Compliance policies, modify the Notifications settings.
B. From Locations, create a new location for noncompliant devices.

C. From Retire Noncompliant Devices, select Clear All Devices Retire State.
D. Modify the Compliance policy settings.

Answer: D

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

NEW QUESTION 9
- (Exam Topic 3)
You plan to implement the endpoint protection device configuration profiles to support the planned changes. You need to identify which devices will be supported, and how many profiles you should implement.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

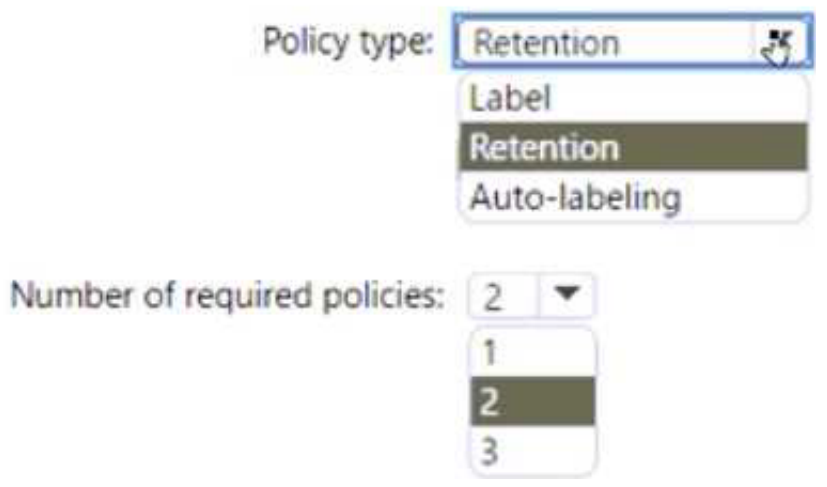


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

NEW QUESTION 10
- (Exam Topic 3)
You need to configure the information governance settings to meet the technical requirements.
Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area

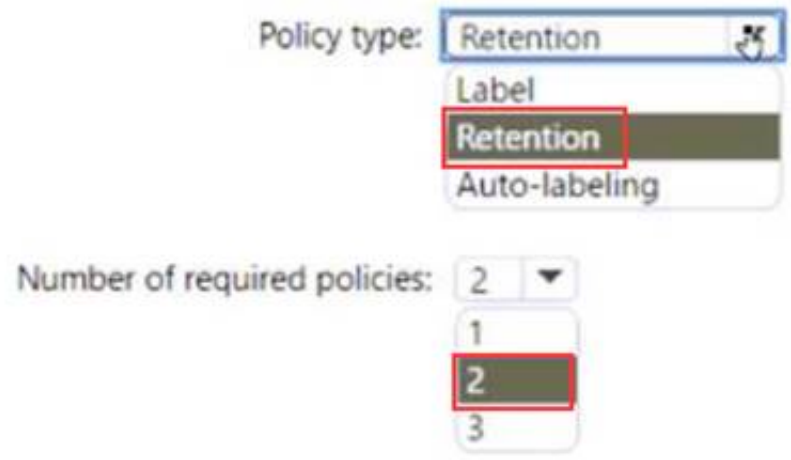


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 10
- (Exam Topic 4)
You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.
Which authentication strategy should you implement for the pilot projects?

A. pass-through authentication
B. pass-through authentication and seamless SSO
C. password hash synchronization and seamless SSO
D. password hash synchronization

Answer: C

Explanation:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365. Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
Fabrikam does NOT plan to implement identity federation.
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

NEW QUESTION 15
- (Exam Topic 4)
Which role should you assign to User1?
Available Choices (select all choices that are correct)

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

Answer: B

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

NEW QUESTION 16
- (Exam Topic 5)
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 20
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
The Microsoft Secure Score for the tenant is shown in the following exhibit.

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

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

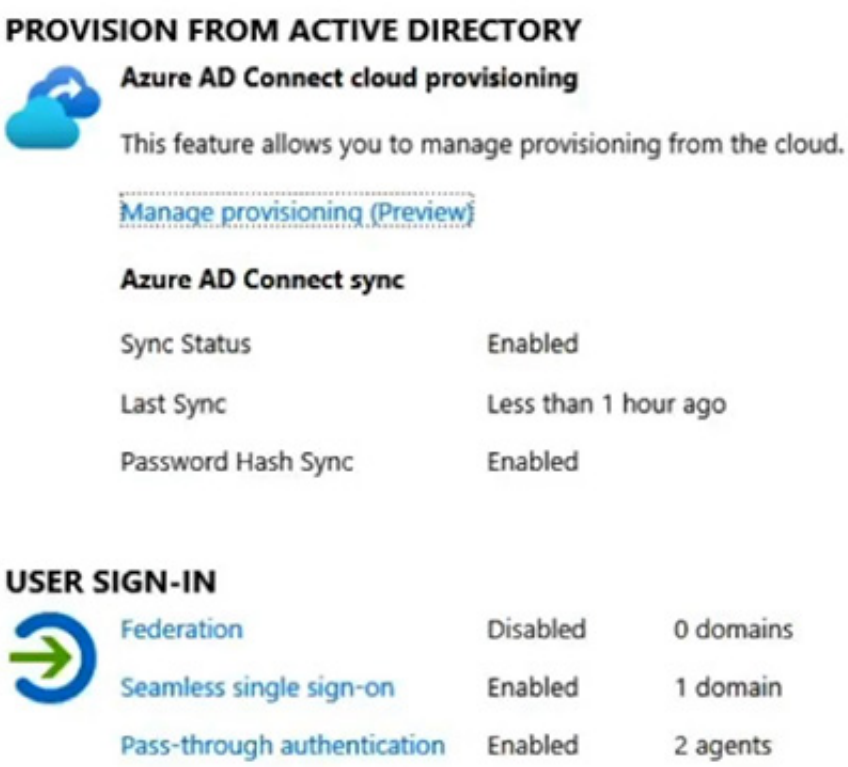
Answer: ABC

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

NEW QUESTION 22
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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



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

A. Yes
B. No

Answer: B

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

NEW QUESTION 23
- (Exam Topic 5)
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 27
- (Exam Topic 5)
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 the Synchronization Rules Editor, you create a new outbound synchronization rule. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 32

- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
You create an account tor a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.
Does this meet the goal?

A. Yes
B. no

Answer: B

NEW QUESTION 34
- (Exam Topic 5)
You have a Microsoft 365 tenant.
Company policy requires that all Windows 10 devices meet the following minimum requirements:
- Require complex passwords.
- Require the encryption of data storage devices.
- Have Microsoft Defender Antivirus real-time protection enabled.

You need to prevent devices that do not meet the requirements from accessing resources in the tenant. Which two components should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a configuration policy
B. a compliance policy
C. a security baseline profile
D. a conditional access policy
E. a configuration profile

Answer: BD

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

NEW QUESTION 38
- (Exam Topic 5)
You have a Microsoft 365 subscription that uses Security & Compliance retention policies. You implement a preservation lock on a retention policy that is assigned to all executive users.
Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point?

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

Answer: AD

NEW QUESTION 39
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:
• Windows 10
• Android
• OS
On which devices can you configure the Endpoint DLP policies?

A. Windows 10 only
B. Windows 10 and Android only
C. Windows 10 and macO Sonly
D. Windows 10, Android, and iOS

Answer: C

Explanation:
Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide

NEW QUESTION 43
- (Exam Topic 5)
You have a Microsoft 365 subscription that contains three groups named All users, Sales team, and Office users, and two users shown in the following table.

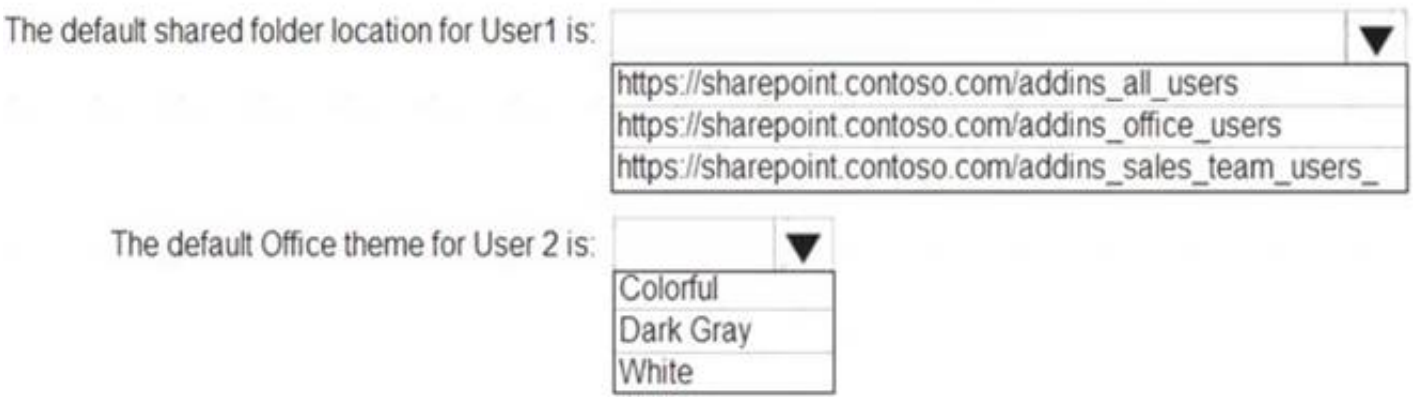
Name	Member of
User1	All users, Sales team
User2	All users, Office users

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

The policies use the settings shown in the following table.

Policy	Default Shared Folder Location	Default Office Theme
All users	https://sharepoint.contoso.com/addins_all_users	Colorful
Office Users Policy	https://sharepoint.contoso.com/addins_office_users	White
Sales Team Policy	https://sharepoint.contoso.com/addins_sales_team_users_	Dark Gray

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

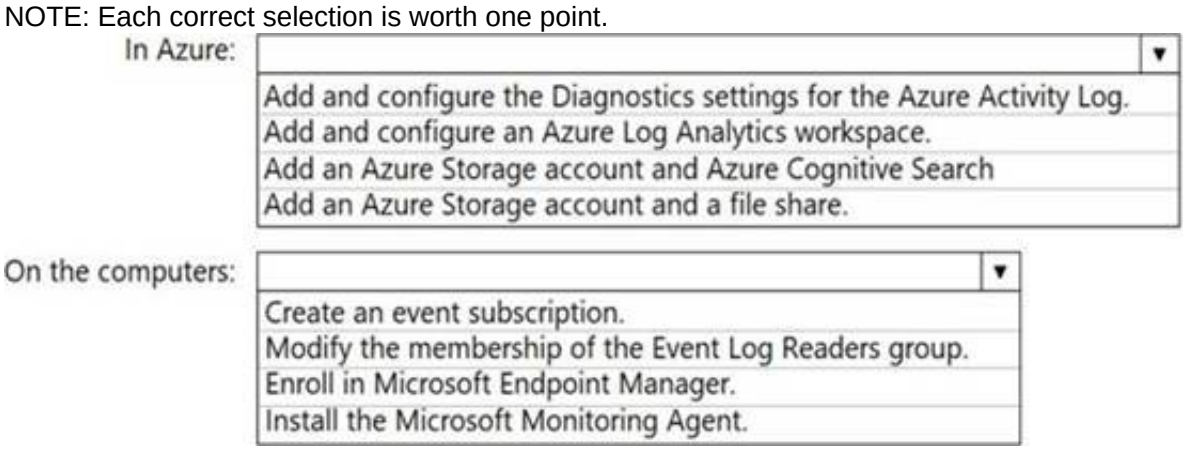


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service

NEW QUESTION 45
- (Exam Topic 5)
You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.
You need to centrally monitor System log events from the computers.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

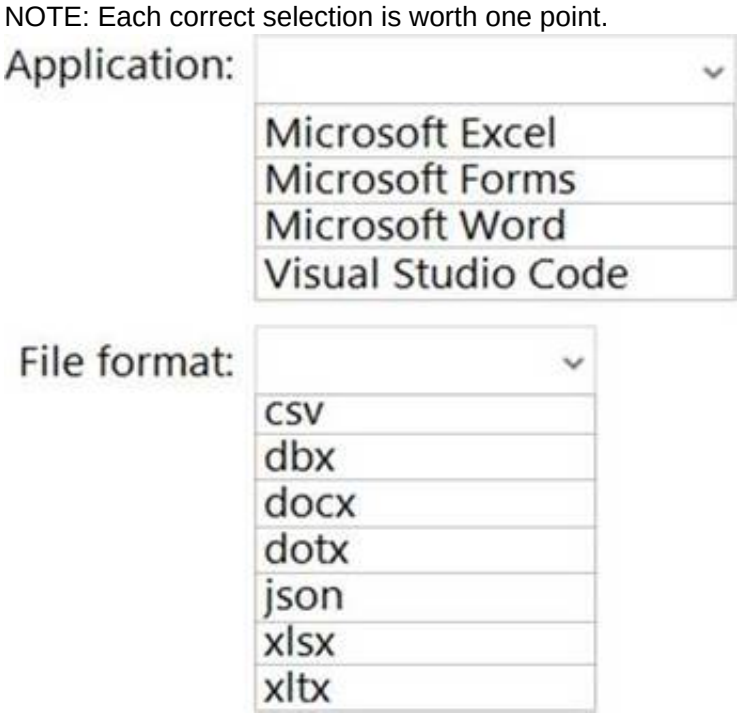


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer

NEW QUESTION 49
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 tenant.
You need to create a custom Compliance Manager assessment template.
Which application should you use to create the template, and in which file format should the template be saved? 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:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-create?view=o365

NEW QUESTION 51
- (Exam Topic 5)
You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

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

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

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

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

Name	Assigned to
Policy1	Group3
Policy2	Group2

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 56
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

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

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

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

Answer: C

NEW QUESTION 59
- (Exam Topic 5)
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 64
- (Exam Topic 5)
You have a Microsoft 365 tenant.
You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Save the audit logs to: [ ]

Azure Active Directory admin center blade to use to view the saved audit logs: [ ]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Save the audit logs to: Azure Log Analytics

Azure Active Directory admin center blade to use to view the saved audit logs: Audit logs

NEW QUESTION 66
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You have an Azure AD tenant that contains the users shown in the following table.

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

You configure Tenant properties as shown in the following exhibit.

Technical contact
User1@contoso.com

Global privacy contact

Privacy statement URL
http://contoso.com/privacy

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

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

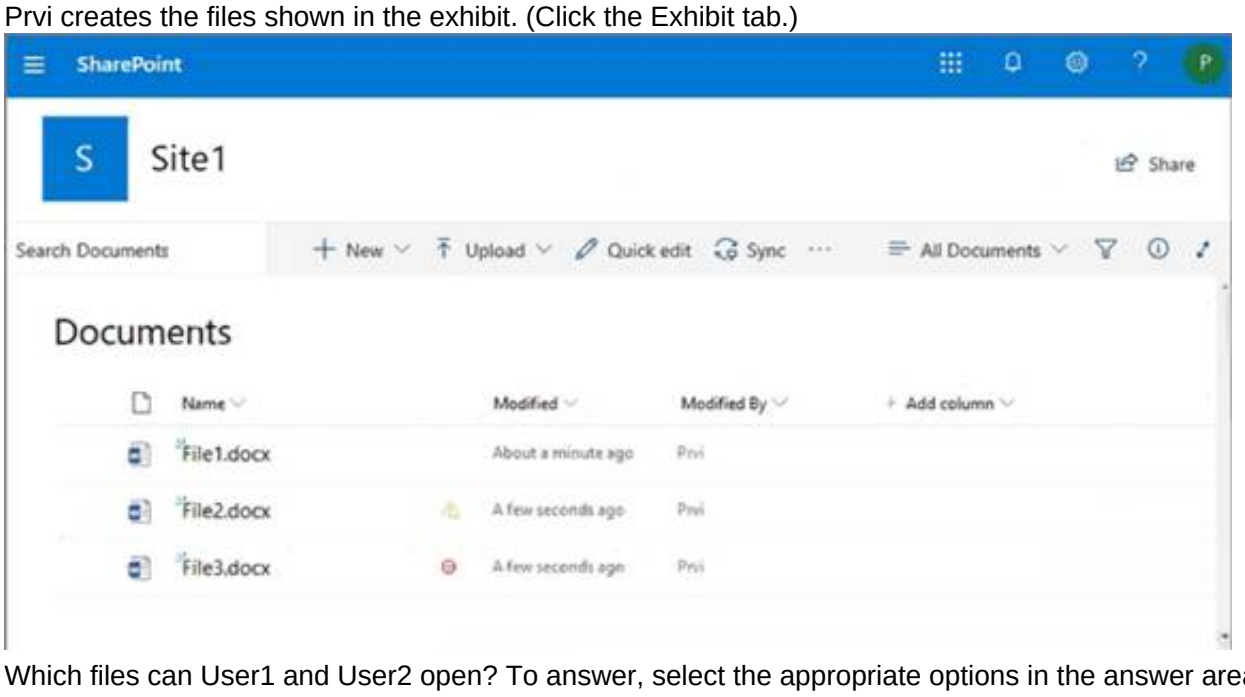
Answer: B

Explanation:
Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified.
Reference:
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365

NEW QUESTION 67
- (Exam Topic 5)
From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

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



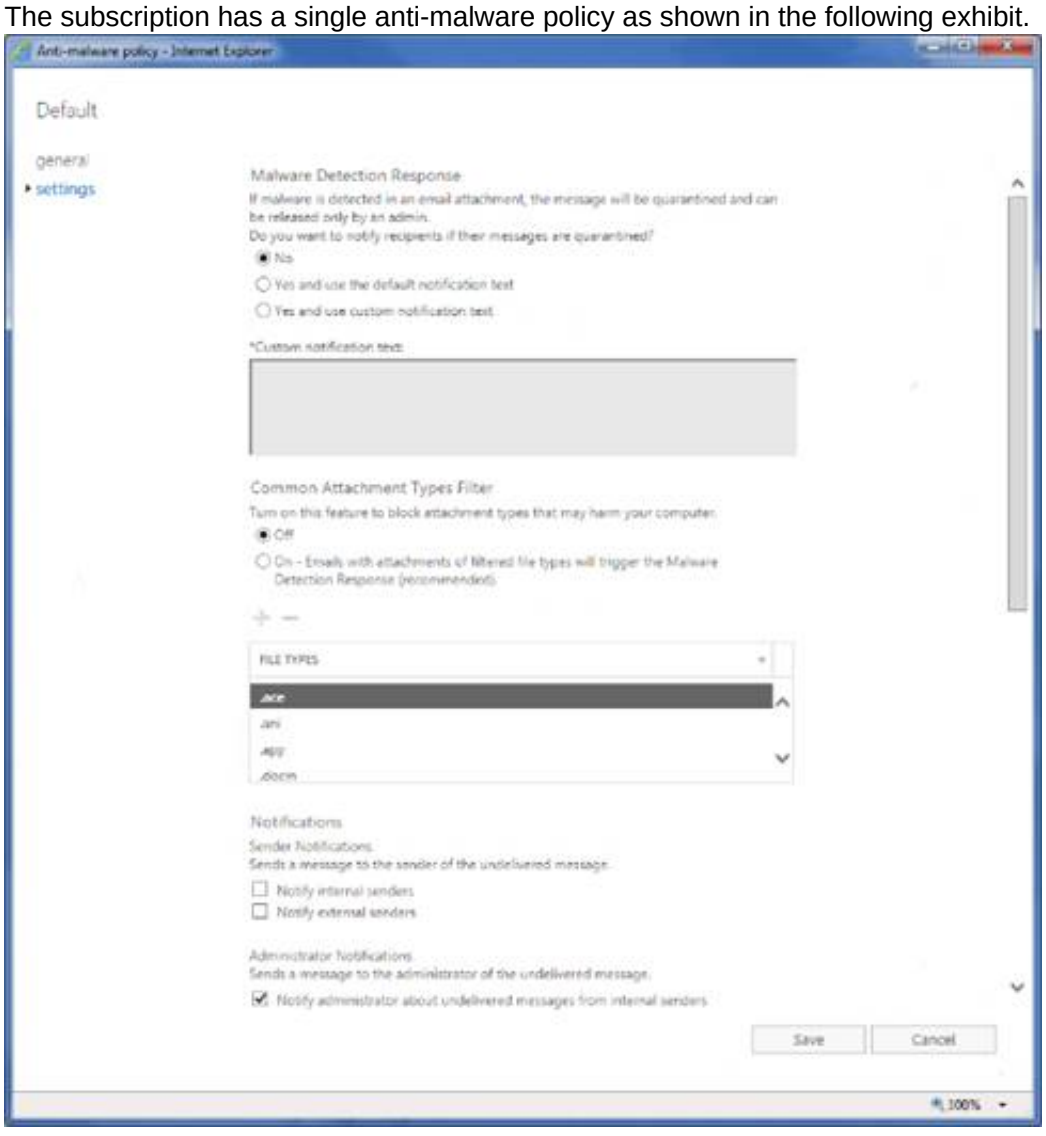
Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/ https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/

NEW QUESTION 69
- (Exam Topic 5)
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=o36

NEW QUESTION 74
- (Exam Topic 5)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You need to ensure that users are prevented from opening or downloading malicious files from Microsoft Teams, OneDrive, or SharePoint Online.
What should you do?

A. Create a newAnti-malware policy
B. Configure the Safe Links global settings.
C. Create a new Anti-phishing policy
D. Configure the Safe Attachments global settings.

Answer: D

Explanation:
Safe Attachments for SharePoint, OneDrive, and Microsoft Teams
In organizations with Microsoft Defender for Office 365, Safe Attachments for SharePoint, OneDrive, and Microsoft Teams provides an additional layer of protection against malware. After files are asynchronously scanned by the common virus detection engine in Microsoft 365, Safe Attachments opens files in a virtual environment to see what happens (a process known as detonation). Safe Attachments for SharePoint, OneDrive, and Microsoft Teams also helps detect and block existing files that are identified as malicious in team sites and document libraries.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-team

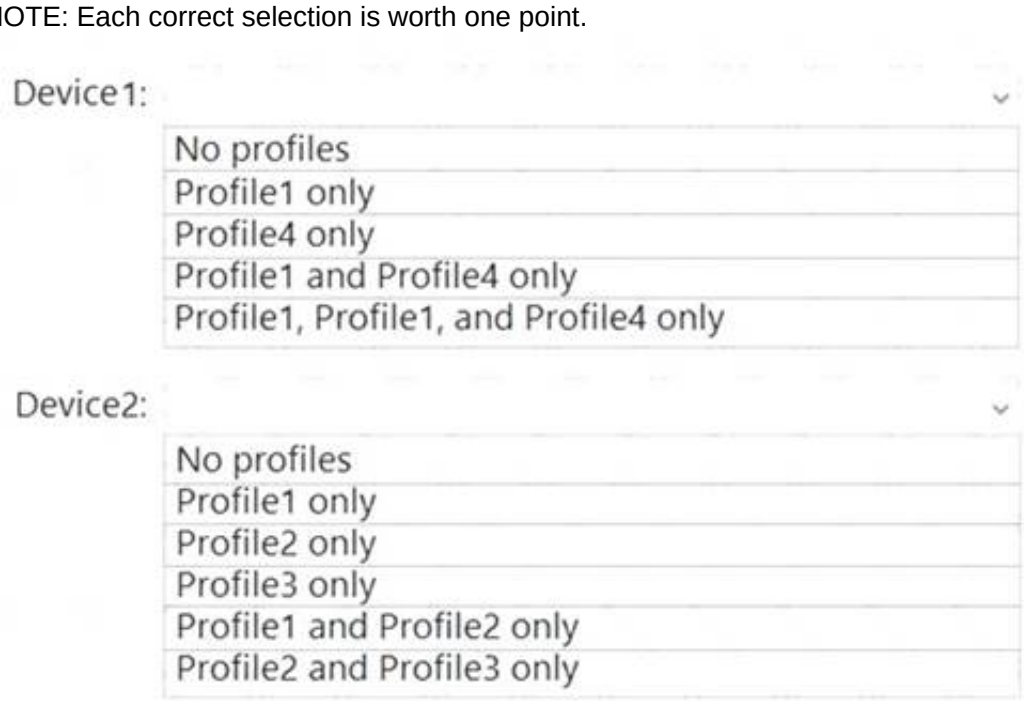
NEW QUESTION 75
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have devices enrolled in Intune as shown in the following table.

Name	Platform	Member of	Scope (Tags)
Device1	Windows 10	Group1, Group3	Tag1
Device2	Android	Group2	Tag2

You create the device configuration profiles shown in the following table.

Name	Platform	Assignments: Included groups	Assignments: Excluded groups	Scope tags
Profile1	Windows 10 and later	Group1	Group3	Tag1, Tag2
Profile2	Android Enterprise	All devices	Group2	Tag1, Tag2
Profile3	Android Enterprise	Group2, Group3	Group3	Tag1
Profile4	Windows 10 and later	Group3	**None**	Default

Which profiles will be applied to each device? 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:
Graphical user interface, text, application, table Description automatically generated

NEW QUESTION 79
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint. You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.
You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Devices that can onboarded to Microsoft Defender for Endpoint:
- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:
- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, table Description automatically generated with medium confidence
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?vie

NEW QUESTION 84
- (Exam Topic 5)
You use Microsoft Defender for Endpoint.
You have the Microsoft Defender for Endpoint device groups shown in the following table

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

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

Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

Answer Area

Computer1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

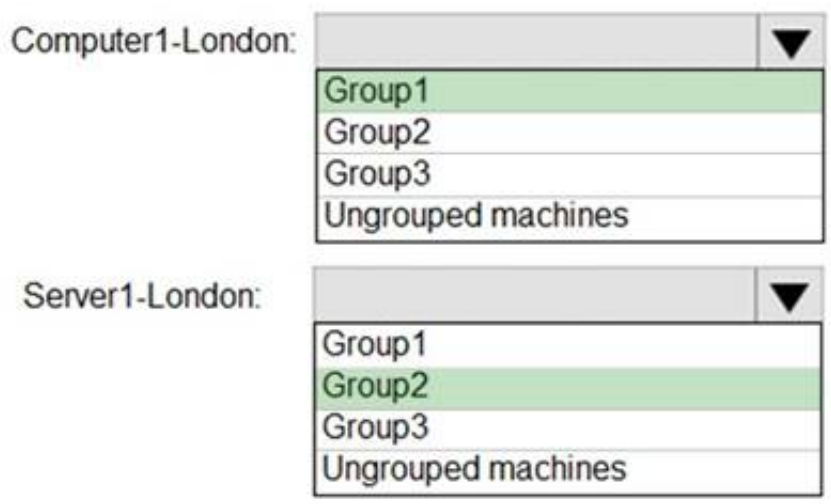
Server1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 85
- (Exam Topic 5)
You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that Used can place a hold on all mailbox content. What permission should you assign to User1?

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

Answer: B

NEW QUESTION 86
- (Exam Topic 5)
You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User1. you need to preserve a copy of all the email messages that contain the word ProjectX.
What should you do first?

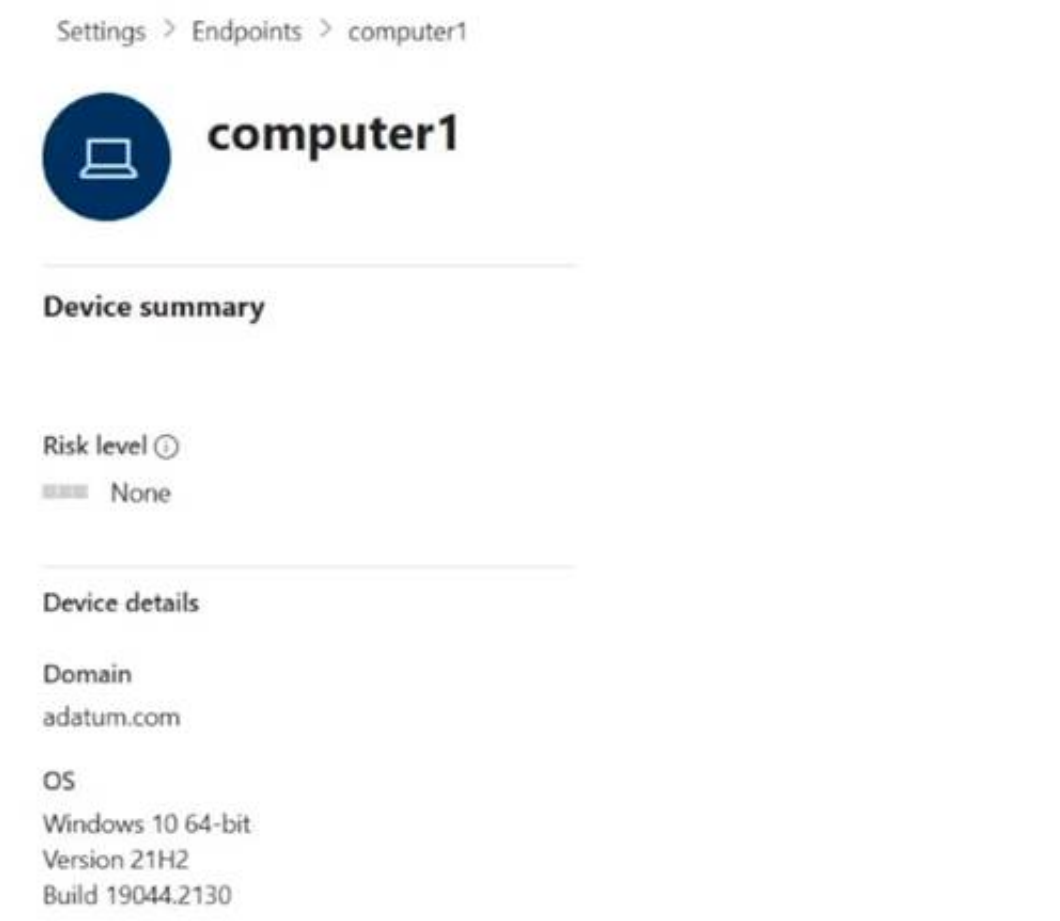
A. From the Exchange admin center create a mail flow rule.
B. From Microsoft 365 Defender, start a message trace.
C. From Microsoft Defender for Cloud Apps, create an activity policy.
D. From the Microsoft Purview compliance portal, create a label and a label policy.

Answer: D

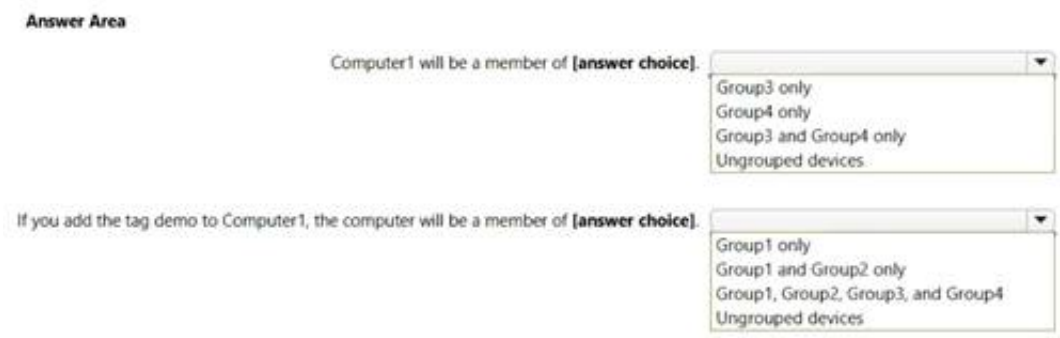
NEW QUESTION 87
- (Exam Topic 5)
HOTSPOT
Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

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

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



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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 88
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
You plan to deploy a monitoring solution that meets the following requirements:
- Captures Microsoft Teams channel messages that contain threatening or violent language.
- Alerts a reviewer when a threatening or violent message is identified.

What should you include in the solution?

A. Data Subject Requests (DSRs)
B. Insider risk management policies
C. Communication compliance policies
D. Audit log retention policies

Answer: C

NEW QUESTION 90
- (Exam Topic 5)
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 94
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant. Users store data in the following locations:
- Microsoft Teams
- Microsoft OneDrive
- Microsoft Exchange Online
- Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.
What is the minimum number of retention policies that you should create?

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

Answer: C

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

NEW QUESTION 96
- (Exam Topic 5)
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 98
- (Exam Topic 5)
You implement Microsoft Azure Advanced Threat Protection (Azure ATP). You have an Azure ATP sensor configured as shown in the following exhibit.

How long after the Azure ATP cloud service is updated will the sensor update?

A. 20 hours
B. 12 hours
C. 7 hours
D. 48 hours

Answer: B

NEW QUESTION 103
- (Exam Topic 5)
You have several devices enrolled in Microsoft Endpoint Manager
You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown In the following table.

Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	**None**	**None**

The device limit restrictions in Endpoint manager are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All users

You add user as a device enrollment manager in Endpoint manager
For each of the following statements, select Yes if the statement is true. Otherwise, select No
Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User2 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User3 can enroll an unlimited number of devices in Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User2 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User3 can enroll an unlimited number of devices in Endpoint Manager.	○	○

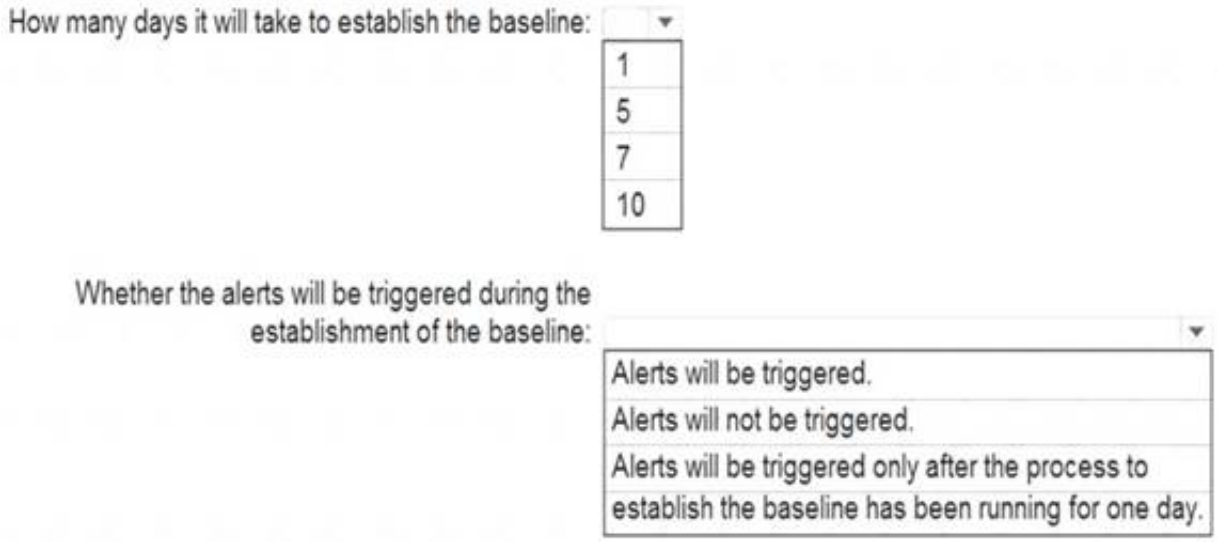
NEW QUESTION 106
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
You configure a new alert policy as shown in the following exhibit.

How do you want the alert to be triggered?

- ○ Every time an activity matches the rule
- ○ When the volume of matched activities reaches a threshold
  - More than or equal to 15 activities
  - During the last 60 minutes
  - On All users
- ◉ When the volume of matched activities becomes unusual
  - On All users

You need to identify the following:
- How many days it will take to establish a baseline for unusual activity.
- Whether alerts will be triggered during the establishment of the baseline.

What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide

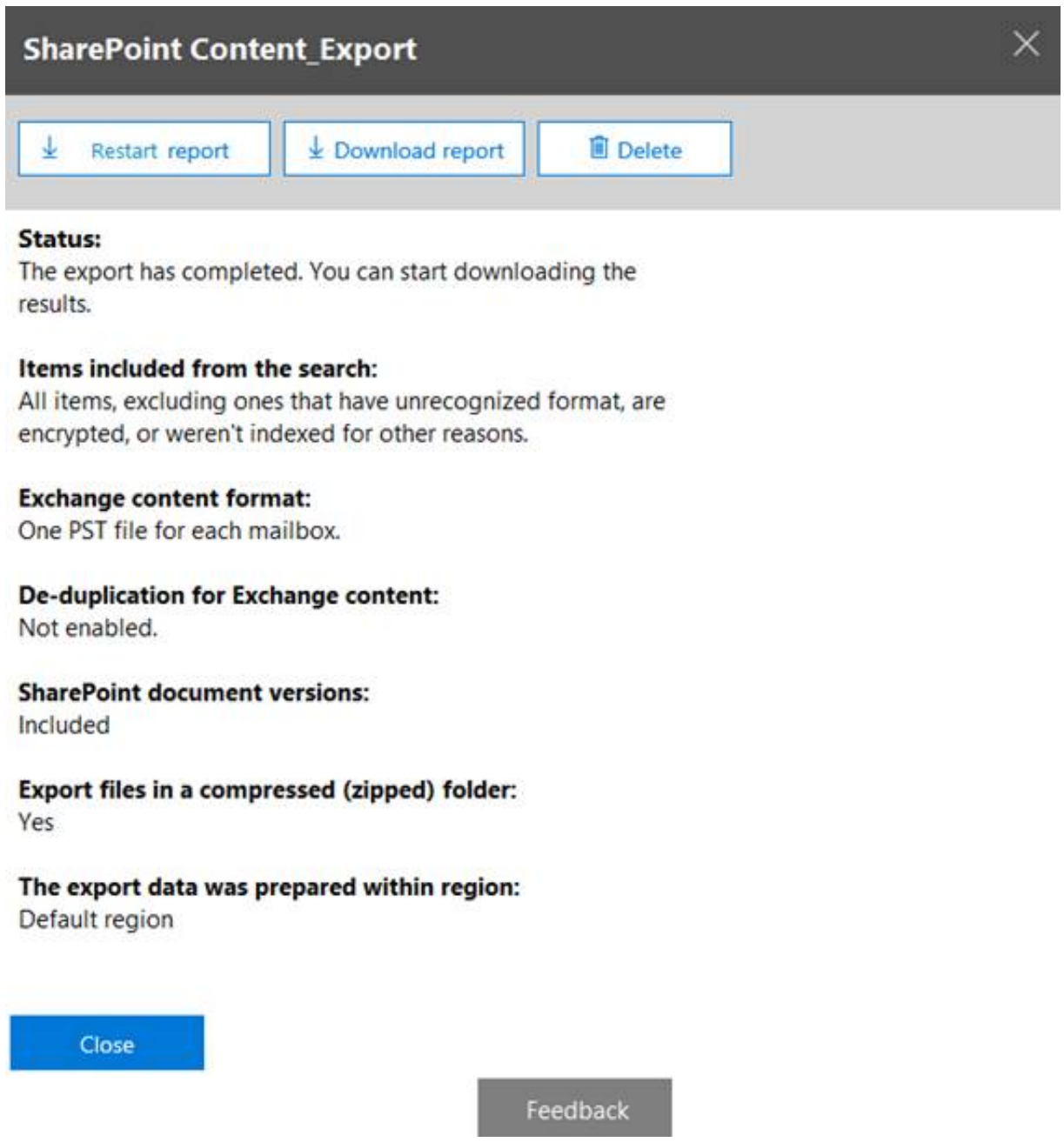
NEW QUESTION 107
- (Exam Topic 5)
Your company has 10,000 users who access all applications from an on-premises data center. You plan to create a Microsoft 365 subscription and to migrate data to the cloud.
You plan to implement directory synchronization.
User accounts and group accounts must sync to 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 112
- (Exam Topic 5)
From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)



What will be excluded from the export?

A. a 10-MB XLSX file
B. a 5-MB MP3 file
C. a 5-KB RTF file
D. an 80-MB PPTX file

Answer: B

Explanation:
Unrecognized file formats are excluded from the search.
Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o3 https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report

NEW QUESTION 113
- (Exam Topic 5)
You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.

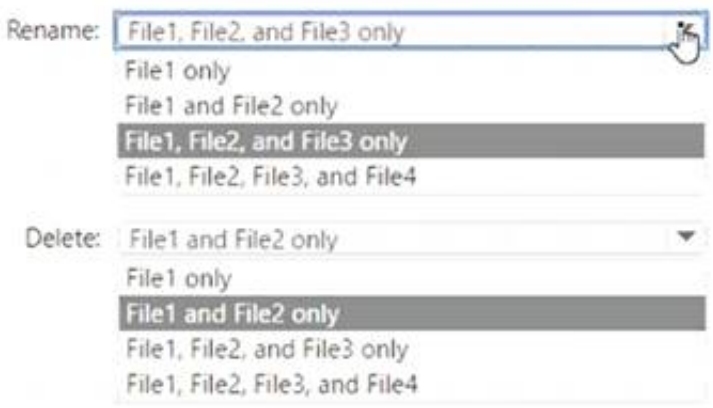
Name	Retention period	During the retention period
Retention1	5 years	Retain items even if users delete
Retention2	5 years	Mark items as a record
Retention3	5 years	Mark items as a regulatory record

Site1 contains the files shown in the following table.

Name	Label
File1	*None*
File2	Retention1
File3	Retention2
File4	Retention3

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

Answer Area

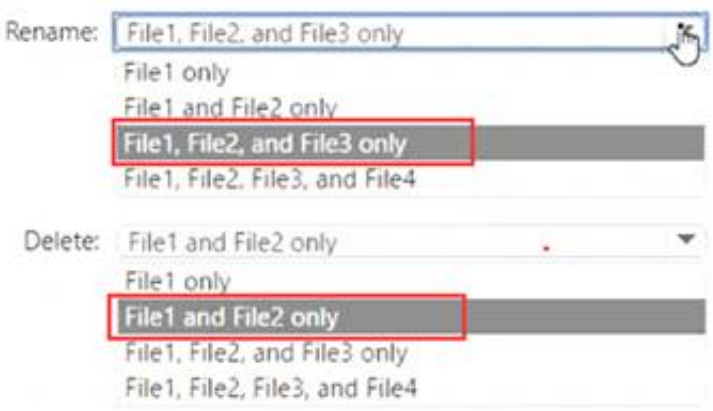


A. Mastered
B. Not Mastered

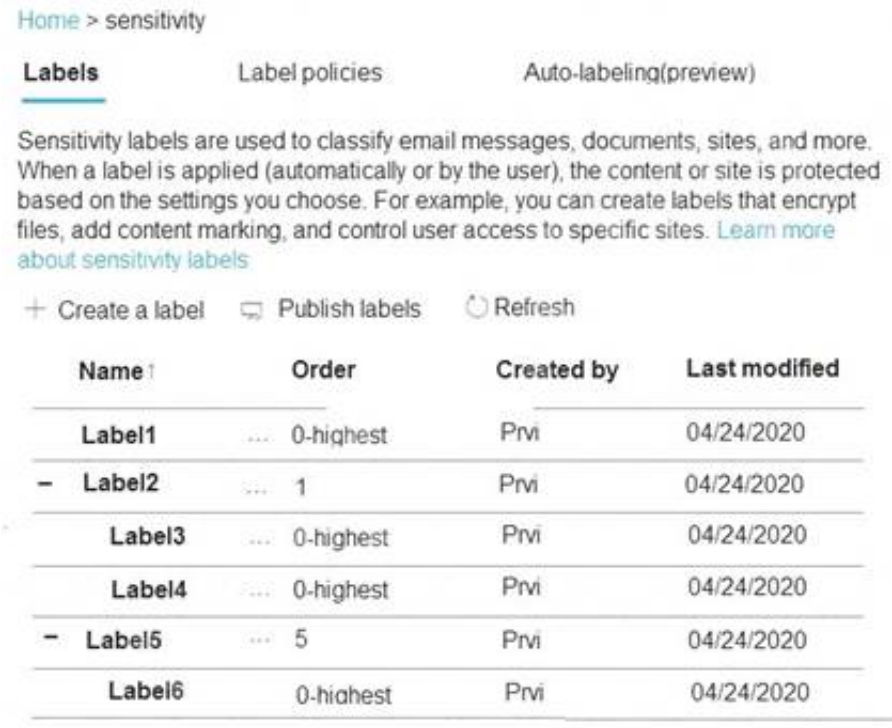
Answer: A

Explanation:

Answer Area



NEW QUESTION 114
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.



Which labels can users apply to content?

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

Answer: C

NEW QUESTION 118
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

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

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

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

Answer: A

NEW QUESTION 122
- (Exam Topic 5)
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 security center.
Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

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

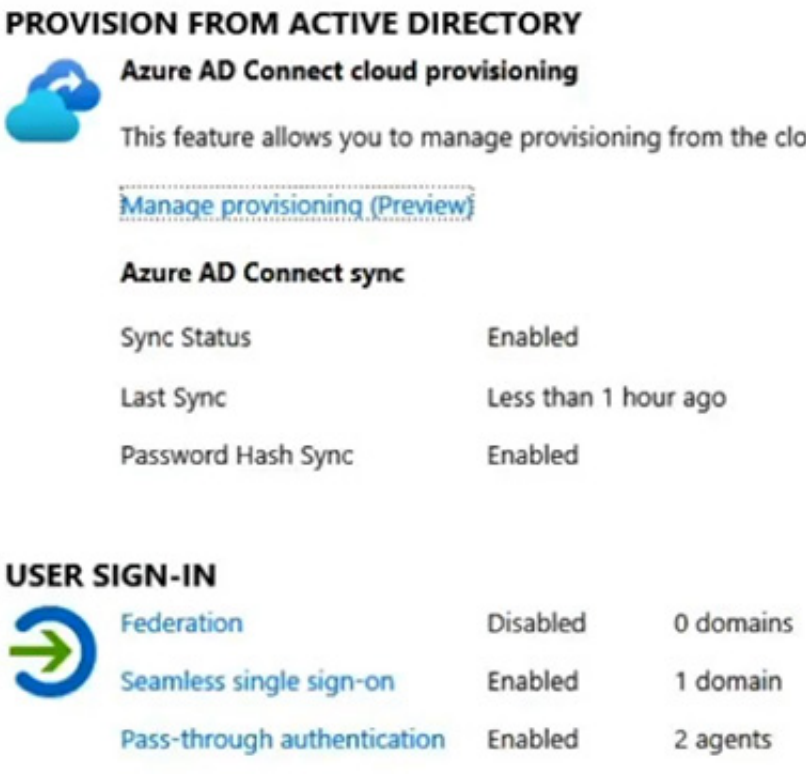
Answer: A

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

NEW QUESTION 124
- (Exam Topic 5)
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 129
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
You define a retention label that has the following settings:
• Retention period 7 years
• Start the retention period bated on: When items were created

You need to prevent the removal of the label once the label K applied to a lie What should you select in the retention label settings?

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

Answer: B

NEW QUESTION 130
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 131
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains the compliance policies shown in the following table.

Name	Require BitLocker	Require the device to be at or under the machine risk score
Policy1	Required	High
Policy2	Not configured	Medium
Policy3	Required	Low

The tenant contains the devices shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Microsoft Defender for Endpoint risk status	Policies applied
Device1	Configured	High	Policy1, Policy3
Device2	Not configured	Medium	Policy2, Policy3
Device3	Not configured	Low	Policy1, Policy2

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated

NEW QUESTION 133
- (Exam Topic 5)
HOTSPOT

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 137
- (Exam Topic 5)
You have a Microsoft 365 subscription that contains a user named User1. User1 requires admin access to perform the following tasks:
Manage Microsoft Exchange Online settings.
Create Microsoft 365 groups.
You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.
What should you use?

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

Answer: D

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

NEW QUESTION 138
- (Exam Topic 5)
You have a Microsoft 365 subscription.
Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.
You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs. D18912E1457D5D1DDCBD40AB3BF70D5D
What should you create to ensure that the DLP policy can detect the customer IDs?

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

Answer: A

Explanation:

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

NEW QUESTION 142
- (Exam Topic 5)
You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).
The tenant has two Compliance Manager assessments as shown in the following table.

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

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

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

You perform the following actions:

- For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.
- Enable multi-factor authentication (MFA) for all users.

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-assessments?view=o365-worl https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwid

NEW QUESTION 143
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that uses Microsoft Intune.
You need to ensure that users can select a department when they enroll their device in Intune. What should you create?

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

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

NEW QUESTION 147
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

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

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

A. only the settings of Policy1
B. only the settings of Policy2
C. only the settings of Policy3

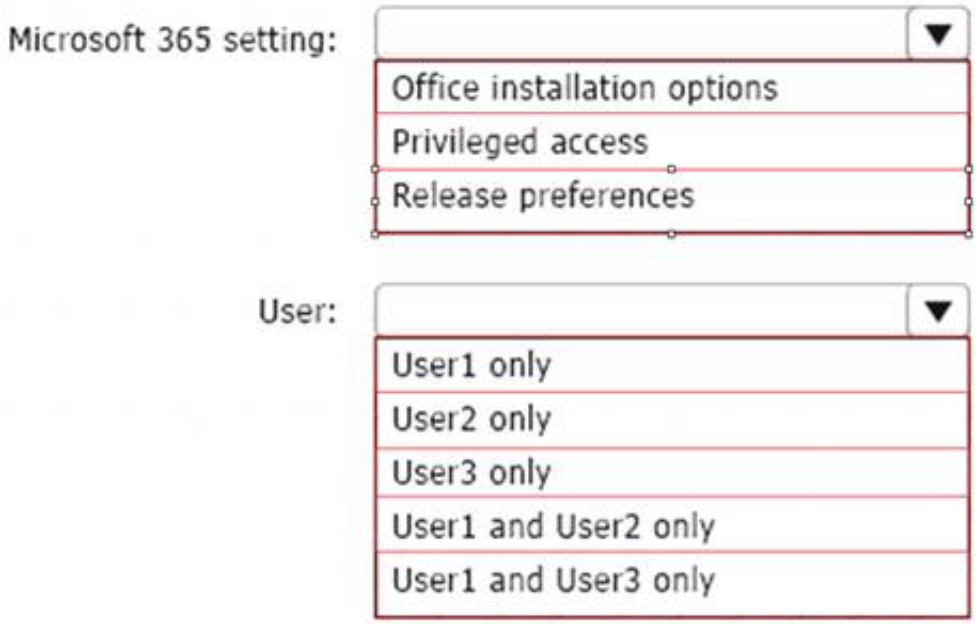
D. no settings

Answer: D

NEW QUESTION 151
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

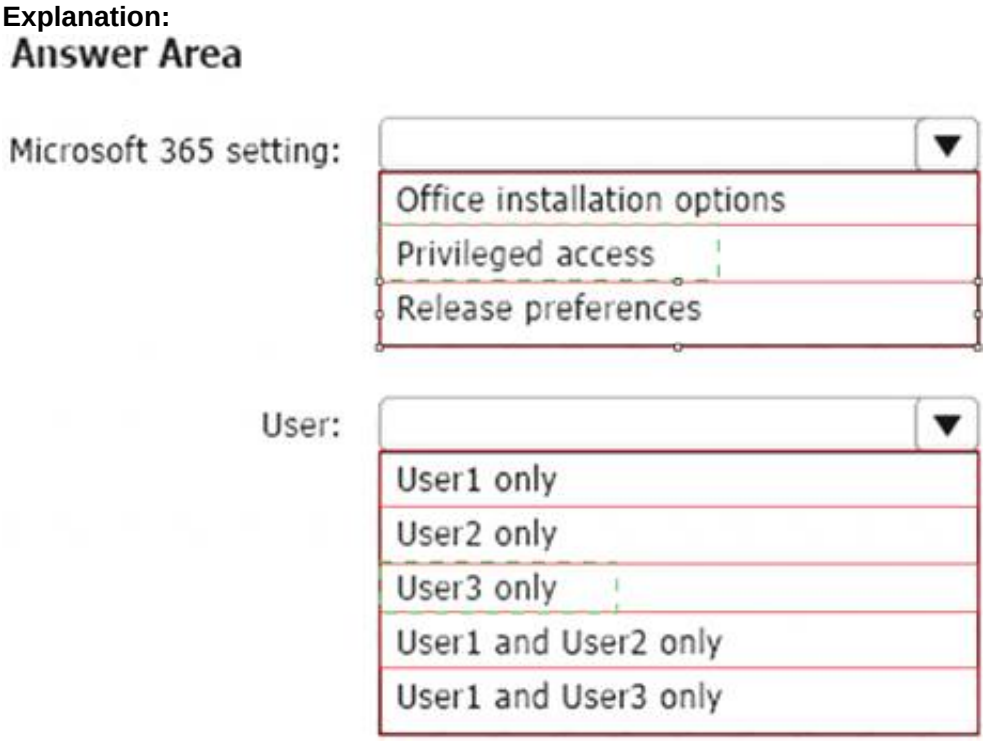
You plan to provide User4 with early access to Microsoft 365 feature and service updates.
You need to identify which Microsoft 365 setting must be configured, and which user can modify the setting. The solution must use the principle of least privilege.
What should you identify? To answer, select the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



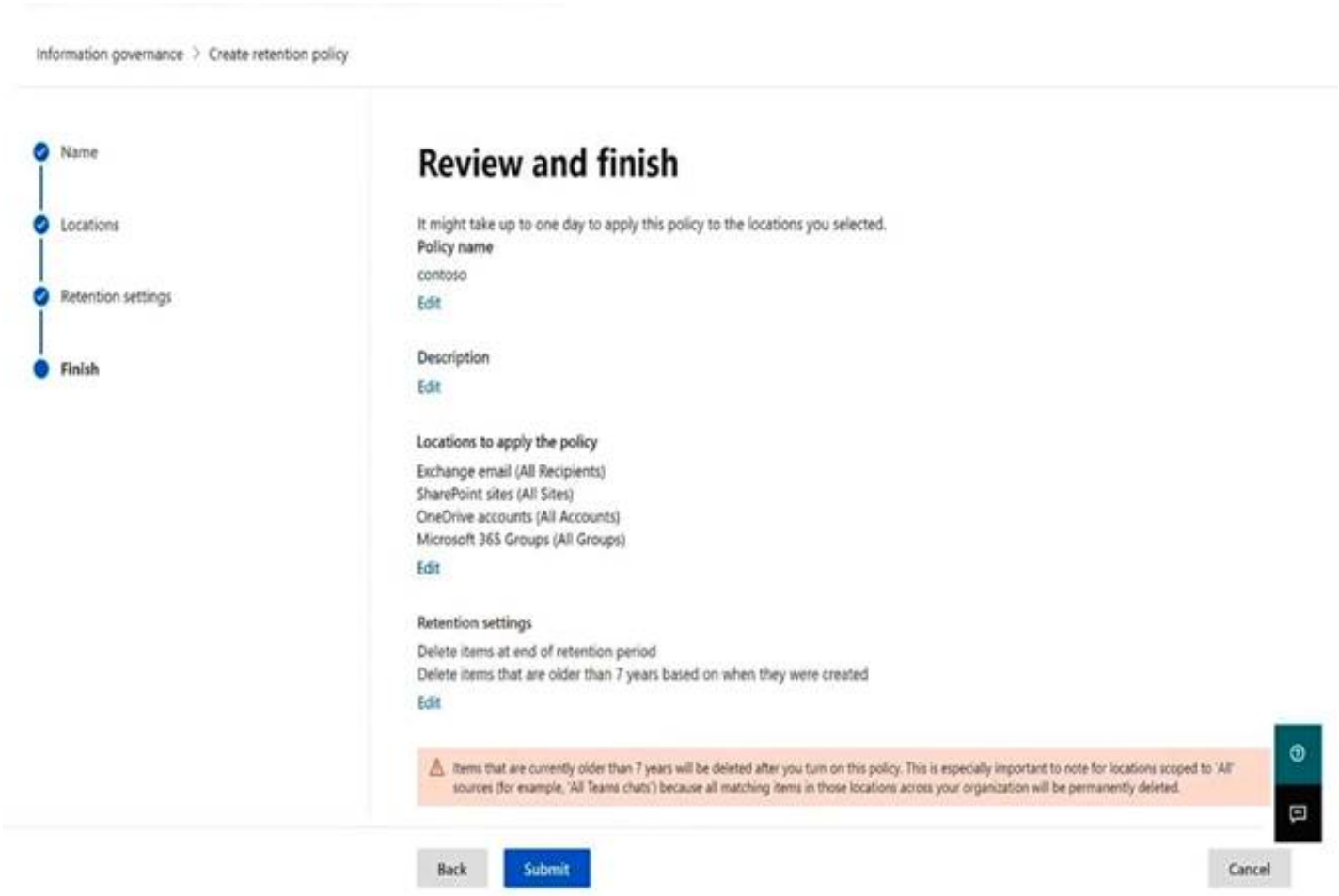
A. Mastered
B. Not Mastered

Answer: A

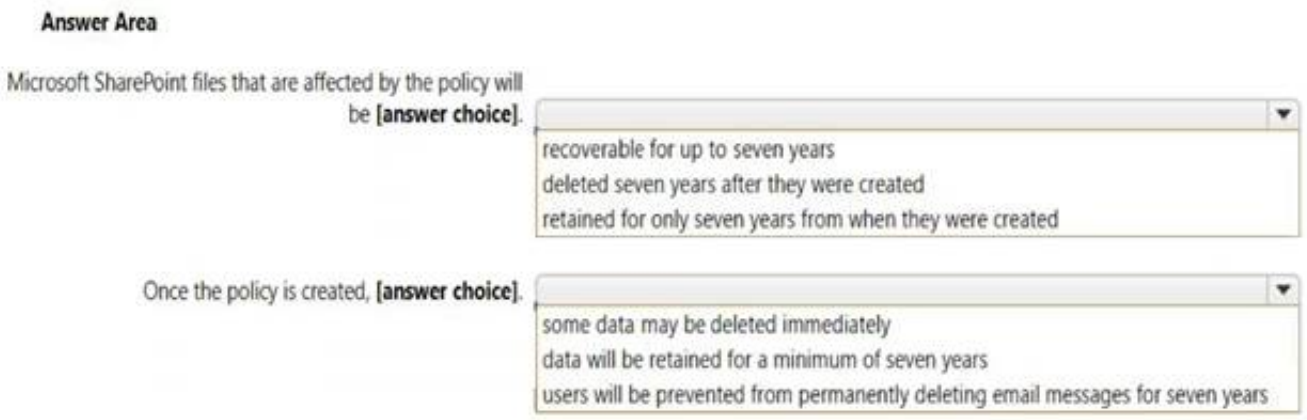
Explanation:



NEW QUESTION 155
- (Exam Topic 5)
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.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

NEW QUESTION 157
- (Exam Topic 5)
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

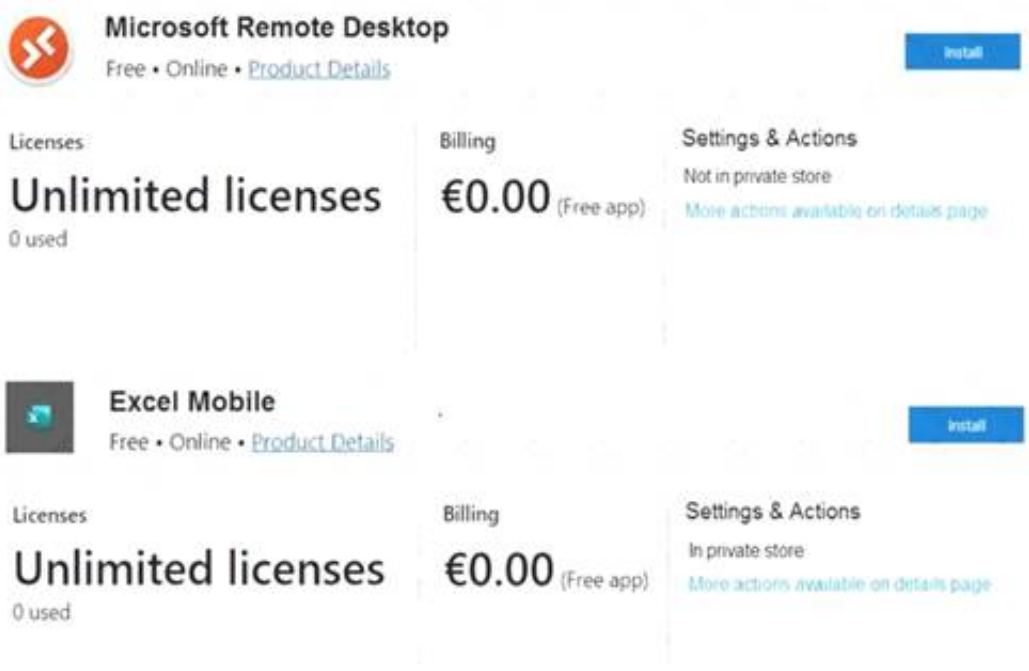
Answer: A

Explanation:

NEW QUESTION 158
- (Exam Topic 5)
You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure Active Directory (Azure AD) role
User1	Purchaser	Billing administrator
User2	Admin	Global administrator
User3	Basic Purchaser	None
User4	Basic Purchaser, Device Guard signer	Global reader

All users have Windows 10 Enterprise devices.
The Products & services settings in Microsoft Store for Business are shown in the following exhibit.



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

Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	○	○
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	○	○
User4 can manage the Microsoft Remote Desktop app from the private store.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

NEW QUESTION 161
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that has sensitivity label support enabled for Microsoft and SharePoint Online.
You need to enable unified labeling for Microsoft 365 groups. Which cmdlet should you run?

A. set-unifiedGroup
B. Set-Labelpolicy
C. Execute-AzureAdLebelSync
D. Add-UnifiedGroupLinks

Answer: C

NEW QUESTION 165
- (Exam Topic 5)
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 Policy1
B. only the settings of Policy2
C. only the settings of Policy3
D. no settings

Answer: C

NEW QUESTION 167
- (Exam Topic 5)
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:
Graphical user interface Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

NEW QUESTION 168
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 169
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:
- MDM user scope: Some
- Groups: Group1
- MAM user scope: Some
- Groups: Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll-device-administrator

NEW QUESTION 171
- (Exam Topic 5)
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 175
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

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

The devices are configured as shown in the following table.

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

You have a Conditional Access policy named CAPolicy1 that has the following settings:
* 1. Assignments
- Users or workload identities: Group1
- Cloud apps or actions: Office 365 SharePoint Online
- Conditions
- Filter for devices: Exclude filtered devices from the policy
- Rule syntax: device.displayName -startsWith "Device"
* 2. Access controls
- Grant
- Grant: Block access
- Session: 0 controls selected
* 3. Enable policy: On
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Answer Area

Statements	Yes	No
User1 can access Site1 from Device1.	○	○
User2 can access Site1 from Device2.	○	○
User2 can access Site1 from Device3.	○	○

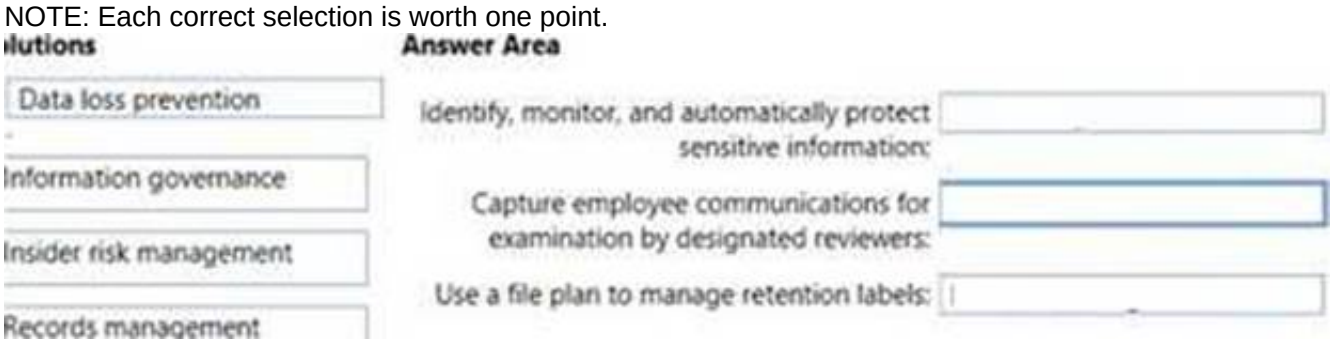
A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 180
- (Exam Topic 5)
DRAG DROP
You have a Microsoft 365 E5 tenant.
You need to implement compliance solutions that meet the following requirements:

• Use a file plan to manage retention labels.
• Identify, monitor, and automatically protect sensitive information.
• Capture employee communications for examination by designated reviewers.
Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated

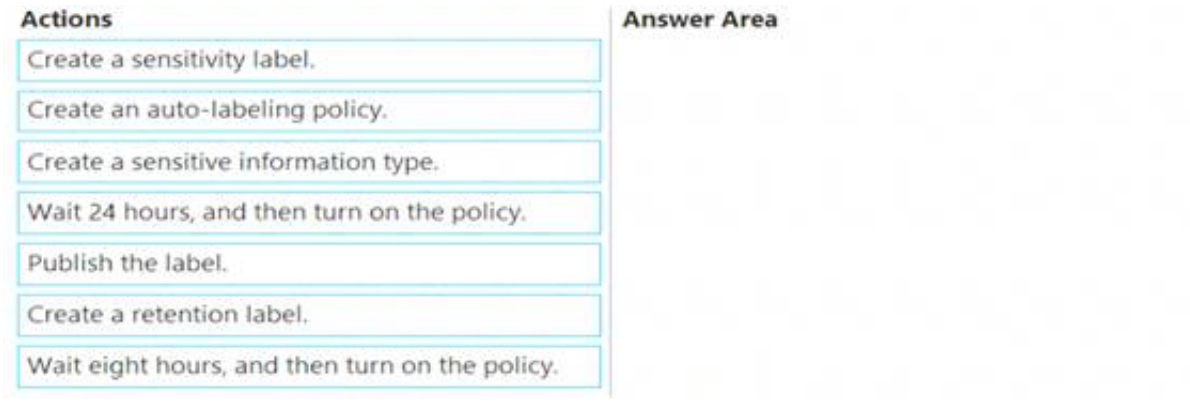
NEW QUESTION 182
- (Exam Topic 5)
Your company has multiple offices.
You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.
You need to ensure that the local administrators can manage only the devices in their respective office. What should you use?

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

Answer: A

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

NEW QUESTION 185
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. You need to automatically label the documents on Site1 that contain credit card numbers.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-labe https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-w

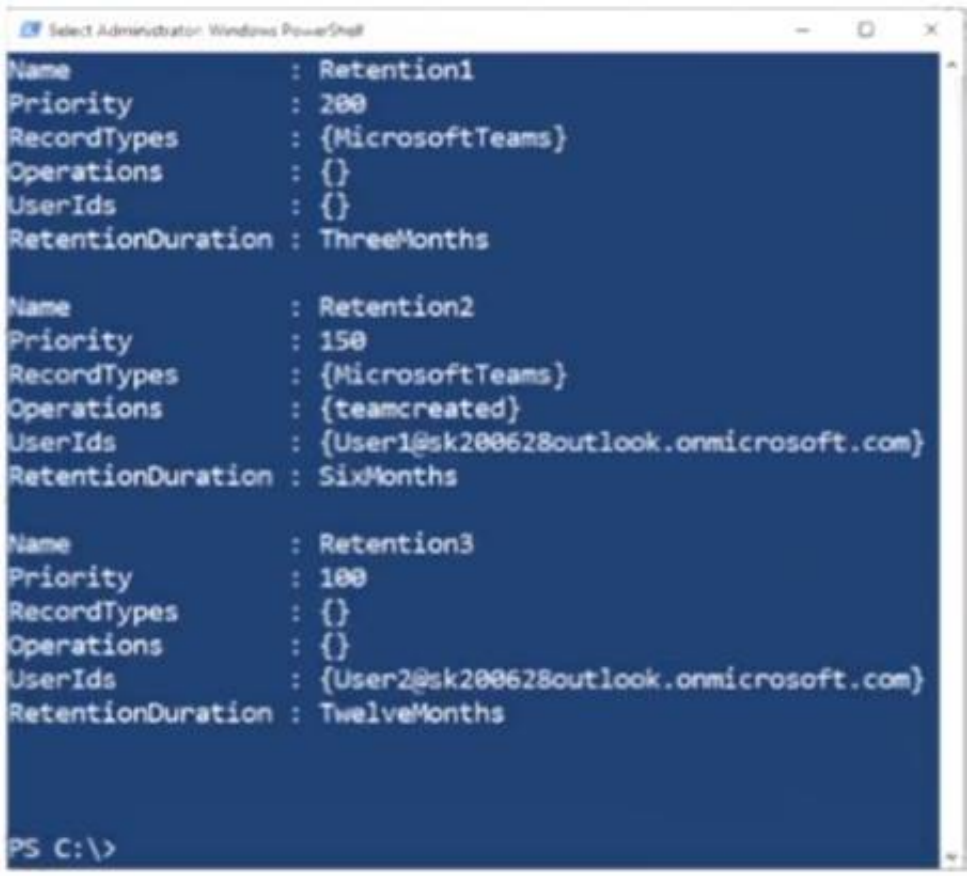
NEW QUESTION 186
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?

A. From the Cloud App Security admin center, select Users and accounts.
B. From the Microsoft 365 security center, view the Threat tracker.

C. From the Microsoft 365 admin center, view the Security & compliance report.
D. From the Azure Active Directory admin center, view the Risky sign-ins report.

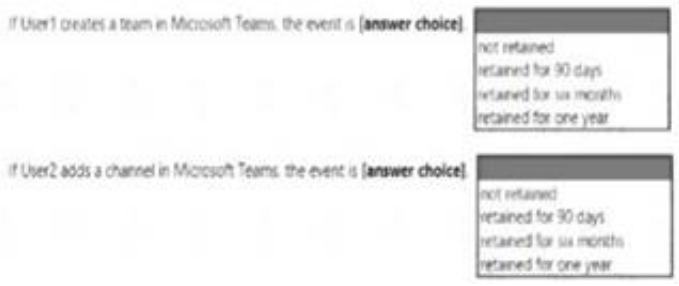
Answer: A

NEW QUESTION 191
- (Exam Topic 5)
You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.



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

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 196
- (Exam Topic 5)
You have a Microsoft 365 subscription that contains the users shown in the following table.

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

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

What is the minimum number of deployment groups required?

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

Answer: C

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

NEW QUESTION 197
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You have the retention policies shown in the following table.

Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx. File1.docx was created on January 1, 2022 and last modified on January 31,2022. The file was NOT modified again.
When will File1.docx be deleted automatically?

A. January 1,2023
B. January 1,2024
C. January 31, 2023
D. January 31, 2024
E. never

Answer: D

Explanation:
for the four different principles:
* 1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system-initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.
* 2. Etc. Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

NEW QUESTION 202
- (Exam Topic 5)
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

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

Answer: D

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

NEW QUESTION 205
- (Exam Topic 5)
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. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings. You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You raise the domain functional level to Windows Server 2019. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 209
- (Exam Topic 5)
You purchase a new computer that has Windows 10, version 2004 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

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

Answer: B

NEW QUESTION 210
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You need to identify which administrative users performed eDiscovery searches during the past week. What should you do from the Security & Compliance admin center?

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

Answer: D

NEW QUESTION 211
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.
Which two policies can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. a data loss prevention (DLP) policy
B. a sensitivity label policy
C. a Microsoft Cloud App Security file policy
D. a communication compliance policy
E. a retention label policy

Answer: AD

NEW QUESTION 216
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.
Company policy requires that the devices have the following configurations:
- Require complex passwords.
- Require the encryption of removable data storage devices.
- Have Microsoft Defender Antivirus real-time protection enabled.

You need to configure the devices to meet the requirements. What should you use?

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

Answer: B

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

NEW QUESTION 220
- (Exam Topic 5)
Your company has a Microsoft 365 E5 subscription. Users in the research department work with sensitive data.
You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents.
Users in other departments must not be restricted.
What should you do?

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

Answer: D

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

NEW QUESTION 225
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role. Does this meet the goal?

A. Yes
B. No

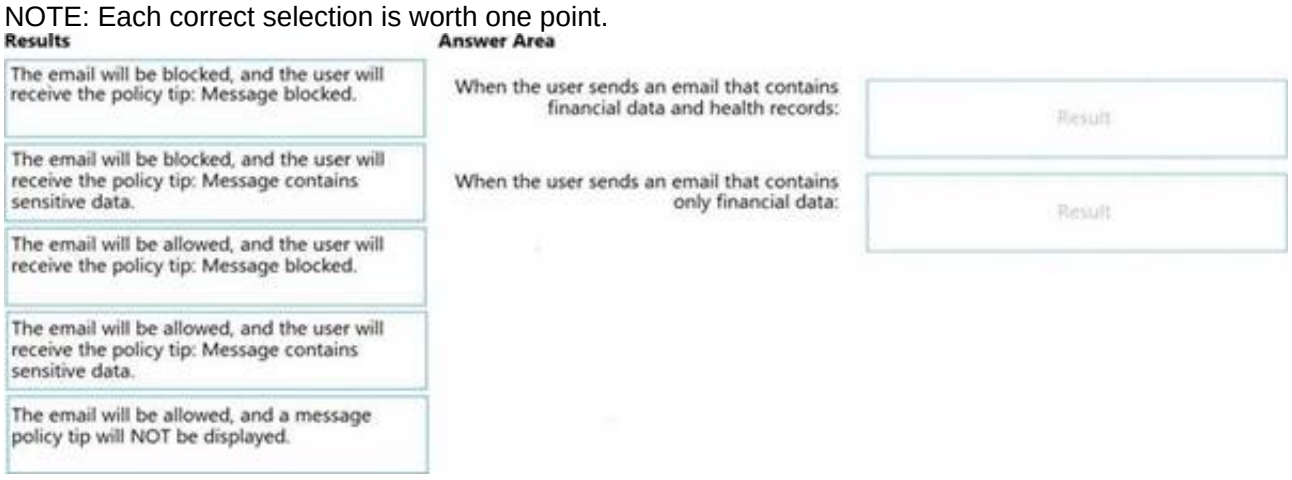
Answer: B

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

NEW QUESTION 226
- (Exam Topic 5)
DRAG DROP
You have a Microsoft 365 subscription.
In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:
- Block emails that contain financial data.
- Display the following policy tip text: Message blocked.

From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:
- Use the following location: Exchange email.
- Display the following policy tip text: Message contains sensitive data.
- When a user sends an email, notify the user if the email contains health records.

What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

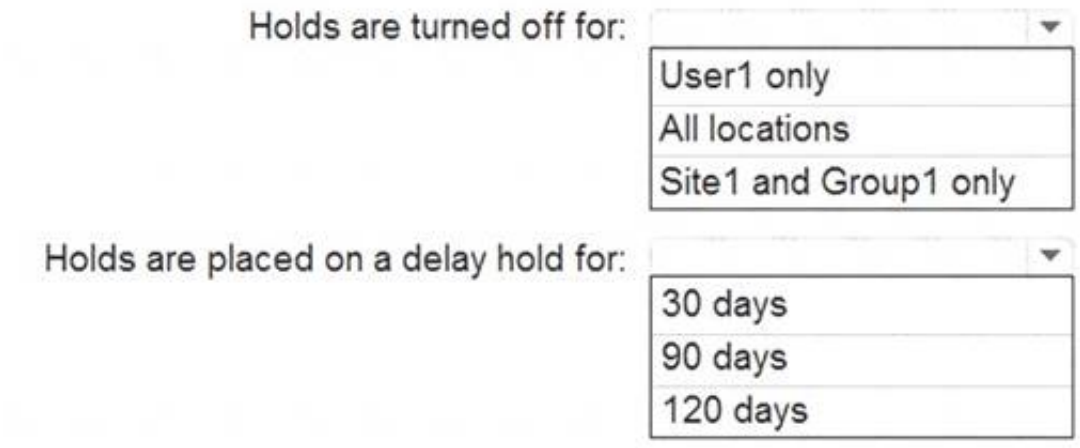
Answer: A

Explanation:
Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked.
If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.
Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data. Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers

NEW QUESTION 231

- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:
- Name: Case1
- Included content: Group1, User1, Site1
- Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders The investigation for Case1 completes, and you close the case.

What occurs after you close Case1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

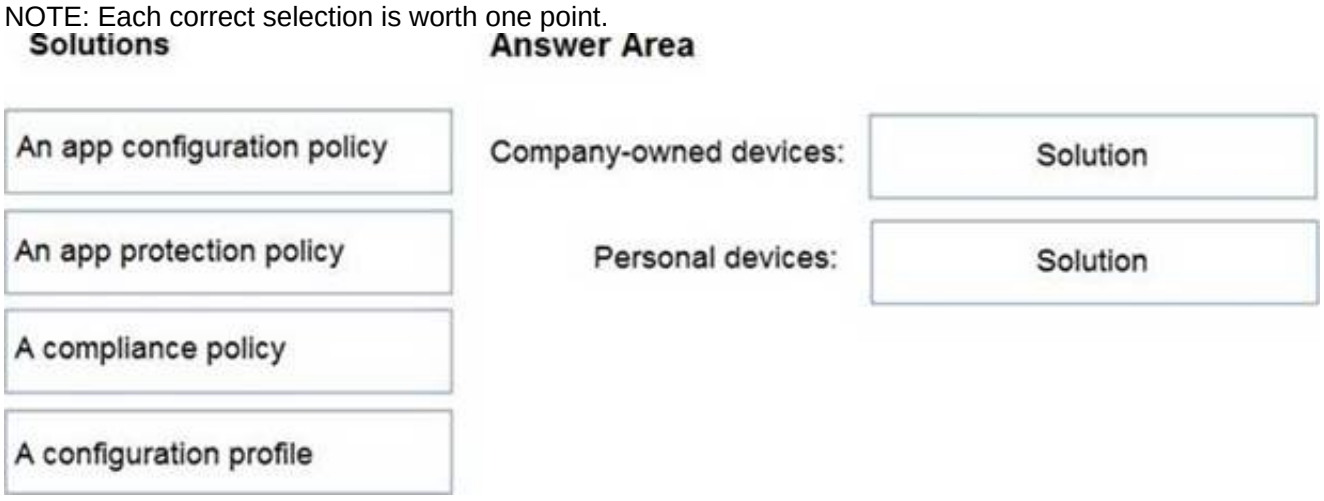


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/close-or-delete-case?view=o365-worldwide

NEW QUESTION 236
- (Exam Topic 5)
Your company has a Microsoft 365 E5 tenant.
Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.
You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.
What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application, Word Description automatically generated

NEW QUESTION 240
- (Exam Topic 5)
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. Reference:
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-assign-member

NEW QUESTION 242
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 246
- (Exam Topic 5)
You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Security Operator
User3	Security Reader
User4	Compliance Administrator

You plan to implement Microsoft Defender for Endpoint.
You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint. You need to identify which user can view security incidents from the Microsoft 365 Defender portal. Which user should you identify?

A. User1
B. User2
C. User3
D. User4

Answer: A

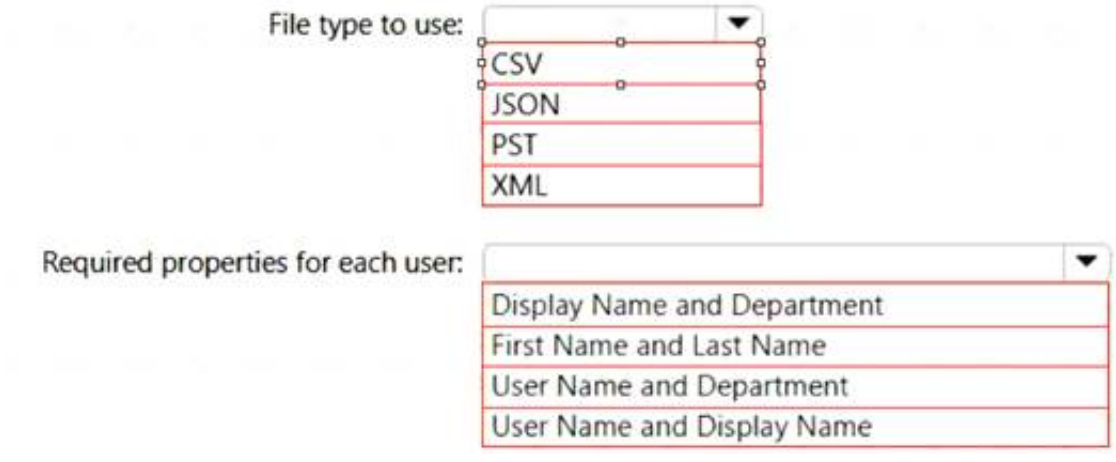
NEW QUESTION 249
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.
What is the maximum number of onmicrosoft.com domains the subscription can contain?

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

Answer: C

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

NEW QUESTION 251
- (Exam Topic 5)
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.
Answer Area



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.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/enterprise/add-several-users-at-the-same-time

NEW QUESTION 254
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.
You need to prevent the members or Group1 from communicating with the members of Group2 by using Microsoft Teams. The solution must comply with regulatory requirements and must not affect other user in the tenant.
What should you use?

A. information barriers

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

Answer: A

NEW QUESTION 259
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that contains the following user:
- Name: User1
- UPN: user1@contoso.com
- Email address: user1@marketmg.contoso.com
- MFA enrollment status: Disabled

When User1 attempts to sign in to Outlook on the web by using the user1@marketing.contoso.com email address, the user cannot sign in.
You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com. What should you do?

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

Answer: D

Explanation:
Microsoft's recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN's to match.
Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user's email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only needs to remember a single name.
Configure the Azure AD multifactor authentication registration policy
Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.
Reference:
https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname

NEW QUESTION 260
- (Exam Topic 5)
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 264
- (Exam Topic 5)
Your on-premises network contains an Active Directory domain named Contoso.com and 500 devices that run either macOS, Windows 8.1. Windows 10, or Windows 11. All the devices are managed by using Microsoft Endpoint Configuration Manager. The domain syncs with Azure Active Directory (Azure AD).
You plan to implement a Microsoft 365 E5 subscription and enable co-management. Which devices can be co-managed after the implementation?

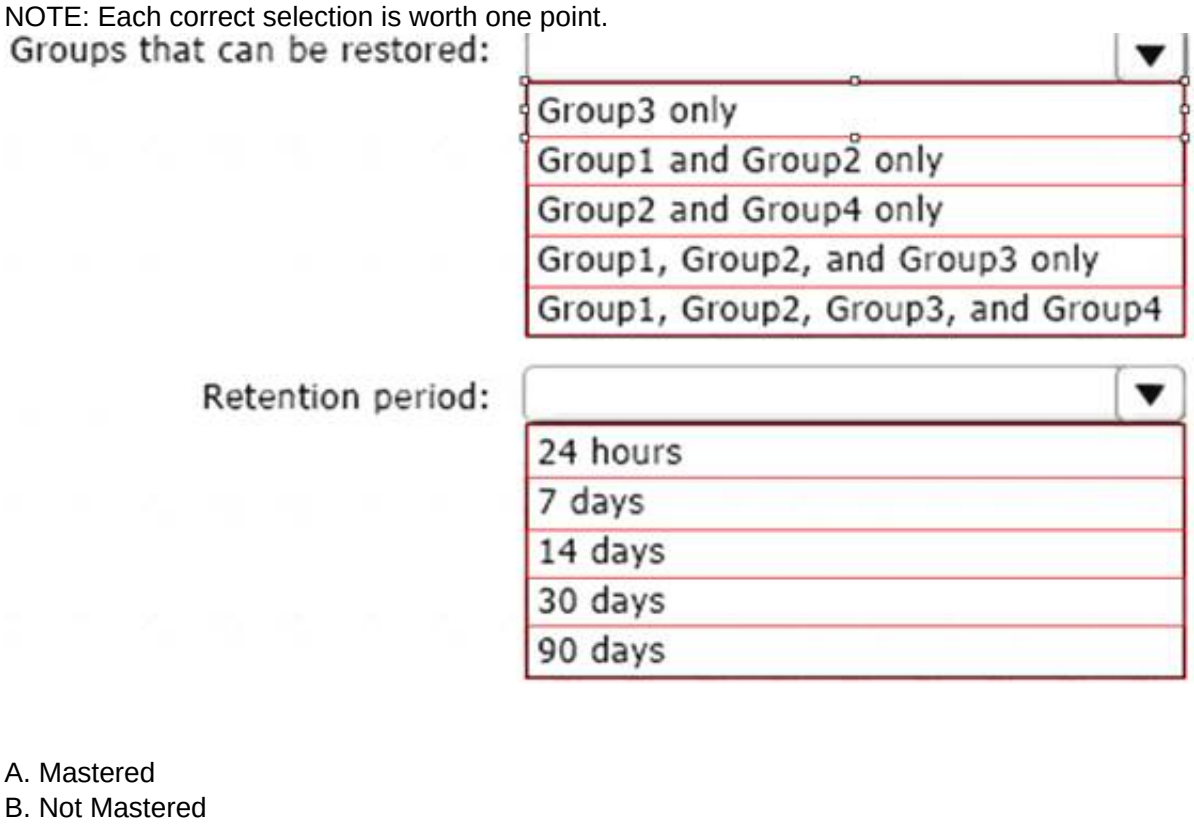
A. Windows 11 and Windows 10 only
B. Windows 11, Windows 10-Windows8.1.andmacOS
C. Windows 11 and macOS only
D. Windows 11 only
E. Windows 11. Windows 10, and Windows8.1 only

Answer: C

NEW QUESTION 265
- (Exam Topic 5)
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.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/restore-deleted-group

NEW QUESTION 270
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MS-102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MS-102 Product From:

https://www.2passeasy.com/dumps/MS-102/

Money Back Guarantee

MS-102 Practice Exam Features:

* MS-102 Questions and Answers Updated Frequently

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

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

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