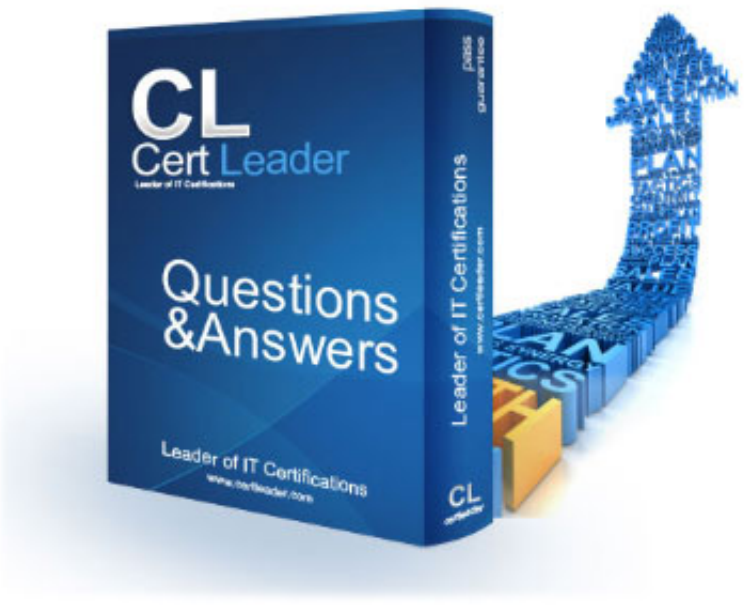
MS-102 Dumps

Microsoft 365 Administrator Exam

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



NEW QUESTION 1
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription.
You need to review metrics for the following: The daily active users in Microsoft Teams Recent Microsoft service issues
What should you use? 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: Usage reports
The daily active users in Microsoft Teams
Microsoft 365 Reports in the admin center - Microsoft Teams usage activity
The brand-new Teams usage report gives you an overview of the usage activity in Teams, including the number of active users, channels and messages so you can quickly see how many users across your organization are using Teams to communicate and collaborate. It also includes other Teams specific activities, such as the number of active guests, meetings, and messages.
Box 2: Service Health
Recent Microsoft service issues
You can view the health of your Microsoft services, including Office on the web, Yammer, Microsoft Dynamics CRM, and mobile device management cloud services, on the Service health page in the Microsoft 365 admin center. If you are experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

NEW QUESTION 2
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Service 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?view=o365-worldwide

NEW QUESTION 3
- (Topic 6)
You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management. You need to add the phone number of the help desk to the Company Portal app. What should you do?

A. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.
B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.
C. From the Microsoft 365 admin center, modify Organization information.
D. From the Microsoft 365 admin center, modify Help desk information.

Answer: A

Explanation:
Reference:
https://systemcenterdudes.com/intune-company-portal-customization/

NEW QUESTION 4
DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You need to automatically label the documents on Site1 that contain credit card numbers. Which three actions should you perform in sequence? To answer, move the appropriate
actions from the list of actions to the answer area and arrange them in the correct order.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 5
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.
You need to remove User1 from the Restricted entities list. What should you use?

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

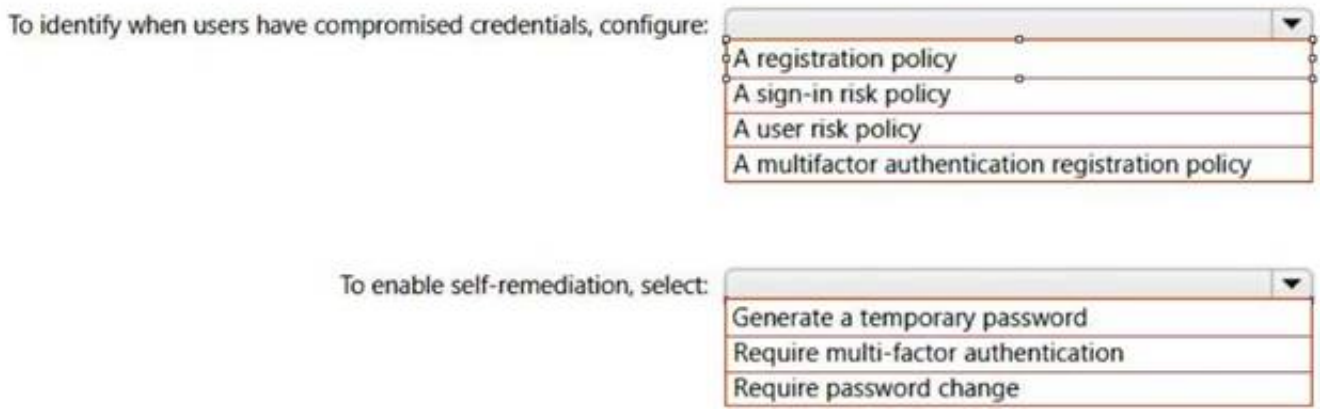
Answer: D

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

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

NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 7
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 8
- (Topic 6)
Your company has offices in five cities. The company has a Microsoft 365 tenant.
Each office is managed by a local administrator. You plan to deploy Microsoft Intune.
You need to recommend a solution to manage resources in intune that meets the following requirements:
? Local administrators must be able to manage only the resources in their respective office.
? Local administrators must be prevented from managing resources in other offices.
? Administrative effort must be minimized.
What should you include in the recommendation?

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

Answer: B

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

NEW QUESTION 9
- (Topic 6)
You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft 365 compliance policies to meet the following requirements:
? Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
? Report on shared documents that contain PII.
What should you create?

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

Answer: B

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

NEW QUESTION 10
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You plan to deploy 1.000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.
You need to recommend a Microsoft Intune enrollment option that meets the following requirements:
• Minimizes user interaction
• Minimizes administrative effort
• Automatically installs corporate apps What should you recommend?

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

Answer: A

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

NEW QUESTION 10
- (Topic 6)
You have a Microsoft 365 subscription.
You discover that some external users accessed center for a Microsoft SharePoint site. You modify the sharePoint sharing policy to prevent sharing, outside your organization. You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the Security $ Compliance admin center you create a threat management
policy.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 13
- (Topic 6)
Your company has 10,000 users who access all applications from an on-premises data center.
You plan to create a Microsoft 365 subscription and to migrate data to the cloud. You plan to implement directory synchronization.
User accounts and group accounts must sync to Azure AD successfully. You discover that several user accounts fail to sync to Azure AD.
You need to resolve the issue as quickly as possible. What should you do?

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

Answer: B

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

NEW QUESTION 15
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.
Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

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

NEW QUESTION 19
- (Topic 6)
You have a Microsoft 365 subscription.
You register two applications named App1 and App2 to Azure AD.
You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

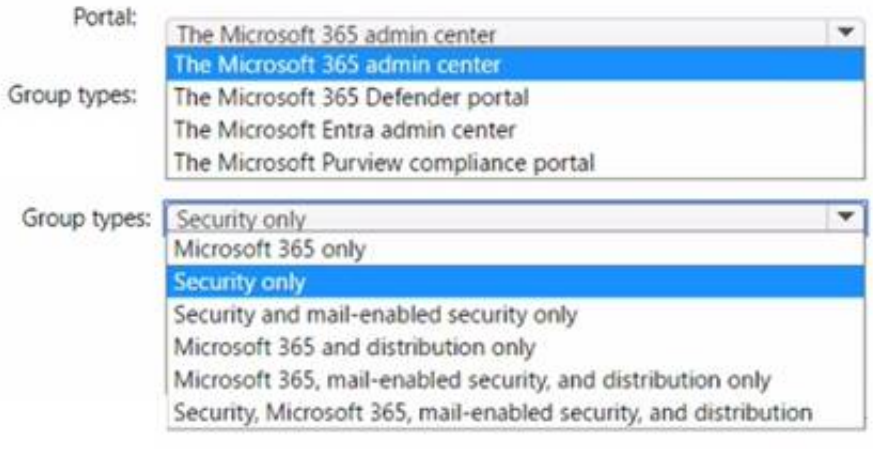
A. From the Microsoft Entra admin center, create a conditional access policy
B. From the Microsoft 365 admin center, configure the Modem authentication settings.
C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.
D. From Multi-Factor Authentication, configure the service settings.

Answer: A

Explanation:
Use Conditional Access policies
If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication

NEW QUESTION 24
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to configure a group naming policy.
Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

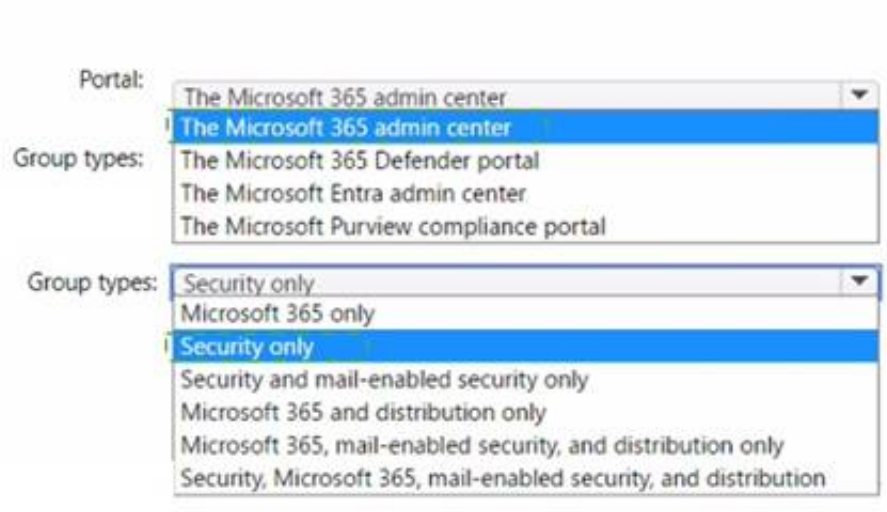


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 25
HOTSPOT - (Topic 6)
You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 27
- (Topic 6)
You have a Microsoft 365 E5 subscription.
On Monday, you create a new user named User1.
On Tuesday, User1 signs in for the first time and perform the following actions:
• Signs in to Microsoft Exchange Online from an anonymous IP address
• Signs in to Microsoft SharePoint Online from a device in New York City.
• Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections
Which types of sign-in risks will Azure AD Identity Protection detect for User1?

A. anonymous IP address only
B. anonymous IP address and atypical travel

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

Answer: C

NEW QUESTION 28
- (Topic 6)
You have a Microsoft 365 tenant that contains the groups shown in the following table.

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

You plan to create a new Windows 10 Security Baseline profile. To which groups can you assign to the profile?

A. Group3 only
B. Group1 and Group3 only
C. Group2 and Group3 only
D. Group1. Group2. and Group3

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile
https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

NEW QUESTION 32
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription that contains the users in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

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

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

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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 33
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:
? Deploy a VPN connection by using a VPN device configuration profile.
? Configure security settings by using an Endpoint Protection device configuration profile.
You support the management tasks.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

VPN device configuration profile:
- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Endpoint Protection device configuration profile:
- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

A. Mastered
B. Not Mastered

Answer: A

Explanation:

VPN device configuration profile:
- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Endpoint Protection device configuration profile:
- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

NEW QUESTION 34
- (Topic 6)
You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:
• Retention period 7 years
• Start the retention period bated on: When items were created
You need to prevent the removal of the label once the label K applied to a lie What should you select in the retention label settings?

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

Answer: B

NEW QUESTION 36
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. A Built-in protection preset security policy is applied to the subscription.
Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: CE

NEW QUESTION 38
- (Topic 6)
You have a Microsoft 365 subscription.
You plan to use Adoption Score and need to ensure that it can obtain device and software metrics.
What should you do?

A. Enable Endpoint analytics.
B. Run the Microsoft 365 network connectivity test on each device.
C. Enable privileged access.
D. Configure Support integration.

Answer: A

NEW QUESTION 40
- (Topic 6)
Your company has multiple offices.
You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.
You need to ensure that the local administrators can manage only the devices in their respective office.
What should you use?

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

Answer: A

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

NEW QUESTION 44
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the resources shown in the following table.

Name	Type
Group1	Microsoft 365 group
Group2	Distribution group
Site1	Microsoft SharePoint site

You create a sensitivity label named Label1. To which resource can you apply Label1?

A. Group1 only
B. Group2 only
C. Sitel only
D. Groupl and Group2 only
E. Group1, Group2, and Sitel

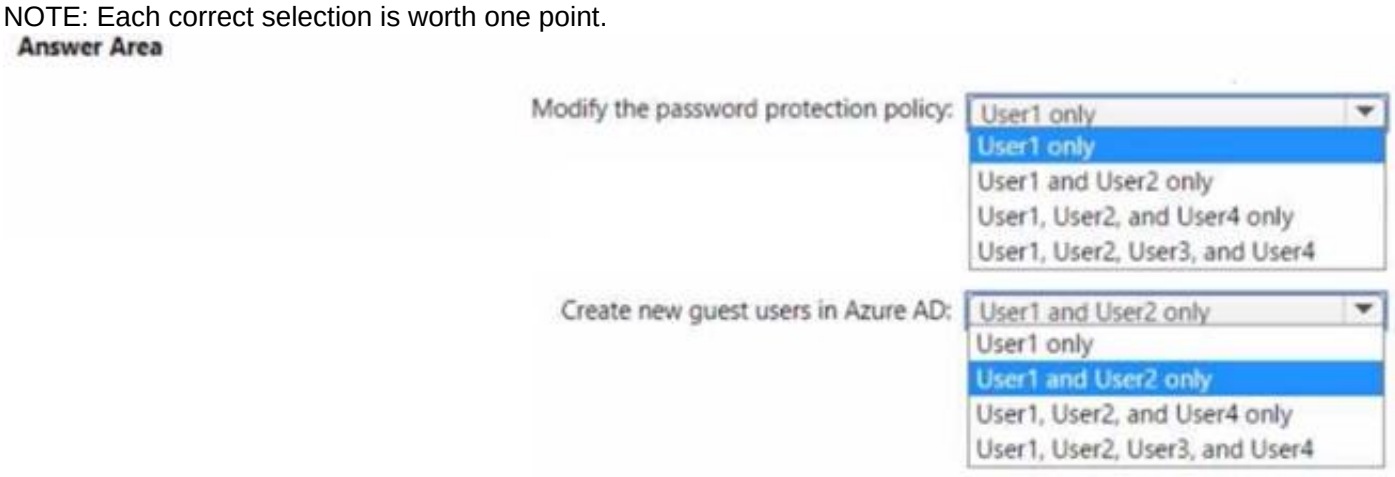
Answer: E

Explanation:
Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory
Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.
In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.
When you configure a label policy, you can:
Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams- groups-sites
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365- worldwide

NEW QUESTION 48
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 subscription that contains the users shown in the following table.

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

External collaboration settings have default configuration.
You need to identify which users can perform the following administrative tasks:
• Modify the password protection policy.
• Create guest user accounts.
Which users should you identify for each task? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 52
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

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

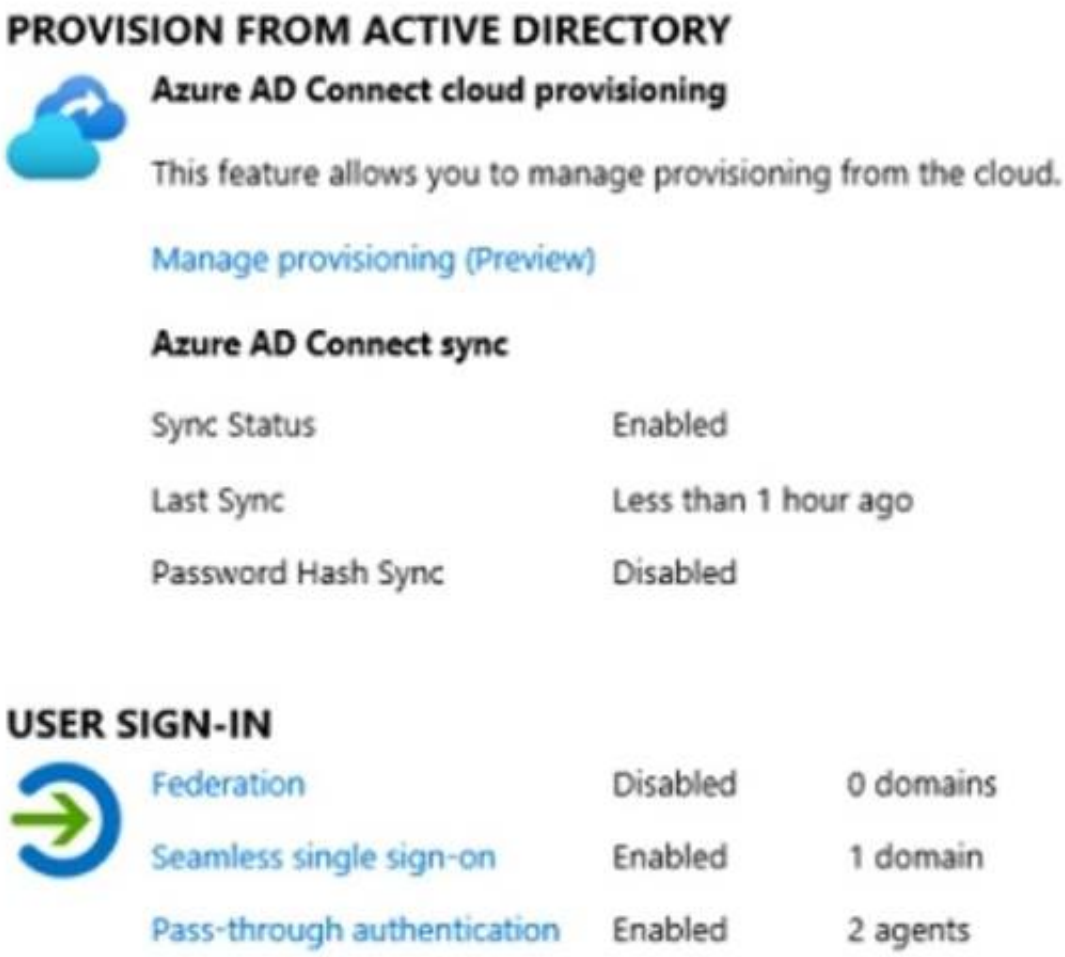
Answer: D

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

NEW QUESTION 57
HOTSPOT - (Topic 6)
HOTSPOT
Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:
? Contoso.com
? East.contoso.com
The forest contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	East.contoso.com
User3	Fabrikam.com

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



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

Statements	Yes	No
User1 can authenticate to Azure AD by using a username of user1@contoso.com.	○	○
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	○	○
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.
Box 2: No
The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.
Box 3: No
The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

NEW QUESTION 61
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Endpoint Management admin center, you create a device configuration profile.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You need to create a trusted location and a conditional access policy.

NEW QUESTION 65
- (Topic 6)
You have a Microsoft 365 subscription that contains the alerts shown in the following table.

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

Which properties of the alerts can you modify?

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

Answer: B

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

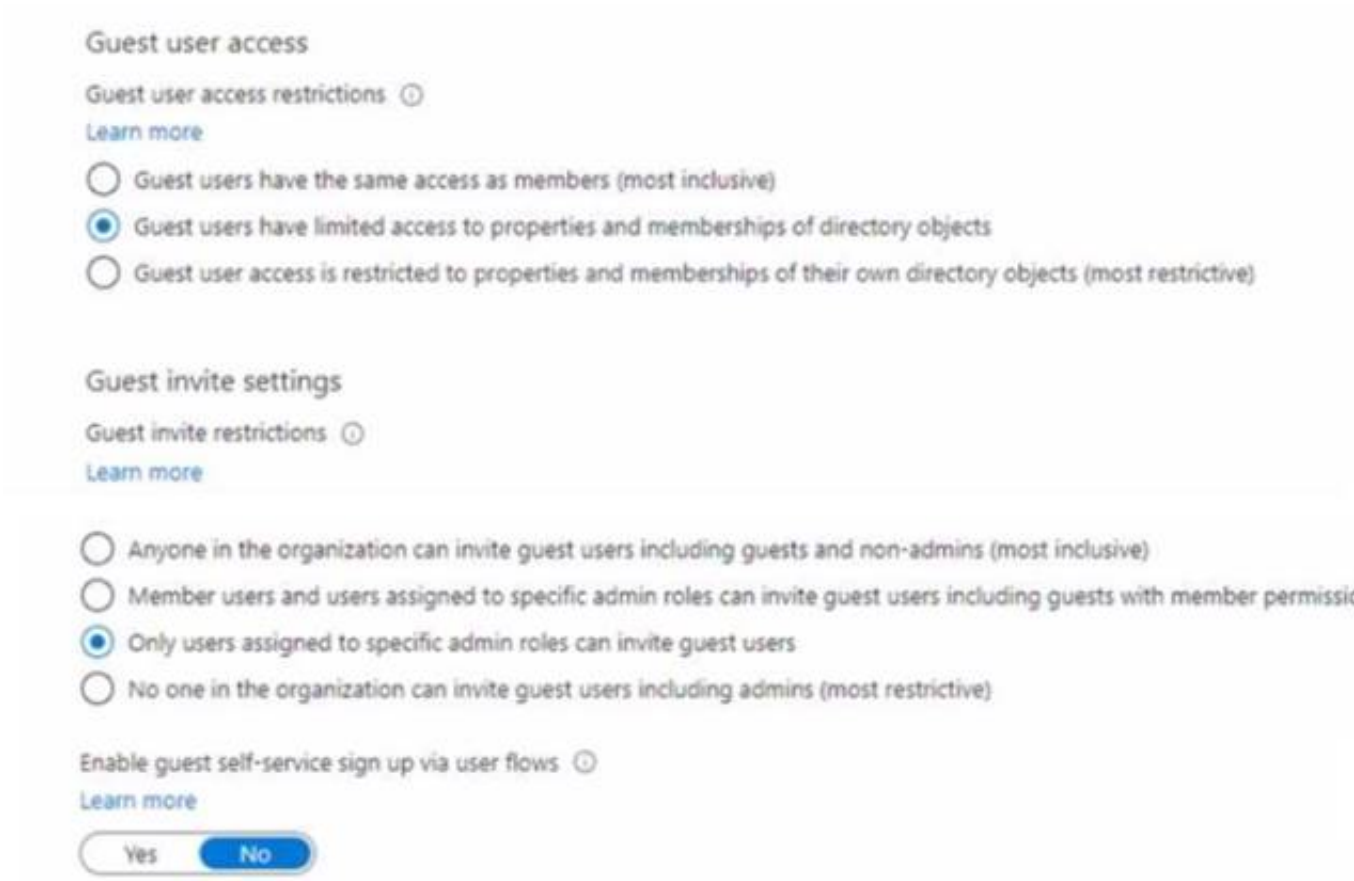
NEW QUESTION 70
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

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

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

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



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

NOTE: Each correct selection is worth one point.

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

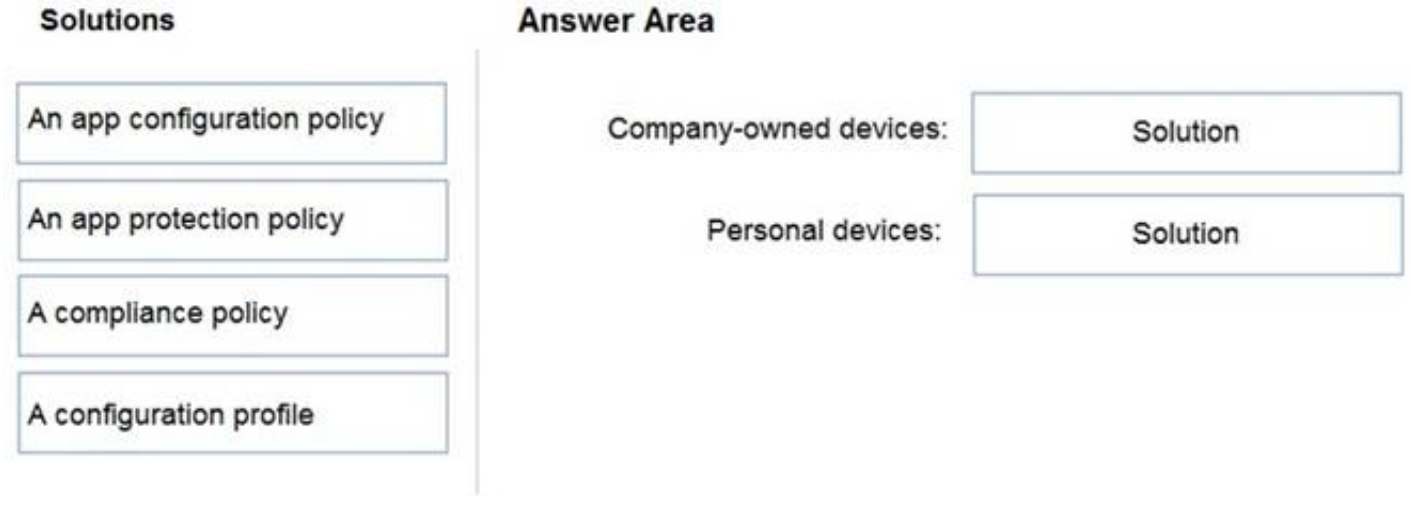
Explanation:

Answer Area

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

NEW QUESTION 75
DRAG DROP - (Topic 6)
Your company has a Microsoft 365 E5 tenant.
Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level

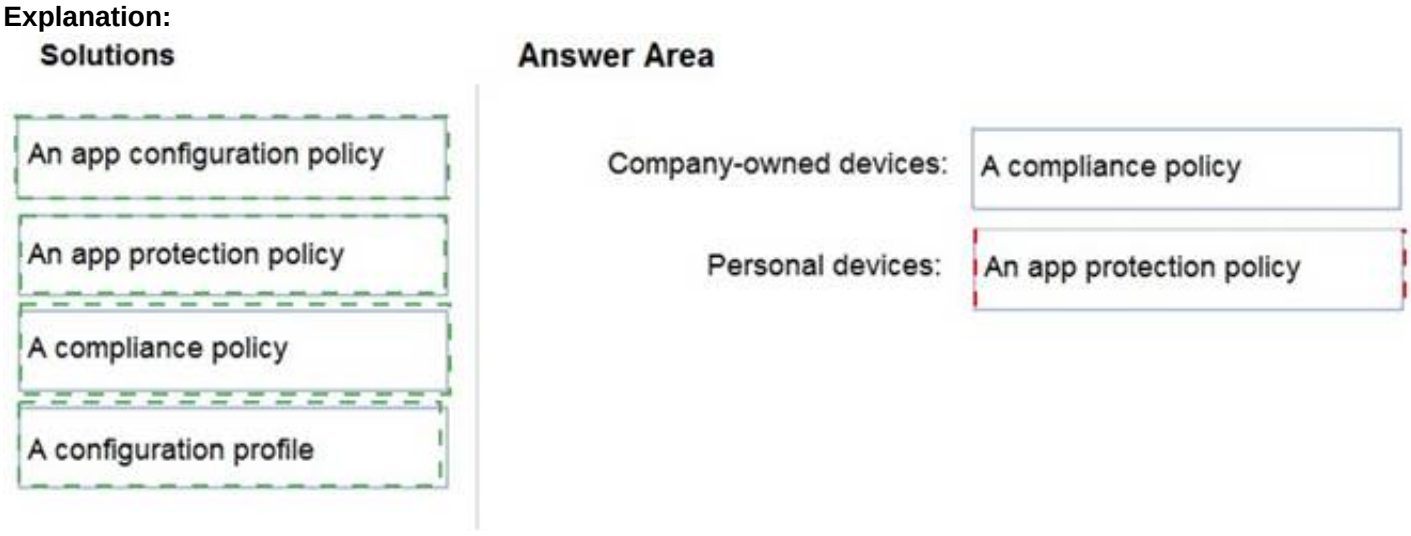
of medium or lower to access Microsoft Exchange Online mailboxes.
You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.
What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 80
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.
You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for
10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.
You plan to onboard all the devices to Microsoft Defender for Endpoint. You need to store the Microsoft Defender for Endpoint data in Europe. What should you do first?

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

Answer: B

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

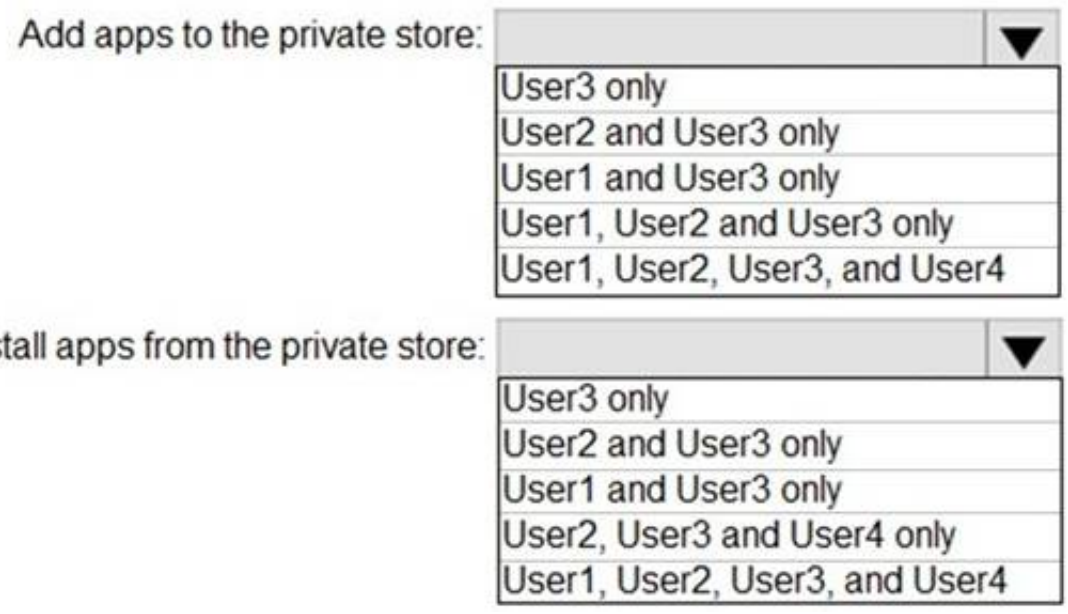
NEW QUESTION 81
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

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

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

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

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



A. Mastered
B. Not Mastered

Answer: A

Explanation:

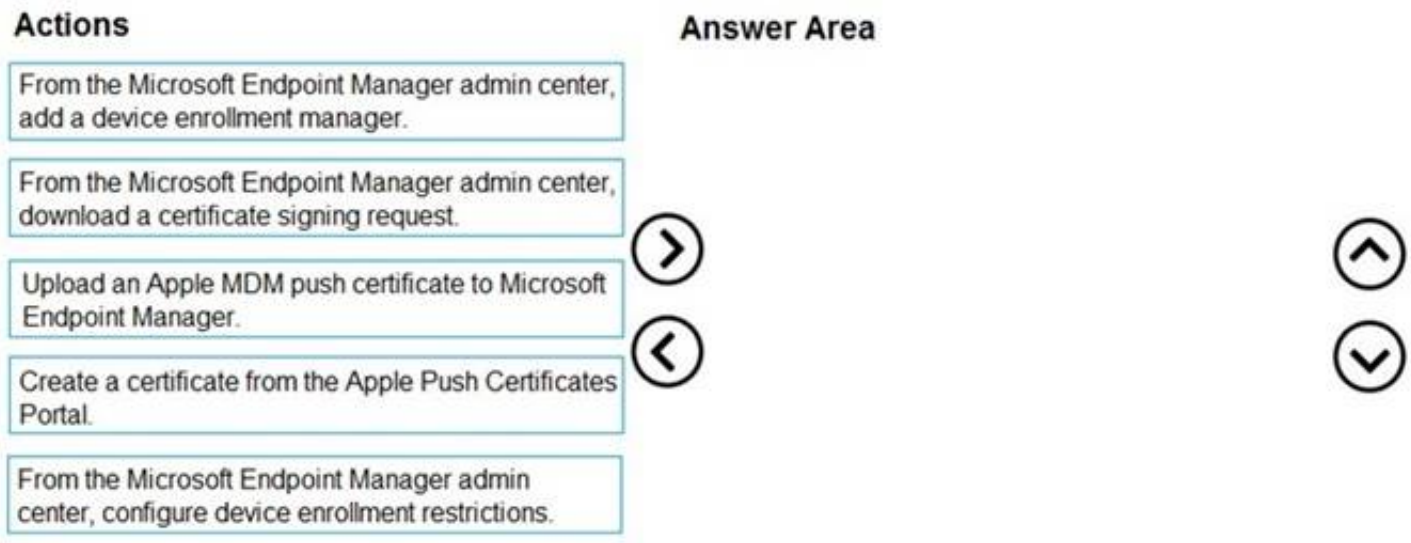
NEW QUESTION 84
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You plan to perform device discovery and authenticated scans of network devices. You install and register the network scanner on a device named Device1.
What should you do next?

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

Answer: C

NEW QUESTION 89
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 E5 subscription. Several users have iOS devices.
You plan to enroll the iOS devices in Microsoft Endpoint Manager.
You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the

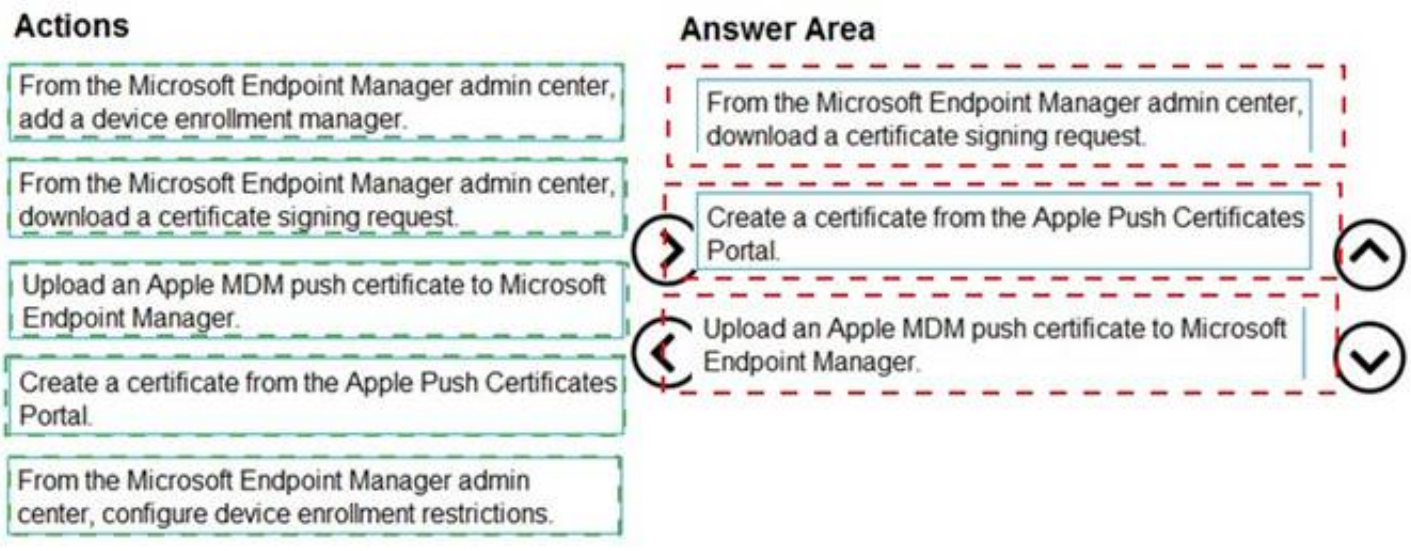
correct order.



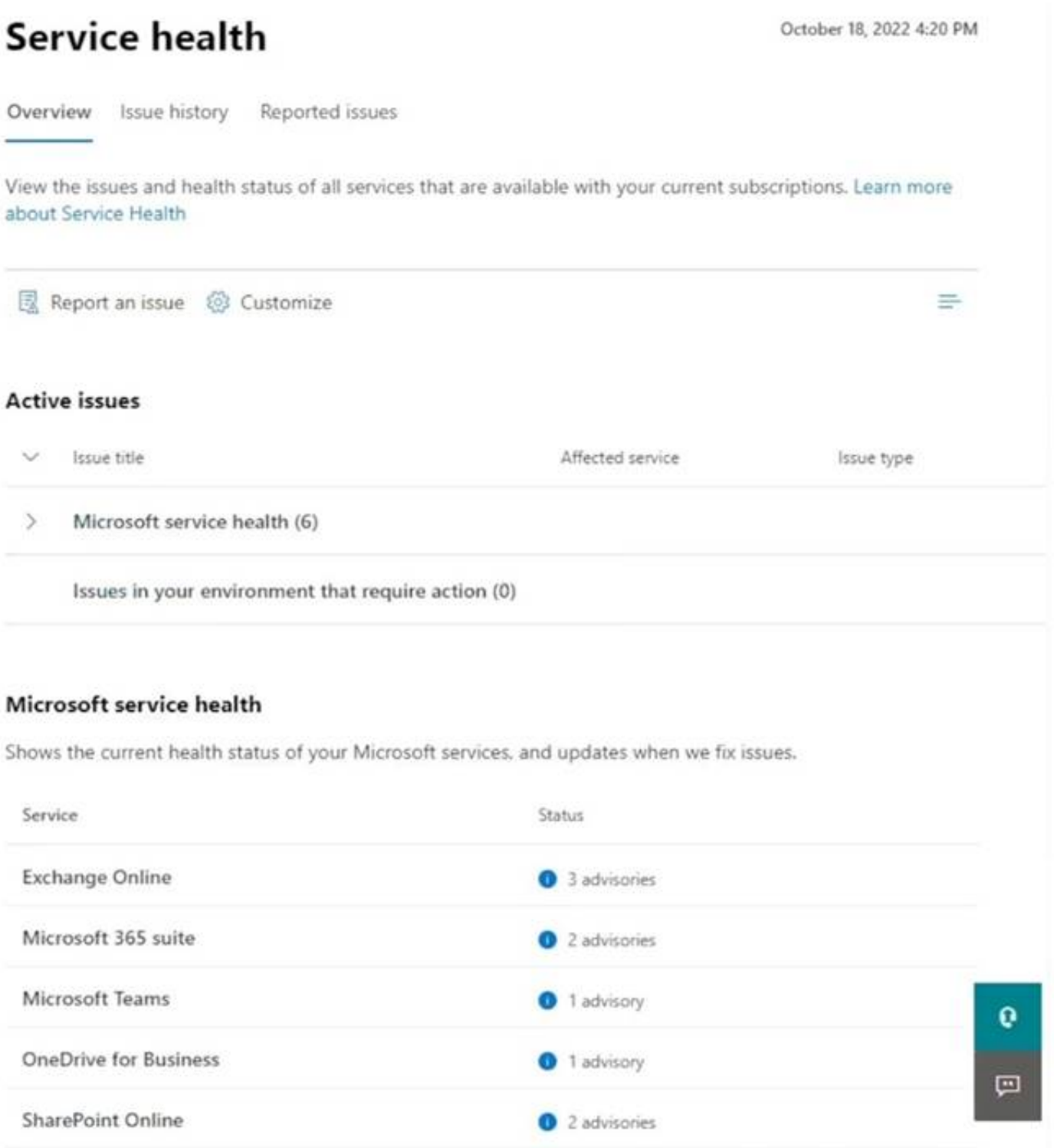
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 91
- (Topic 6)
You have a Microsoft 365 subscription.
You view the Service health Overview as shown in the following exhibit.



You need to ensure that a user named User1 can view the advisories to investigate service health issues.
Which role should you assign to User1?

A. Message Center Reader
B. Reports Reader
C. Service Support Administrator
D. Compliance Administrator

Answer: B

Explanation:
Service Support admin
Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:
- Open and manage service requests
- View and share message center posts
- Monitor service health
Incorrect:
* Message center reader
Assign the Message center reader role to users who need to do the following:
- Monitor message center notifications
- Get weekly email digests of message center posts and updates
- Share message center posts
- Have read-only access to Azure AD services, such as users and groups
* Reports reader
Assign the Reports reader role to users who need to do the following:
- View usage data and the activity reports in the Microsoft 365 admin center
- Get access to the Power BI adoption content pack
- Get access to sign-in reports and activity in Azure AD
- View data returned by Microsoft Graph reporting API
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

NEW QUESTION 94
- (Topic 6)
You have a Microsoft 365 subscription.
You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.
To which location can the policy be applied?

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

Answer: B

NEW QUESTION 97
- (Topic 6)
You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.
You need to prevent the members or Group1 from communicating with the members of Group2 by using Microsoft Teams. The solution must comply with regulatory requirements and must not affect other user in the tenant.
What should you use?

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

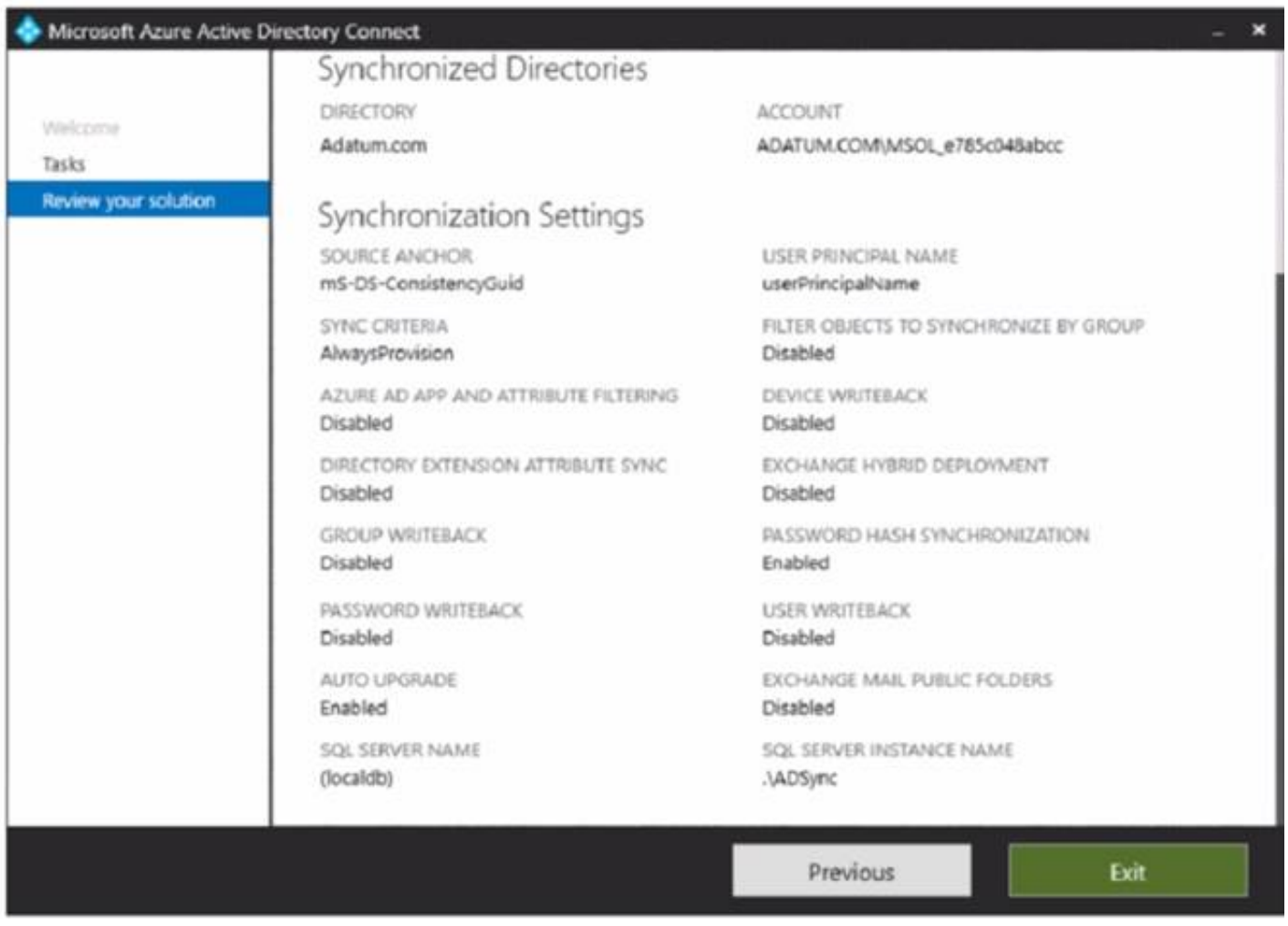
Answer: A

NEW QUESTION 102
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature. You need to block users from downloading a file named File1.exe.
What should you use?

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

Answer: A

NEW QUESTION 103
HOTSPOT - (Topic 6)
Your network contains an on-premises Active Directory domain that is synced to Azure AD as shown in the following exhibit.



An on-premises Active Directory user account named Allan You is synchronized to Azure AD. You view Allan's account from Microsoft 365 and notice that his username is set to Allan @>ddatum.onmicrosoft.com.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From the Azure portal, you can reset the password of Allan Yoo.	○	○
From the Azure portal, you can configure the job title of Allan Yoo.	○	○
From the Azure portal, you can configure the usage location of Allan Yoo.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From the Azure portal, you can reset the password of Allan Yoo.	○	○
From the Azure portal, you can configure the job title of Allan Yoo.	○	○
From the Azure portal, you can configure the usage location of Allan Yoo.	○	○

NEW QUESTION 107
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

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

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

Name	Role
User1	*None*
User2	Purchaser
User3	Basic Purchaser

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

Can add apps to the private store: ▼
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Can assign apps from Microsoft Store for Business: ▼
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 108
- (Topic 6)
You have a Microsoft 365 E5 subscription.
From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.
What is the longest time range that can be included in the report?

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

Answer: C

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

NEW QUESTION 112
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft intune. The subscription contains the resources shown in the following table.

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.
You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table.
On Thursday, you review the results of the app deployments.

Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

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
Word is installed on Device1.	○	○
App3 is displayed in the Company Portal.	○	○
Excel is installed on Device1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Word is installed on Device1.	○	○
App3 is displayed in the Company Portal.	○	○
Excel is installed on Device1.	○	○

NEW QUESTION 115
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.

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

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

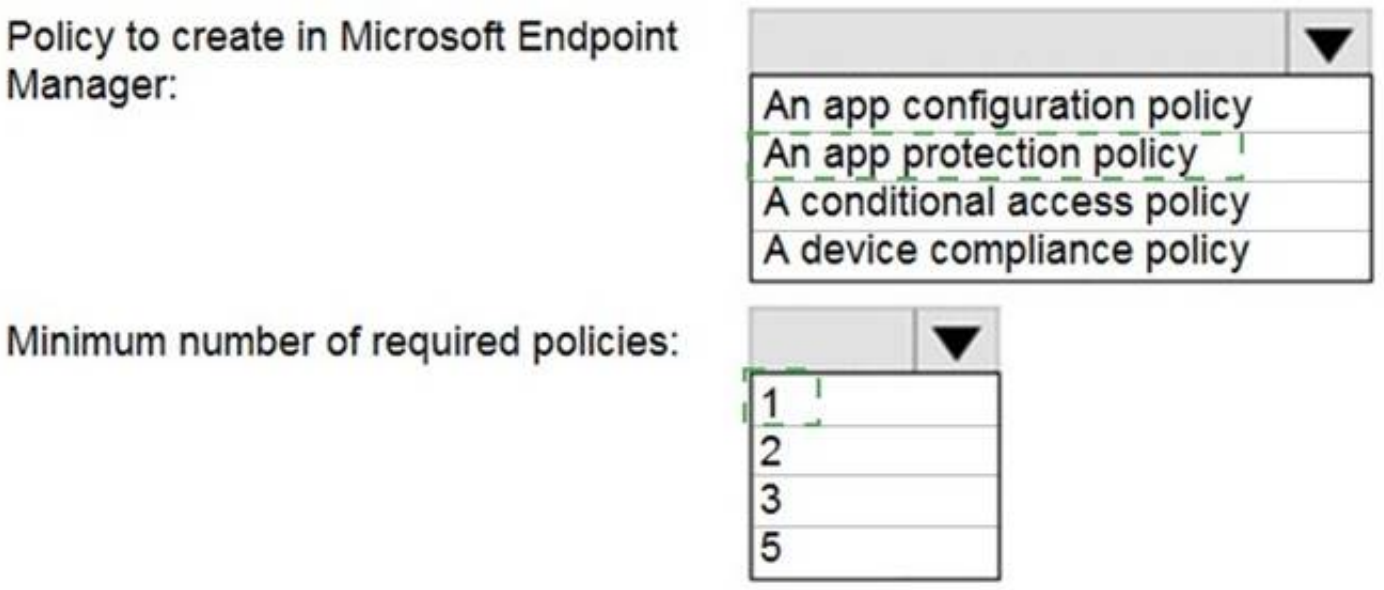
Policy to create in Microsoft Endpoint Manager:
- An app configuration policy
- An app protection policy
- A conditional access policy
- A device compliance policy

Minimum number of required policies:
- 1
- 2
- 3
- 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

The devices are managed by using Microsoft Intune.
You plan to use a configuration profile to assign the Delivery Optimization settings. Which devices will support the settings?

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

Answer: A

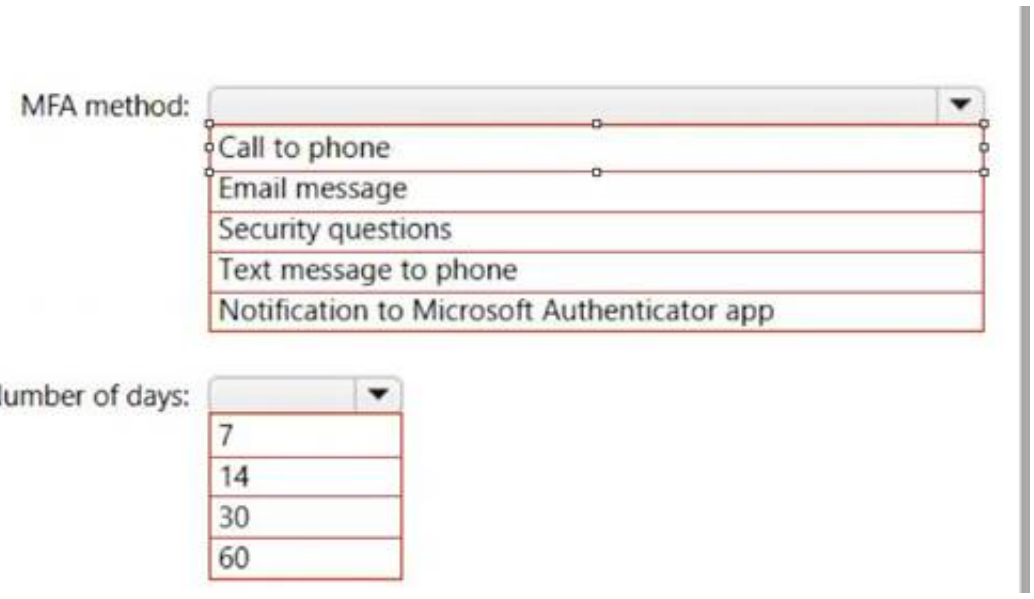
NEW QUESTION 121
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goats. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. You deploy a Microsoft Entra tenant.
Another administrator configures the domain to synchronize to the Microsoft Entra tenant.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.
You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.
Solution: From Microsoft Entra Connect, you modify the filtering settings. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 123
HOTSPOT - (Topic 6)
HOTSPOT
You have a new Microsoft 365 E5 tenant. Enable Security defaults is set to Yes.
A user signs in to the tenant for the first time.
Which multi-factor authentication (MFA) method can the user use, and how many days does the user have to register for MFA? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Notification to Microsoft Authenticator app
Do users have 14 days to register for Azure AD Multi-Factor Authentication?
Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won't be able to sign in until MFA registration is completed.
Box 2: 14
Azure AD Identity Protection will prompt your users to register the next time they sign in interactively and they'll have 14 days to complete registration. During this 14-day period, they can bypass registration if MFA isn't required as a condition, but at the end of the period they'll be required to register before they can complete the sign-in process.

NEW QUESTION 126
- (Topic 6)
You have a Microsoft 365 subscription.
You need to configure a compliance solution that meets the following requirements: Defines sensitive data based on existing data samples
Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages
Which two components should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AE

Explanation:
A: Classifiers
This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.
Where you can use classifiers
Classifiers are available to use as a condition for: Office auto-labeling with sensitivity labels
Auto-apply retention label policy based on a condition Communication compliance
Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.
Data loss prevention
E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp

NEW QUESTION 129
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender.
You need to compare your company's security configurations to Microsoft best practices and review improvement actions to increase the security posture.
What should you use?

A. Microsoft Secure Score
B. Cloud discovery
C. Exposure distribution
D. Threat tracker
E. Exposure score

Answer: A

NEW QUESTION 132
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

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

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

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

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

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

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

Answer Area

Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	○
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	○
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	○	○

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 136
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 141
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains the users shown in the following table.

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

You have the named locations shown in the following table.

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

You create a conditional access policy that has the following configurations:
• Users or workload identities: o Include: Group1
o Exclude: Group2
• Cloud apps or actions: Include all cloud apps
• Conditions:
o Include: Any location o Exclude: Montreal
• Access control: Grant access, Require multi-factor authentication User1 is on the multi-factor authentication (MFA) blocked users list.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 144
- (Topic 6)
Your company has on-premises servers and an Azure AD tenant.
Several months ago, the Azure AD Connect Hearth agent was installed on all the servers. You review the health status of all the servers regularly.
Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect Servers list.
You suspect that another administrator removed Server1 from the list. You need to ensure that you can view the health status of Server1.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. From Azure Cloud shell, run the Connect-Azure AD cmdlet.
B. From Server1, change the Azure AD Connect Health Services Startup type to Automatic (Delayed Start)
C. From Server1, change the Azure AD Connect Health Services Startup type to Automatic
D. From Windows PowerShell, run the Rejister-ArureADConnectHealthsyncAgent cmdlet.

E. From Server1, reinstall the Azure AD Connect Health agent

Answer: DE

NEW QUESTION 148
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

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

Name	Platform
Device1	Windows 10
Device2	Android

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

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

A. Mastered
B. Not Mastered

Answer: A

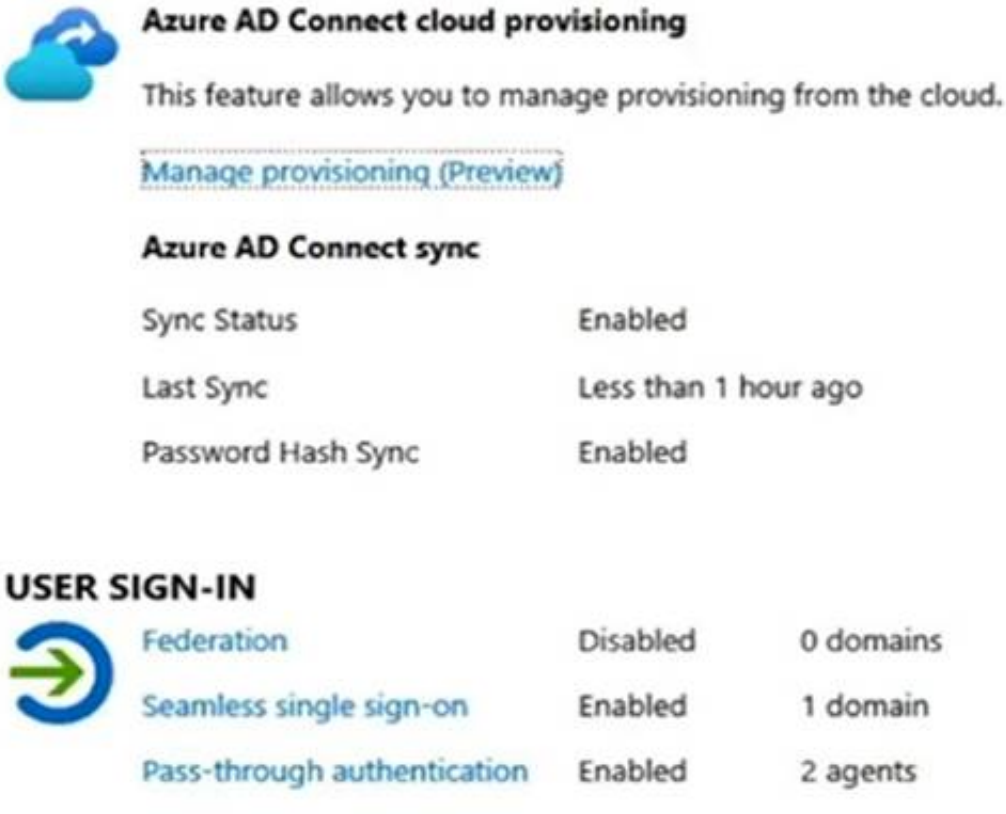
Explanation:

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

NEW QUESTION 150
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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



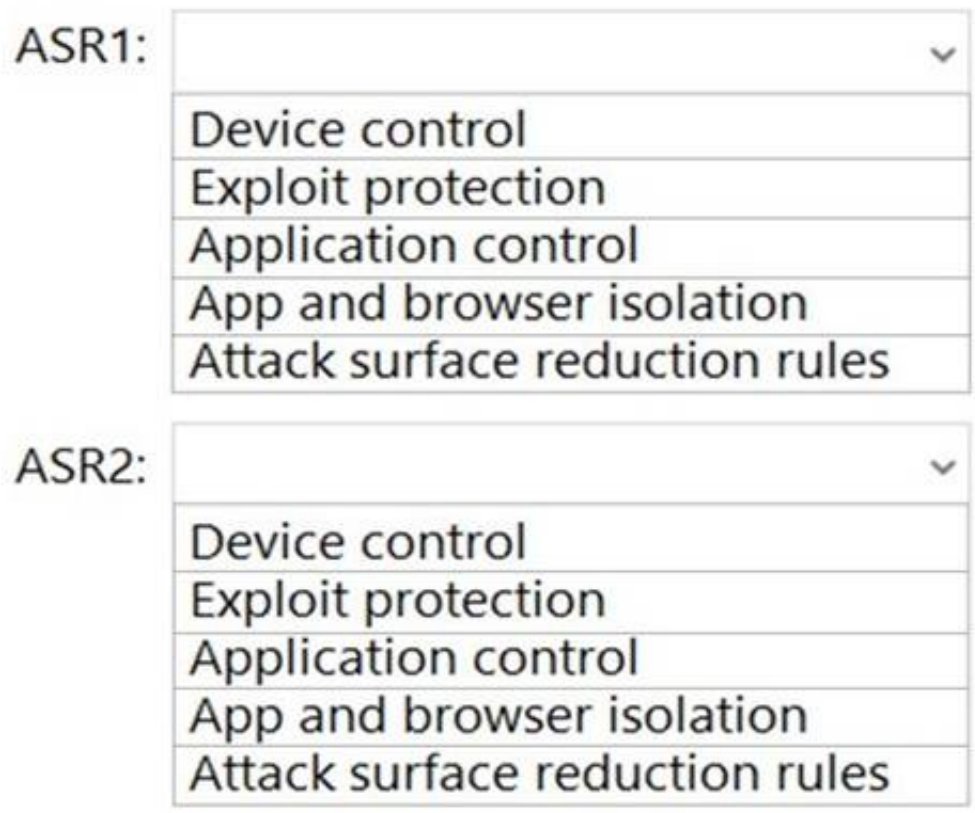
User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet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

A. Yes
B. No

Answer: A

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

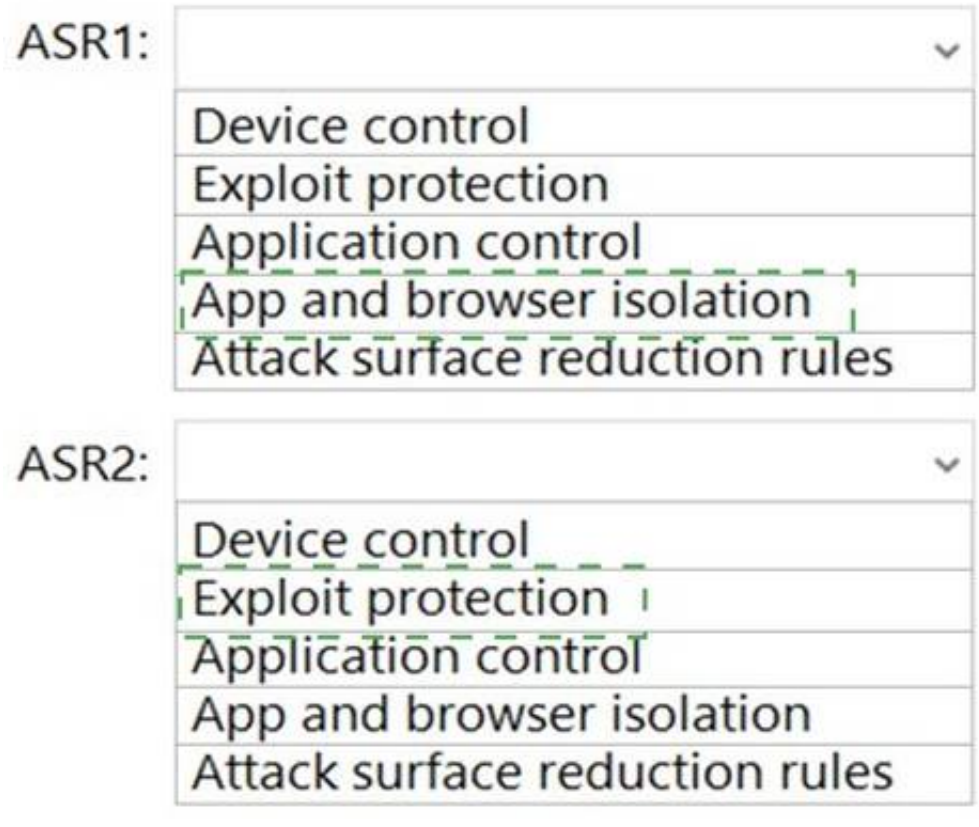
NEW QUESTION 153
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.
You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard. ASR2 will be used to configure Microsoft Defender SmartScreen.
Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 154
- (Topic 6)
Your on-premises network contains an Active Directory domain. You have a Microsoft 365 E5 subscription.
You plan to implement a hybrid configuration that has the following requirements:
• Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources
• Supports the use of Azure AD Identity Protection
You need to configure Azure AD Connect to support the planned implementation. Which two options should you select? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AB

NEW QUESTION 159
- (Topic 6)
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.
Where can you store data from the LinkedIn connector?

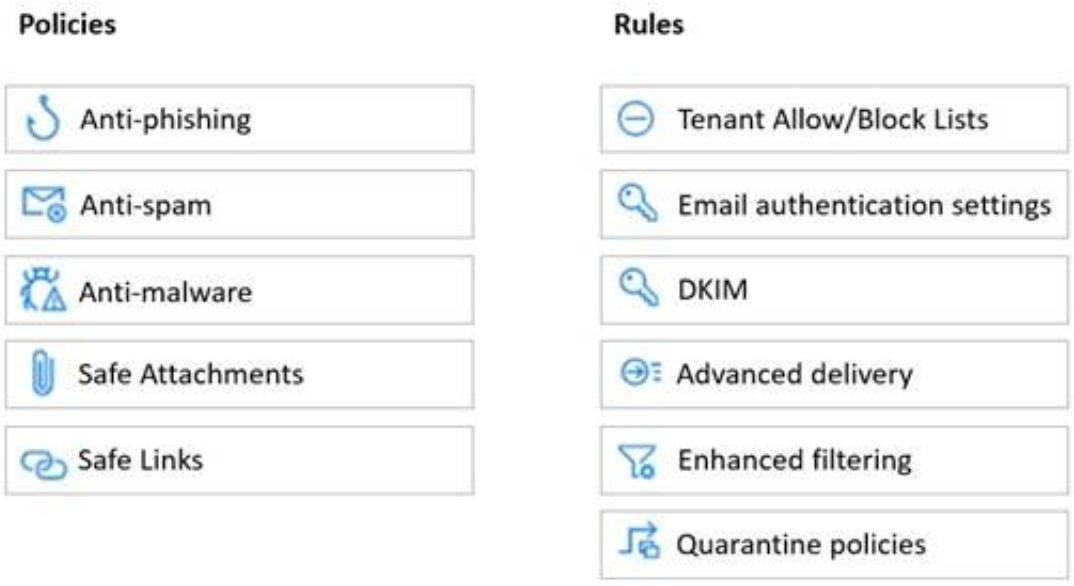
A. a Microsoft OneDrive for Business folder
B. a Microsoft SharePoint Online document library
C. a Microsoft 365 mailbox
D. Azure Files

Answer: C

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

NEW QUESTION 162
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to use a mailbox named Mailbox1 to analyze malicious email messages. You need to configure Microsoft Defender for Office 365 to meet the following requirements:
• Ensure that incoming email is NOT filtered for Mailbox1.
• Detect impersonation and spoofing attacks on all other mailboxes in the subscription. Which two settings should you configure? To answer, select the appropriate settings in the
answer area.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Safe Attachments policy: This policy allows you to specify how to handle email attachments that might contain malware. You can create a custom policy for Mailbox1 and set the action to Do not scan attachments. This will ensure that incoming email is not filtered for Mailbox1. You can also enable the Redirect attachment option to send a copy of the original attachment to another mailbox for analysis1.
? Anti-phishing policy: This policy helps you protect your organization from impersonation and spoofing attacks. You can create a default policy for all other mailboxes in the subscription and enable the following features: Impersonation protection, Spoof intelligence, and Domain authentication. These features will help you detect and block emails that try to impersonate your users, domains, or trusted senders2.

NEW QUESTION 165
FILL IN THE BLANK - (Topic 6)
You have a Microsoft 365 subscription.
From Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.
You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.
Solution: From Windows PowerShell, you run the New-complianceSecurityFilter cmdlet with the appropriate parameters.
Does this meet the goal?
A Yes

A. No

Answer: A

NEW QUESTION 169
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that contains the groups shown in the following table.

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

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

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

NEW QUESTION 171
- (Topic 6)
You enable the Azure AD Identity Protection weekly digest email. You create the users shown in the following table.

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

Which users will receive the weekly digest email automatically?

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

Answer: E

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

NEW QUESTION 172
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

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

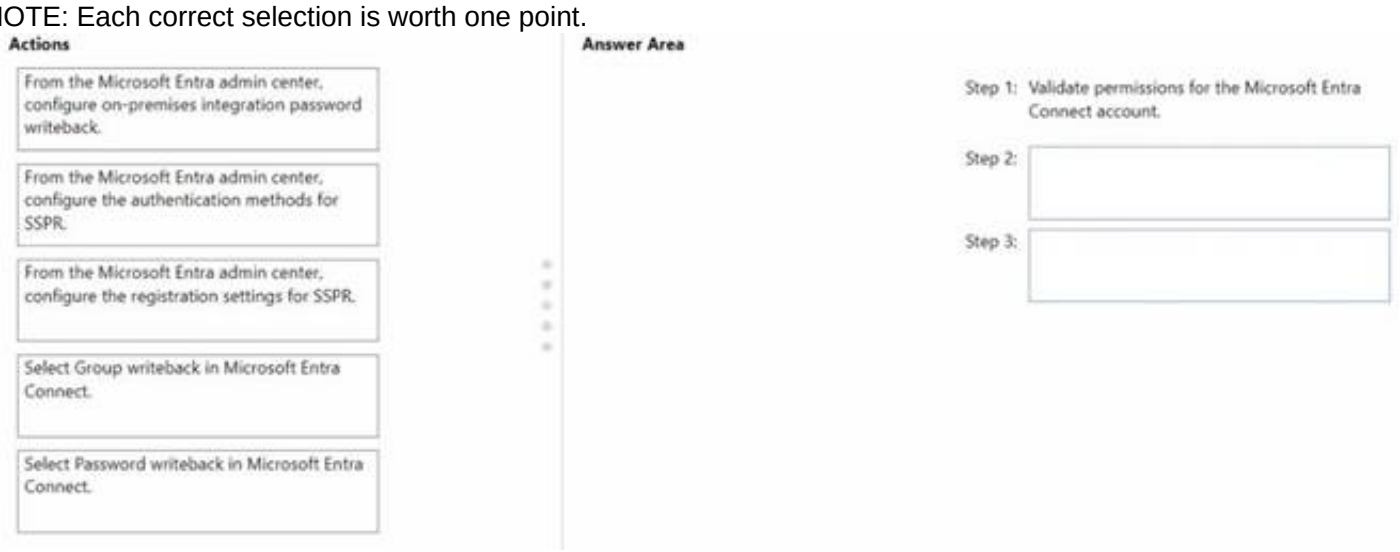
You perform the following actions:
? Provision the private store in Microsoft Store for Business.
? Add an app named App1 to the private store.
? Set Private store availability for App1 to Specific groups, and then select Group3.
For each of the following statements, select Yes if the statement is true.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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 173
DRAG DROP - (Topic 6)
You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.
All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.
You plan to implement self-service password reset (SSPR).
You need to ensure that when a user resets or changes a password, the password syncs with AD DS.
Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 174
HOTSPOT - (Topic 6)
From the Microsoft Purview compliance portal, you create a retention policy named Policy 1.
You need to prevent all users from disabling the policy or reducing the retention period. How should you configure the Azure PowerShell command? To answer select the
appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 177
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You create an account tor a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.
Does this meet the goal?

A. Yes
B. no

Answer: B

NEW QUESTION 179
- (Topic 6)
You have a Microsoft 365 subscription that contains the users shown in the following table.

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

You need to configure group-based licensing to meet the following requirements:

? To all users, deploy an Office 365 E3 license without the Power Automate license option.
? To all users, deploy an Enterprise Mobility + Security E5 license.
? To the users in the research department only, deploy a Power BI Pro license.
? To the users in the marketing department only, deploy a Visio Plan 2 license.
What is the minimum number of deployment groups required?

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

Answer: C

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

NEW QUESTION 181
- (Topic 6)
You have a Microsoft 365 subscription.
You plan to implement Microsoft Purview Privileged Access Management. Which Microsoft Office 365 workloads support privileged access?

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

Answer: A

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

NEW QUESTION 183
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

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

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

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

Answer: A

NEW QUESTION 186
- (Topic 6)
You have a Microsoft 365 subscription.
You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.
What is the maximum number of onmicrosoft.com domains the subscription can contain?

A. 1
B. 2
C. 5

D. 10

Answer: C

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

NEW QUESTION 191
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 196
- (Topic 6)
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 199
- (Topic 6)
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant includes a user named User1.
You enable Azure AD Identity Protection.
You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.
To which role should you add User1?

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

Answer: A

NEW QUESTION 201
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

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

The devices are configured as shown in the following table.

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

You have a Conditional Access policy named CAPolicy1 that has the following settings: 1.Assignments

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 202
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription.
Your network uses an IP address space of 51.40.15.0/24.
An Exchange Online administrator recently created a role named Role1 from a computer on the network.
You need to identify the name of the administrator by using an audit log search.
For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

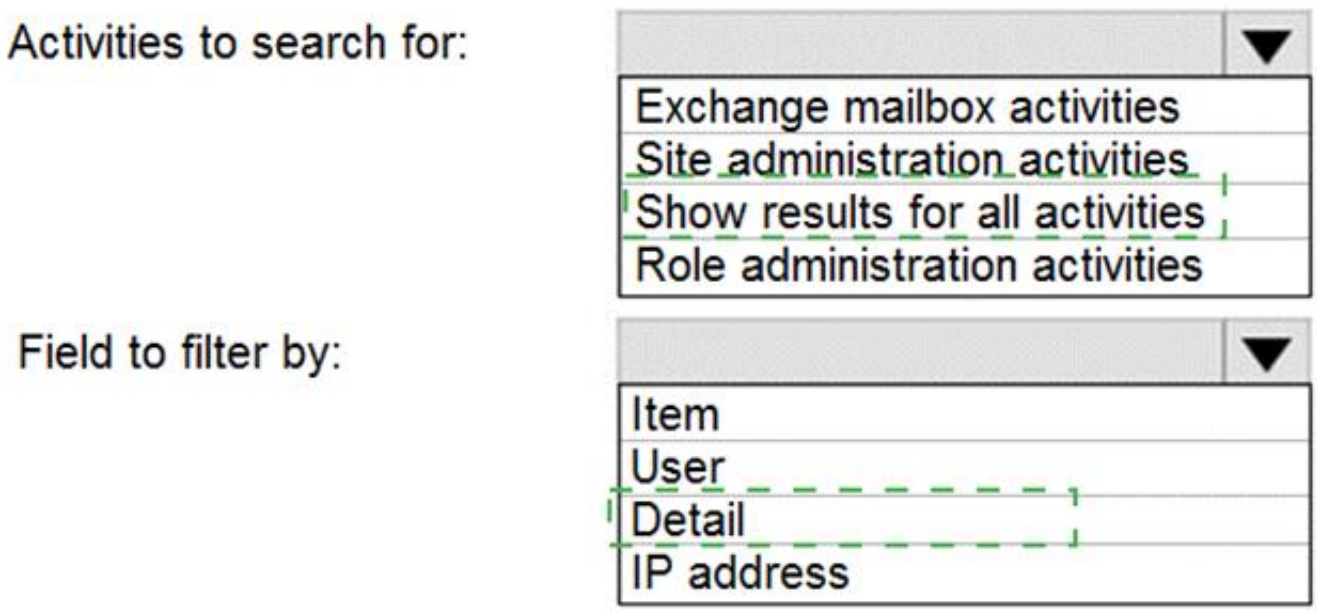
Activities to search for:
- Exchange mailbox activities
- Site administration activities
- Show results for all activities
- Role administration activities

Field to filter by:
- Item
- User
- Detail
- IP address

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 206
- (Topic 6)
You have a Microsoft 365 subscription.
You have an Azure AD tenant that contains the users shown in the following table.

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

You configure Tenant properties as shown in the following exhibit.

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

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

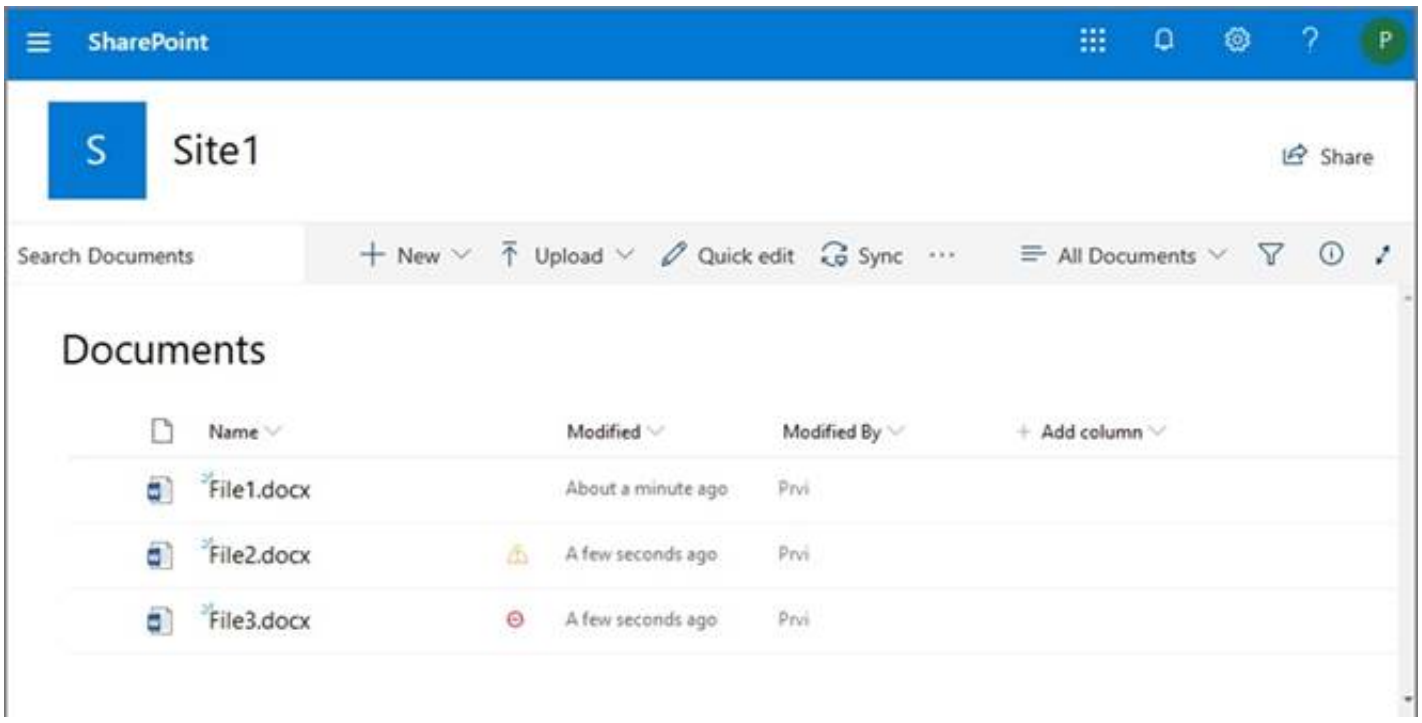
Answer: B

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

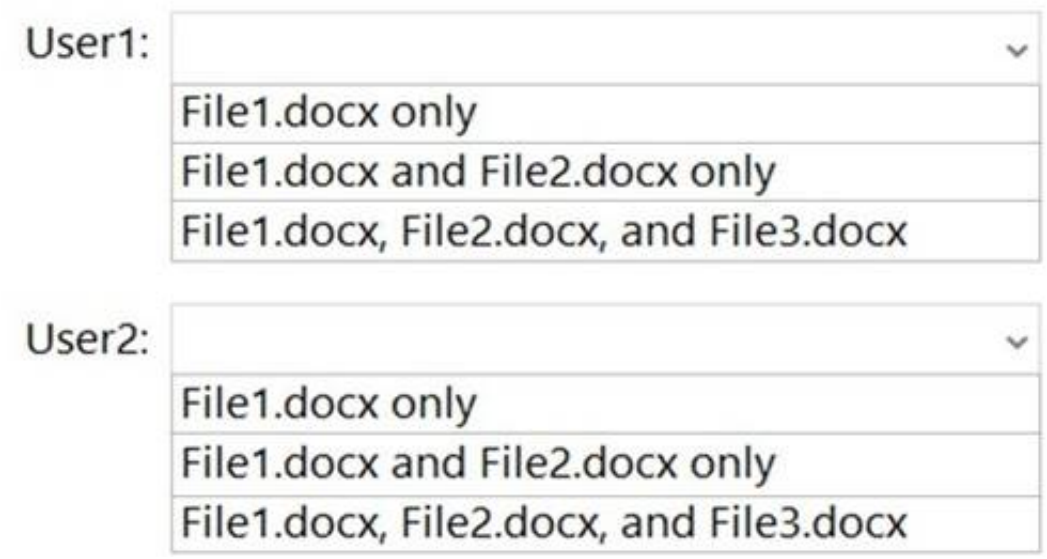
NEW QUESTION 210
HOTSPOT - (Topic 6)
From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

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



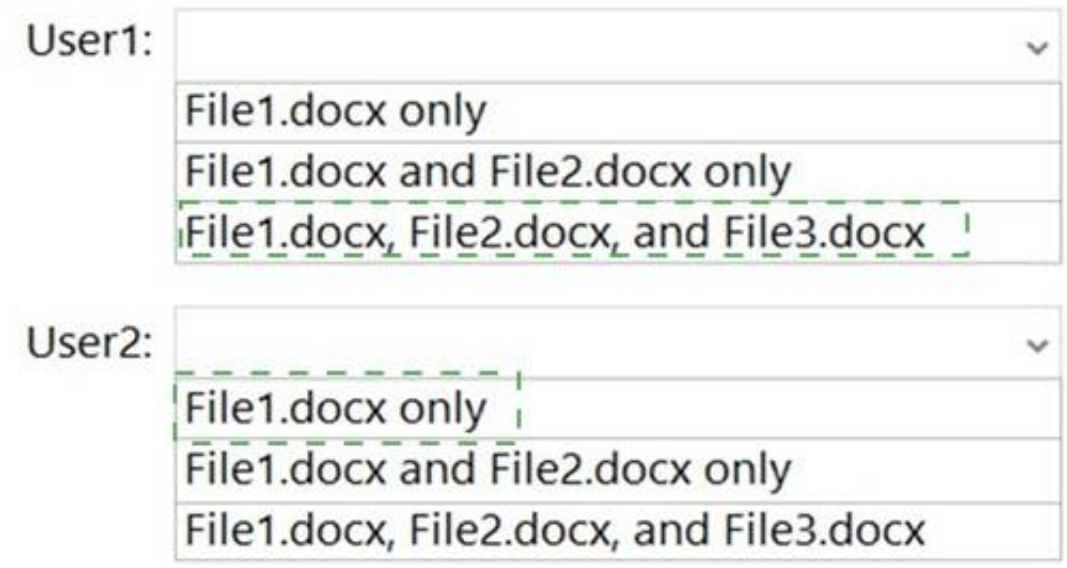
Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 213
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription and an Azure AD tenant named contoso.com.
All users have computers that run Windows 11, are joined to contoso.com, and are protected by using BitLocker Drive Encryption (BitLocker).
You plan to create a user named Admin1 that will perform following tasks:
• View BitLocker recovery keys.
• Configure the usage location for the users in contoso.com.
You need to assign roles to Admin1 to meet the requirements. The solution must use the principle of least privilege. Which two roles should you assign? To answer, select the appropriate roles in the answer area.
NOTE: Each correct selection is worth one point

Answer Area

Devices

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

Global

- [ ] Global Administrator

Identity

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Devices

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

Global

- [ ] Global Administrator

Identity

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

NEW QUESTION 217
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Conditional Access is configured to block high-risk sign-ins for all users.
All users are in France and are registered for multi-factor authentication (MFA). Users in the media department will travel to various countries during the next month.
You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention.
What should you configure?

A. an exclusion group
B. the MFA registration policy
C. named locations
D. self-service password reset (SSPR)

Answer: D

Explanation:
Self-remediation with self-service password reset
If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock

NEW QUESTION 218
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.

You need to deploy the policy. What should you do first?

A. Review the sensitive information in Activity explorer
B. Turn on the policy
C. Run the policy in simulation mode
D. Configure Azure Information Protection analytics

Answer: C

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

NEW QUESTION 223
- (Topic 6)
You have Windows 10 devices that are managed by using Microsoft Endpoint Manager. You need to configure the security settings in Microsoft Edge.
What should you create in Microsoft Endpoint Manager?

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

Answer: C

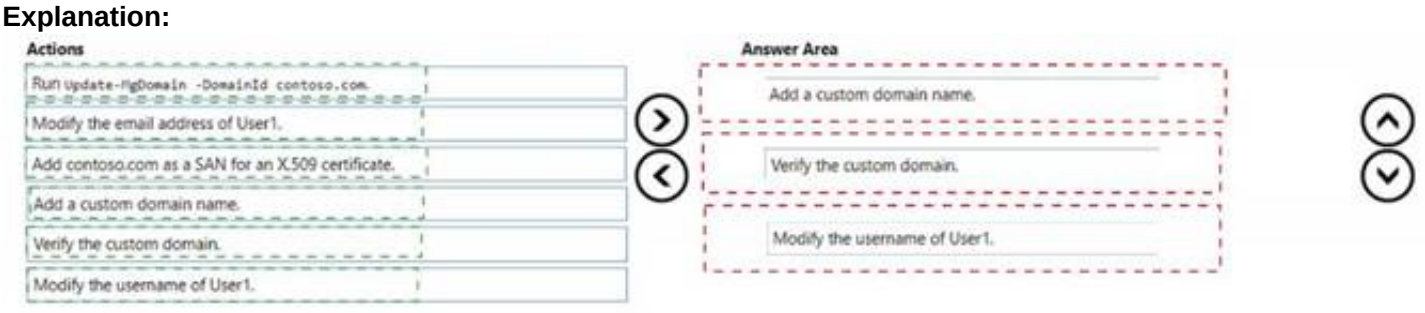
Explanation:
Reference:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

NEW QUESTION 224
DRAG DROP - (Topic 6)
Your company has an Azure AD tenant named contoso.onmicrosoft.com.
You purchase a domain named contoso.com from a registrar and add all the required DNS records.
You create a user account named User1. User1 is configured to sign in as userl@contoso.onmicrosoft.com.
You need to configure User1 to sign in as user1@contoso.com.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



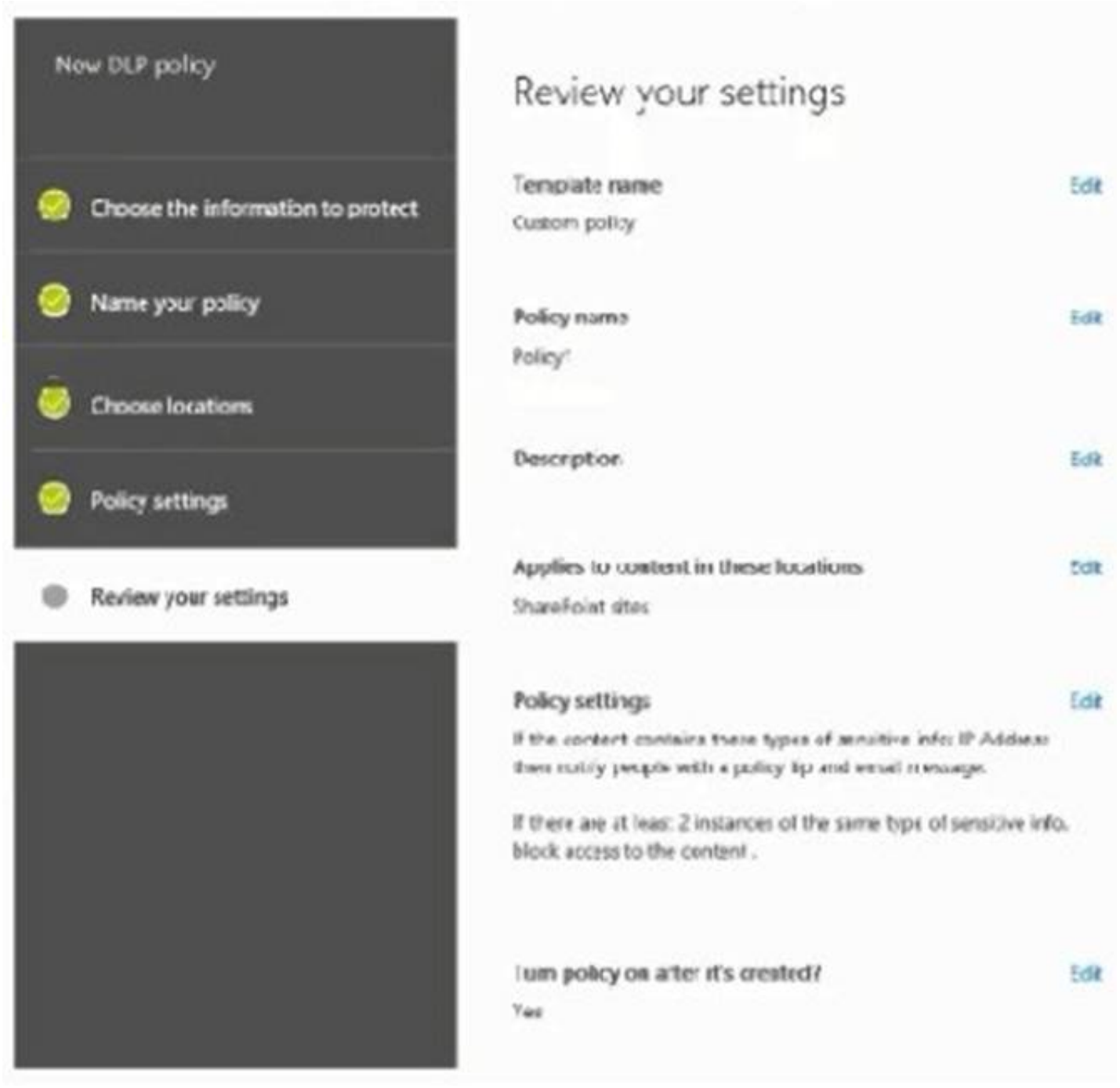
NEW QUESTION 228
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has he files in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	2
File4.bmp	3
File5.doc	3

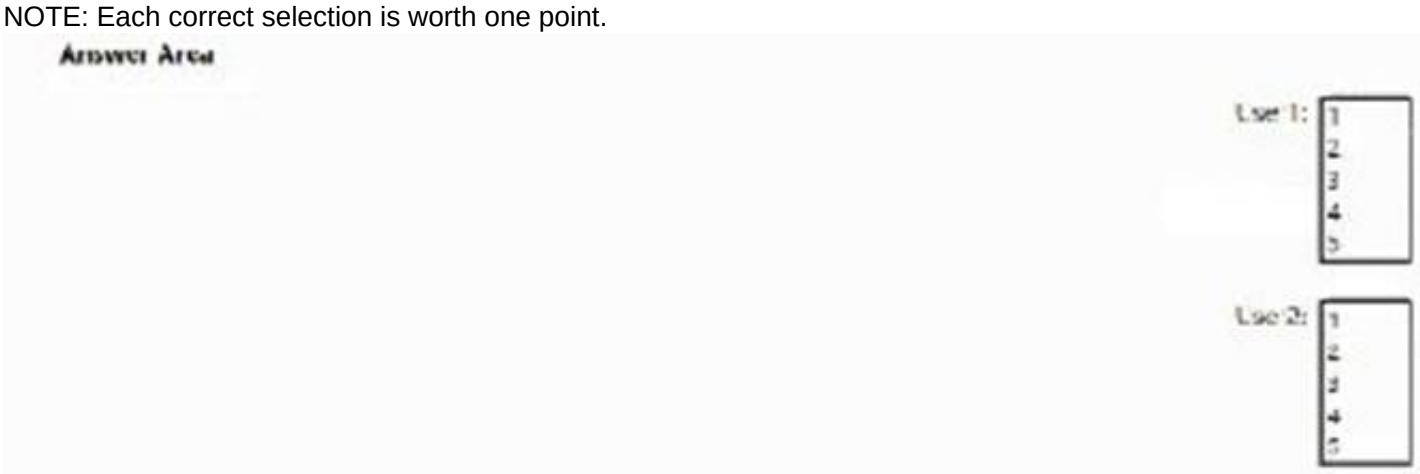
The Site1 users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Visitor

You create a data less prevention (DLP) policy names Policy1 as shown in the following exhibit.



How many files will be visible to user1 and User2 after Policy' is applied to answer, selected 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 232
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users have the devices shown in the following table.

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

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

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

Answer: C

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

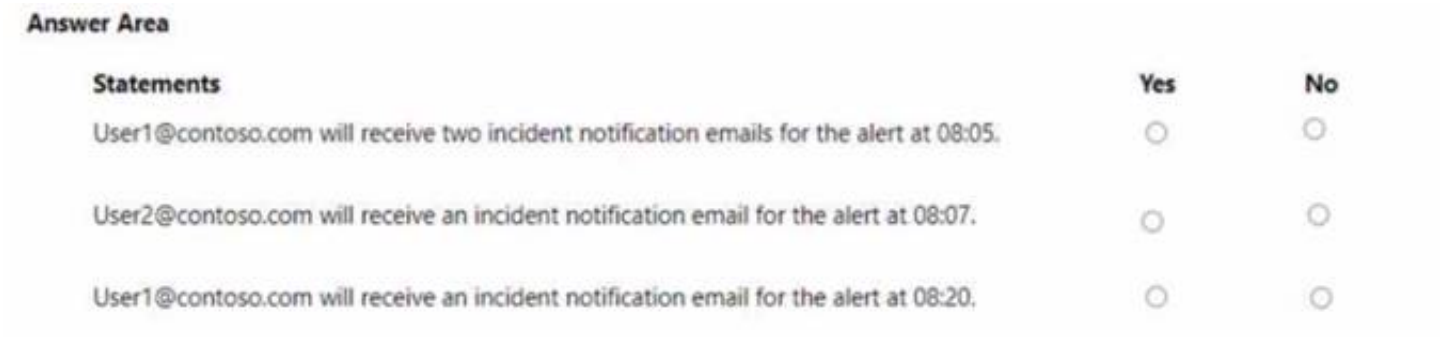
NEW QUESTION 236
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

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

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

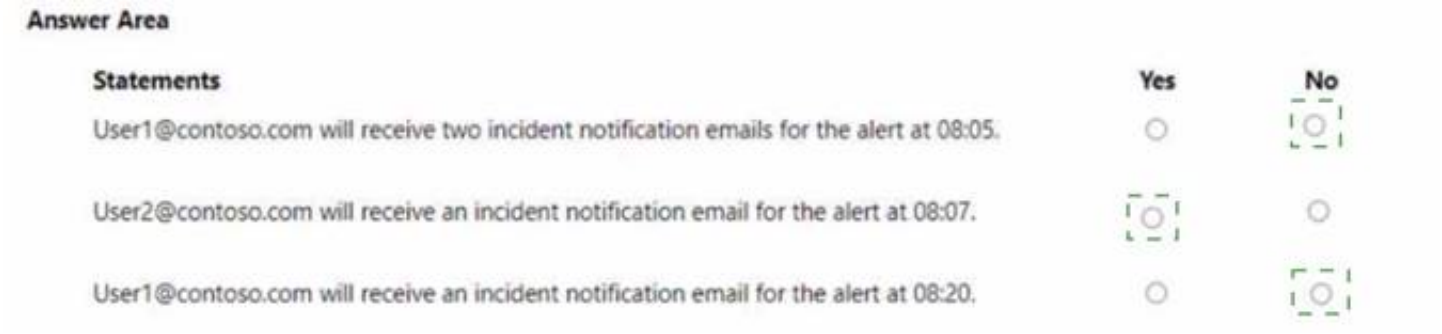
For each of the following statements, select Yes if the statement is true. Otherwise, select No1.
NOTE: Each correct selection is worth one point.



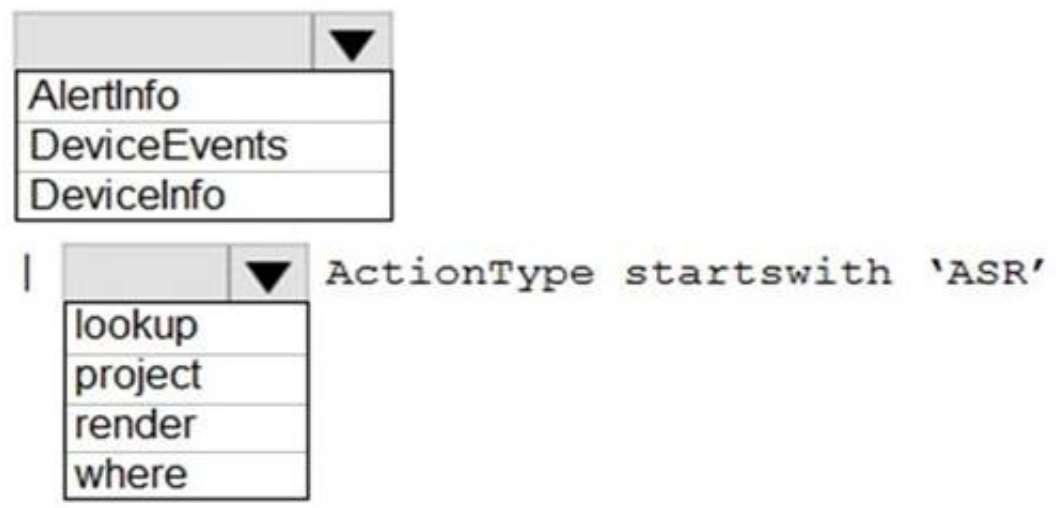
A. Mastered
B. Not Mastered

Answer: A

Explanation:



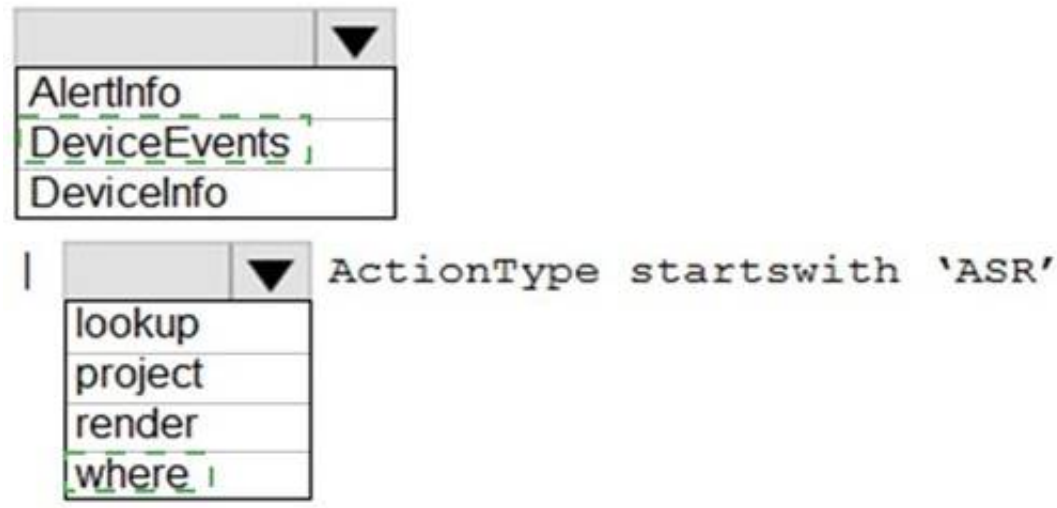
NEW QUESTION 237
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices. You plan to attack surface reduction (ASR) rules for the Windows 10 devices.
You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.
You need to find the ASR rules that match the activities on the devices.
How should you complete the Kusto query? To answer, select the appropriate options in
the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 241
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Endpoint security.

You need to create a group and assign the Endpoint Security Manager role to the group. Which type of group can you use?

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

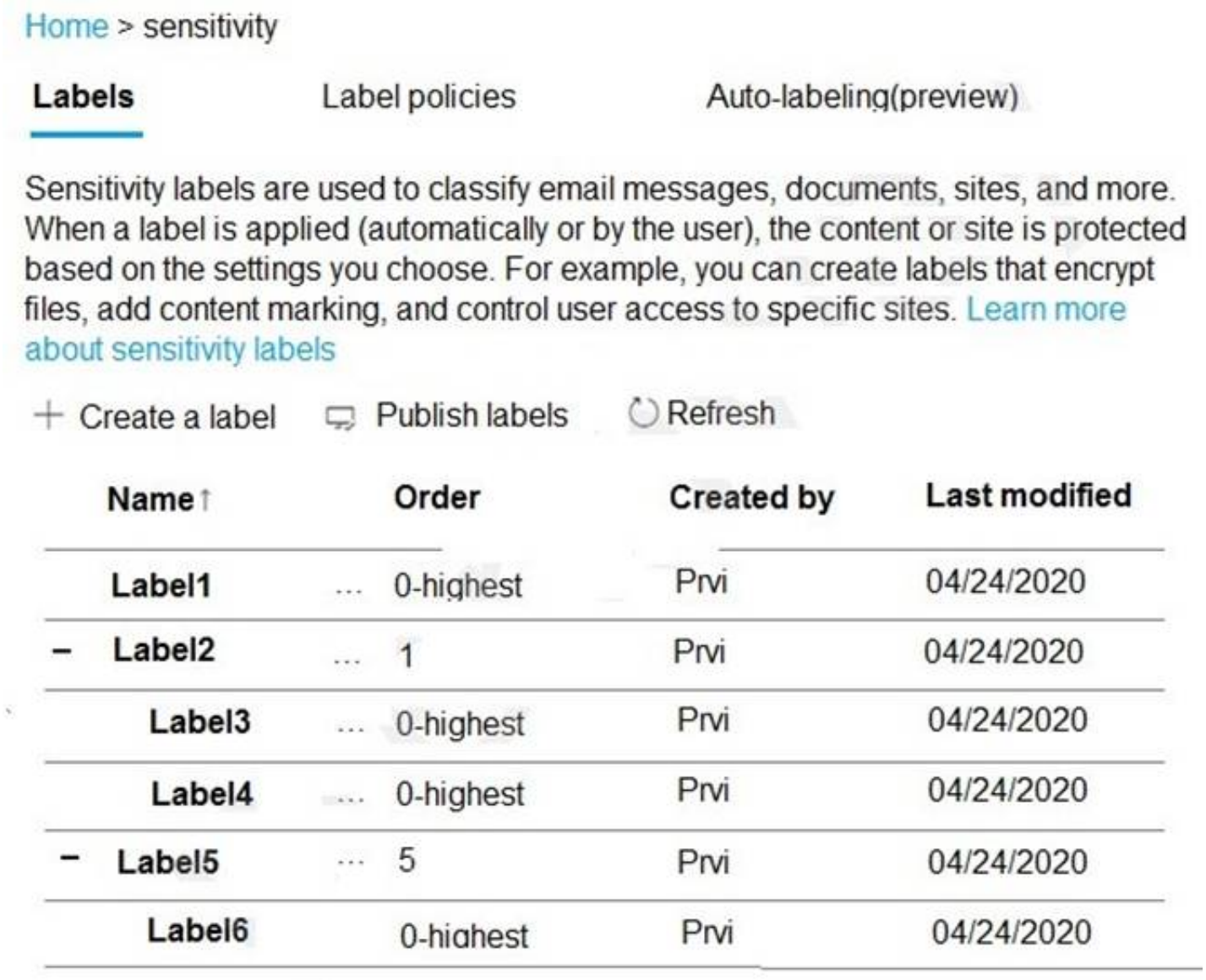
Answer: D

NEW QUESTION 246
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune.
You plan to use Endpoint analytics to identify hardware issues.
You need to enable Window health monitoring on the devices to support Endpoint analytics What should you do?

A. Configure the Endpoint analytics baseline regression threshold.
B. Create a configuration profile.
C. Create a Windows 10 Security Baseline profile
D. Create a compliance policy.

Answer: B

NEW QUESTION 251
- (Topic 6)
You have the sensitivity labels shown in the following exhibit.



Which labels can users apply to content?

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

Answer: D

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

NEW QUESTION 255
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed. Solution: From Device Manager, you view the computer properties. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 260
- (Topic 6)
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

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

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

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

Answer: B

NEW QUESTION 261
- (Topic 6)
You have a Microsoft 365 subscription.
You need to receive a notification each time a user in the service desk department grants Full Access permissions for a user mailbox.
What should you configure?

A. a data loss prevention (DLP) policy
B. an alert policy
C. an audit search
D. an insider risk management policy

Answer: B

NEW QUESTION 266
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected.
What should you use to create the policy?

A. the Microsoft 365 admin center
B. the Microsoft Purview compliance portal
C. the Microsoft Defender for Cloud Apps portal
D. the Microsoft Apps admin center

Answer: C

NEW QUESTION 271
HOTSPOT - (Topic 6)
Your company uses Microsoft Defender for Endpoint.
The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

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

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:
• Triggering IOC: Any IOC
• Action: Hide alert
• Suppression scope: Alerts on ATP1 device group
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 273
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 277
FILL IN THE BLANK - (Topic 6)
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

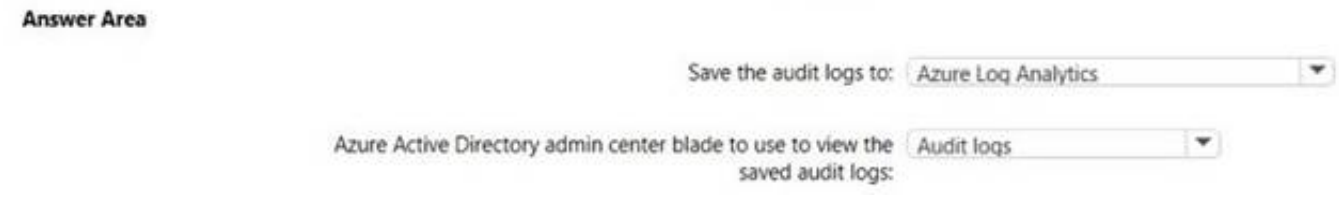
Save the audit logs to: [ ]

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

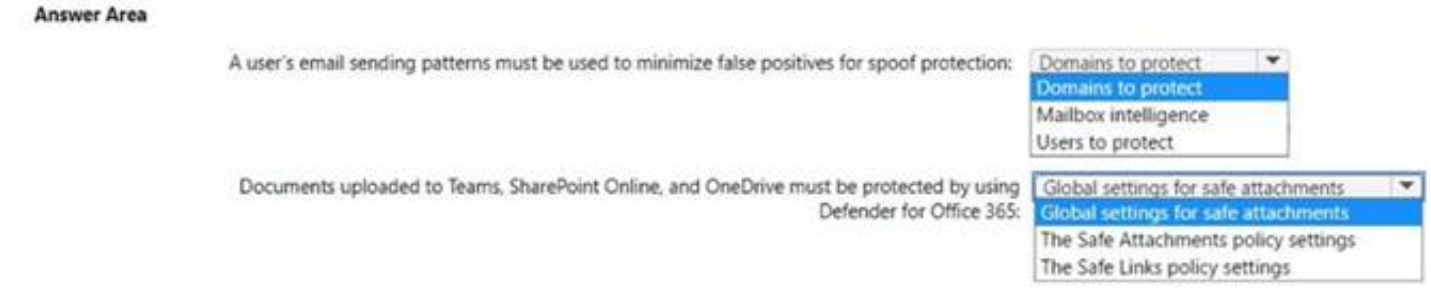
A. Mastered
B. Not Mastered

Answer: A

Explanation:



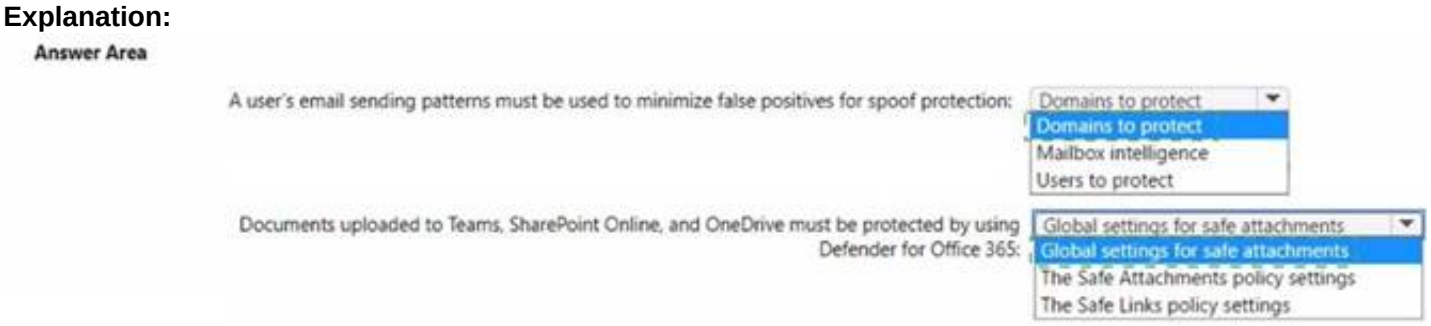
NEW QUESTION 282
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to configure Microsoft Defender for Office 365 to meet the following requirements:
• A user's email sending patterns must be used to minimize false positives for spoof protection.
• Documents uploaded to Microsoft Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365.
What should you configure for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 284
- (Topic 6)
You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Source	Last sign in
User1	Azure AD	Yesterday
User2	Active Directory Domain Services (AD DS)	Two days ago
User3	Active Directory Domain Services (AD DS)	Never

Azure AD Connect has the following settings:
? Password Hash Sync: Enabled
? Pass-through authentication: Enabled
You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.
Which users should you identify?

A. none
B. Used only1
C. User1 and User2 only
D. User1. User2, and User3

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn¨

NEW QUESTION 285
- (Topic 6)
: 241
You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?

A. Microsoft Store for Business

B. Apple Business Manager
C. Apple iTunes Store
D. Apple Configurator

Answer: B

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

NEW QUESTION 288
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.
You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.
Solution: From the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 292
- (Topic 6)
You have a Microsoft 365 E5 tenant. Users store data in the following locations:
? Microsoft Teams
? Microsoft OneDrive
? Microsoft Exchange Online
? Microsoft SharePoint Online
You need to retain Microsoft 365 data for two years.
What is the minimum number of retention policies that you should create?

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

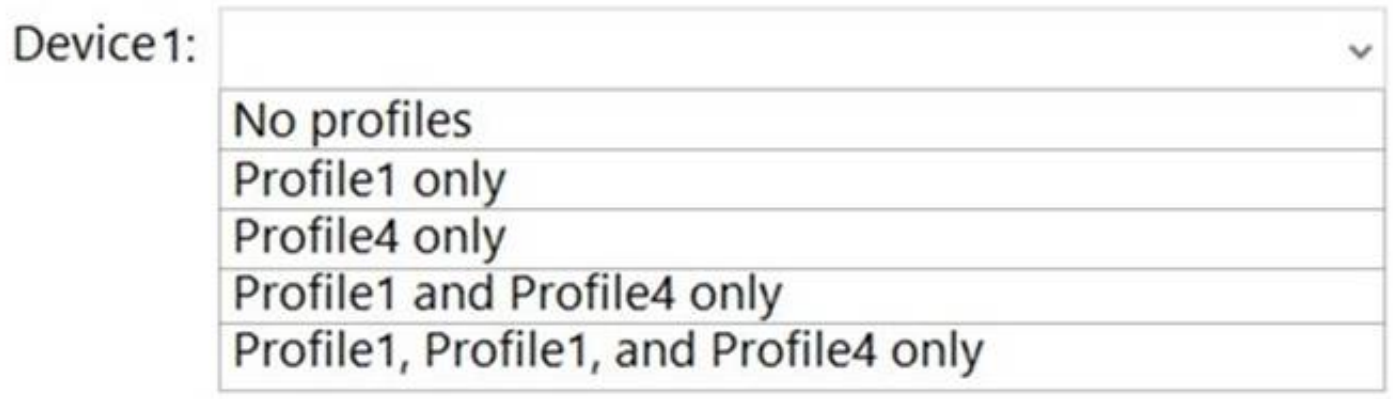
Answer: C

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

NEW QUESTION 296
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have devices enrolled in Intune as shown in the following table.
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

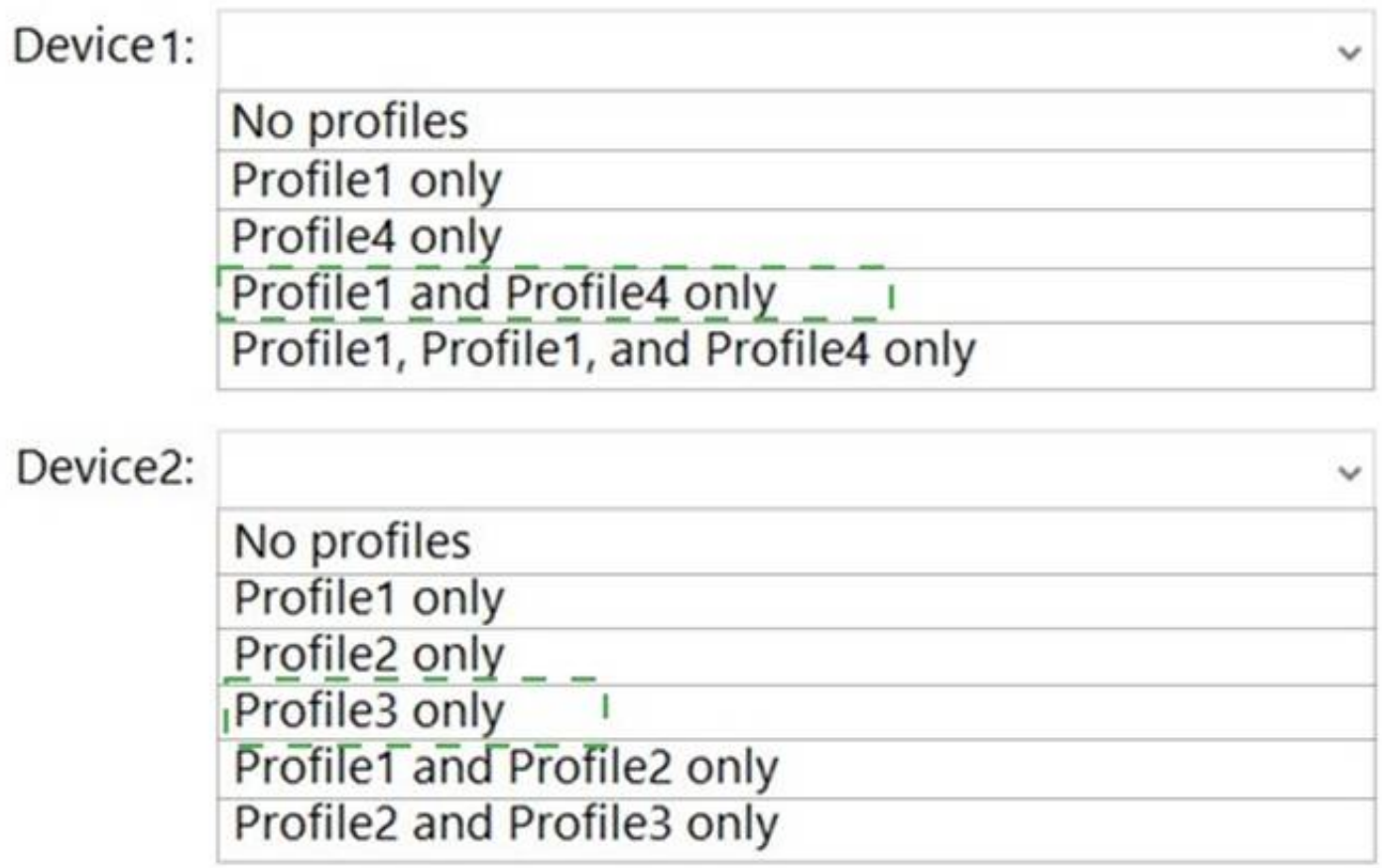
Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 300
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:
? Show app and profile configuration progress: Yes
? Allow users to collect logs about installation errors: Yes
? Only show page to devices provisioned by out-of-box experience (OOBE): No
? Assignments: 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.

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○

NEW QUESTION 305
- (Topic 6)
Your on-premises network contains an Active Directory domain.
You have a Microsoft 365 subscription.
You need to sync the domain with the subscription. The solution must meet the following requirements:
On-premises Active Directory password complexity policies must be enforced. Users must be able to use self-service password reset (SSPR) in Azure AD. What should you use?

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

Answer: D

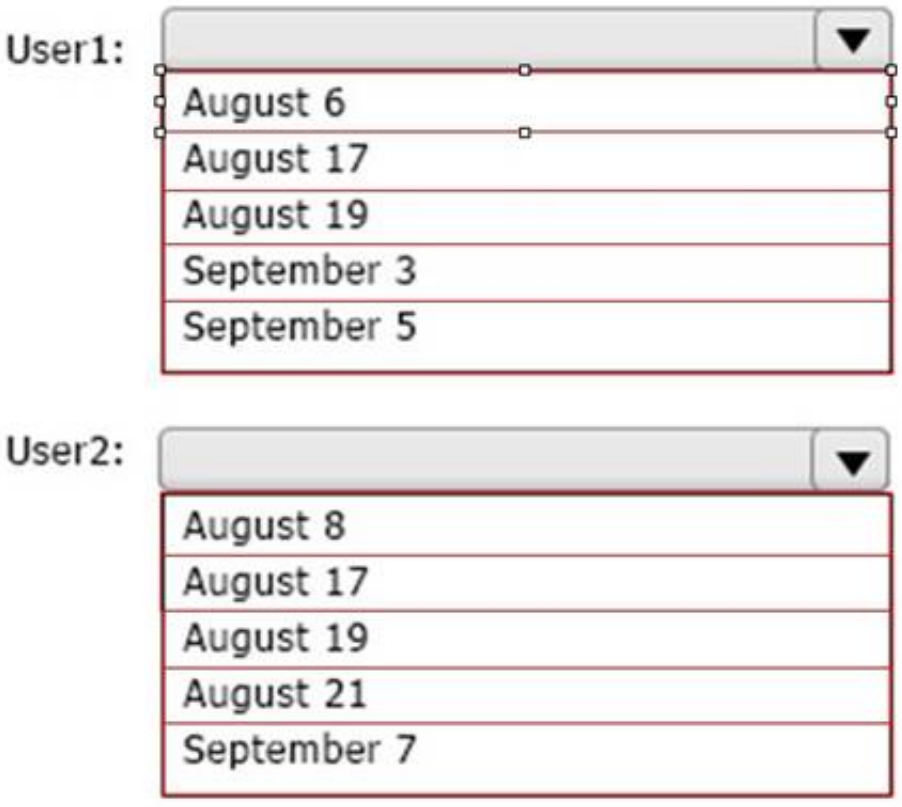
Explanation:
Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.
This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication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

NEW QUESTION 310
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:
? Assignments: All users
? Controls: Require Azure AD multifactor authentication registration
? Enforce Policy: On
? On August 3, you create two users named User1 and User2.

Users authenticate by using Azure Multi-Factor Authentication (MFA) for the first time on the dates shown in the following table.

User	Date
User1	August 5
User2	August 7

By which dates will User1 and User2 be forced to complete their Azure MFA registration? 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: August 19
Note: Security defaults will trigger a 14 day grace period for registration after a user's first login and security defaults being enabled. After 14 days users will be required to register for MFA and will not be able to skip.
Conditional Access by itself without Azure Identity Protection does not allow for the 14 day grace period. Identity Protection includes the registration policy that allows registration on its own with no apps assigned to the policy. If a Conditional Access policy requires Multi- Factor Authentication, then the user must be able to pass that MFA request.
Box 2: August 21

NEW QUESTION 314
- (Topic 6)
You have a Microsoft 365 subscription.
You have a data loss prevention (DLP) policy that blocks sensitive data from being shared in email messages.
You need to modify the policy so that when an email message containing sensitive data is sent to both external and internal recipients, the message is only prevented from being delivered to the external recipients.
What should you modify?

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

Answer: C

NEW QUESTION 316
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.
Which conditions can you use in the DLP rules of the policy?

A. sensitive info types
B. content search queries
C. keywords
D. sensitivity labels

Answer: C

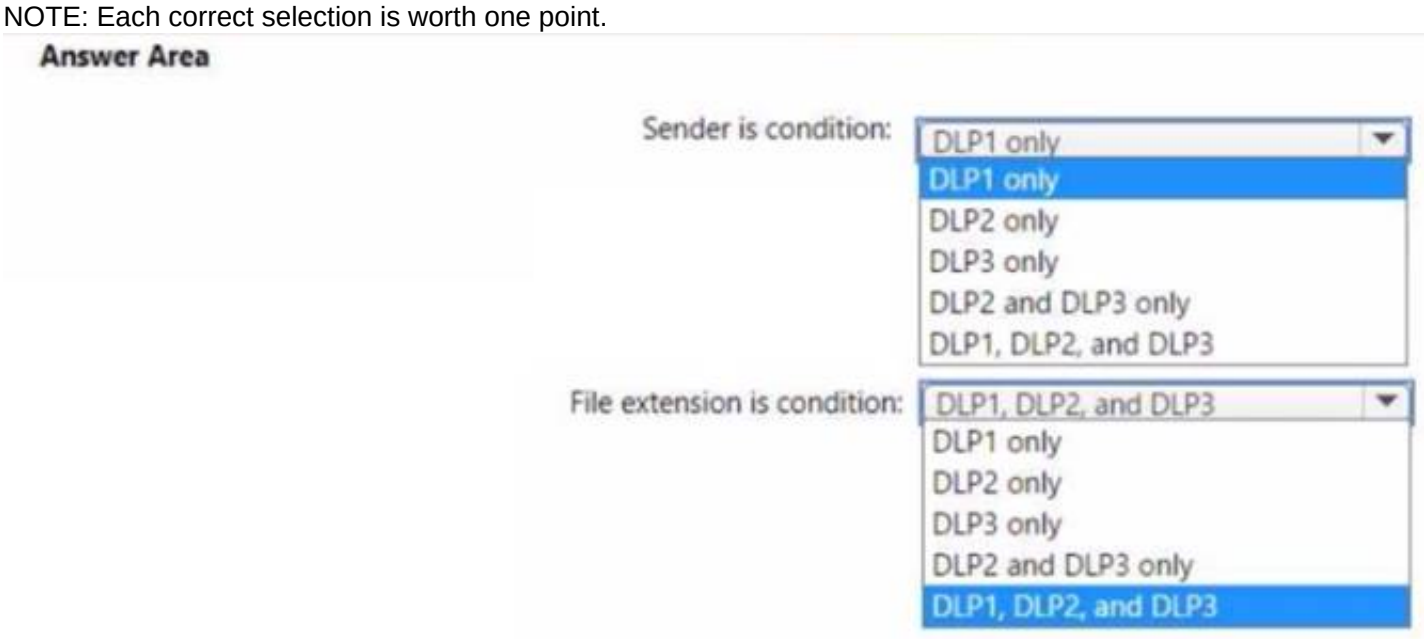
Explanation:

Apply retention labels to content automatically if it matches specific conditions, that includes cloud attachments that are shared in email or Teams, or when the content contains:
Specific types of sensitive information.
Specific keywords that match a query you create.
Pattern matches for a trainable classifier.
Note: Retention policies can be applied to the following locations: Exchange mailboxes
SharePoint classic and communication sites OneDrive accounts
Microsoft 365 Group mailboxes & sites Skype for Business
Exchange public folders
Teams channel messages (standard channels and shared channels) Teams chats
Teams private channel messages Yammer community messages Yammer user messages
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-exchange-conditions-and-actions

NEW QUESTION 318
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to create the data loss prevention (DLP) policies shown in the following table.

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

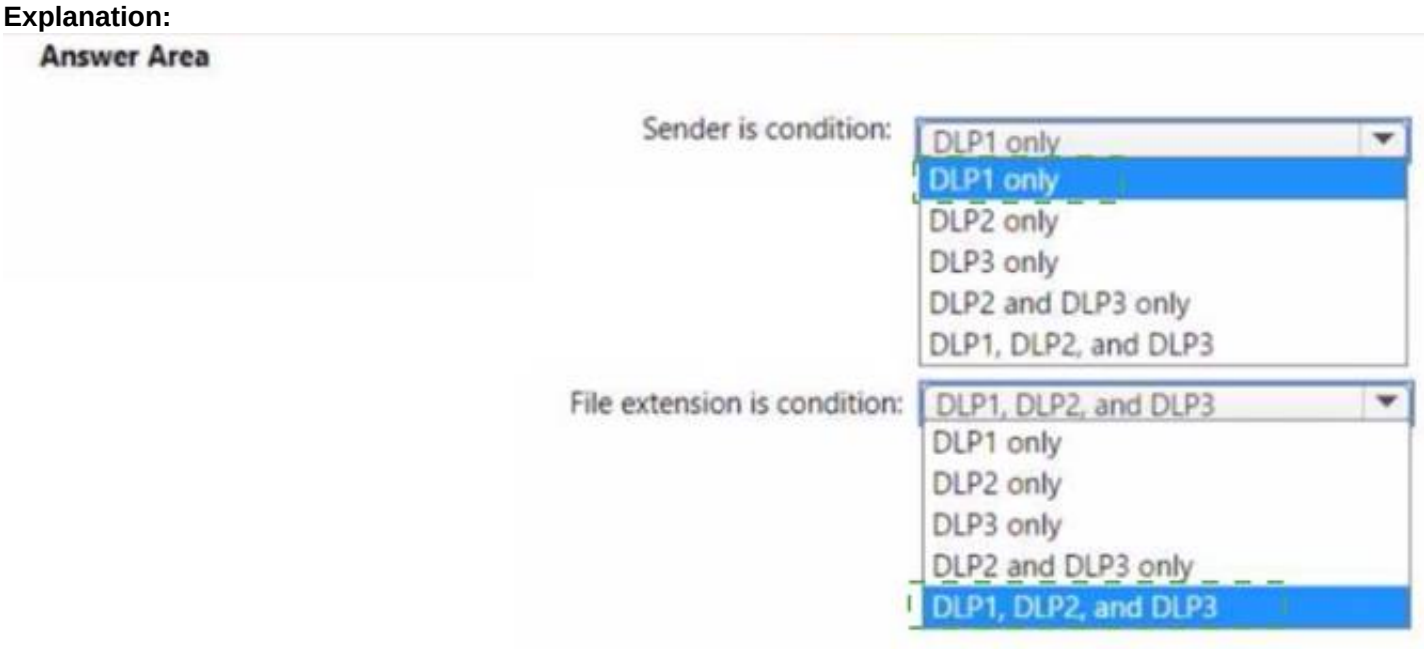
You need to create DLP rules for each policy.
Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 321
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 325
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP).
You need to create a detection exclusion in Azure ATP. Which tool should you use?

A. the Security & Compliance admin center
B. Microsoft Defender Security Center
C. the Microsoft 365 admin center
D. the Azure Advanced Threat Protection portal
E. the Cloud App Security portal

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/what-is https://docs.microsoft.com/en-us/defender-for-identity/excluding-entities-from-detections

NEW QUESTION 328
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.
The subscription has the following two anti-spam policies:
• Name: AntiSpam1
• Priority: 0
• Induce these users, groups and domains o Users: User3
o Groups: Group!
• Exclude these users, groups and domains o Groups: Group2
• Message limits
o Set a daily message limit 100

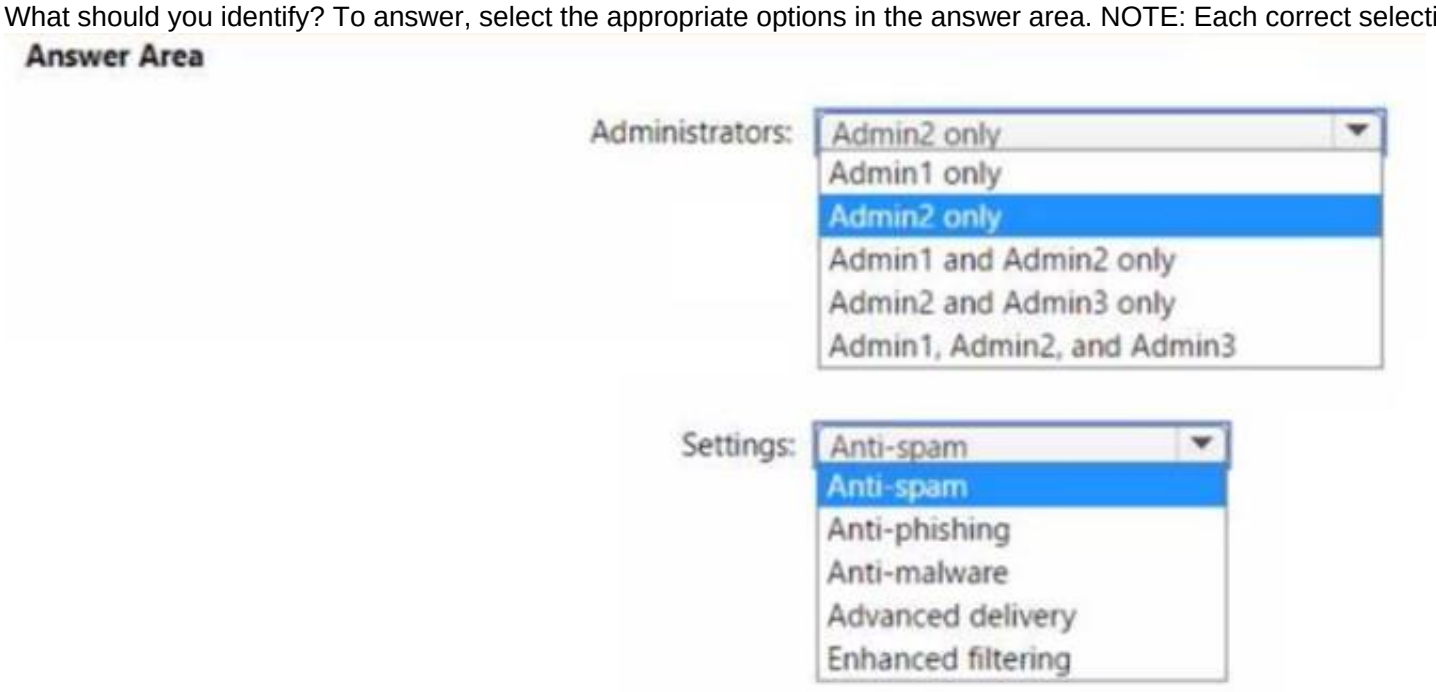
• Name: AntiSpam2
• Priority: 1
• Include these users, groups and domains o Users: User! o Groups: Group2
• Exclude these users, groups and domains o Users: User3
• Message limits
o Set a daily message limit 50
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 329
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table.
User1 reports that after sending 1,000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:
• Which administrators can unblock User1
• What to configure to allow User1 to send at least 2,000 emails per day without being blocked
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 330
- (Topic 6)
You have a new Microsoft 365 E5 tenant.
You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.
What should you do first?

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

Answer: A

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

NEW QUESTION 335
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft intune.
in the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices,
You enable device clean-up rules
What can you configure as the minimum number of days before a device a removed automatically?

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

Answer: D

NEW QUESTION 336
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the security groups shown in the following table.

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

The subscription contains the users shown in the following table.

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

You have a Conditional Access policy that has the following settings:
• Assignments o Users
Include: Group1
Exclude: Group2. Group3 o Target resources
Cloud apps App1
Access controls Grant
Block access
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 340
HOTSPOT - (Topic 6)
Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD) Password hash synchronization is disabled.
You plan to implement co-management.
You need to configure Azure AD Connect and the domain to support co-management. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

NEW QUESTION 345
- (Topic 6)

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

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

Answer: C

NEW QUESTION 348
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription. You need to meet the following requirements:
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label. Which two settings should you use in the Microsoft Purview compliance portal? To answer,
select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Information protection
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection
All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is select a single checkbox. By enabling automatic scan, you

enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files
without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.
To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels:
In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information Protection -> Microsoft Information Protection.
Note: Encryption of data at rest
Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.
BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology. Box 2: Settings
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.
* 1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
* 2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
* 3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
* 4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
* 5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.

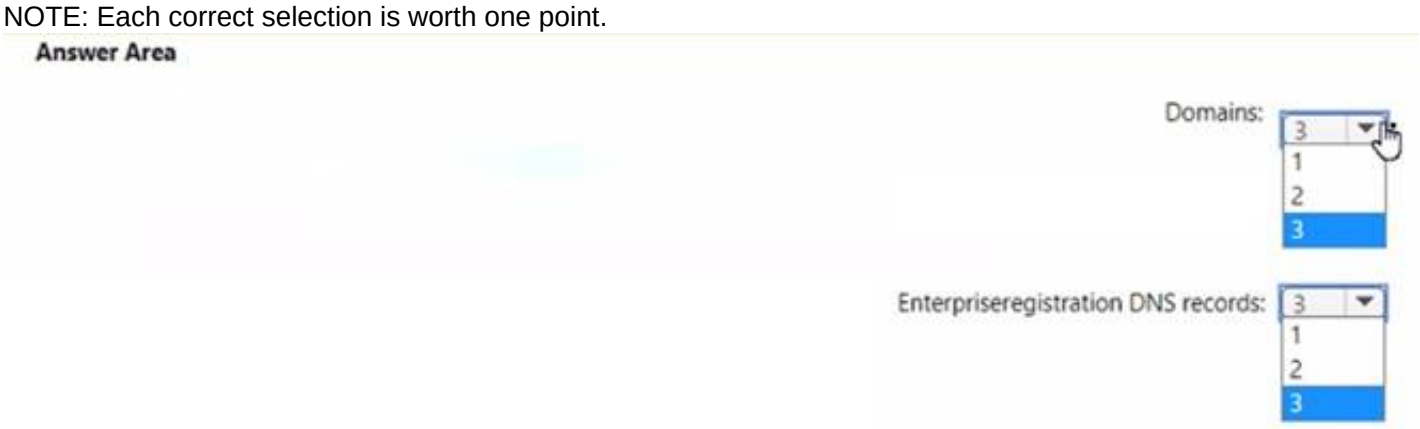
NEW QUESTION 350
- (Topic 6)
You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.
Company policy requires that the devices have the following configurations:
? Require complex passwords.
? Require the encryption of removable data storage devices.
? Have Microsoft Defender Antivirus real-time protection enabled.
You need to configure the devices to meet the requirements.
What should you use?

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

Answer: B

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

NEW QUESTION 351
HOTSPOT - (Topic 6)
You work at a company named Contoso, Ltd.
Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.
Contoso purchases a company named Fabrikam, Inc.
Contoso plans to add the following domains to the Microsoft 365 subscription:
• fabrikam.com
• east.fabrikam.com
• west.contoso.com
You need to ensure that the devices in the new domains can register by using Autodiscover.
How many domains should you verify, and what is the minimum number of enterprise registration DNS records you should add? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 356
HOTSPOT - (Topic 6)
You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

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

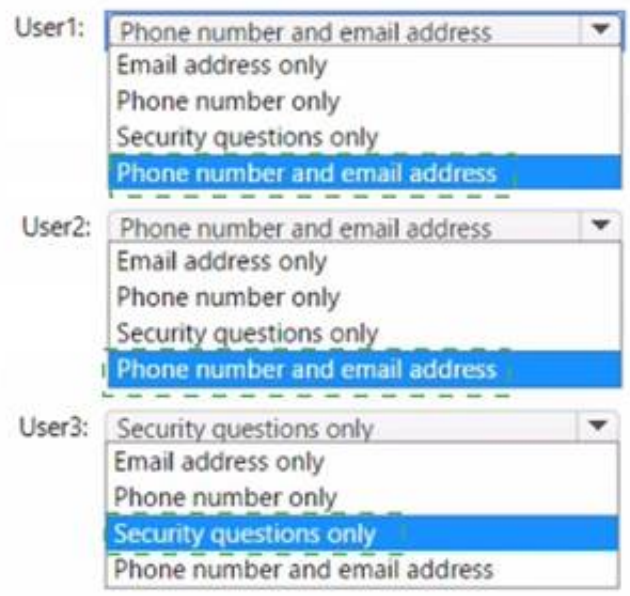
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



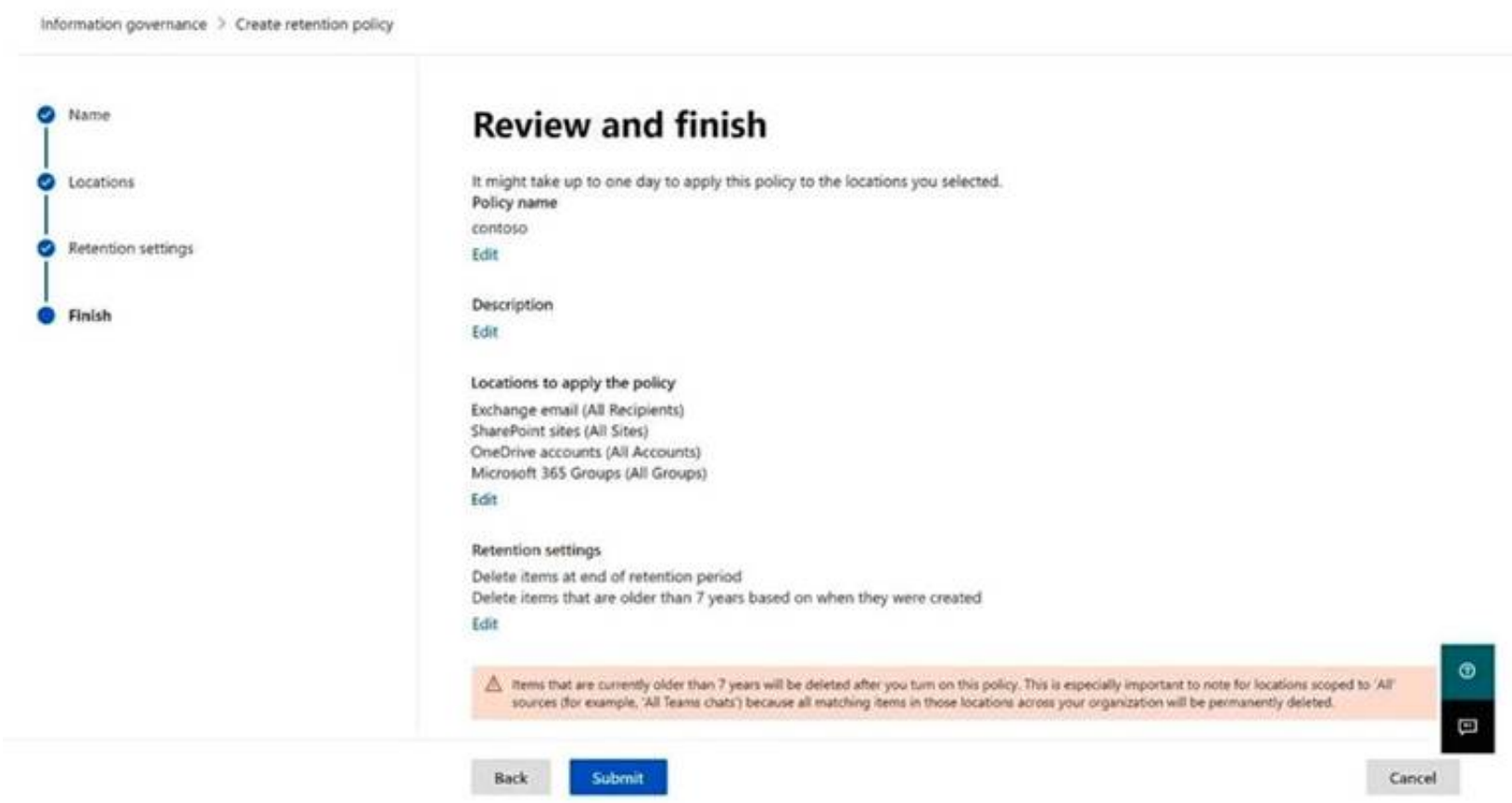
NEW QUESTION 360
- (Topic 6)
You purchase a new computer that has Windows 10, version 21H1 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

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

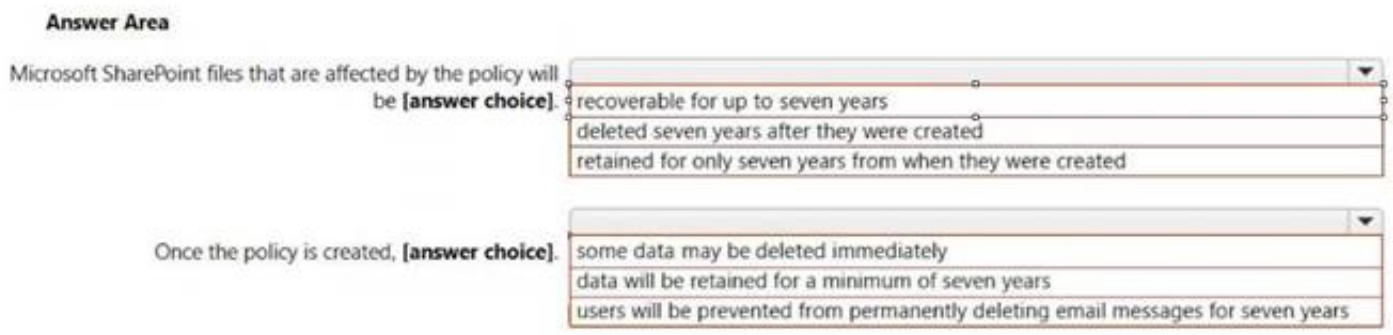
Answer: C

NEW QUESTION 361
HOTSPOT - (Topic 6)
HOTSPOT

You have a Microsoft 365 tenant.
You plan to create a retention policy as shown in the following exhibit.



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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 362
- (Topic 6)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.
The tenant contains the users shown in the following table.

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

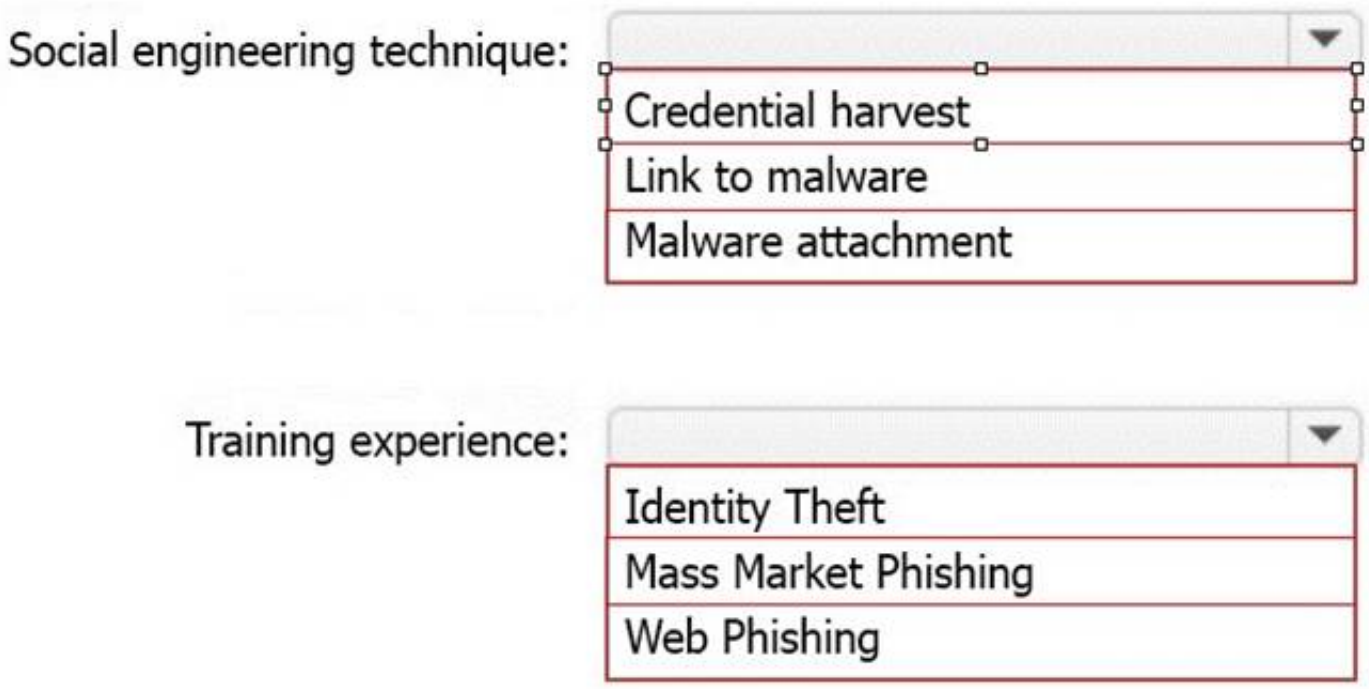
You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User3 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 365
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E3 subscription.
You plan to launch Attack simulation training for all users.
Which social engineering technique and training experience will be available? 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: Credential Harvest
Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering.
Note: In Attack simulation training, multiple types of social engineering techniques are available:
Credential Harvest Malware Attachment Link to Malware
Etc.
Box 2: Mass Market Phishing

NEW QUESTION 366
HOTSPOT - (Topic 6)
You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

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

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

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

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

Name	Assigned to
Policy1	Group3
Policy2	Group2

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 371
- (Topic 6)
You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.

Domains

+ Add domain | Buy domain | Refresh

Domain name	Status	Choose columns
Sub1.contoso221018.onmicrosoft.com (D...	Possible service issues	
contoso.com	Incomplete setup	
contoso221018.onmicrosoft.com	Healthy	
Sub2.contoso221018.onmicrosoft.com	Incomplete setup	

Which domain name suffixes can you use when you create users?

A. only Sub1.contoso221018.onmicrosoft.com
B. onlycontoso.com and Sub2.contoso221018.onmicrosoft.com
C. onlvcontoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com
D. all the domains in the subscription

Answer: B

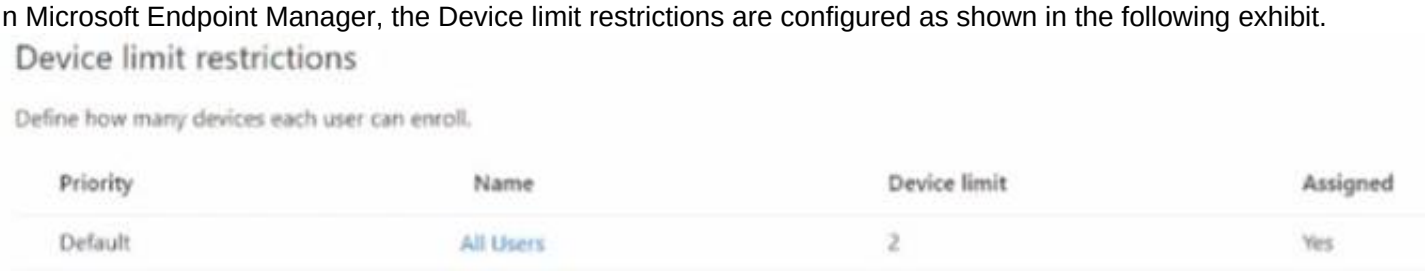
NEW QUESTION 376
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the following user:
? Name: User1
? UPN: user1@contoso.com
? Email address: user1@marketmg.contoso.com
? MFA enrollment status: Disabled
When User1 attempts to sign in to Outlook on the web by using the user1@marketing.contoso.com email address, the user cannot sign in.
You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com.
What should you do?

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

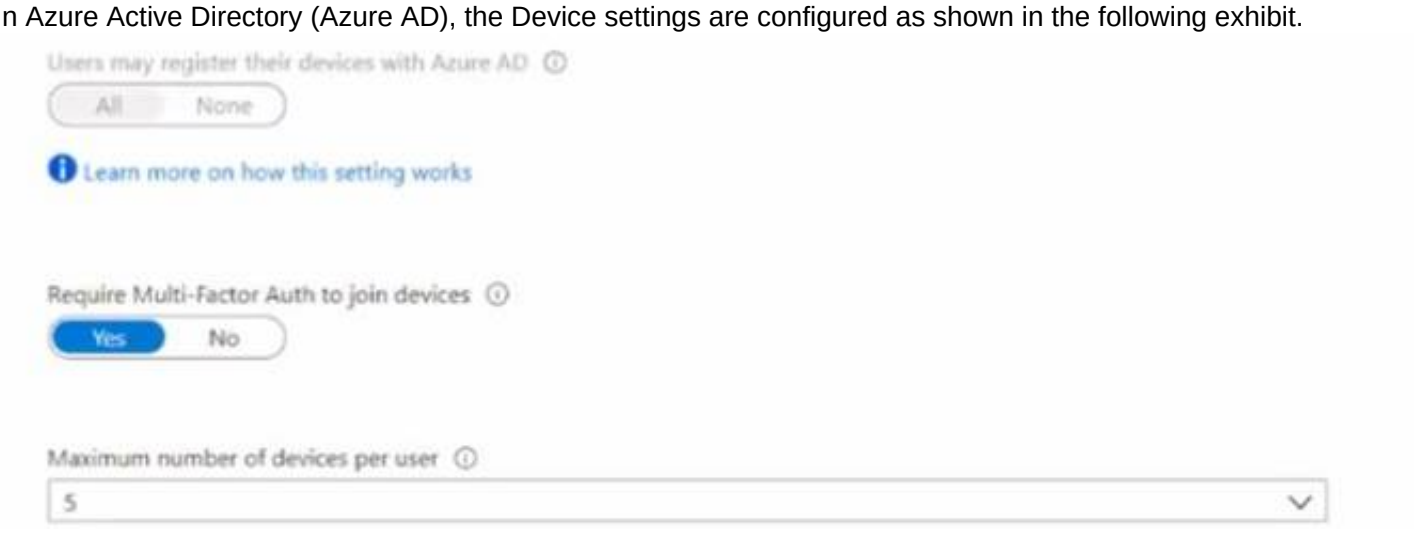
Answer: D

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

NEW QUESTION 377
HOTSPOT - (Topic 6)
You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.
In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.



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



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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 378

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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