Microsoft

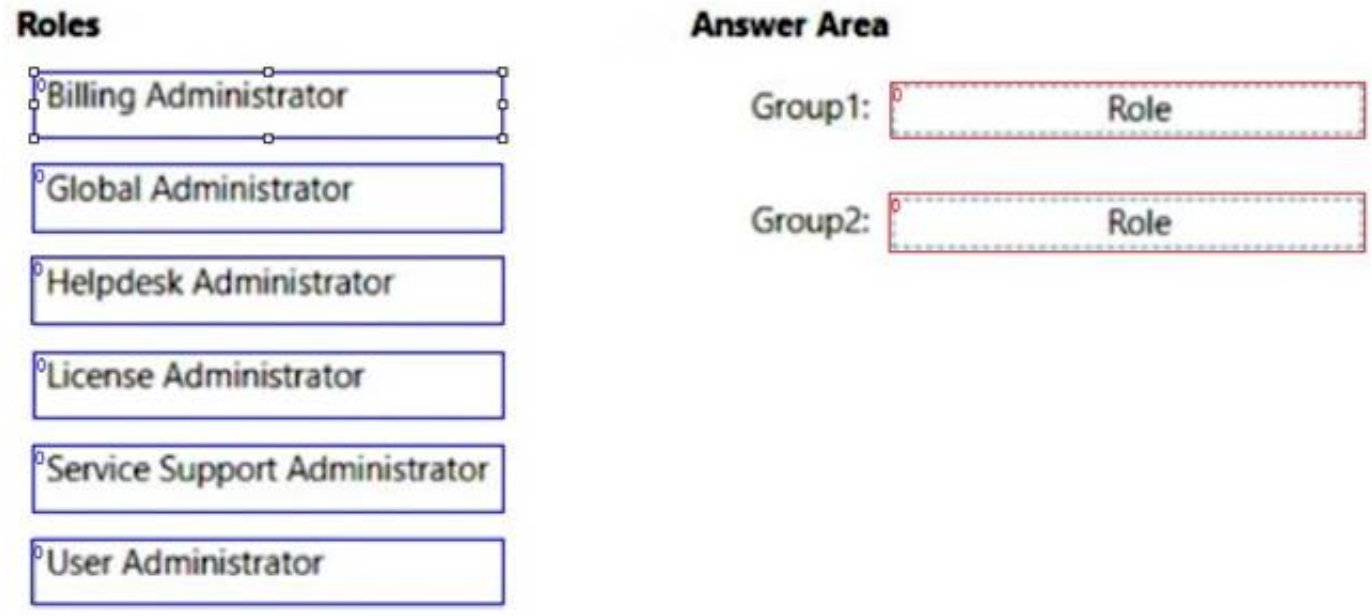
Exam Questions MS-102

Microsoft 365 Administrator Exam

NEW QUESTION 1
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.
You need to ensure that each group can perform the tasks shown in the following table.

Group	Task
Group1	• Manage service requests. • Purchase new services. • Manage subscriptions. • Monitor service health.
Group2	• Assign licenses. • Add users and groups. • Create and manage user views. • Update password expiration policies.

The solution must use the principle of least privilege.
Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Billing admin manage service request Purchase new services Etc.
Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.
Box 2: User admin User admin
Assign the User admin role to users who need to do the following for all users:
- Add users and groups
- Assign licenses
- Manage most users properties
- Create and manage user views
- Update password expiration policies
- Manage service requests
- Monitor service health

NEW QUESTION 2
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 3
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage 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 4
- (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?

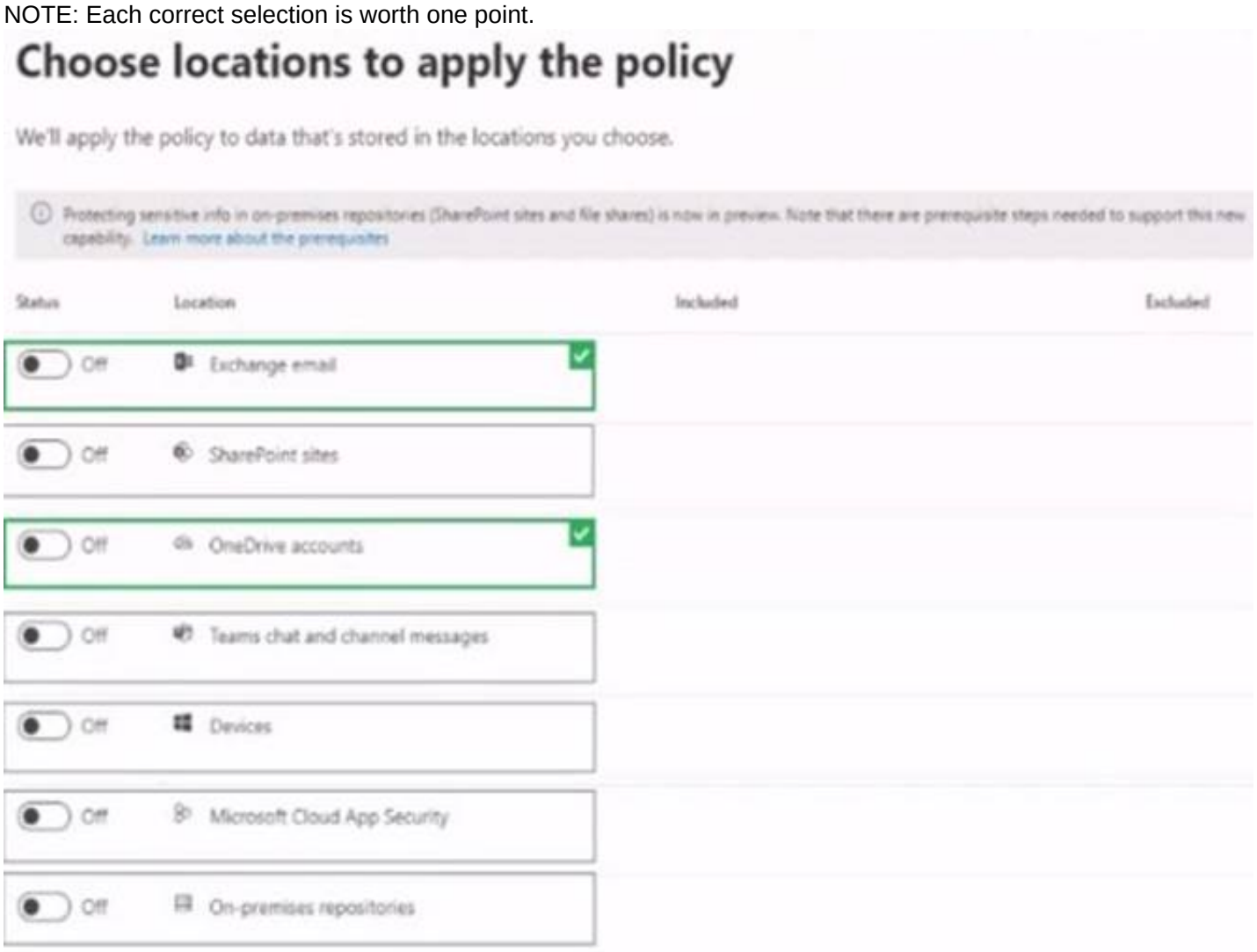
A. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.
B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.
C. From the Microsoft 365 admin center, modify Organization information.
D. From the Microsoft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

Answer: A

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

NEW QUESTION 5
HOTSPOT - (Topic 6)

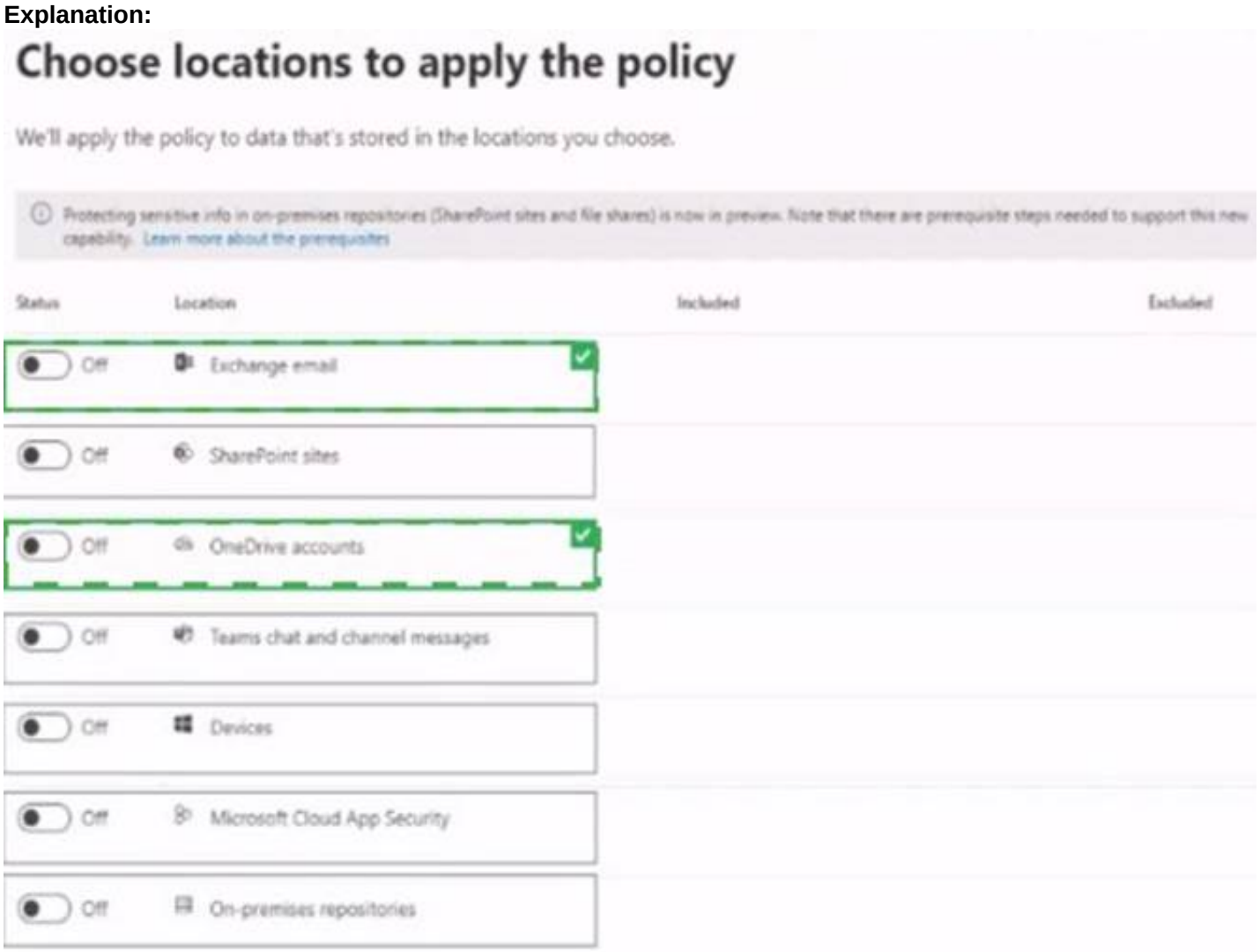
You have a Microsoft 365 E5 tenant
You create a data toss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.
To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.
NOTE: Each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



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 6
- (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 7
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to implement device configuration profiles in Microsoft Intune. Which platform can you manage by using the profiles?

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

Answer: D

NEW QUESTION 8
- (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 9
- (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 10
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the resources shown in the following table.

Name	Type
Mailbox1	Microsoft Exchange Online mailbox
Account1	Microsoft OneDrive account
Site1	Microsoft SharePoint Online site
Channel	Microsoft Teams channel

To which resources can you apply a sensitivity label by using an auto-labeling policy?

A. Mailbox1 and Site1 only

B. Mailbox1, Account1, and Site1 only
C. Account1 and Site1 only
D. Mailbox1, Account1, Site1, and Channel1
E. Account1, Site1, and Channel1 only

Answer: E

Explanation:

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

NEW QUESTION 10
- (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

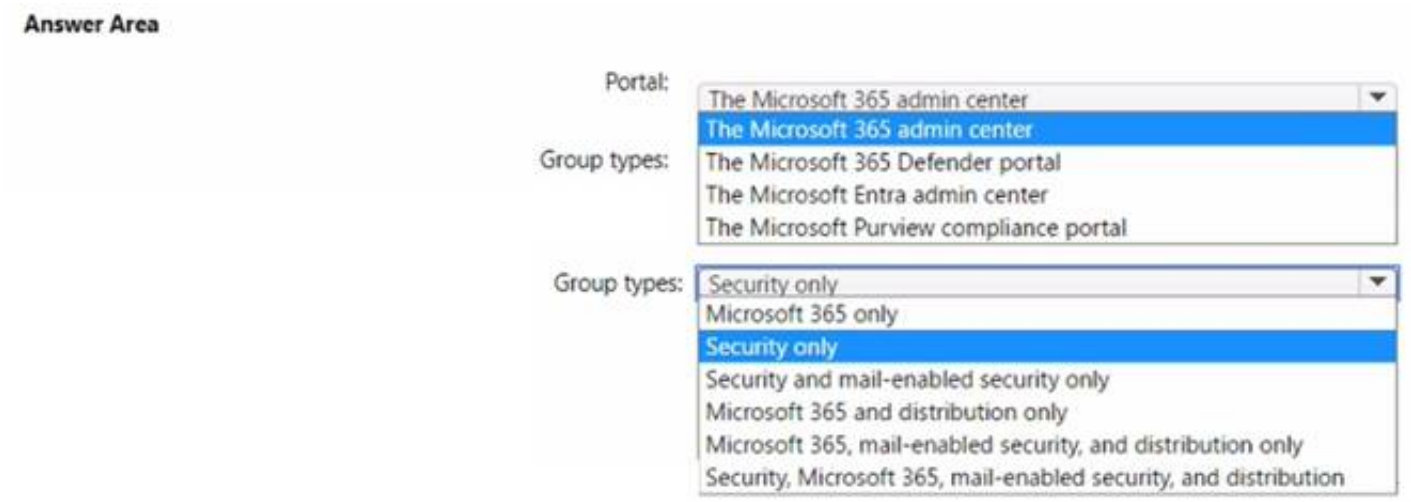
NEW QUESTION 17
- (Topic 6)
You have a Microsoft 365 subscription.
You register two applications named App1 and App2 to Azure AD.
You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

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 22
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 23
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

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

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

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

Answer: D

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

NEW QUESTION 27
- (Topic 6)
You have a Microsoft 365 tenant that contains 500 Windows 10 devices and a Microsoft Endpoint Manager device compliance policy.
You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps.
Which policy type should you configure?

A. conditional access
B. account protection

C. attack surface reduction (ASR)
D. Endpoint detection and response

Answer: A

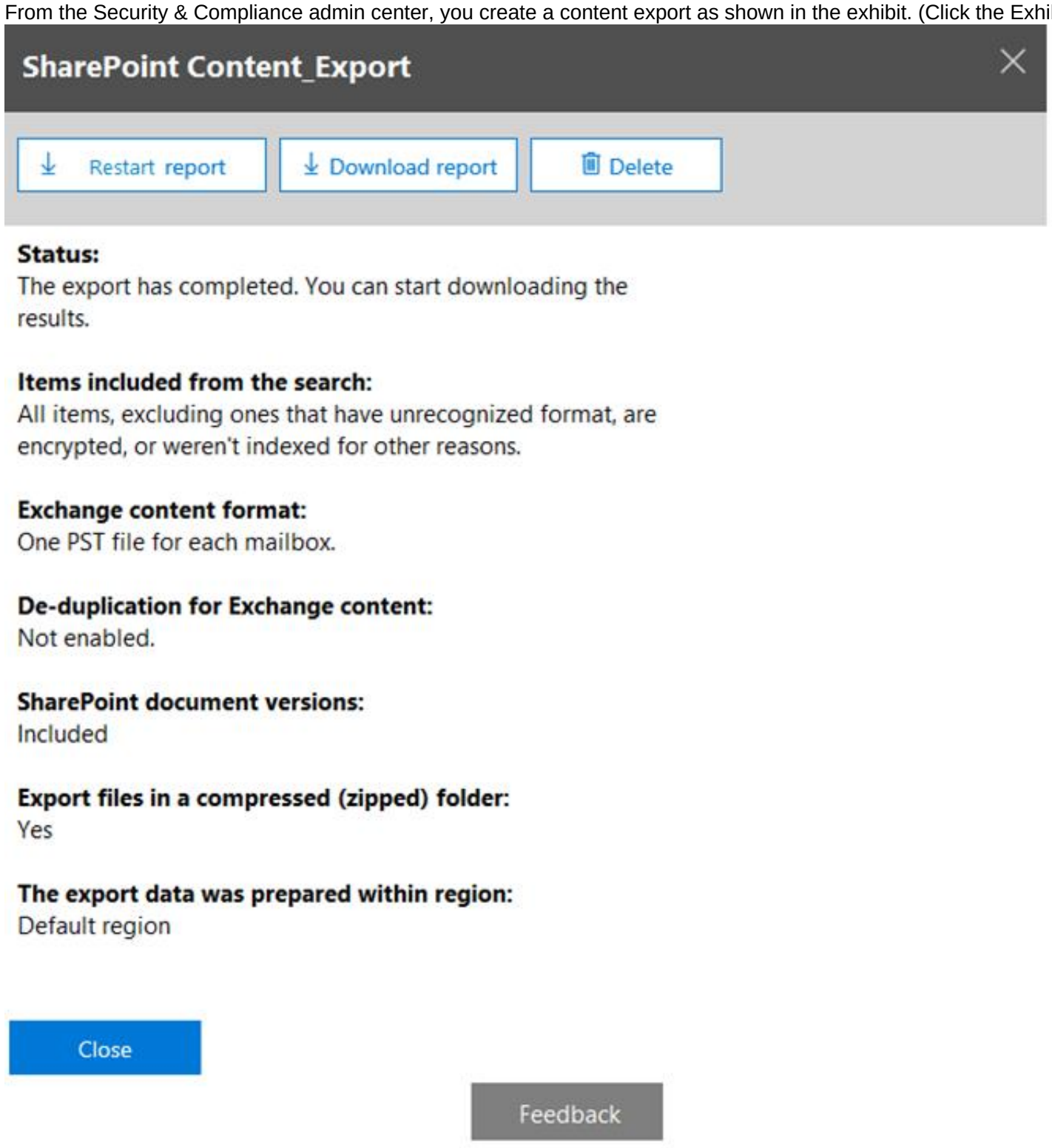
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION 28
- (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 31
- (Topic 6)
From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)



What will be excluded from the export?

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

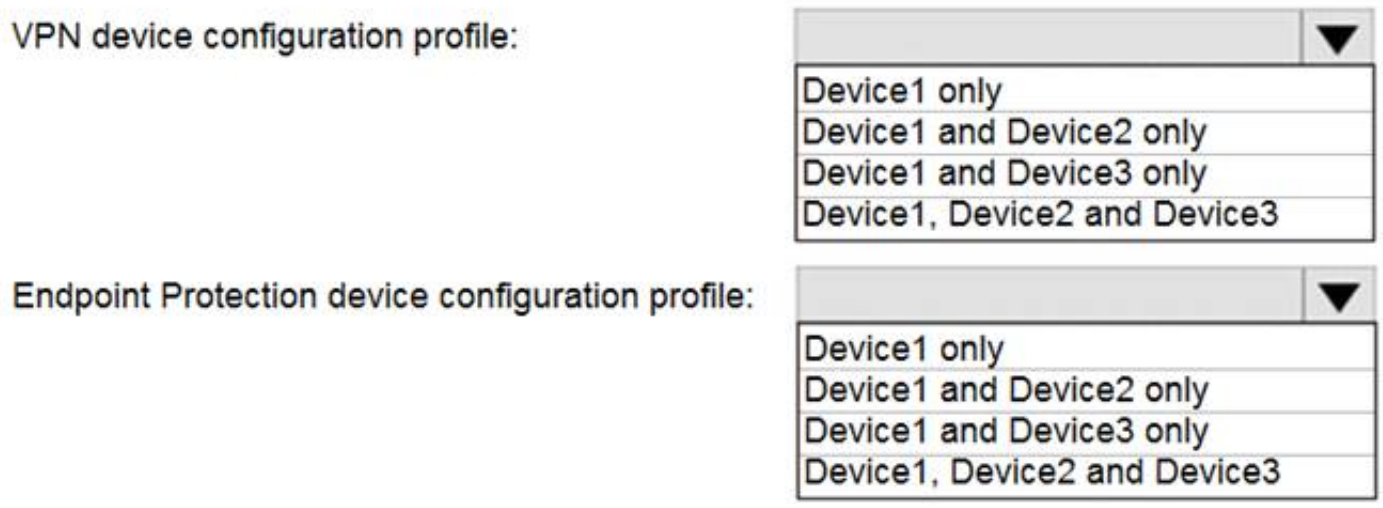
Answer: B

Explanation:
Unrecognized file formats are excluded from the search.
Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be
unsupported file types.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide
https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search- report

NEW QUESTION 36
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

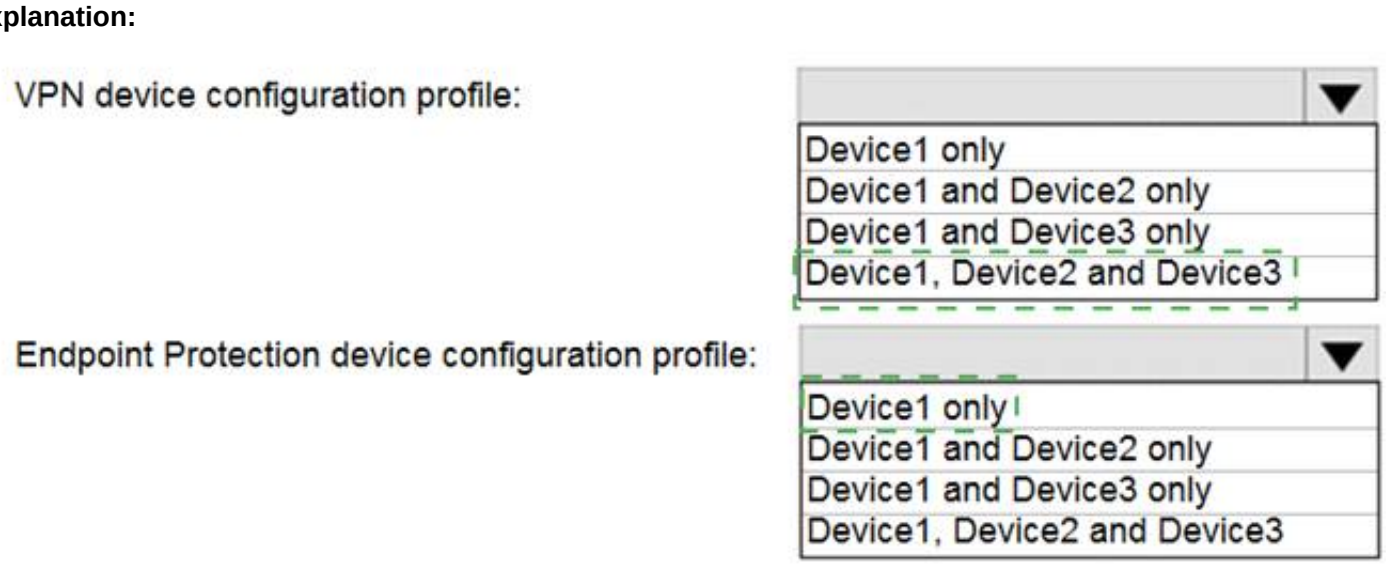
You plan to perform the following device management tasks in Microsoft Endpoint Manager:
? Deploy a VPN connection by using a VPN device configuration profile.
? Configure security settings by using an Endpoint Protection device configuration profile.
You support the management tasks.
What should you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



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 41
- (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

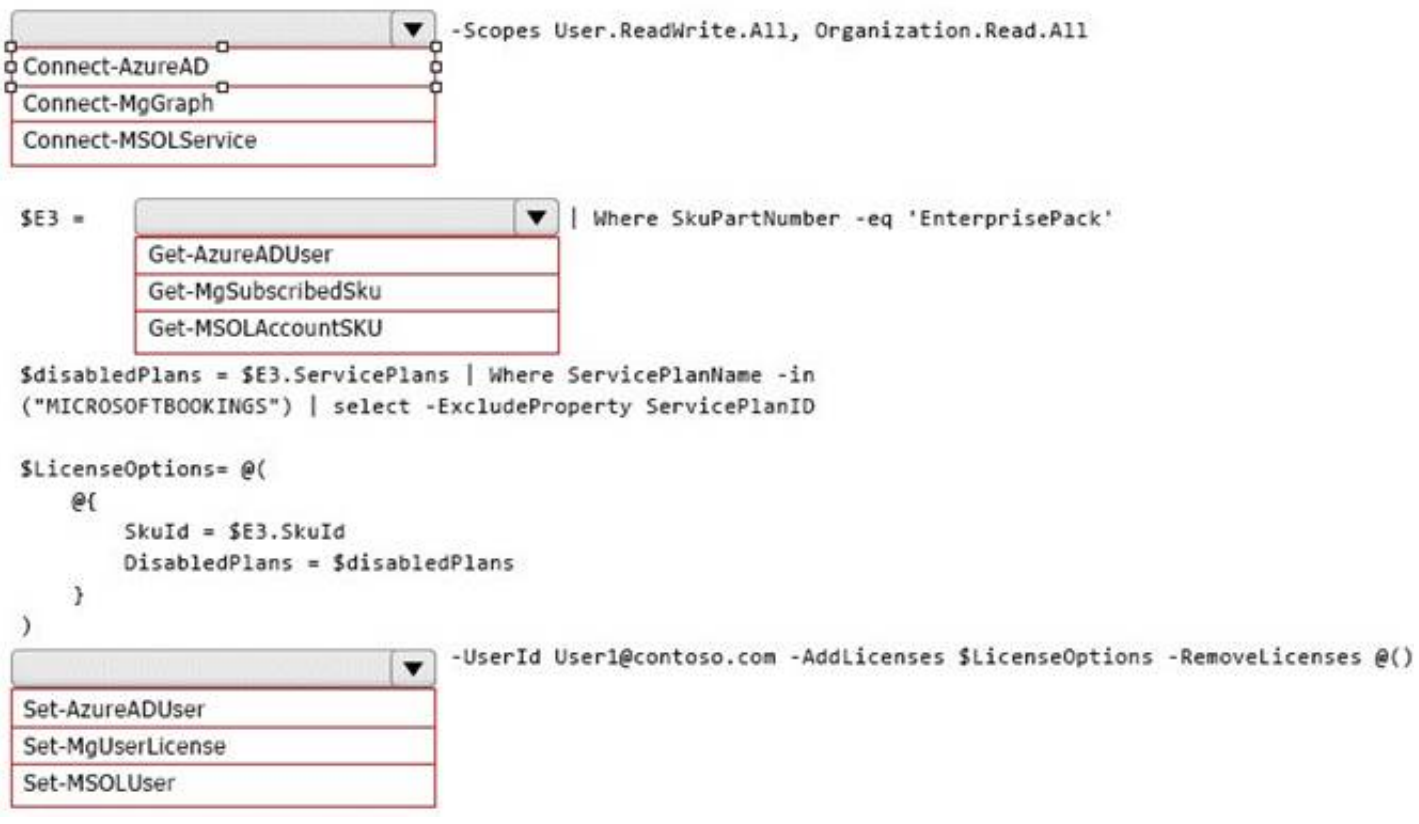
NEW QUESTION 45
- (Topic 6)
You purchase a new computer that has Windows 10, version 2004 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

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

Answer: B

NEW QUESTION 47
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription.
A user named user1@contoso.com was recently provisioned.
You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Connect-MgGraph
Assign Microsoft 365 licenses to user accounts with PowerShell Use the Microsoft Graph PowerShell SDK
First, connect to your Microsoft 365 tenant.
Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the 'Assign license' Microsoft Graph API reference page.
The Organization.Read.All permission scope is required to read the licenses available in the tenant.
Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All Box 2: Get-MgSubscribedSku
Run the Get-MgSubscribedSku command to view the available licensing plans and the
number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.
Box 3: Set-MgUserLicense Assigning licenses to user accounts
To assign a license to a user, use the following command in PowerShell.
Set-MgUserLicense -UserId $userUPN -AddLicenses @{SkuId = "<SkuId>"} - RemoveLicenses @()
This example assigns a license from the SPE_E5 (Microsoft 365 E5) licensing plan to the unlicensed user belindan@litwareinc.com:
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId =
$e5Sku.SkuId} -RemoveLicenses @()

NEW QUESTION 52
- (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 54
- (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 57
- (Topic 6)
You have a Microsoft E5 subscription.
You need to ensure that administrators who need to manage Microsoft Exchange Online are assigned the Exchange Administrator role for five hours at a time.
What should you implement?

A. Azure AD Privileged Identity Management (PIM)
B. a conditional access policy
C. a communication compliance policy)
D. Azure AD Identity Protection
E. groups that have dynamic membership

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

NEW QUESTION 61
- (Topic 6)
You have a Microsoft 365 F5 subscription.
You plan to deploy 100 new Windows 10 devices.
You need to order the appropriate version of Windows 10 for the new devices. The version must
Meet the following requirements.
Be serviced for a minimum of 24 moths.
Support Microsoft Application Virtualization (App-V) Which version should you identify?

A. Window 10 Pro, version 1909
B. Window 10 Pro, version 2004
C. Window 10 Pro, version 1909
D. Window 10 Enterprise, version 2004

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/release-health/release-information
https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported- configurations

NEW QUESTION 62
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 subscription that contains the users shown in the following table.

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

NEW QUESTION 63
- (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 67
- (Topic 6)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.
The tenant contains the users shown in the following table.

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

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

A. Yes
B. No

Answer: A

NEW QUESTION 71
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.

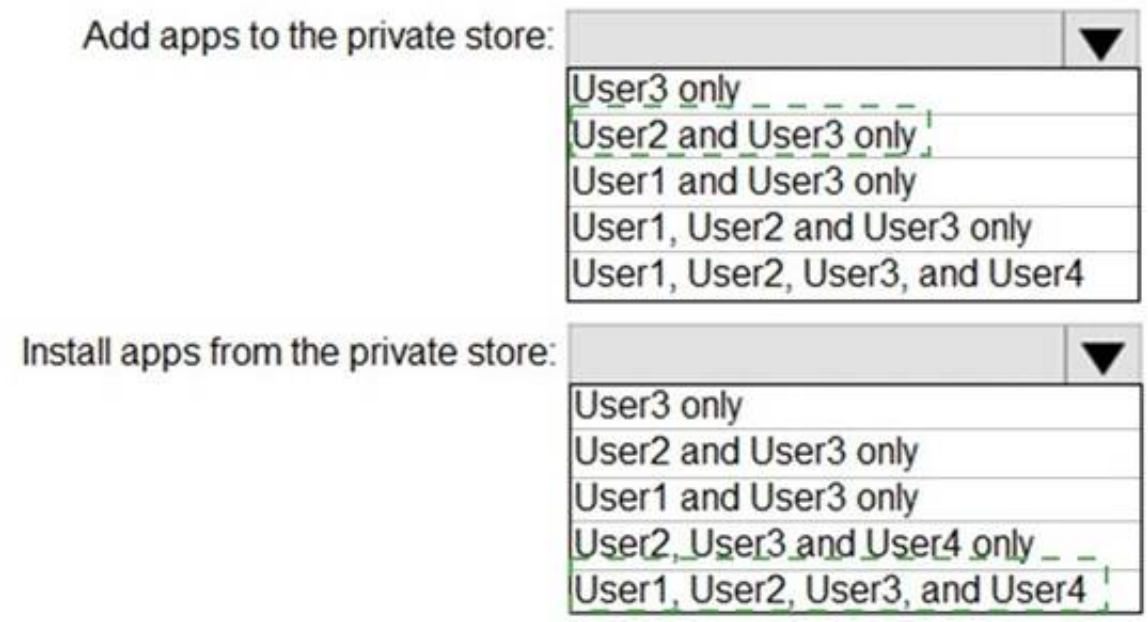
Add apps to the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Install apps from the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User2, User3 and User4 only
- User1, User2, User3, and User4

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 75
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.
The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.
You need to identify the following information:
• The number of email messages quarantined by zero-hour auto purge (ZAP)
• The number of times users clicked a malicious link in an email message
Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

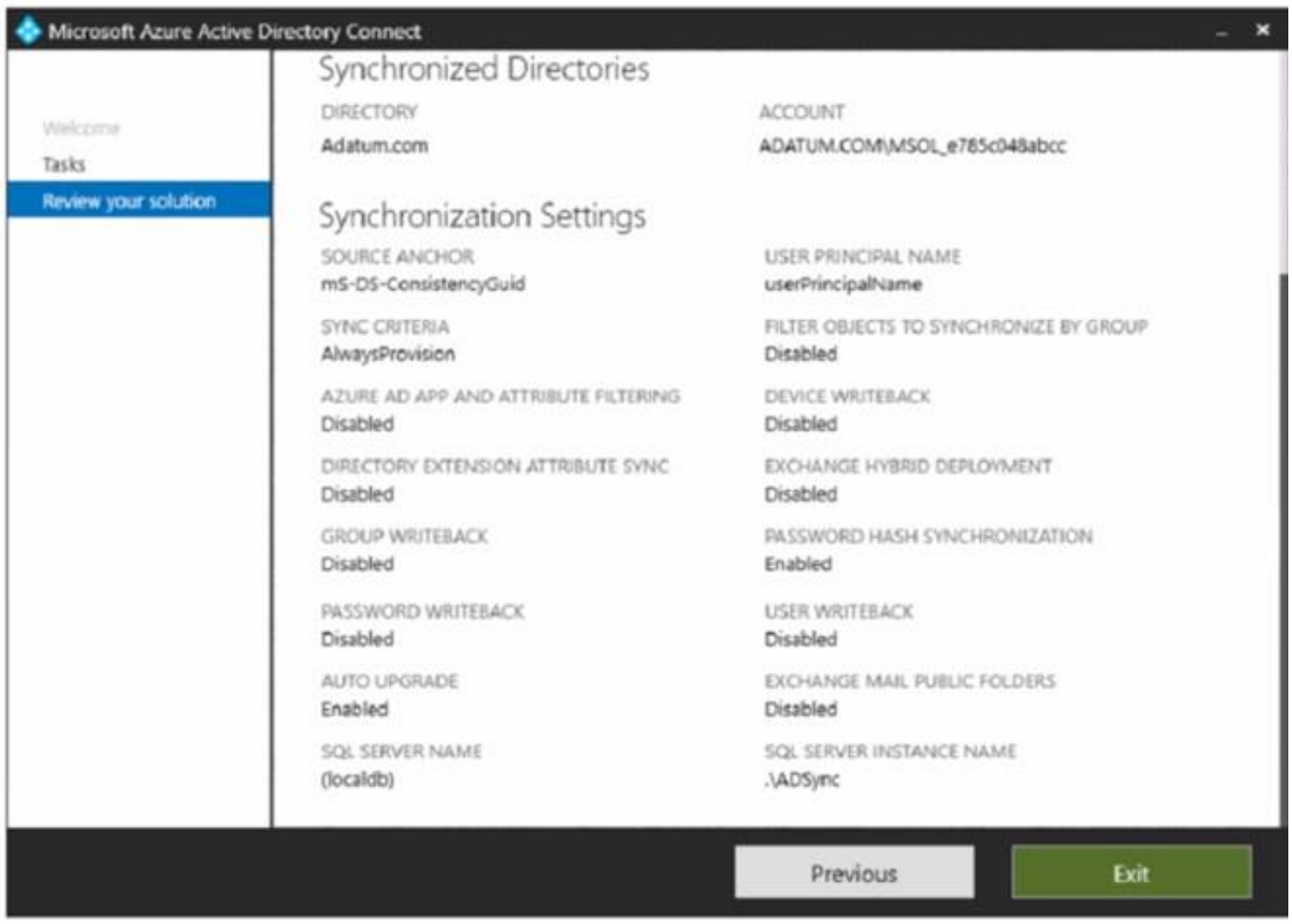
NEW QUESTION 78
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature. You need to block users from downloading a file named File1.exe.
What should you use?

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

Answer: A

NEW QUESTION 82

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 87
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Reports Reader
User2	Exchange Administrator
User3	User Experience Success Manager

Which users can review the Adoption Score in the Microsoft 365 admin center?

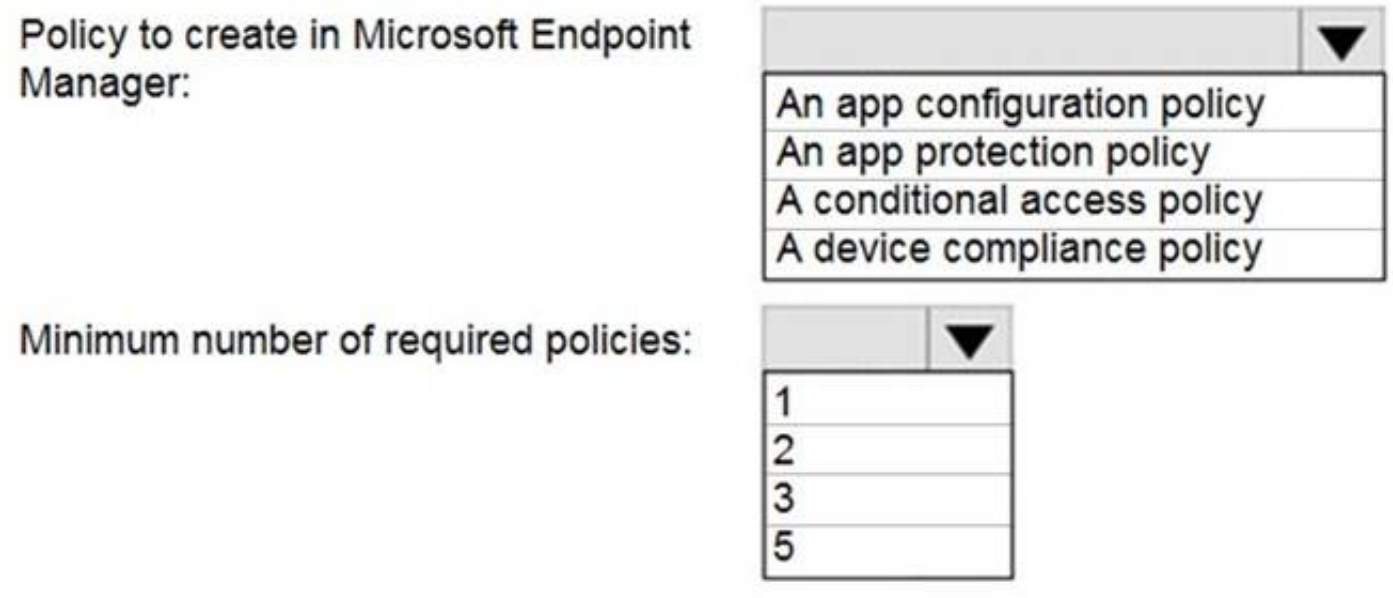
A. User! only
B. User2onry
C. User1 and User2 only
D. User! and User3 only
E. User1, User2. and User3

Answer: E

NEW QUESTION 89
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.

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

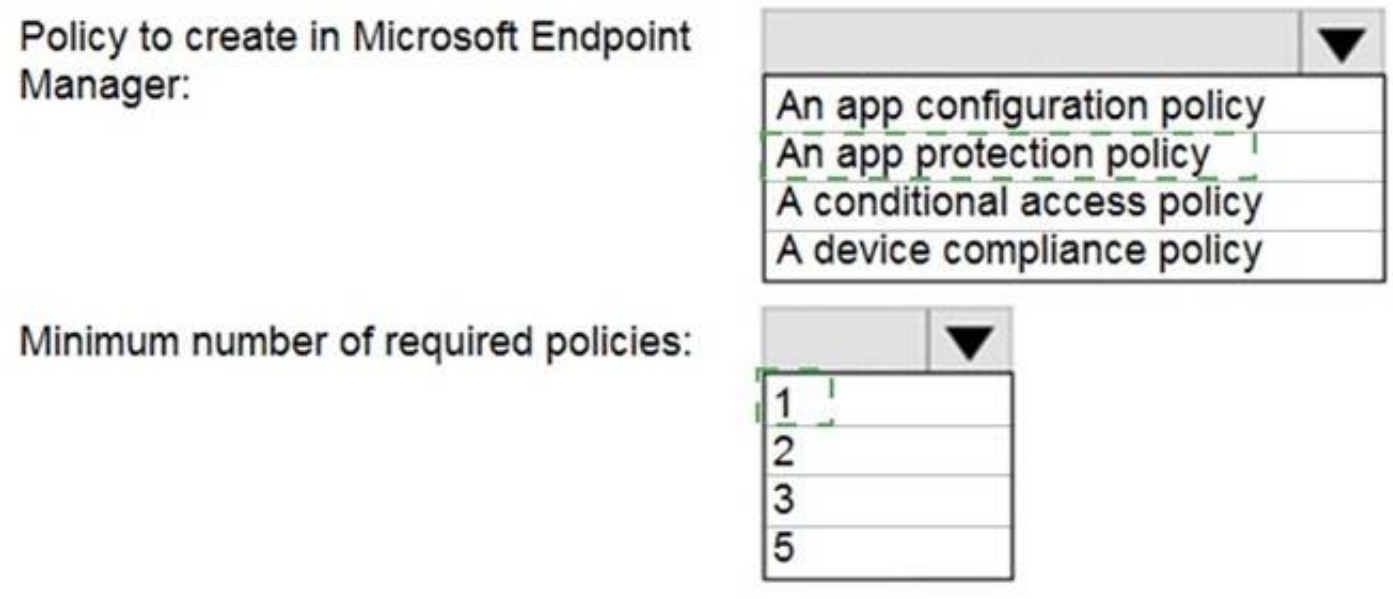
All the devices have an app named App1 installed.
You need to prevent users from copying data from App1 and pasting the data into other apps.
Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in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



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 92
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 97
- (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 99
- (Topic 6)
You need to notify the manager of the human resources department when a user in the department shares a file or folder from the departments Microsoft SharePoint Online site. What should you do?

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

Answer: D

NEW QUESTION 102
- (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 105
- (Topic 6)
You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.
Devices are onboarded by using Microsoft Defender for Endpoint.
You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.
What should you create first?

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

Answer: B

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

NEW QUESTION 109
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it as a result these questions will not appear in the review screen.
Your network contains an Active Directory forest. You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
• Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
• User passwords must be 10 characters or more.
Solution: implement password hash synchronization and modify the password settings from
the Default Domain Policy in Active Directory. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 110
- (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 114
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.	○	○

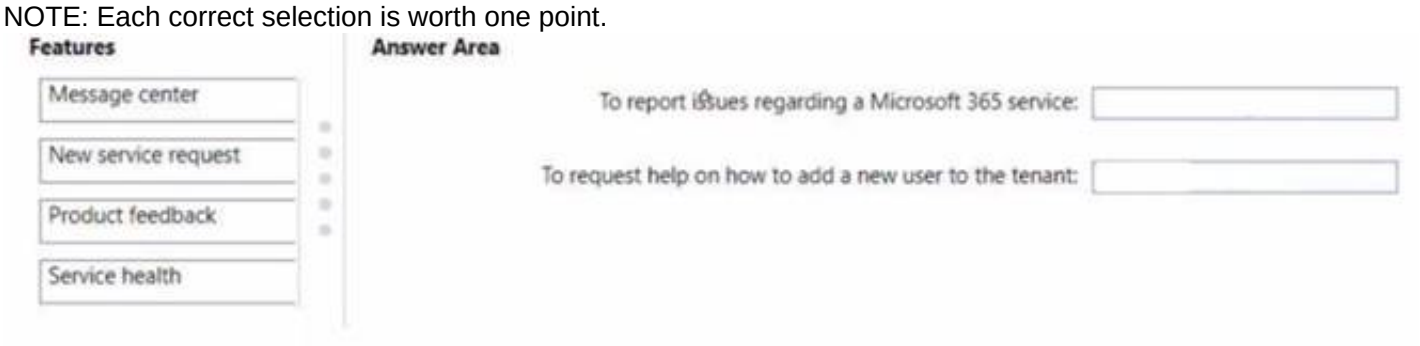
NEW QUESTION 115
- (Topic 6)
Your company has on-premises servers and an Azure AD tenant.
Several months ago, the Azure AD Connect Hearth agent was installed on all the servers. You review the health status of all the servers regularly.
Recently, you attempted to view the health status of a server named 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 117
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You need to meet the following requirements:
• Report a Microsoft 365 service issue.

• Request help on how to add a new user to an Azure AD tenant.
What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature 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

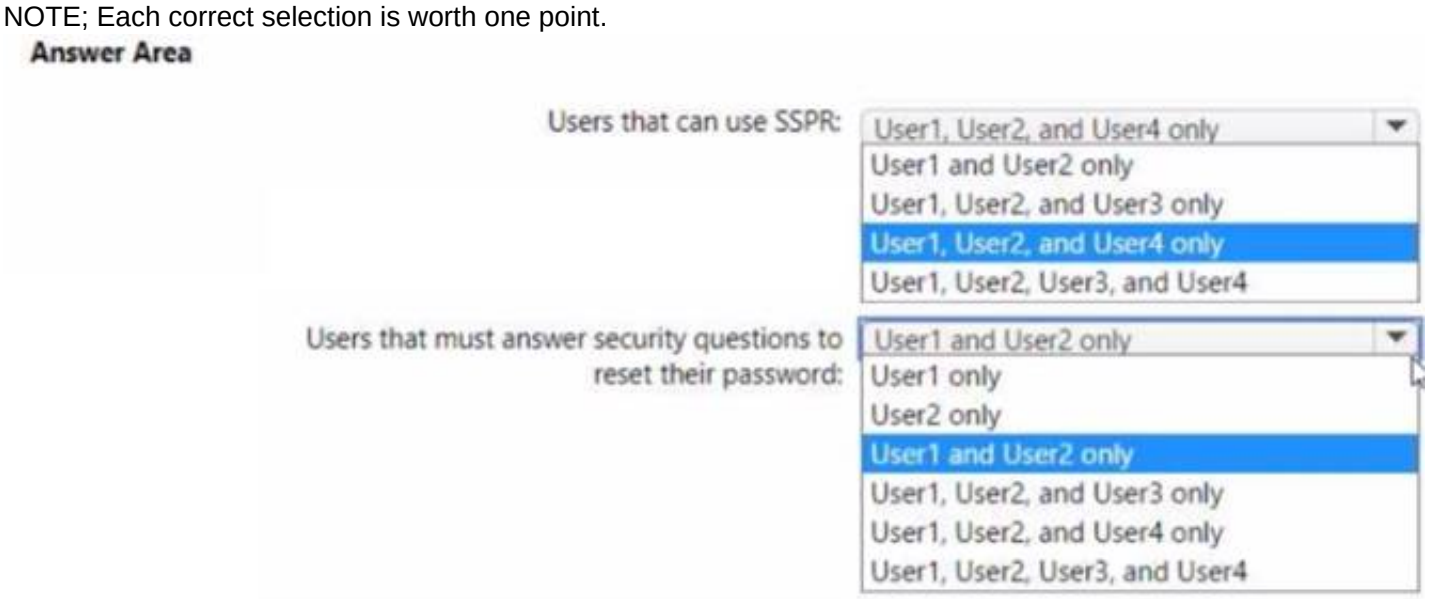
Answer: A

Explanation:

NEW QUESTION 121
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

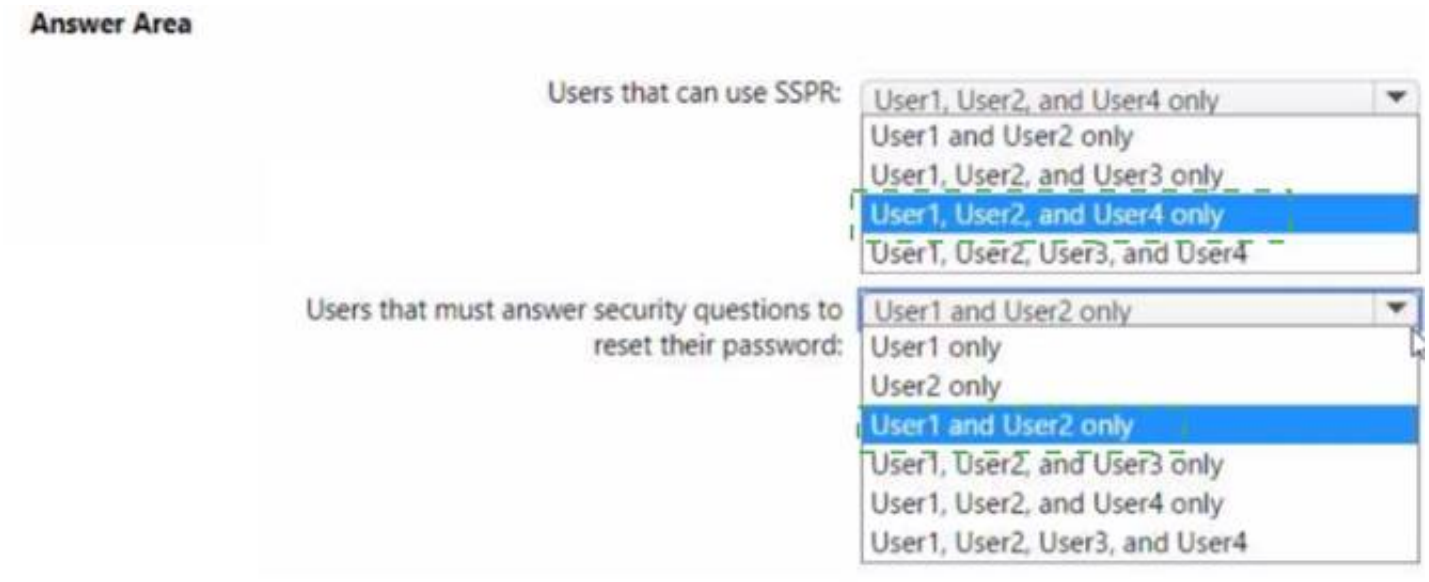
You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.
Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.
NOTE;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



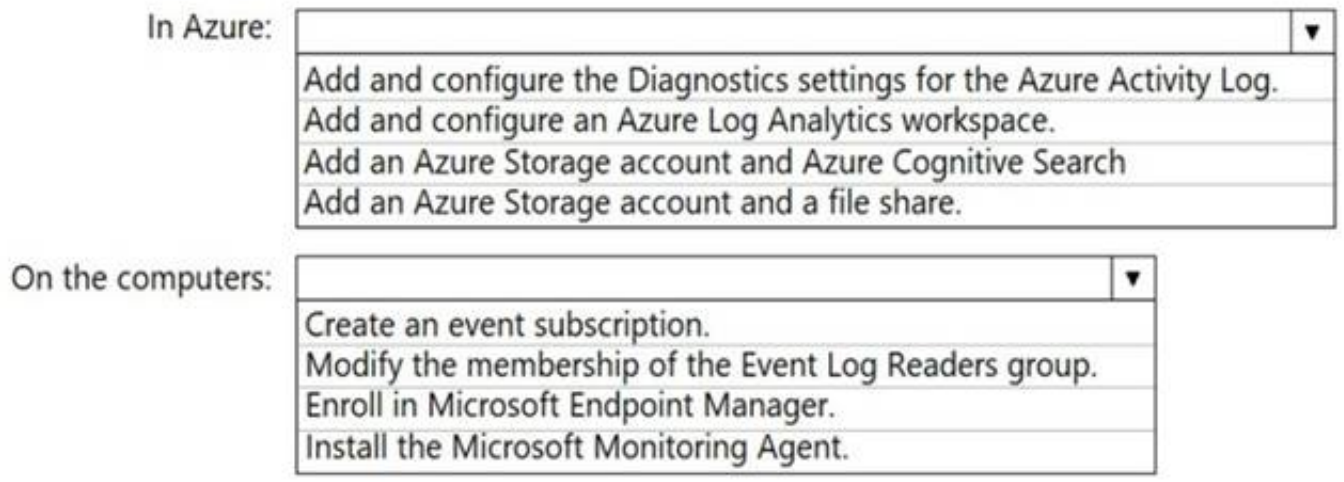
A. Mastered
B. Not Mastered

Answer: A

Explanation:



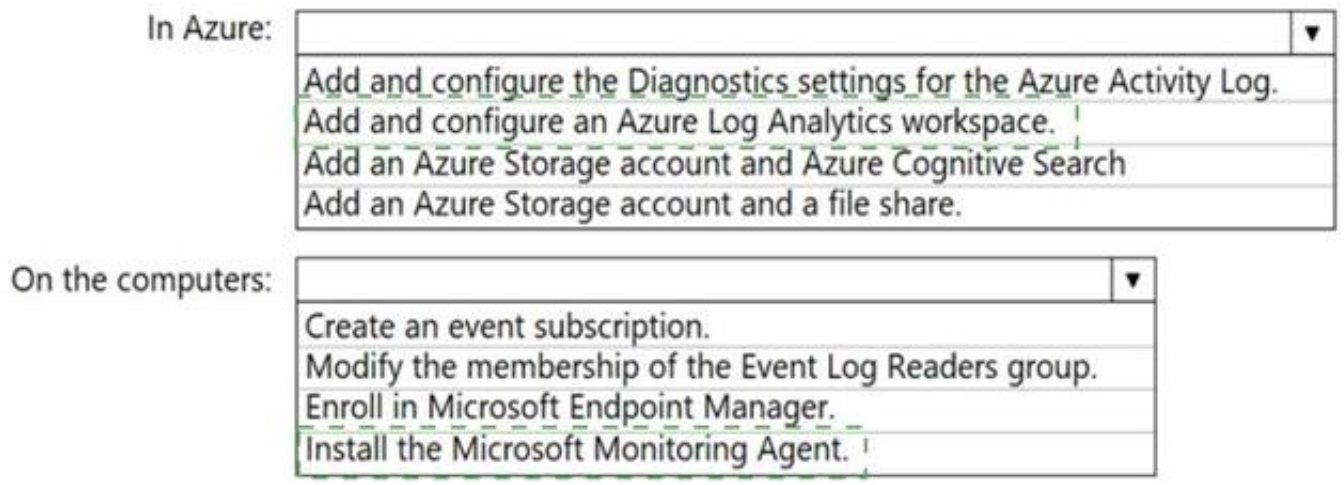
NEW QUESTION 126
HOTSPOT - (Topic 6)
You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.
You need to centrally monitor System log events from the computers.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



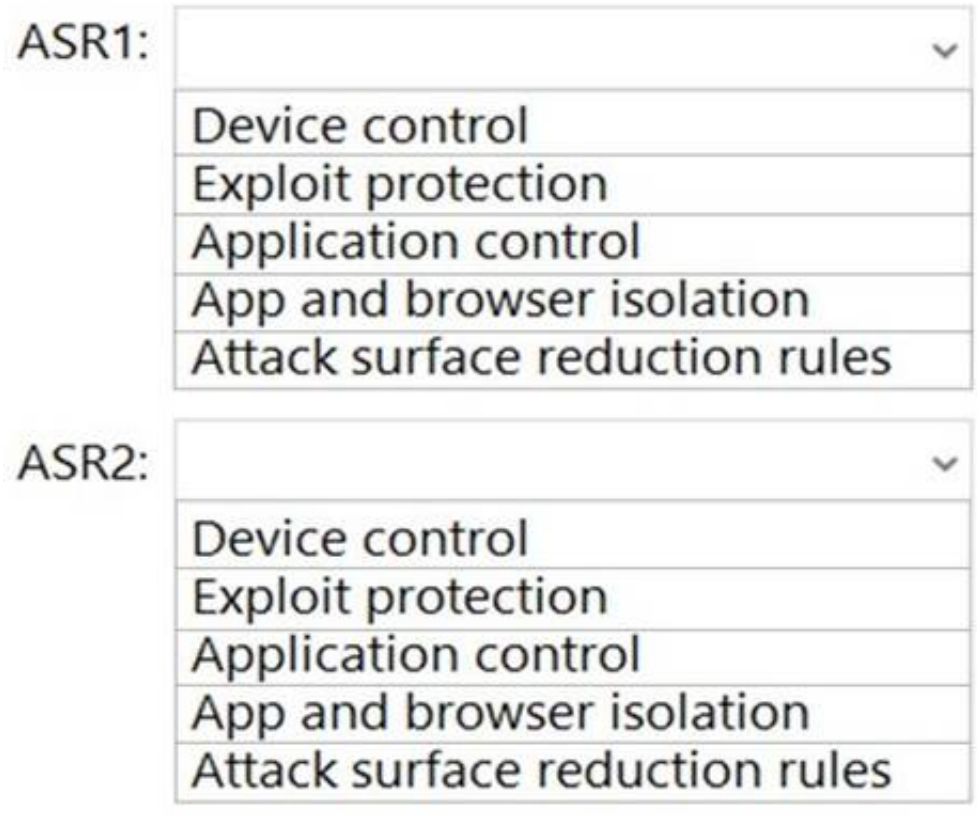
A. Mastered
B. Not Mastered

Answer: A

Explanation:



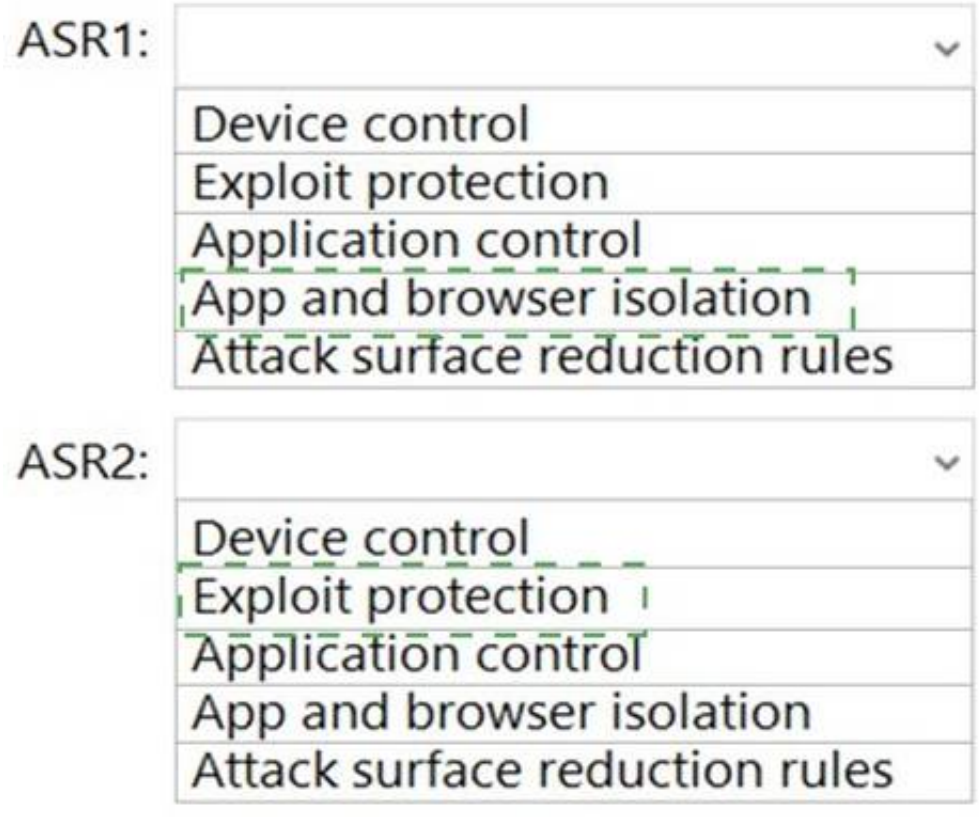
NEW QUESTION 129
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.
You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender 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 130
- (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.

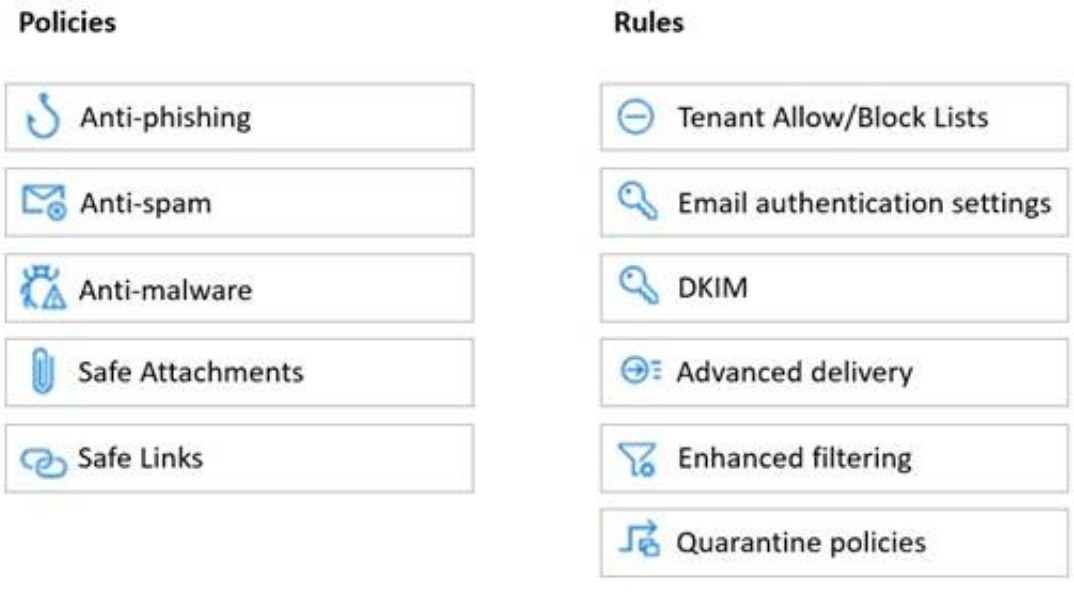
A. Password Hash Synchronization
B. Password writeback
C. Directory extension attribute sync
D. Enable single sign-on
E. Pass-through authentication

Answer: AB

NEW QUESTION 131
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 133
- (Topic 6)
You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

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

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

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

Answer: AE

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

NEW QUESTION 138
- (Topic 6)
You have a Microsoft 365 subscription.
You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.
You need to prevent the users from bypassing the DLP policy. What should you configure?

A. actions
B. incident reports
C. exceptions
D. user overrides

Answer: D

Explanation:
A DLP policy can be configured to allow users to override a policy tip and report a false positive.
You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word.
If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention- policies

NEW QUESTION 143
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 144
HOTSPOT - (Topic 6)
HOTSPOT

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

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

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

NEW QUESTION 146
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

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

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 150
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription.
You deploy the anti-phishing policy shown in the following exhibit.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the **[answer choice]** setting.
- Add trusted senders and domains
- Enable domains to protect
- Enable users to protect
- Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the **[answer choice]** setting.
- Add trusted senders and domains
- Enable intelligence for impersonation protection
- Enable spoof intelligence

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Enable users to protect
Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.
User impersonation protection
User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.

You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation
is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).
When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender's email address, the action for impersonated users is applied to the message.
Box 2: Add trusted senders and domains Trusted senders and domains
Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren't applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.

NEW QUESTION 154
- (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 159
- (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 162
- (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 166
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.

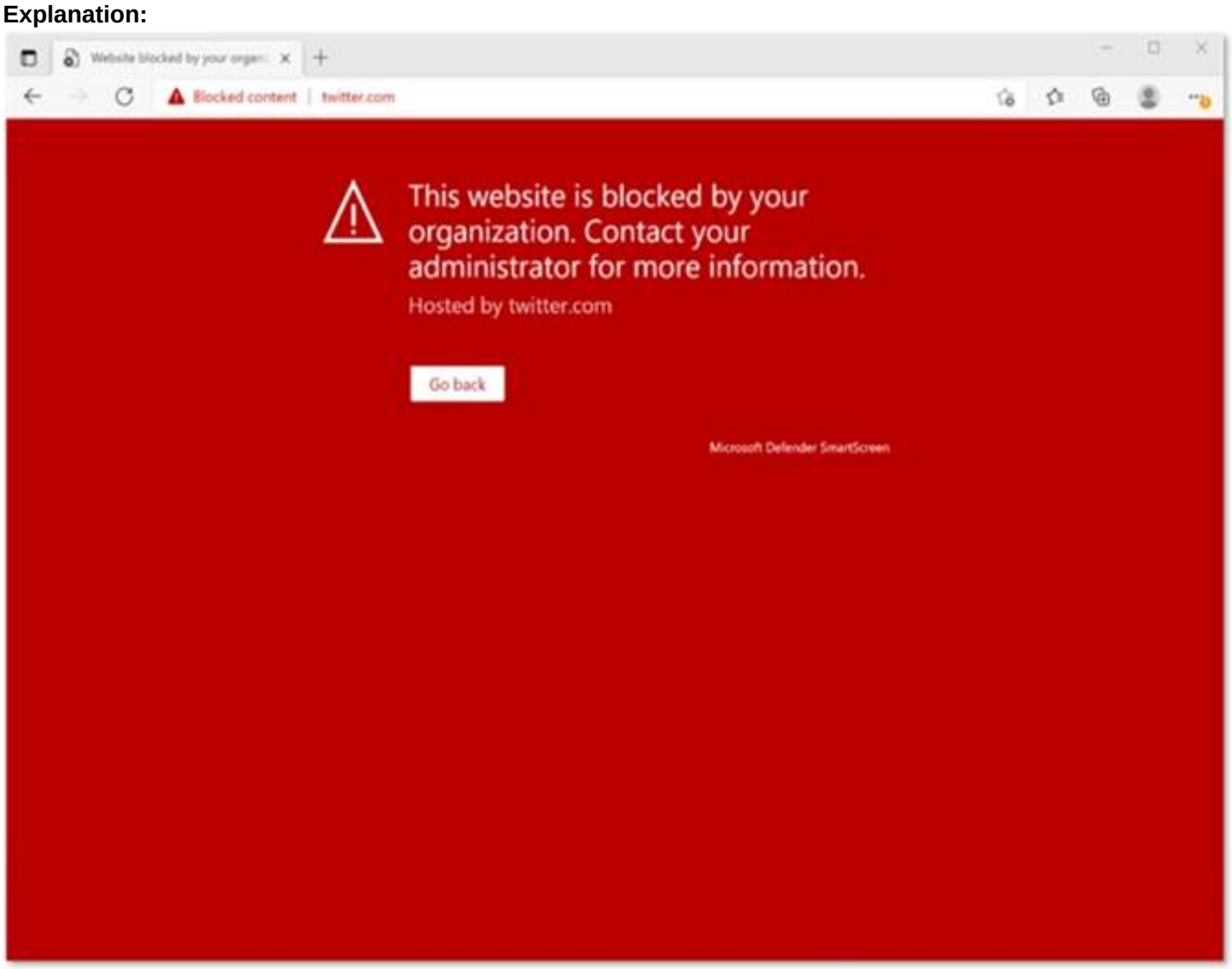
NEW QUESTION 170
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

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

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

Answer: E

Explanation:



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

NEW QUESTION 173
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

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

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

Answer: C

NEW QUESTION 175
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 176
- (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 177
- (Topic 6)
You have a Microsoft 365 subscription that uses Security & Compliance retention policies.
You implement a preservation lock on a retention policy that is assigned to all executive users.

Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point?

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

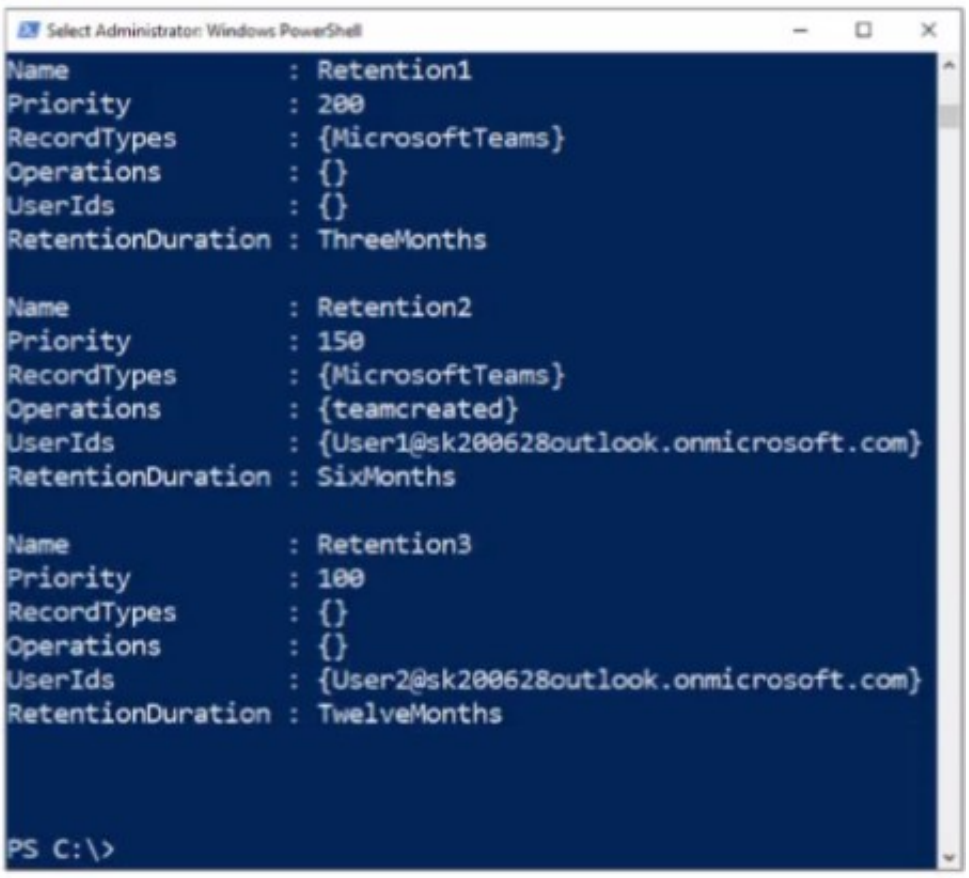
Answer: AB

NEW QUESTION 181
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it As a result these questions will not appear in the review screen.
Your network contains an Active Directory forest. You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
• Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
• User passwords must be 10 characters or more.
Solution: implement password hash synchronization and configure password protection in the Azure AD tenant.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 186
HOTSPOT - (Topic 6)
You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.



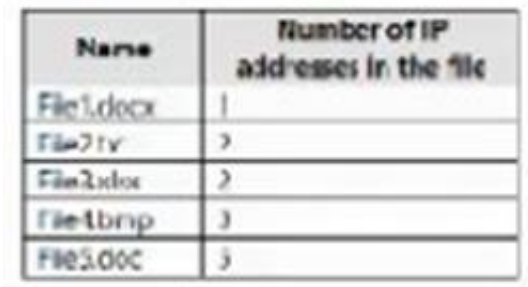
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic NOTE Each correct selection is worth one point.

A. Mastered
B. Not Mastered

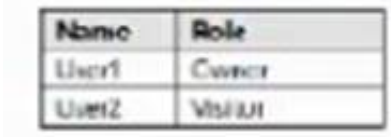
Answer: A

Explanation:

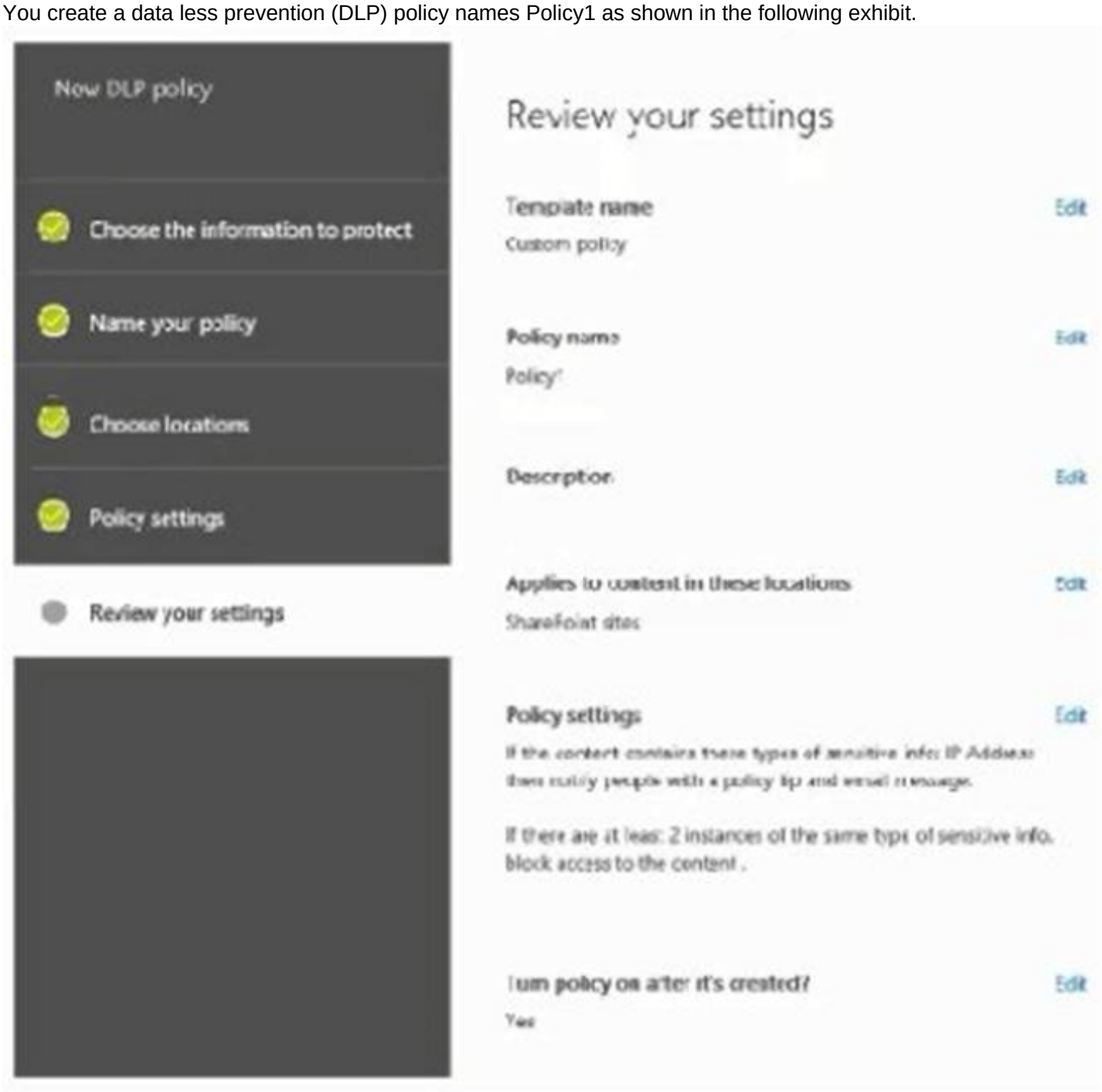
NEW QUESTION 189
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has he files in the following table.



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



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



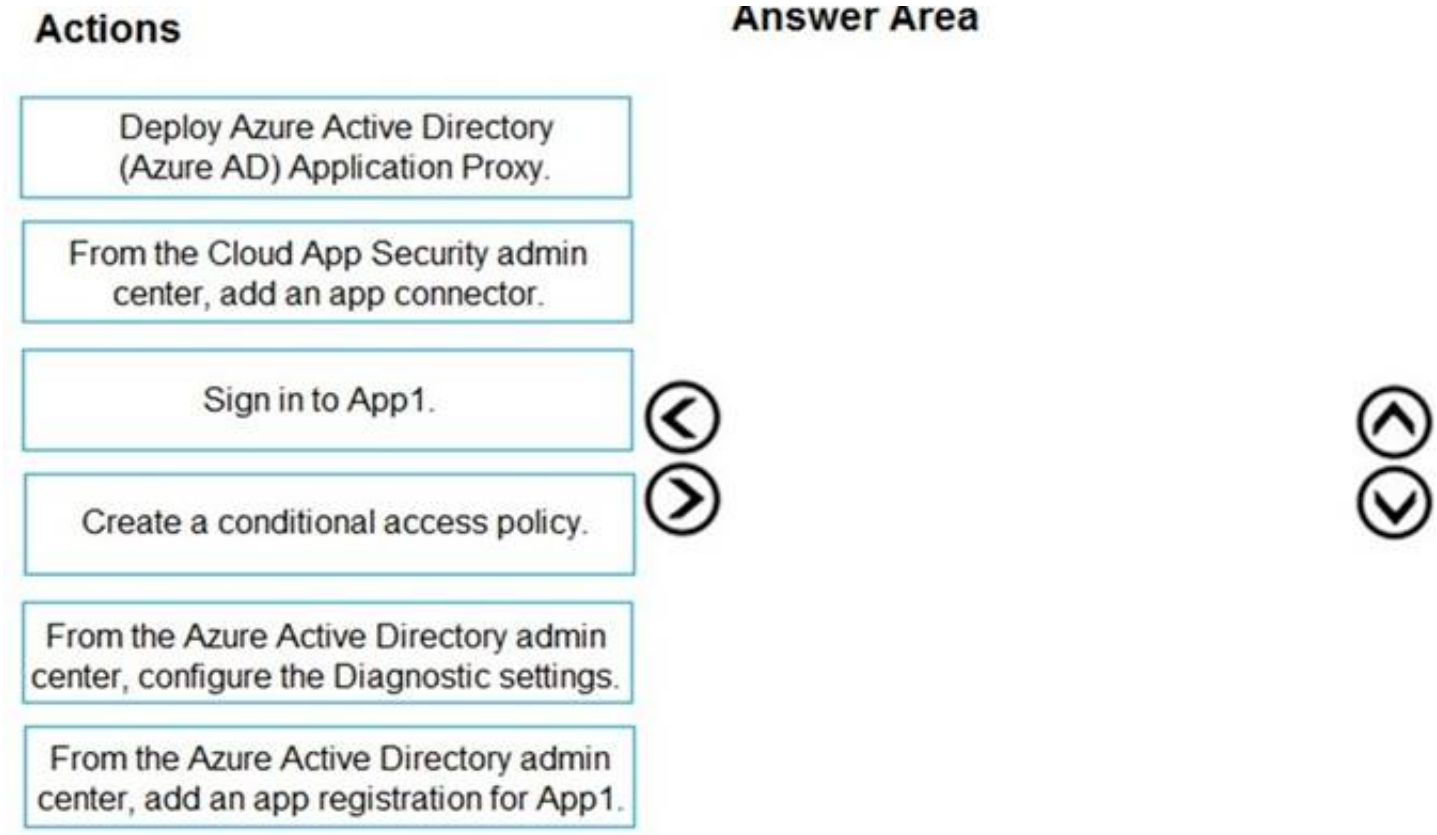
How many files will be visible to user1 and User2 after Policy' is applied to answer, selected select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

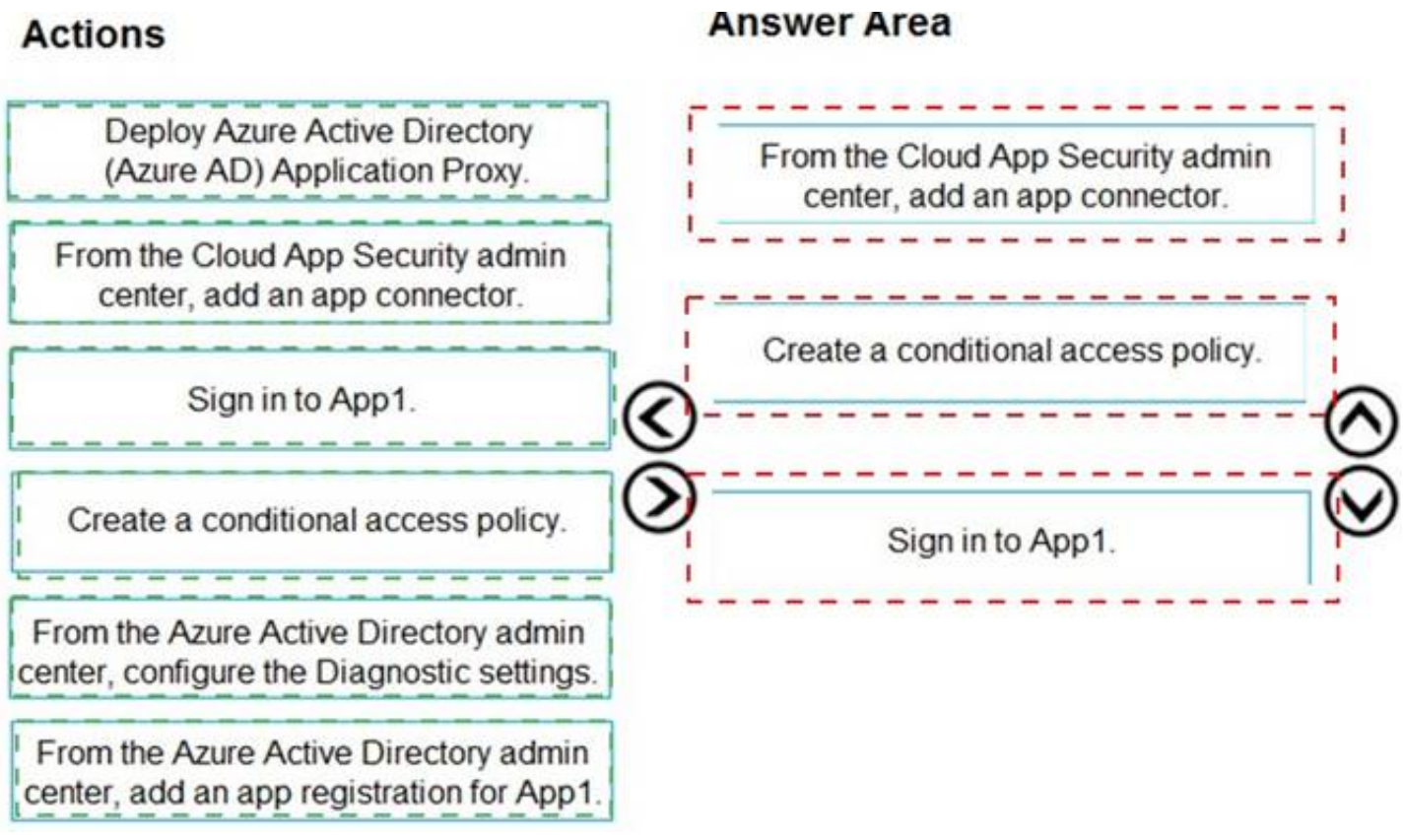
NEW QUESTION 191
DRAG DROP - (Topic 6)
Your company purchases a cloud app named App1.
You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls.
Which three actions should you perform in sequence? To answer, move the appropriate actions 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 192
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it as a result these questions will not appear in the review screen.
Your network contains an Active Directory forest. You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
• Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
• User passwords must be 10 characters or more.
Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 196
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.
You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory.
What should you configure in the profile?

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

Answer: A

NEW QUESTION 200
DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

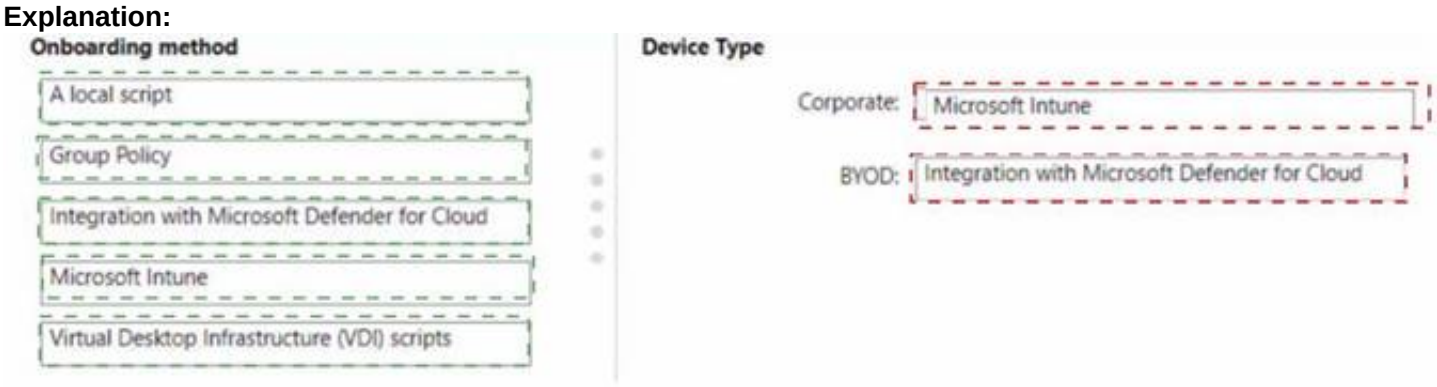
Type	Number of devices	Operating system	Enrollment status
Corporate	150	Windows 11	Azure AD-joined, Microsoft Intune-managed
Bring your own device (BYOD)	25	Windows 11	Unmanaged

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must minimize administrative effort.
What should you use to onboard each type of device? To answer, drag the appropriate onboarding methods to the correct device types. Each onboarding method 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 205
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

Site1 contains the files shown in the following table.

Name	Matched DLP rule
File1.docx	Rule1, Rule2, Rule3
File2.docx	Rule1, Rule3, Rule4

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

File1.docx:

- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Rule1 tip only
File1 matches Rule1, Rule2, and Rule3. Rule1 has the highest priority.
Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.
Box 2: Rule1 tip only
Note: User Override support
The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).
It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.
If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched.

NEW QUESTION 208
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: You run idfix.exe and export the 10 user accounts.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The question states that “all the user account synchronizations completed successfully”. If there were problems with the 10 accounts that needed fixing with idfix.exe, there would have been synchronization errors in Azure AD Connect Health.
It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync- configure-filtering

NEW QUESTION 209
- (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 210
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 213
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. You need to perform the following tasks:
• Create a sensitive info type named SIT1 based on a regular expression.
• Add a watermark to all new documents that are matched by SIT1.

Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 218
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.
From Azure AD Identity Protection, you enable a sign-in risk policy.
Users report that when they use the VDI solution, they are regularly blocked when they attempt to access Microsoft 365.
What should you configure?

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

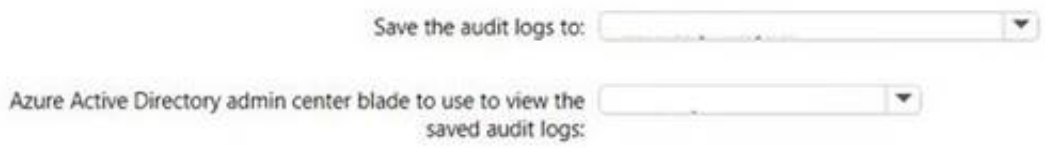
Answer: B

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

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

NEW QUESTION 221
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

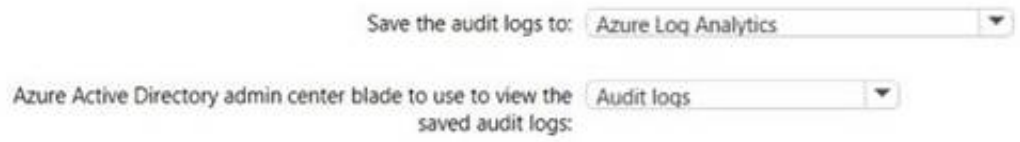


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 225
- (Topic 6)
Your company has a Microsoft E5 tenant.
The company must meet the requirements of the ISO/IEC 27001:2013 standard. You need to assess the company's current state of compliance.
What should you use?

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

Answer: C

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

NEW QUESTION 226
- (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 231
- (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

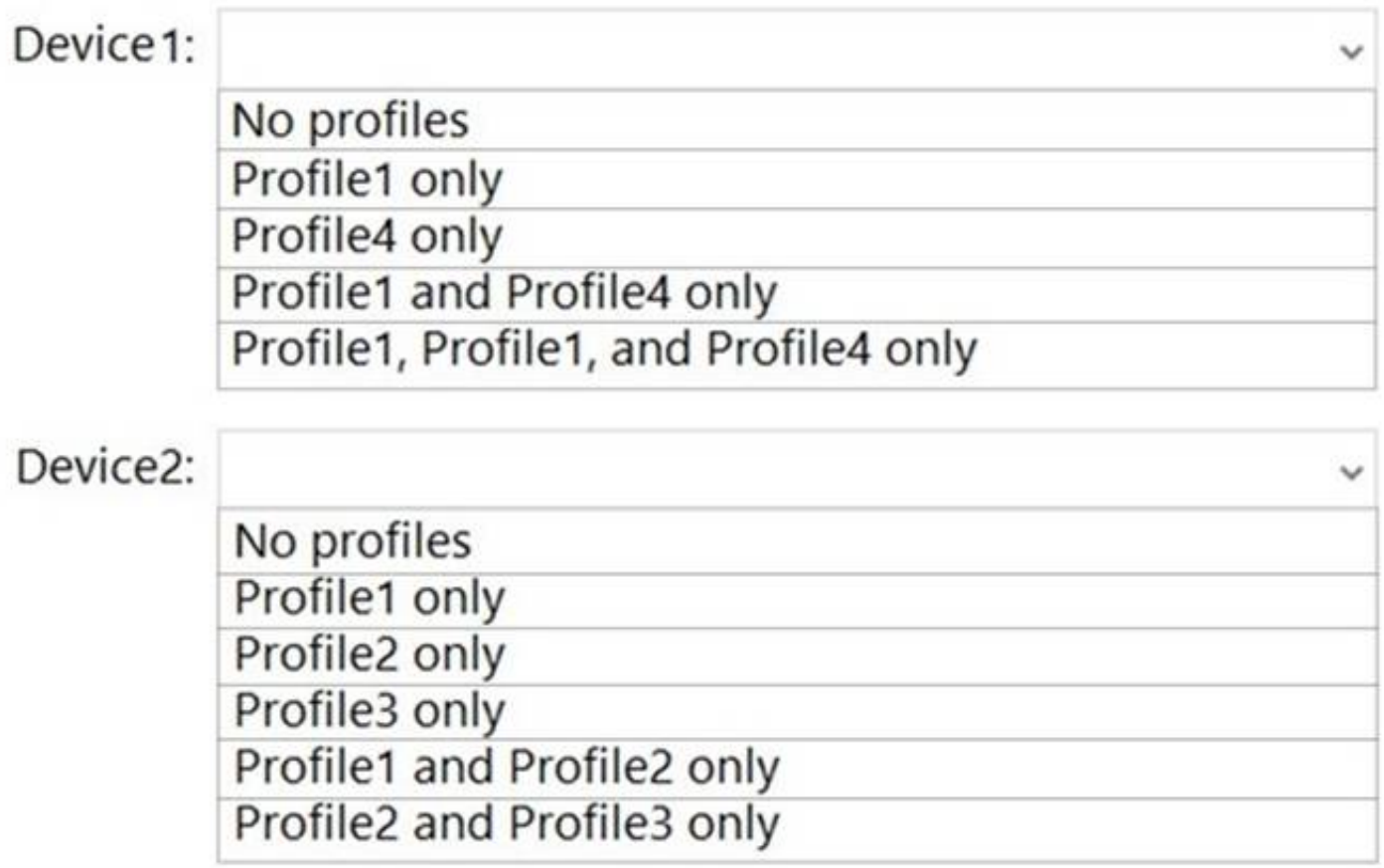
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide

NEW QUESTION 235
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

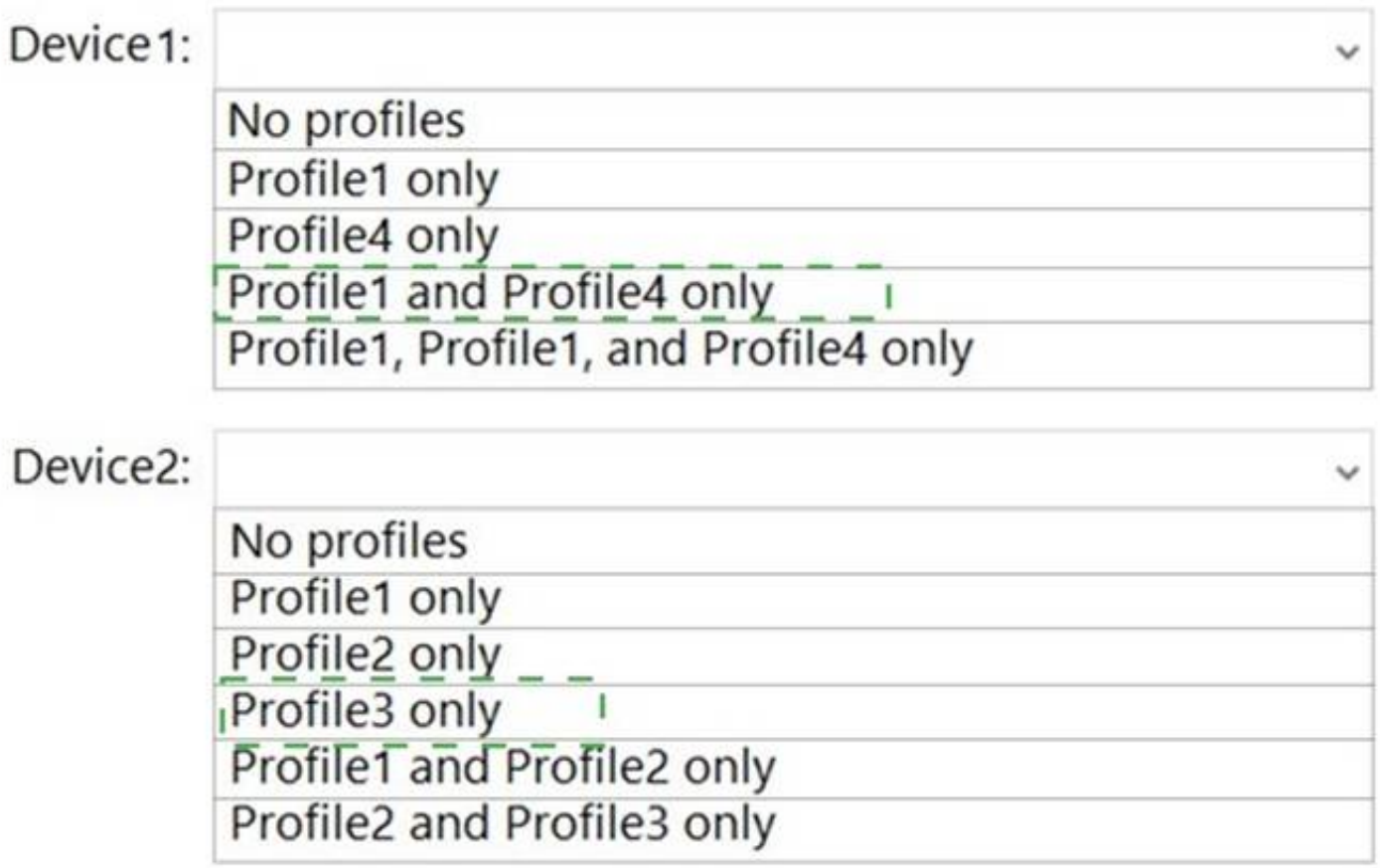
Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 240
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Al users have Mac computers. ATI the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender for Endpoint.
You need to configure Microsoft Defender for Endpoint on the computers. What should you create from the Endpoint Management admin center?

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

Answer: D

NEW QUESTION 244
- (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 248
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select Update & Security to view the update history. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 252
HOTSPOT - (Topic 6)
You have several devices enrolled in Microsoft Endpoint Manager.
You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

The device type restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	○
User2 can enroll Android devices in Endpoint Manager.	○	○
User3 can enroll iOS devices in Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

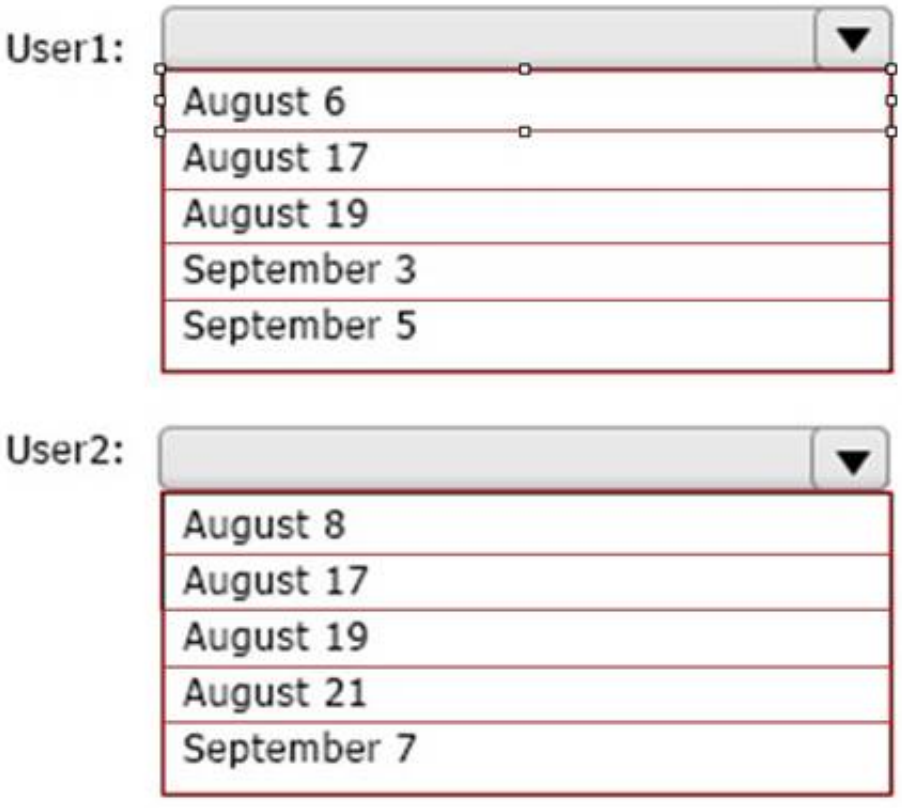
Explanation:
Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	○
User2 can enroll Android devices in Endpoint Manager.	○	○
User3 can enroll iOS devices in Endpoint Manager.	○	○

NEW QUESTION 256
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.



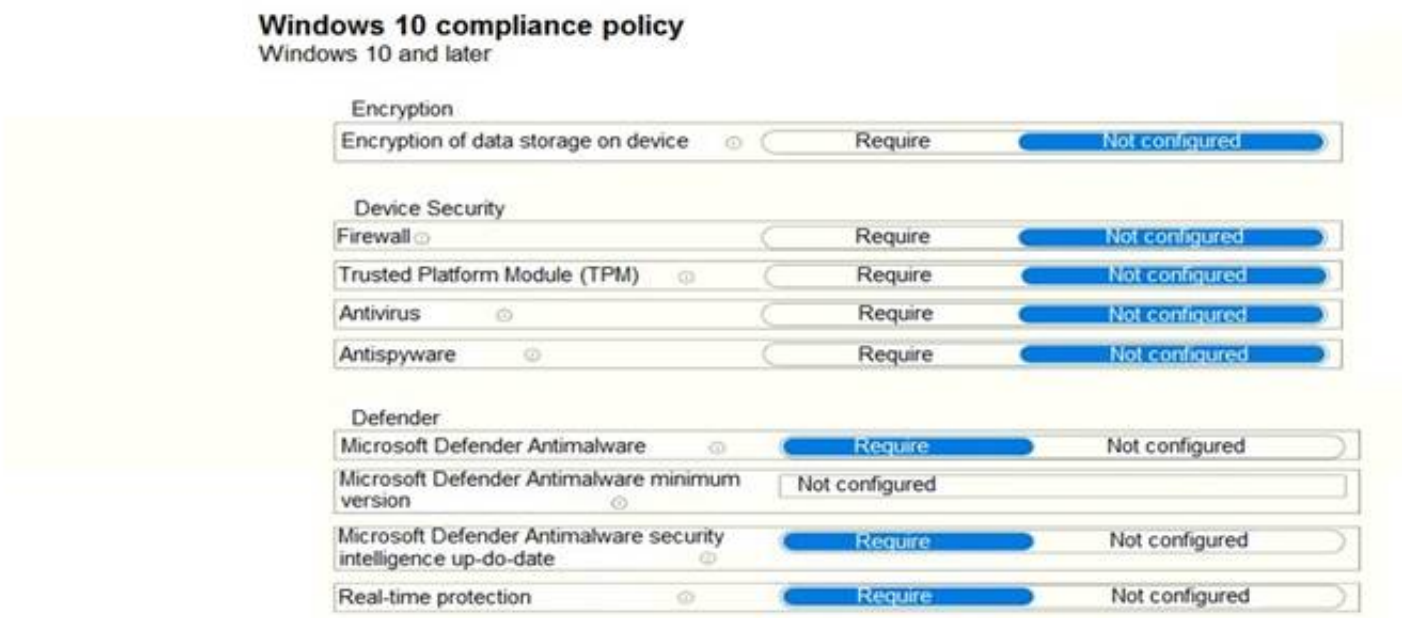
A. Mastered
B. Not Mastered

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 261
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.
You deploy a third-party antivirus solution to the devices.
You need to ensure that the devices are marked as compliant.
Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

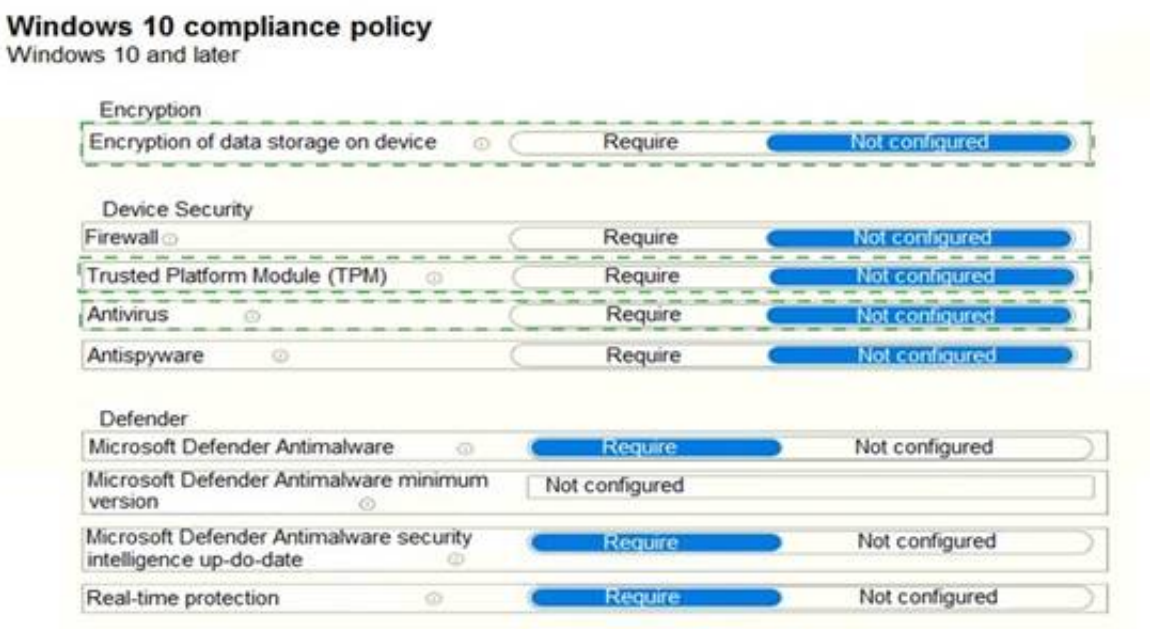


A. Mastered
B. Not Mastered

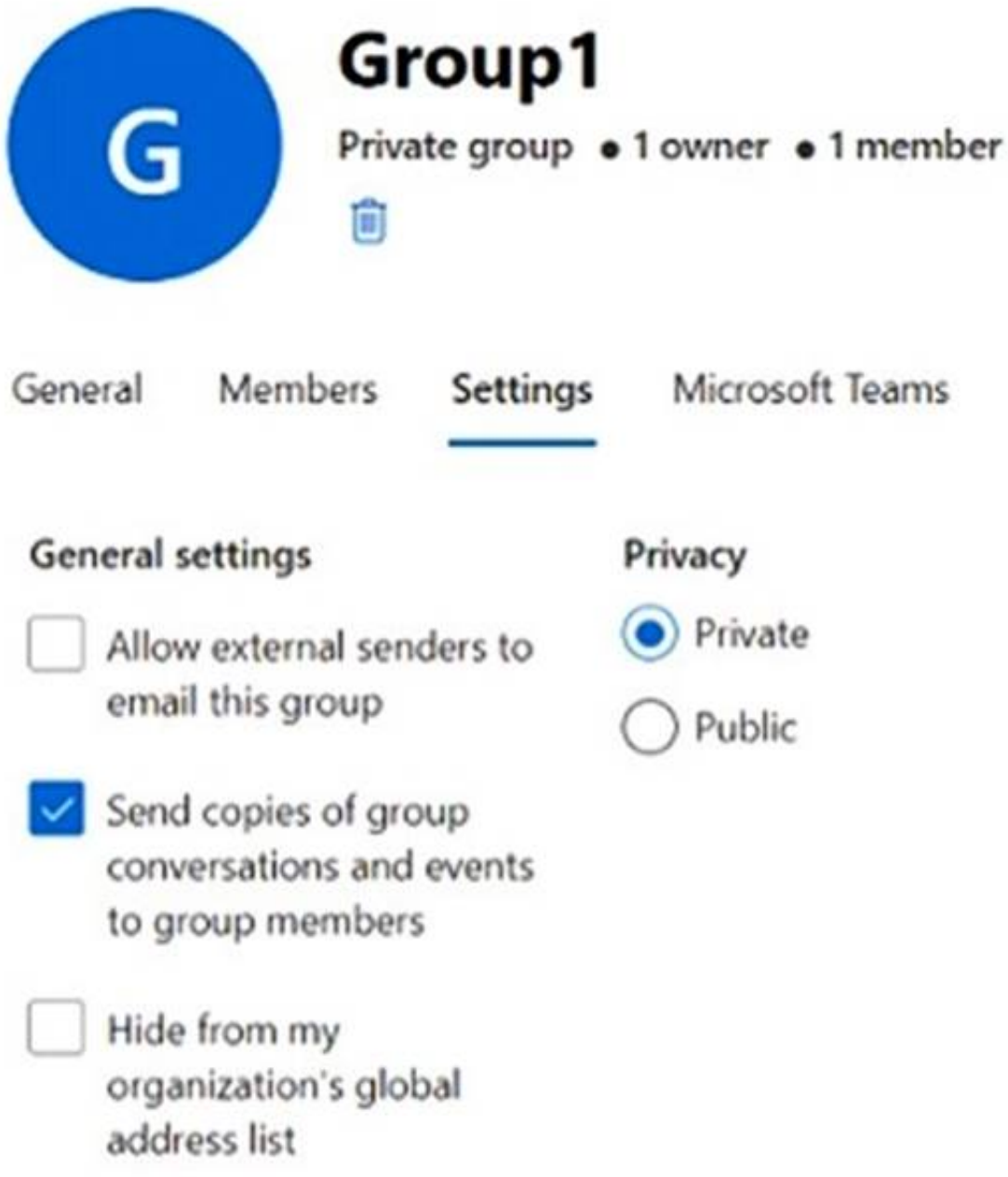
Answer: A

Explanation:

Answer Area

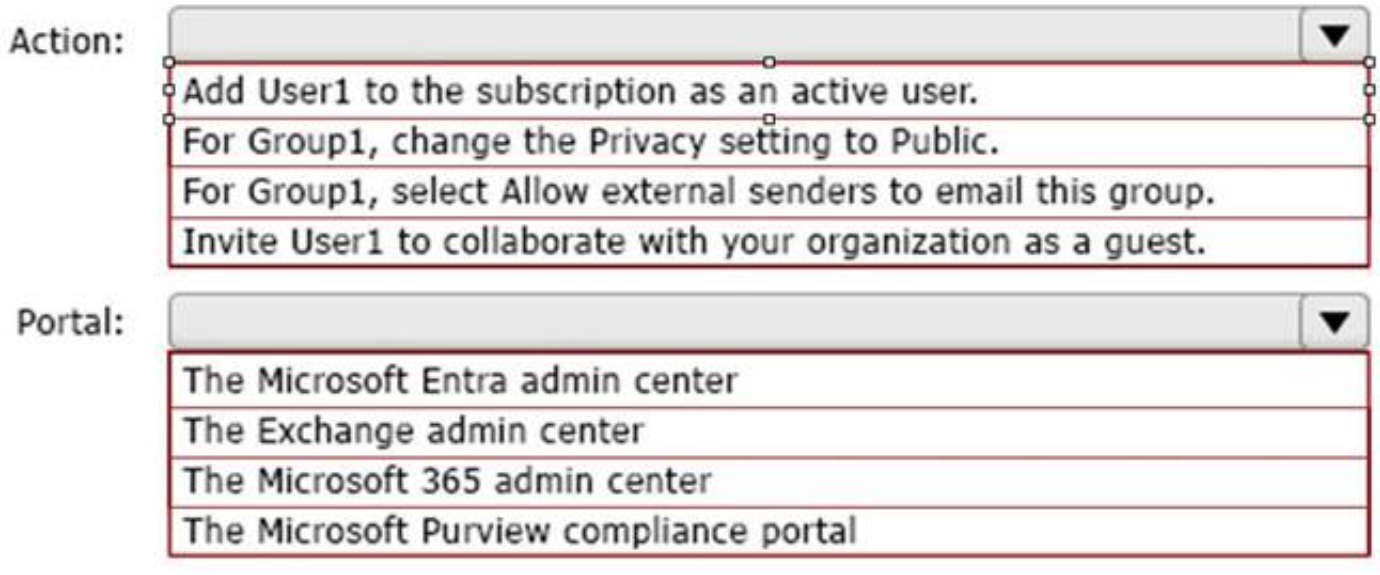


NEW QUESTION 262
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



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

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 264
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

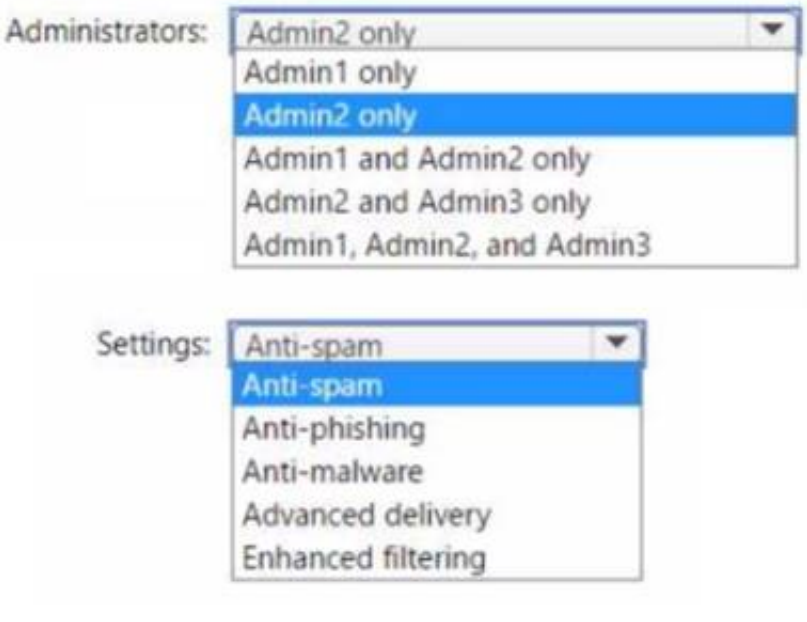
NEW QUESTION 266
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You need to access service health alerts from a mobile phone.
What should you use?

A. the Microsoft Authenticator app
B. the Microsoft 365 Admin mobile app
C. Intune Company Portal
D. the Intune app

Answer: B

NEW QUESTION 270
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.

Answer Area

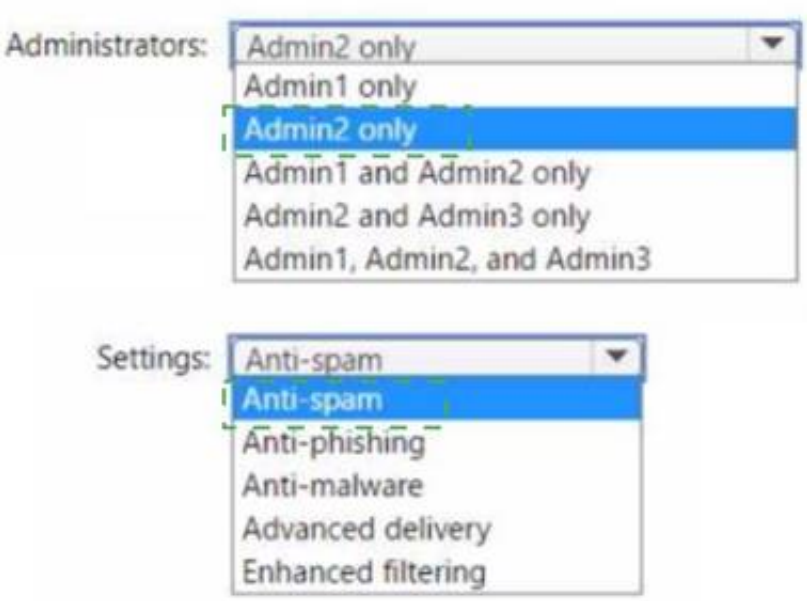


A. Mastered
B. Not Mastered

Answer: A

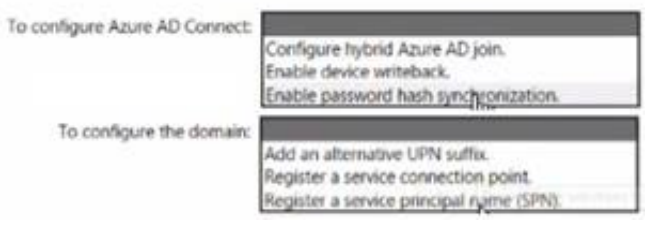
Explanation:

Answer Area



NEW QUESTION 273
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



A. Mastered
B. Not Mastered

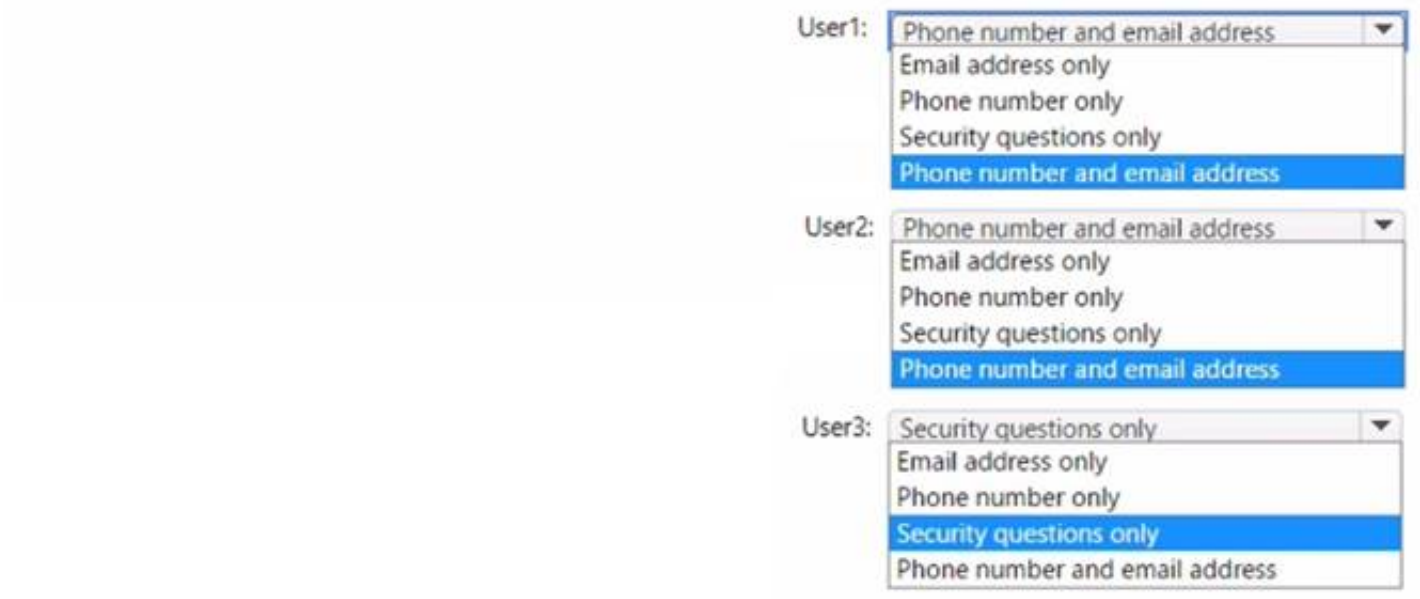
Answer: A

Explanation:

NEW QUESTION 277
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*

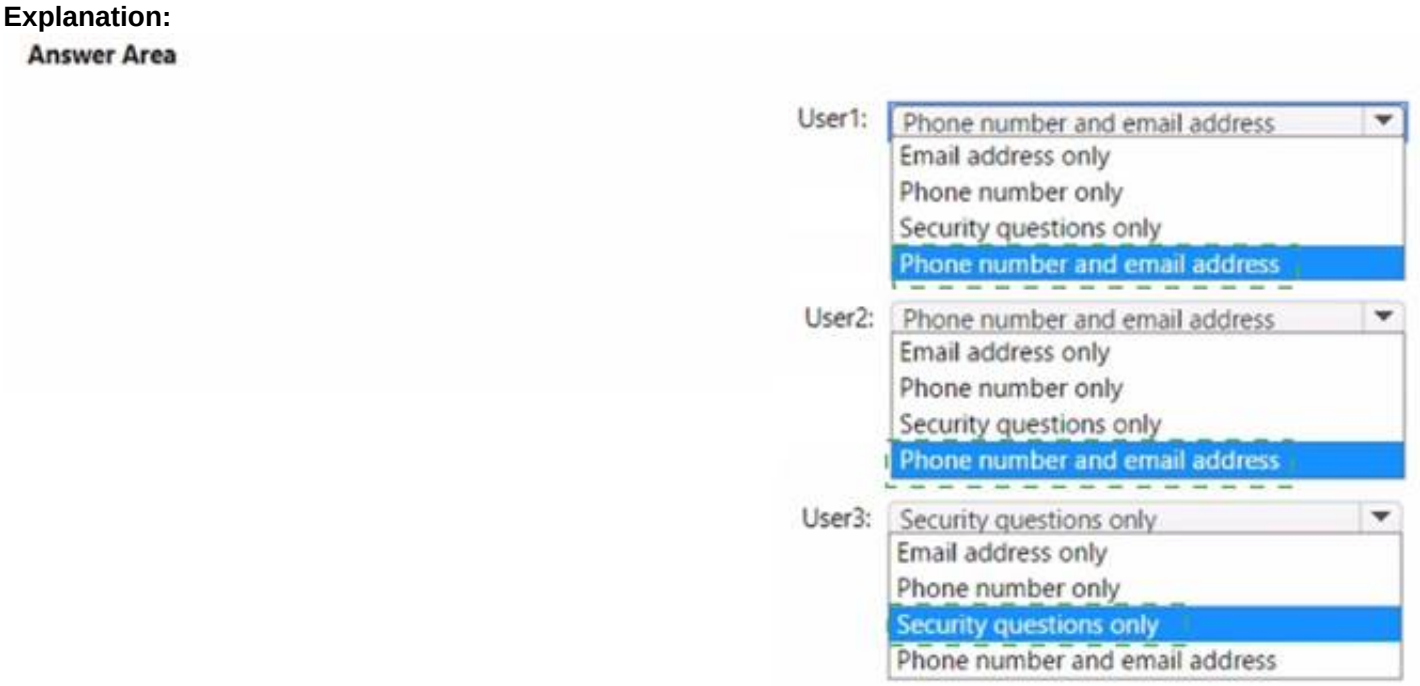
You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.
What information must be configured for each user before the user can perform a self- service password reset? To answer, select the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



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 280
HOTSPOT - (Topic 6)
You have device compliance policies shown in the following table.

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 282
- (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

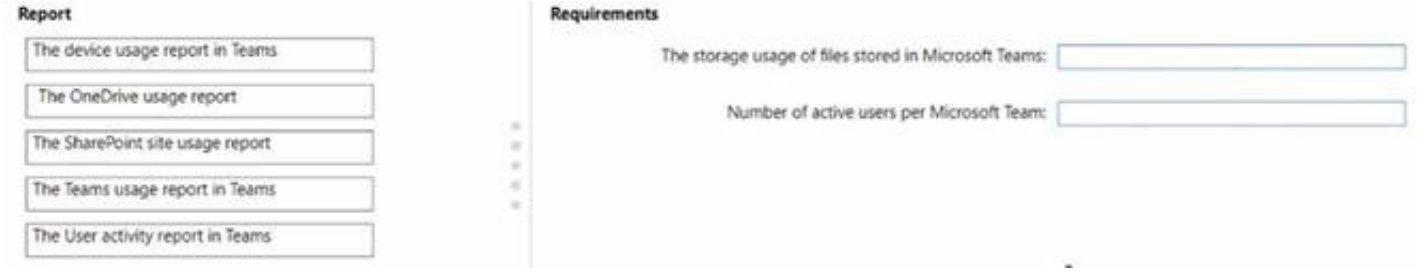
You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User3 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 287
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You need to review reports to identify the following:
• The storage usage of files stored in Microsoft Teams
• The number of active users per team
Which report should you review for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report may be used once, more

than once, or not at all. You may need to drag the split bar between panes or scroll to view content



A. Mastered
B. Not Mastered

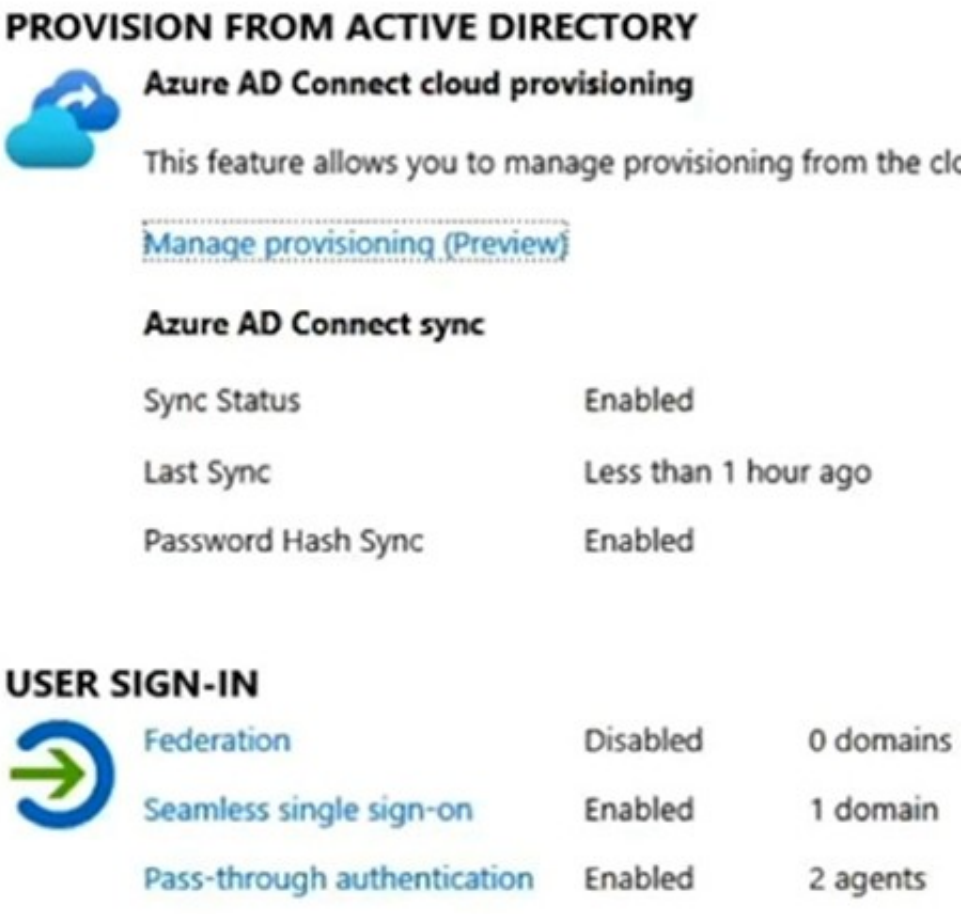
Answer: A

Explanation:

NEW QUESTION 291
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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



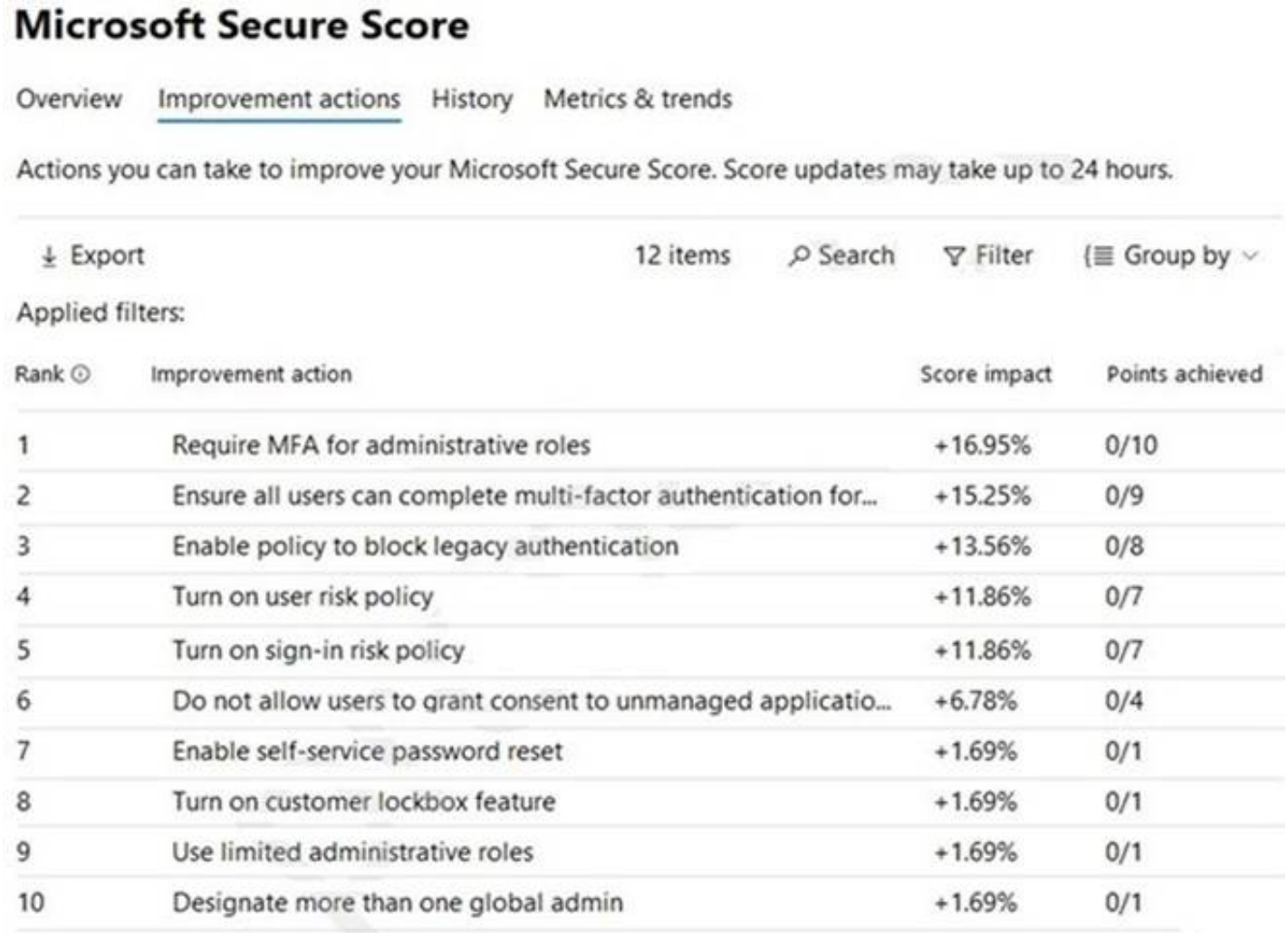
User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.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

A. Yes
B. No

Answer: B

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

NEW QUESTION 296
- (Topic 6)
You have a Microsoft 365 E5 tenant.
The Microsoft Secure Score for the tenant is shown in the following exhibit.



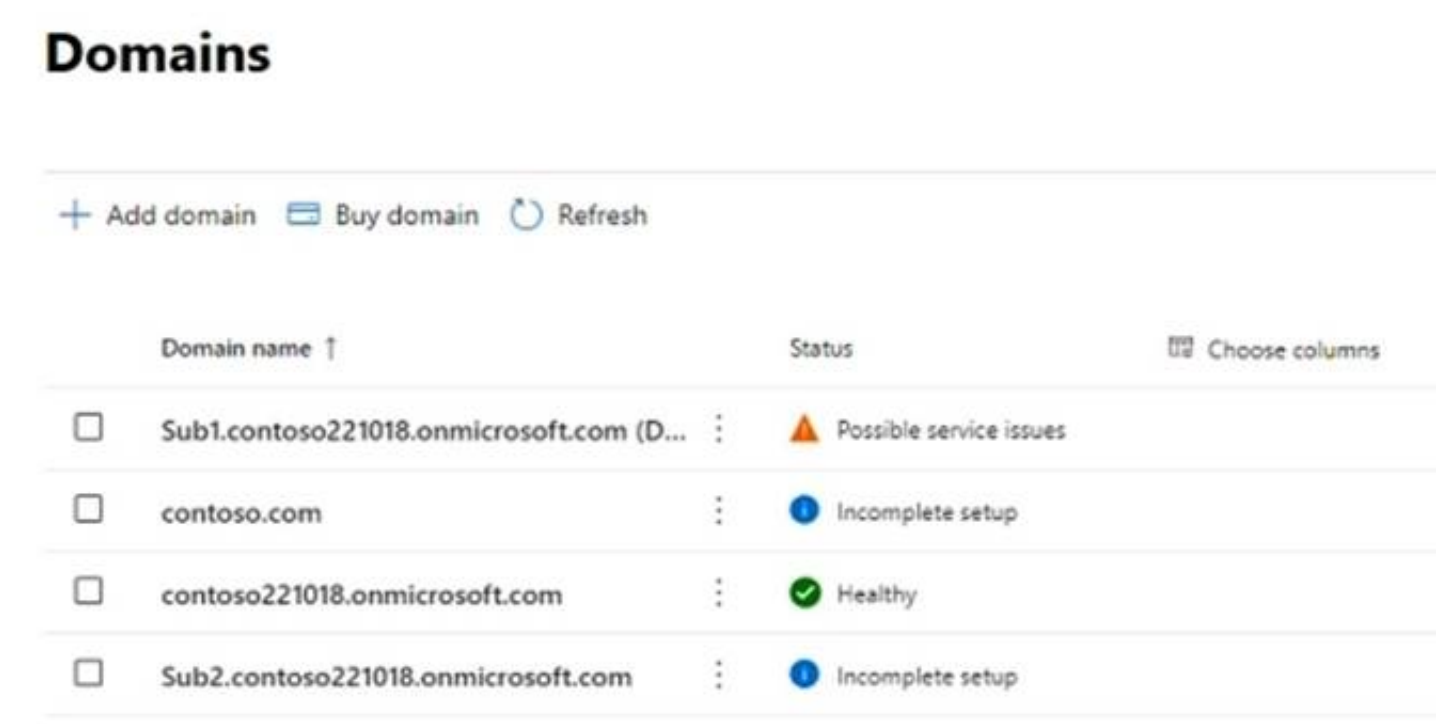
You plan to enable Security defaults for Azure Active Directory (Azure AD). Which three improvement actions will this affect?

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

Answer: ABC

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

NEW QUESTION 301
- (Topic 6)
You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.



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

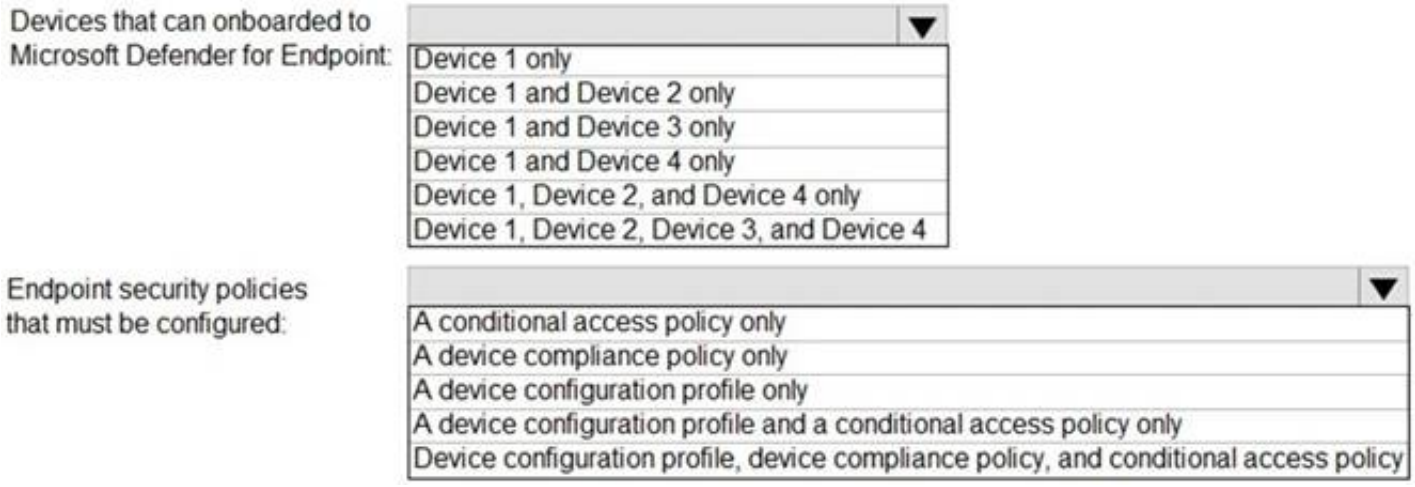
A. only Sub1.contoso221018.onmicrosoft.com
B. onlycontoso.com and Sub2.contoso221018.onmicrosoft.com
C. onlvcontoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com
D. all the domains in the subscription

Answer: B

NEW QUESTION 303
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint. You have devices enrolled in Microsoft Intune as shown in the following table.

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

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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, table Description automatically generated with medium confidence

NEW QUESTION 308
- (Topic 6)
Your on-premises network contains an Active Directory domain named Contoso.com and 500 devices that run either macOS, Windows 8.1. Windows 10, or Windows 11. All the devices are managed by using Microsoft Endpoint Configuration Manager. The domain syncs with Azure Active Directory (Azure AD).
You plan to implement a Microsoft 365 E5 subscription and enable co-management. Which devices can be co-managed after the implementation?

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

Answer: C

NEW QUESTION 312
- (Topic 6)
You have a Microsoft 365 subscription. You add a domain named contoso.com.
When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.com.
You need to change the email address used to verify the domain. What should you do?

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

Answer: C

NEW QUESTION 317
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

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

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

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

Answer: A

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

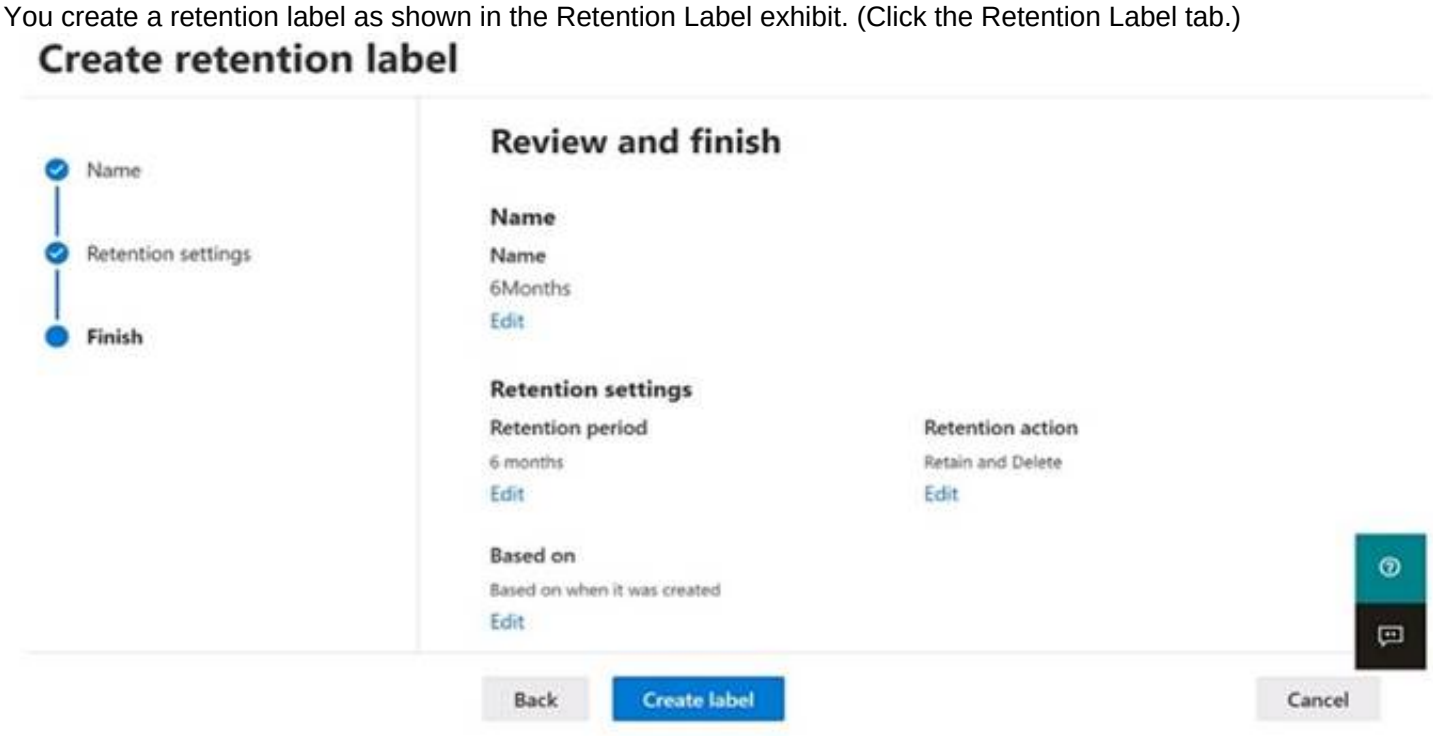
NEW QUESTION 321
- (Topic 6)
You have a Microsoft 365 subscription.
You suspect that several Microsoft Office 365 applications or services were recently updated.
You need to identify which applications or services were recently updated.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. From the Microsoft 365 admin center review the Service health blade
B. From the Microsoft 365 admin center, review the Message center blade.
C. From the Microsoft 365 admin center review the Products blade.
D. From the Microsoft 365 Admin mobile agg, review the messages.

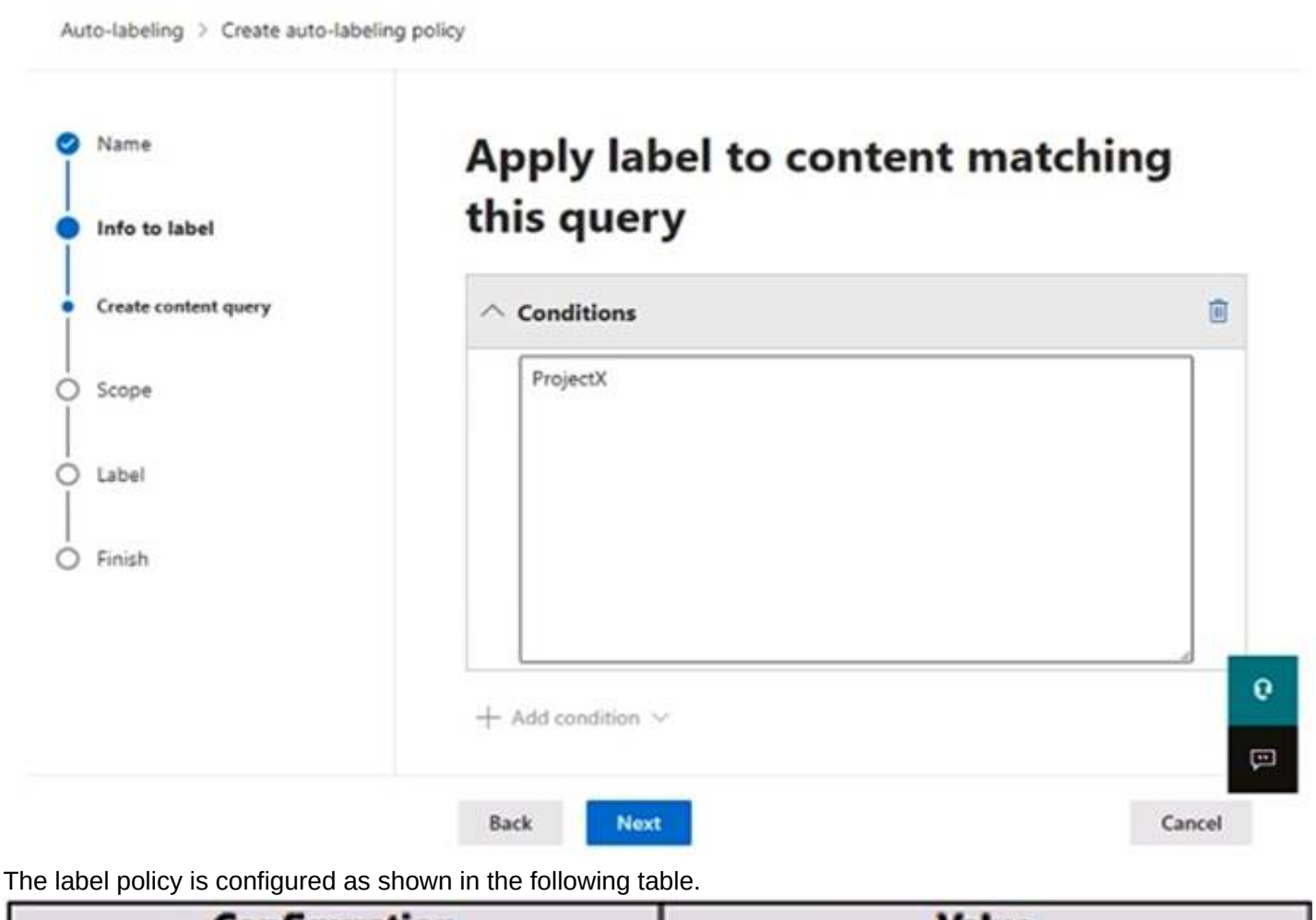
Answer: BD

Explanation:
The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where Microsoft posts official messages with information including new and changed features, planned maintenance, or other important announcements.
The messages displayed in the Message center can also be viewed by using the Office
365 Admin mobile app. Reference:
https://docs.microsoft.com/en-us/office365/admin/manage/message-center https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app

NEW QUESTION 322
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 tenant.
You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)



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



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

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 326
DRAG DROP - (Topic 6)
DRAG DROP
Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD). The domain contains the servers shown in the following table.

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

You use Azure Information Protection.
You need to ensure that you can apply Azure Information Protection labels to the file stores on Server1.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

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

A. Mastered
B. Not Mastered

Answer: A

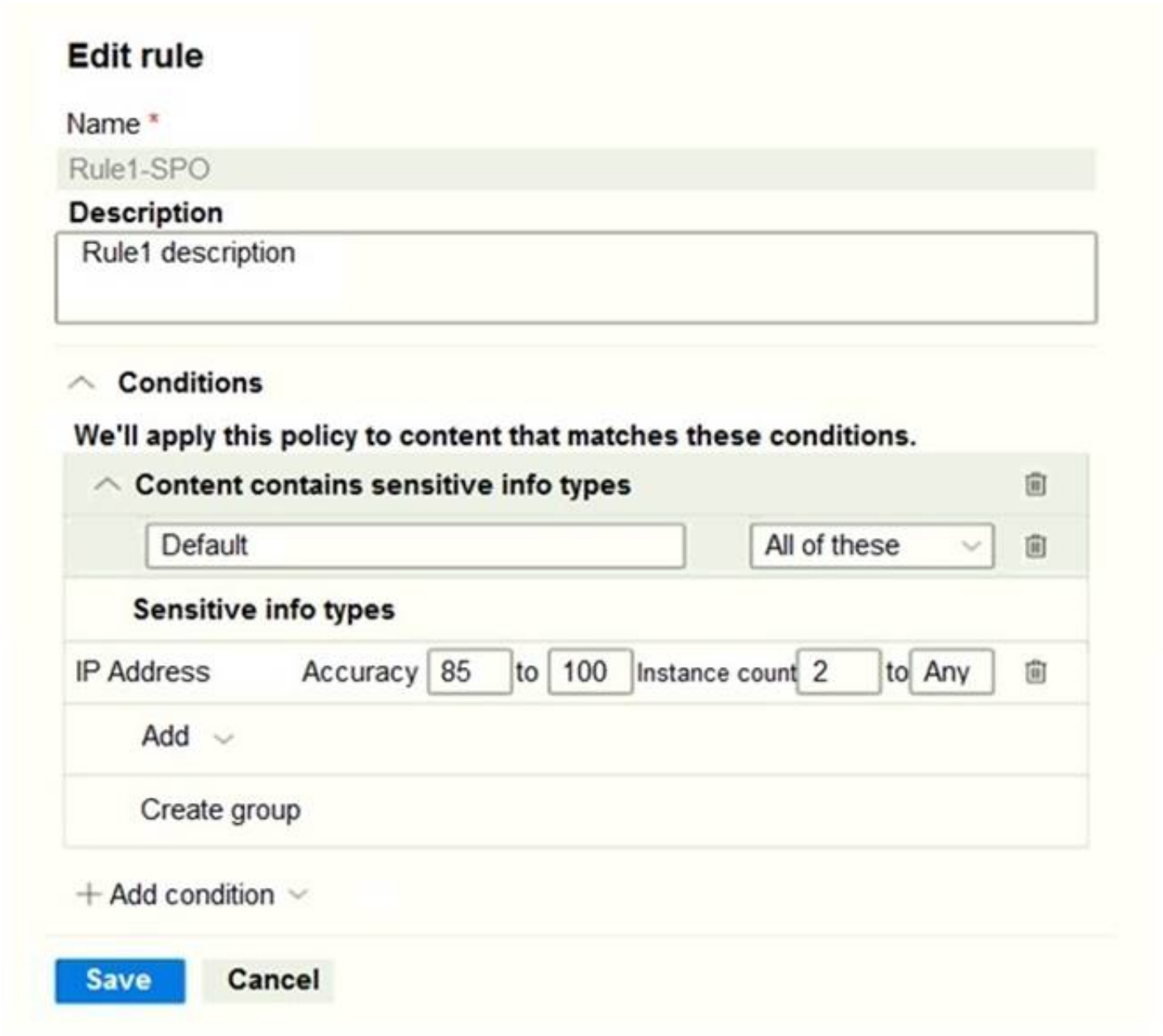
Explanation:

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

NEW QUESTION 327
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.

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

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



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

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

A. Mastered
B. Not Mastered

Answer: A

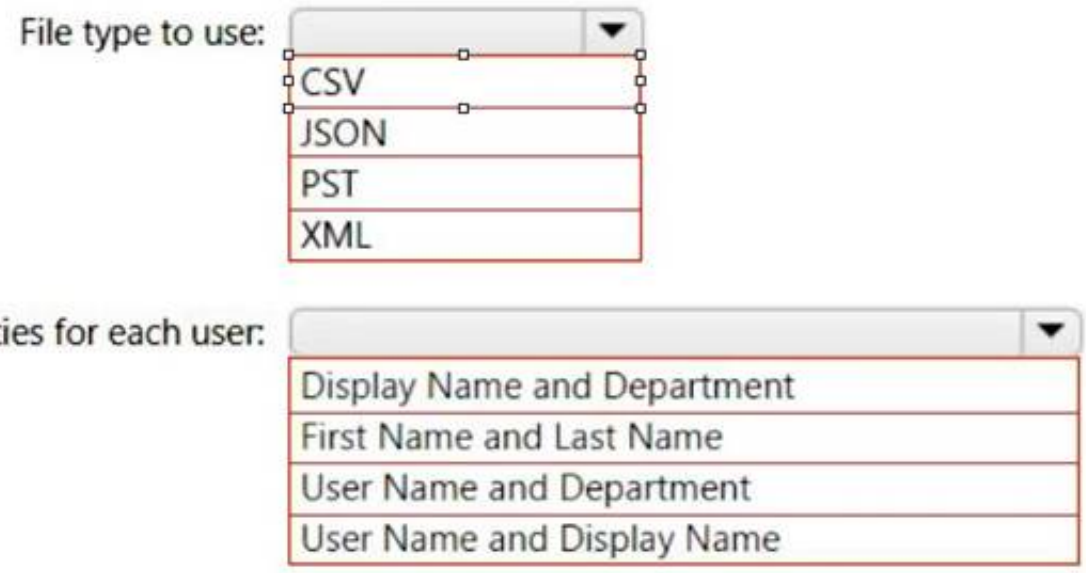
Explanation:

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

NEW QUESTION 330
HOTSPOT - (Topic 6)
HOTSPOT
Your company uses a legacy on-premises LDAP directory that contains 100 users. The company purchases a Microsoft 365 subscription.

You need to import the 100 users into Microsoft 365 by using the Microsoft 365 admin center.
Which type of file should you use and which properties are required? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: CSV
Add multiple users in the Microsoft 365 admin center
? Sign in to Microsoft 365 with your work or school account.
? In the admin center, choose Users > Active users.
? Select Add multiple users.
? On the Import multiple users panel, you can optionally download a sample CSV file with or without sample data filled in.
? Etc.
Note: More information about how to add users to Microsoft 365 Not sure what CSV format is?
A CSV file is a file with comma separated values. You can create or edit a file like this with any text editor or spreadsheet program, such as Excel.
Box 2: User Name and Display Name
What if I don't have all the information required for each user? The user name and display name are required, and you cannot add a new user without this information. If you don't have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.

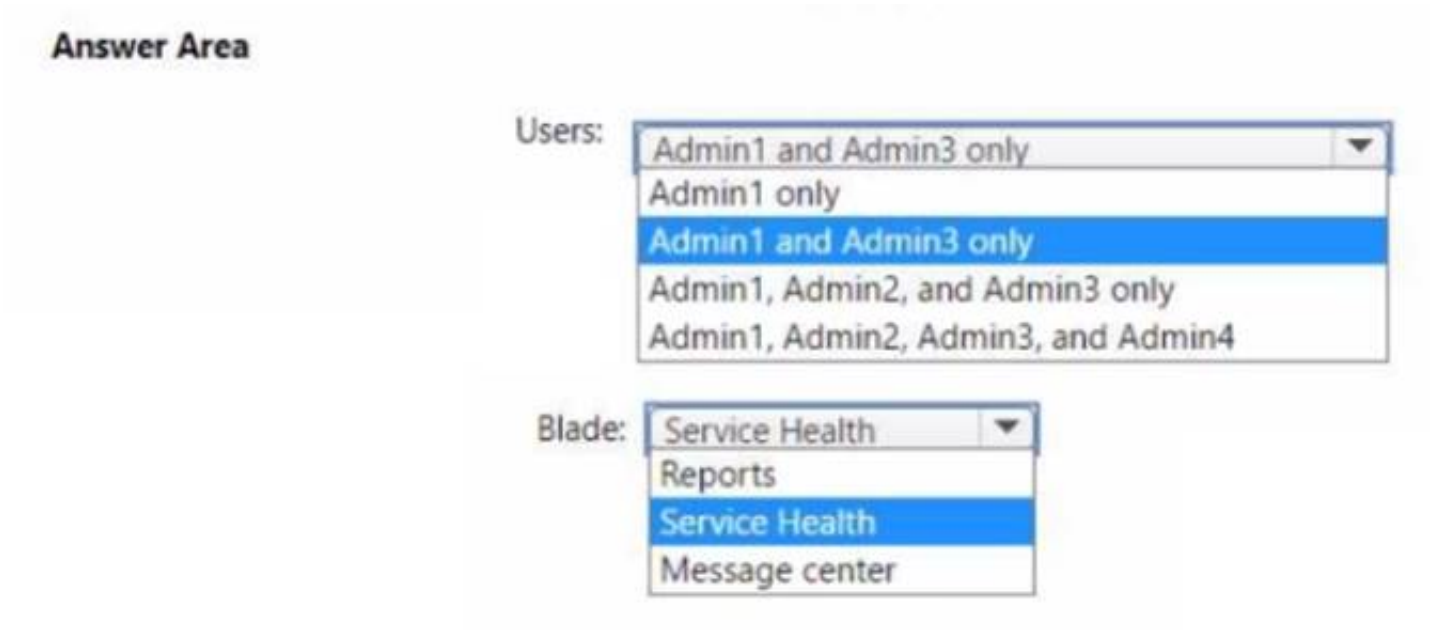
NEW QUESTION 334
HOTSPOT - (Topic 5)
You need to configure the Office 365 service status notifications and limit access to the service and feature updates. The solution must meet the technical requirements.
What should you configure in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

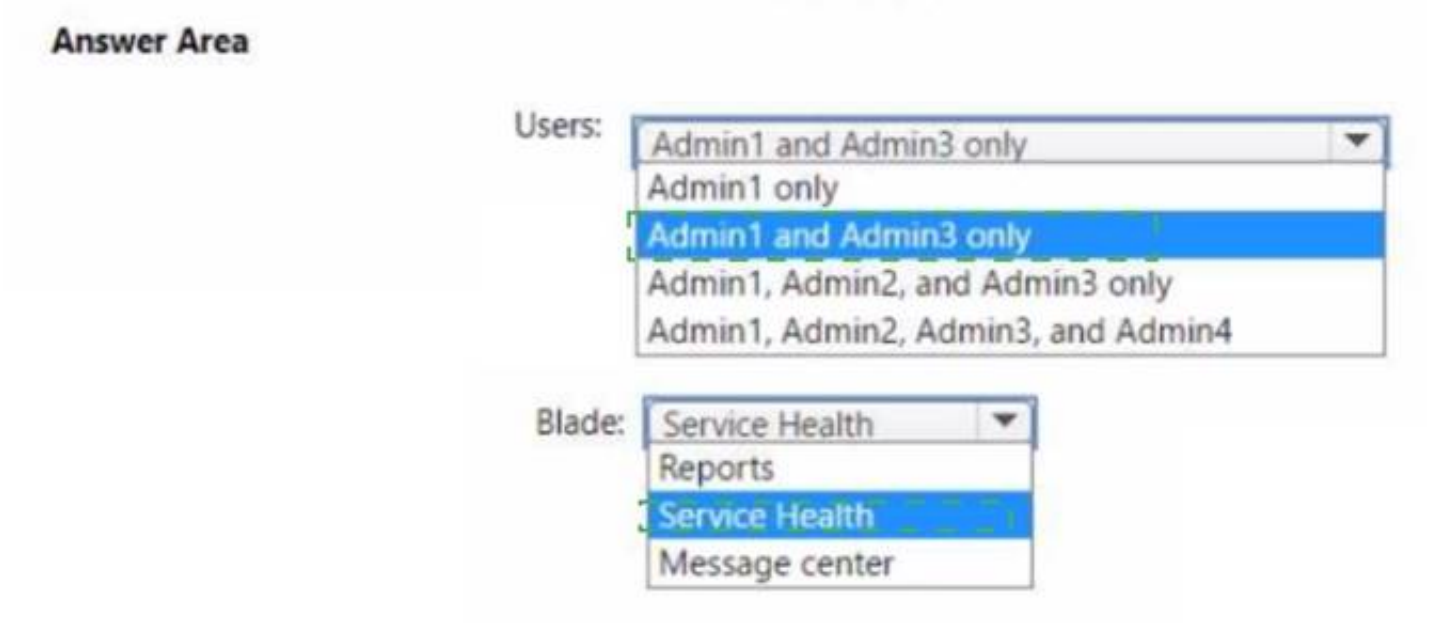
NEW QUESTION 335
HOTSPOT - (Topic 5)
You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.
Which users can review the incidents and advisories, and which blade should the users use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 337
- (Topic 5)
You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs.
What should you do?

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

Answer: A

NEW QUESTION 338
- (Topic 4)
You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.
Which authentication strategy should you implement for the pilot projects?

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

Answer: C

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

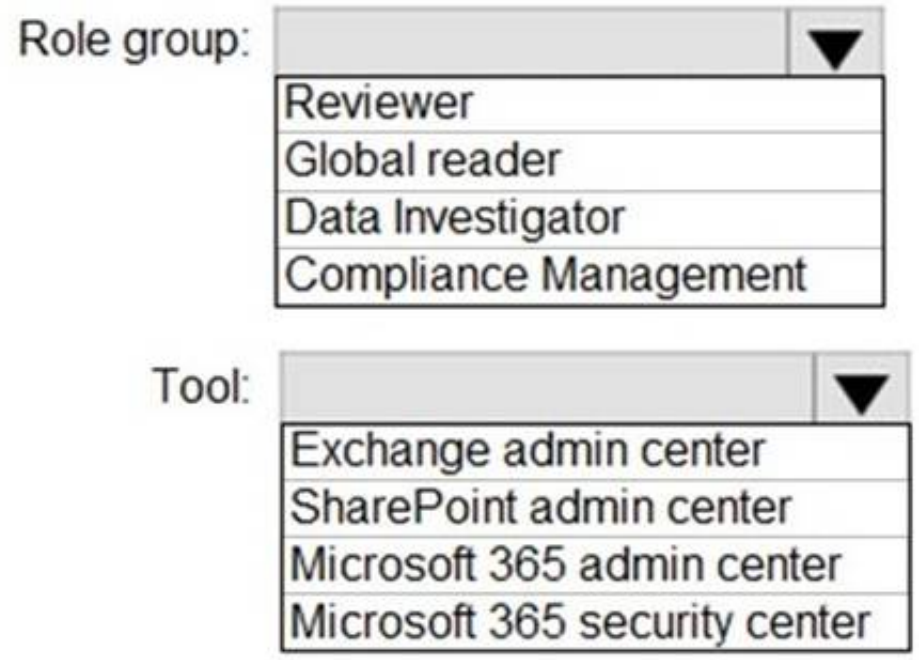
NEW QUESTION 343
- (Topic 3)
You create the planned DLP policies.
You need to configure notifications to meet the technical requirements. What should you do?

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

Answer: D

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

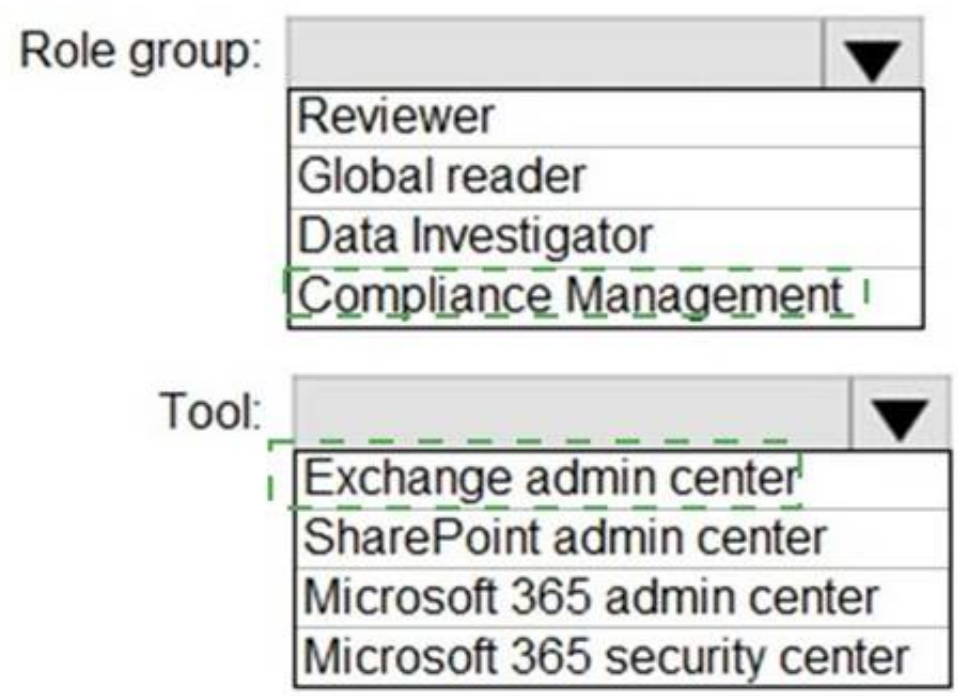
NEW QUESTION 346
HOTSPOT - (Topic 3)
You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements.
To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



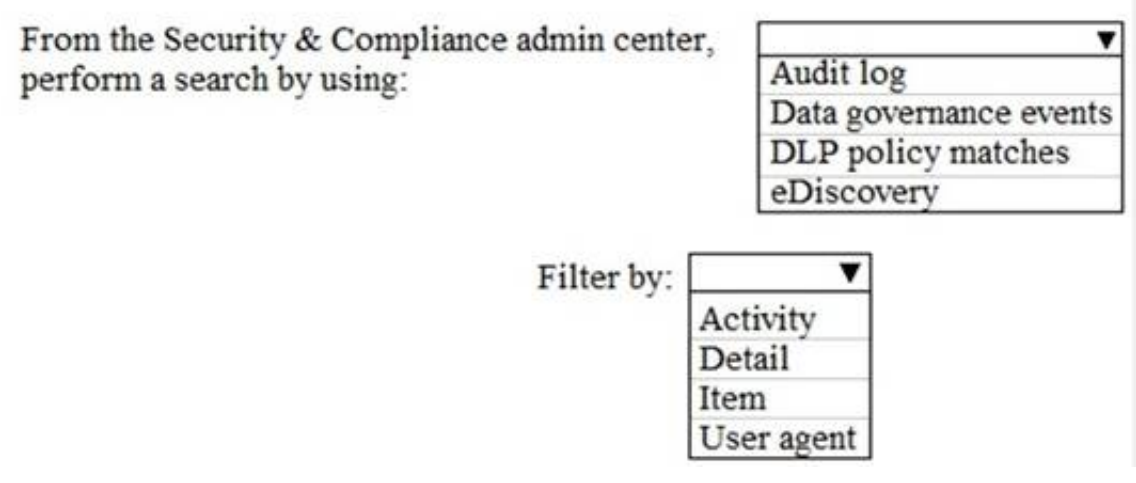
NEW QUESTION 351
- (Topic 3)
You need to configure the compliance settings to meet the technical requirements. What should you do in the Microsoft Endpoint Manager admin center?

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

Answer: D

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

NEW QUESTION 353
HOTSPOT - (Topic 2)
You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#step-3-filter-the-search-results

NEW QUESTION 354
- (Topic 1)
You need to create the Microsoft Store for Business. Which user can create the store?

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

Answer: C

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

NEW QUESTION 356
- (Topic 2)
You need to protect the U.S. PII data to meet the technical requirements. What should you create?

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

Answer: A

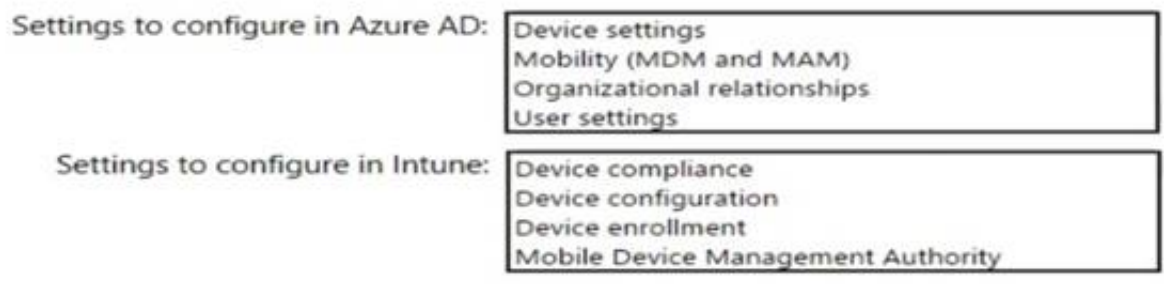
NEW QUESTION 358
HOTSPOT - (Topic 1)
As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

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

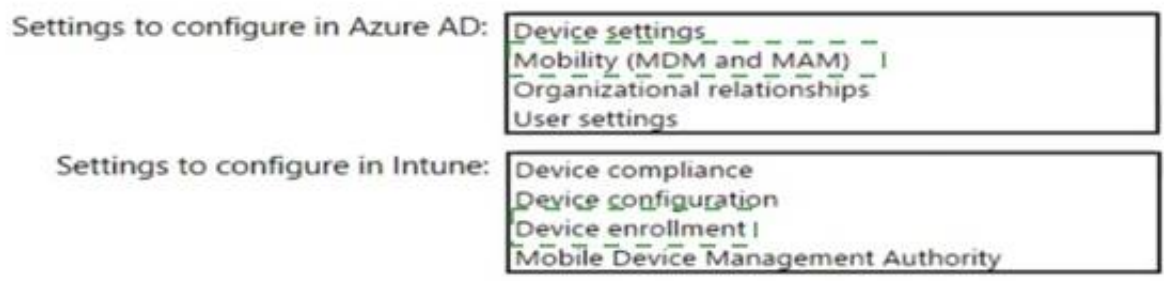
NEW QUESTION 361
HOTSPOT - (Topic 1)
You need to meet the technical requirements and planned changes for Intune. What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area



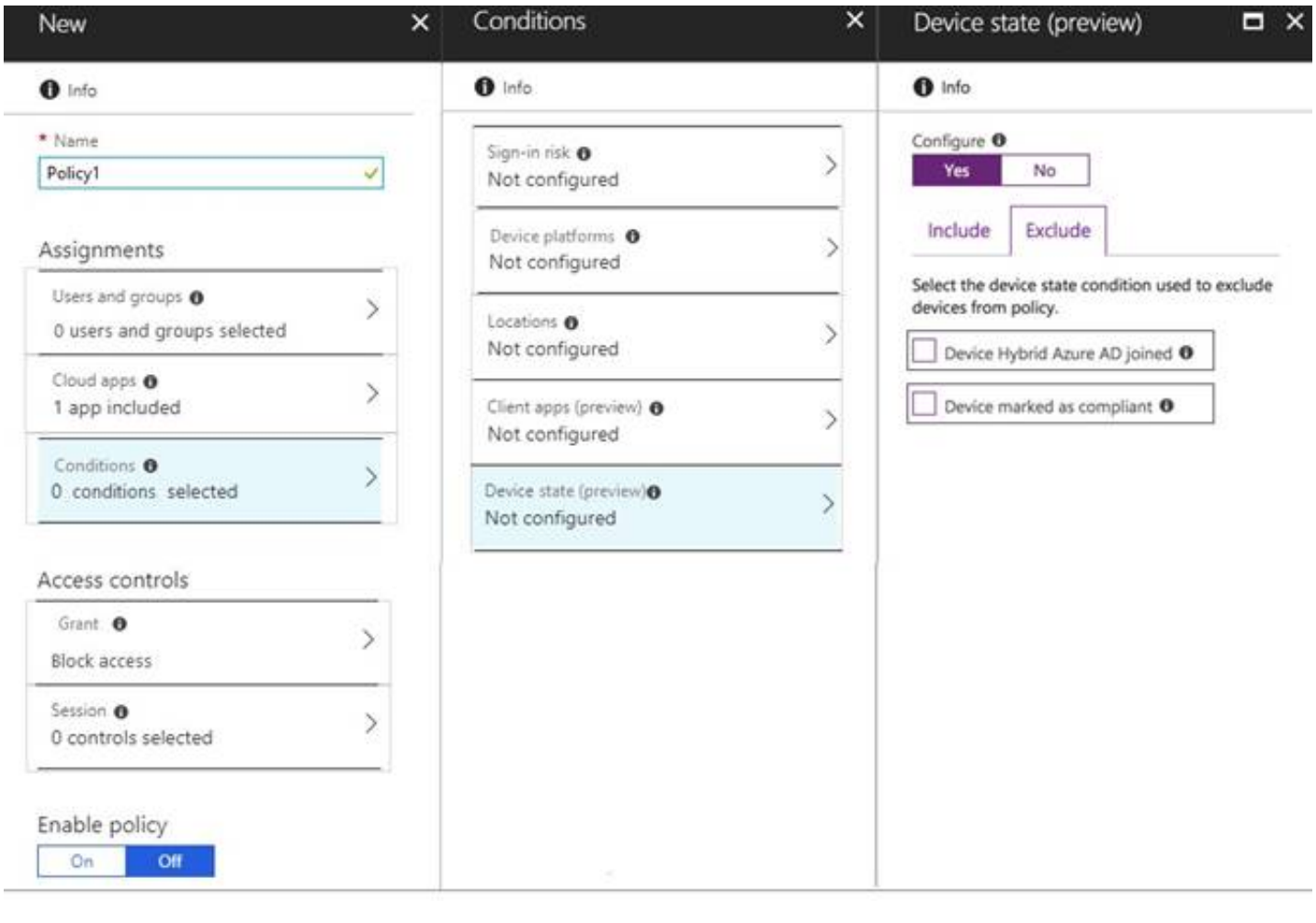
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 363
HOTSPOT - (Topic 1)
You need to configure a conditional access policy to meet the compliance requirements. You add Exchange Online as a cloud app.
Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 365
- (Topic 1)
You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?

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

Answer: C

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

NEW QUESTION 369
- (Topic 1)
You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.
What is the minimum of dedicated support technicians required?

A. 1
B. 4
C. 7
D. 31

Answer: B

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

NEW QUESTION 371
- (Topic 1)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.
Does this meet the goal?

A. Yes
B. NO

Answer: A

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

NEW QUESTION 372
- (Topic 6)
You have a Microsoft 365 subscription that contains the users shown in the following table.

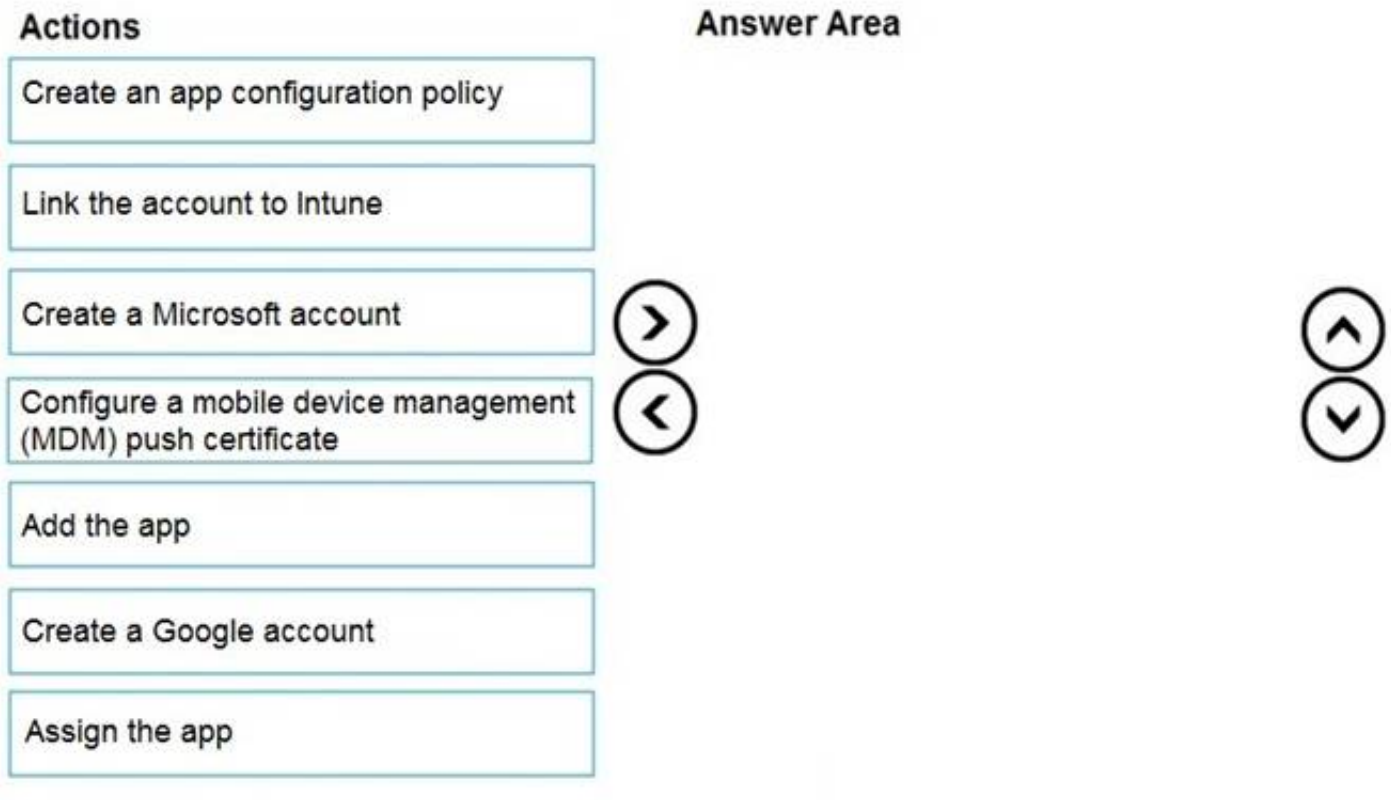
Name	Microsoft 365 admin role	Microsoft Exchange Online admin role
User1	Global Administrator	*None*
User2	Exchange Administrator	*None*
User3	Service Support Administrator	*None*
User4	*None*	Organization Management

You plan to use Exchange Online to manage email for a DNS domain. An administrator adds the DNS domain to the subscription.
The DNS domain has a status of Incomplete setup.
You need to identify which user can complete the setup of the DNS domain. The solution must use the principle of least privilege.
Which user should you identify?

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

Answer: A

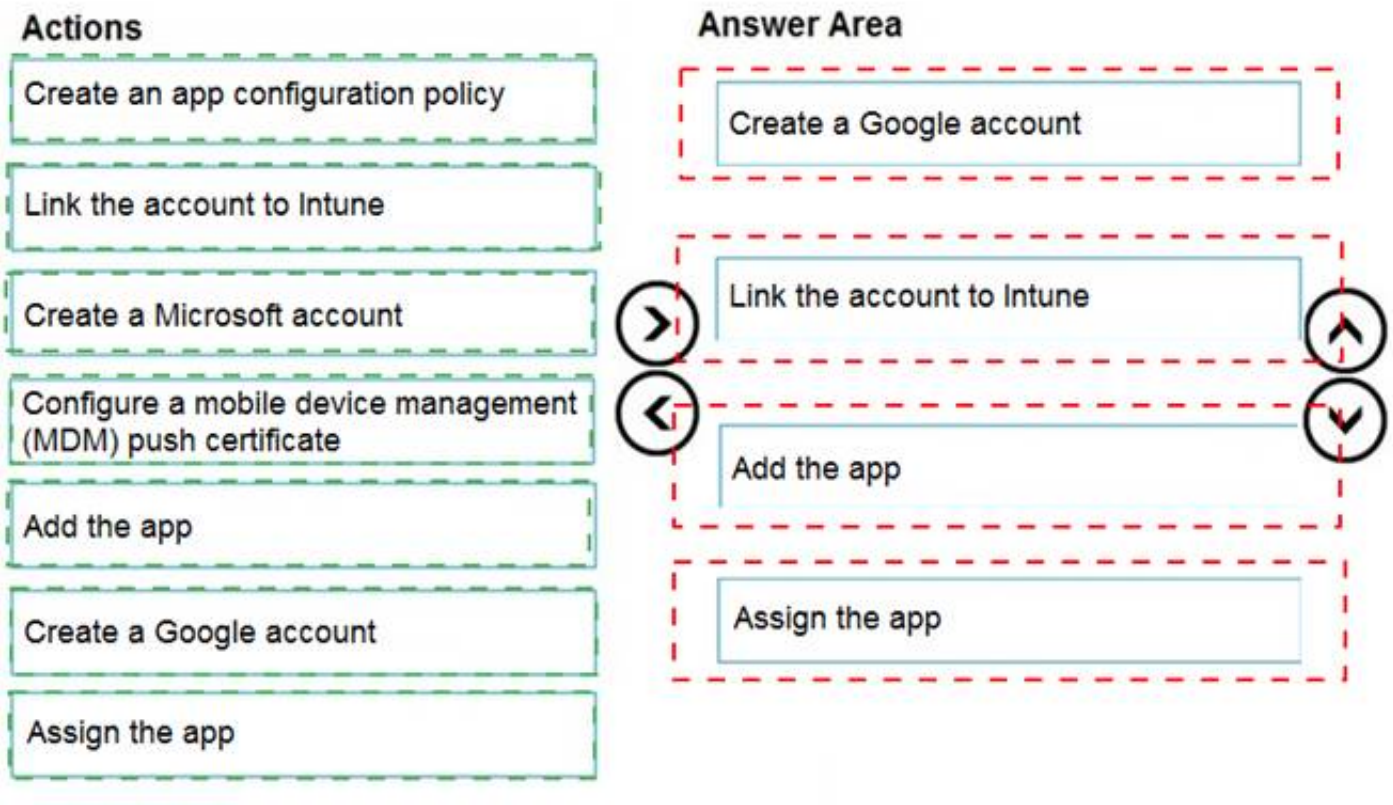
NEW QUESTION 374
DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune.
You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 376
- (Topic 6)
You have a Microsoft 365 subscription that contains a user named User1. User1 requires admin access to perform the following tasks:
Manage Microsoft Exchange Online settings. Create Microsoft 365 groups.
You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.
What should you use?

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

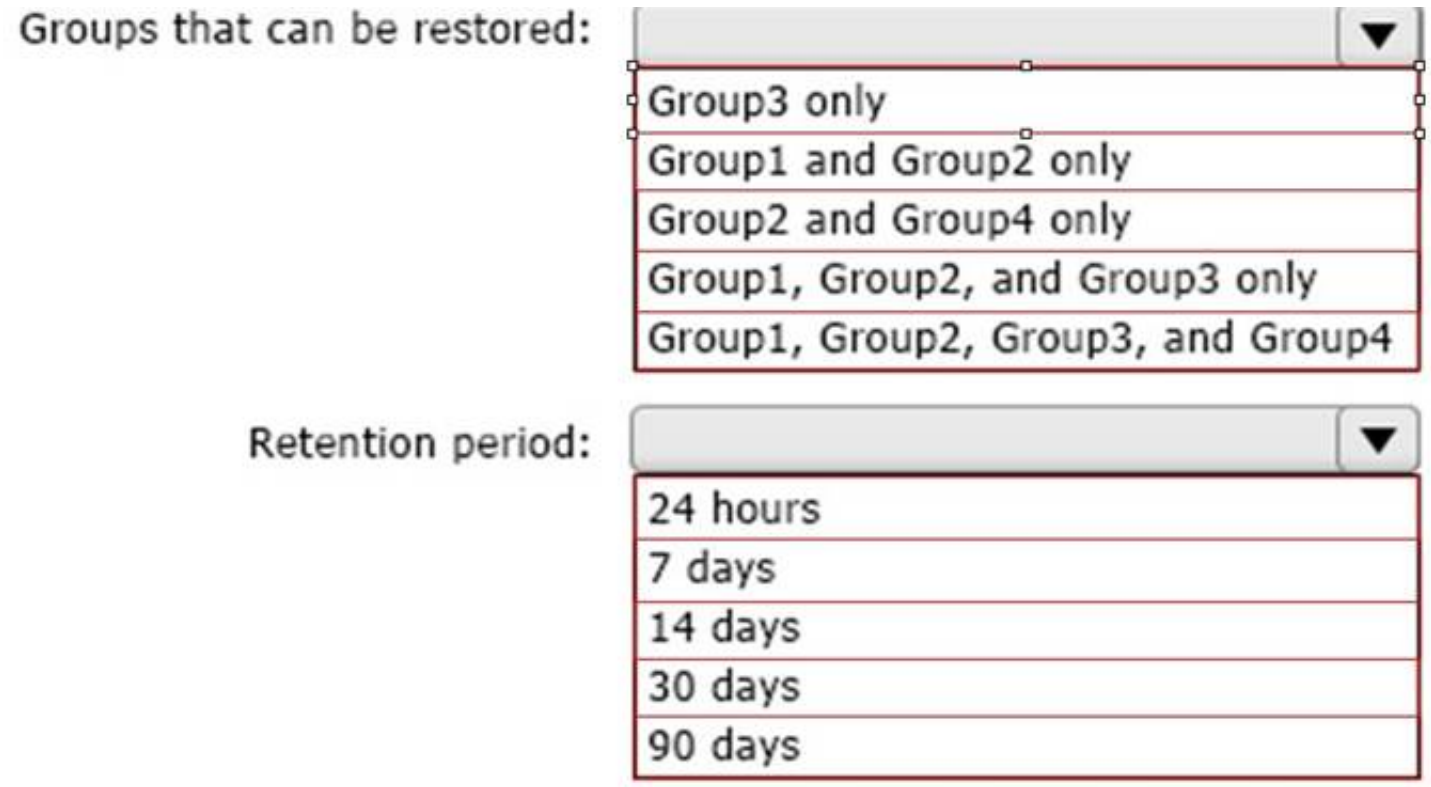
Answer: D

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

NEW QUESTION 379
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

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

All the groups are deleted.
Which groups can be restored, and what is the retention period? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Group3 only
Box 2: 30 days
If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a "soft-delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

NEW QUESTION 383
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365 and contains a user named User1.
User1 emails a product catalog in the PDF format to 300 vendors. Only 200 vendors receive the email message, and User1 is blocked from sending email until the next day.
You need to prevent this issue from reoccurring. What should you configure?

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

Answer: A

NEW QUESTION 386
- (Topic 6)
You have an Azure AD tenant that contains the users shown in the following table

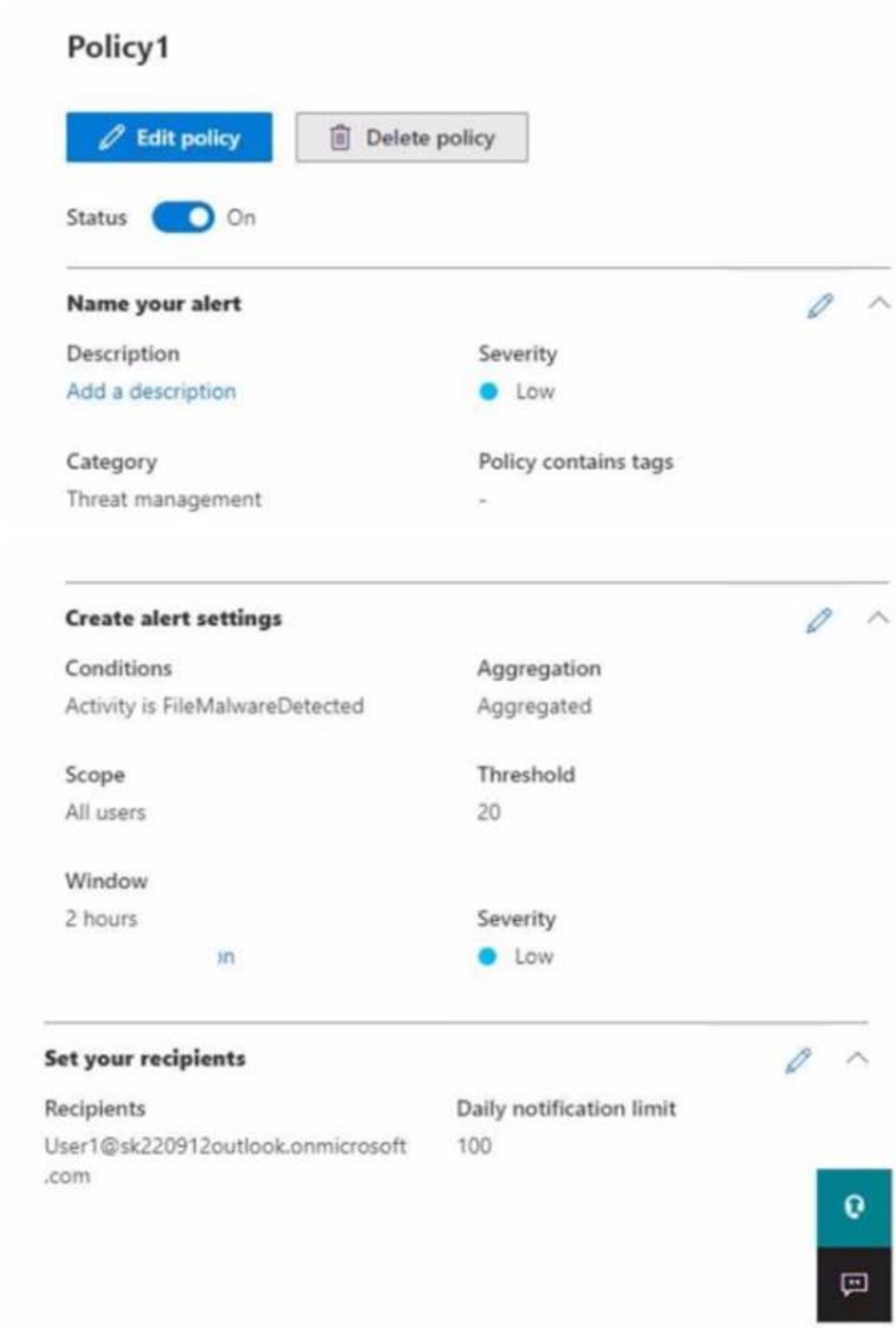
Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Exchange Administrator

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

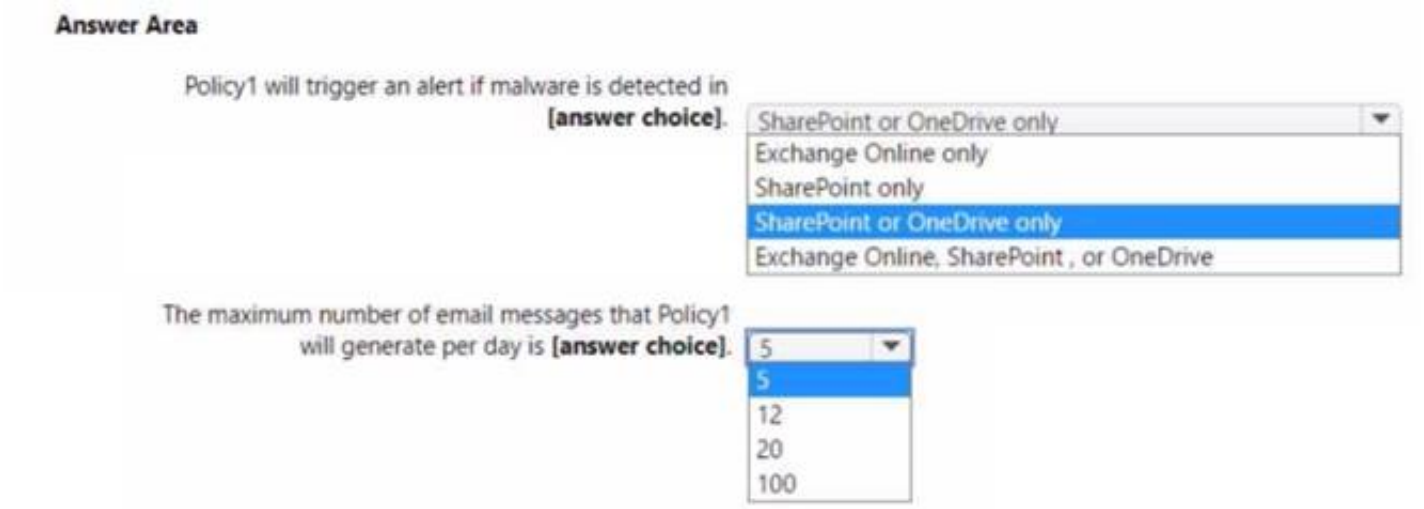
A. the Microsoft Purview compliance portal
B. the Microsoft 365 admin center
C. the Microsoft 365 Defender portt1
D. the Microsoft Entra admin center

Answer: A

NEW QUESTION 389
HOTSPOT - (Topic 6)
You have Microsoft 365 subscription.
You create an alert policy as shown in the following exhibit.



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



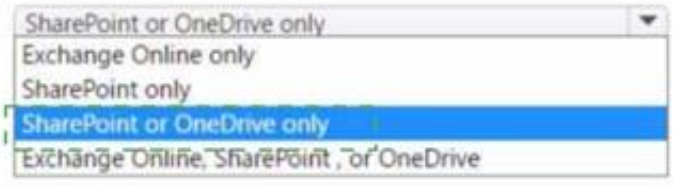
A. Mastered
B. Not Mastered

Answer: A

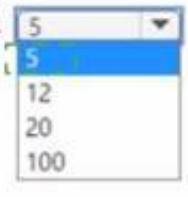
Explanation:

Answer Area

Policy1 will trigger an alert if malware is detected in **[answer choice]**.



The maximum number of email messages that Policy1 will generate per day is **[answer choice]**.



NEW QUESTION 391

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

MS-102 Practice Exam Features:

* MS-102 Questions and Answers Updated Frequently

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

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

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