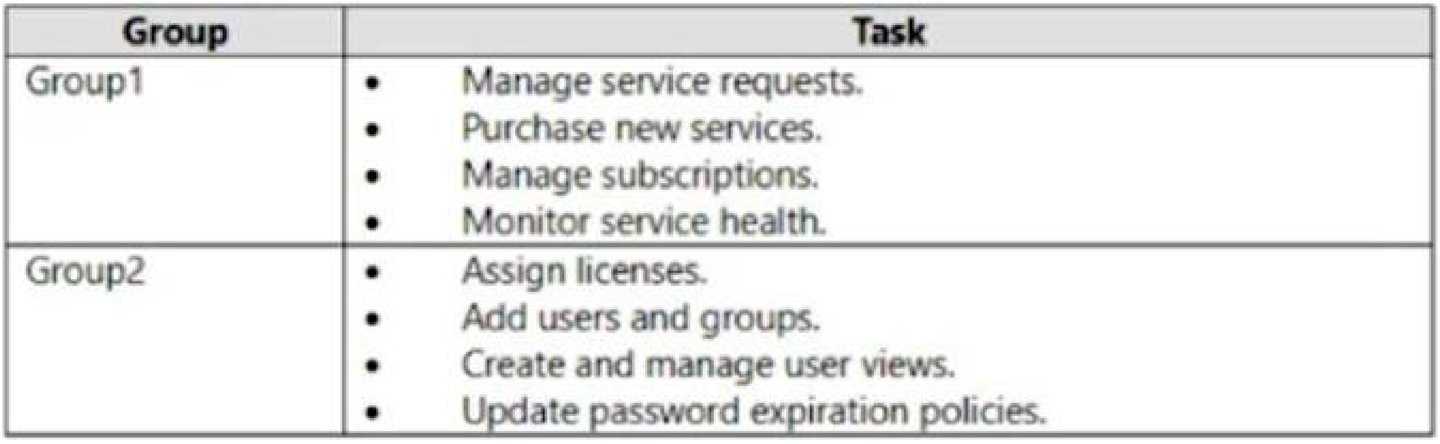
Exam Questions MS-102

Microsoft 365 Administrator Exam

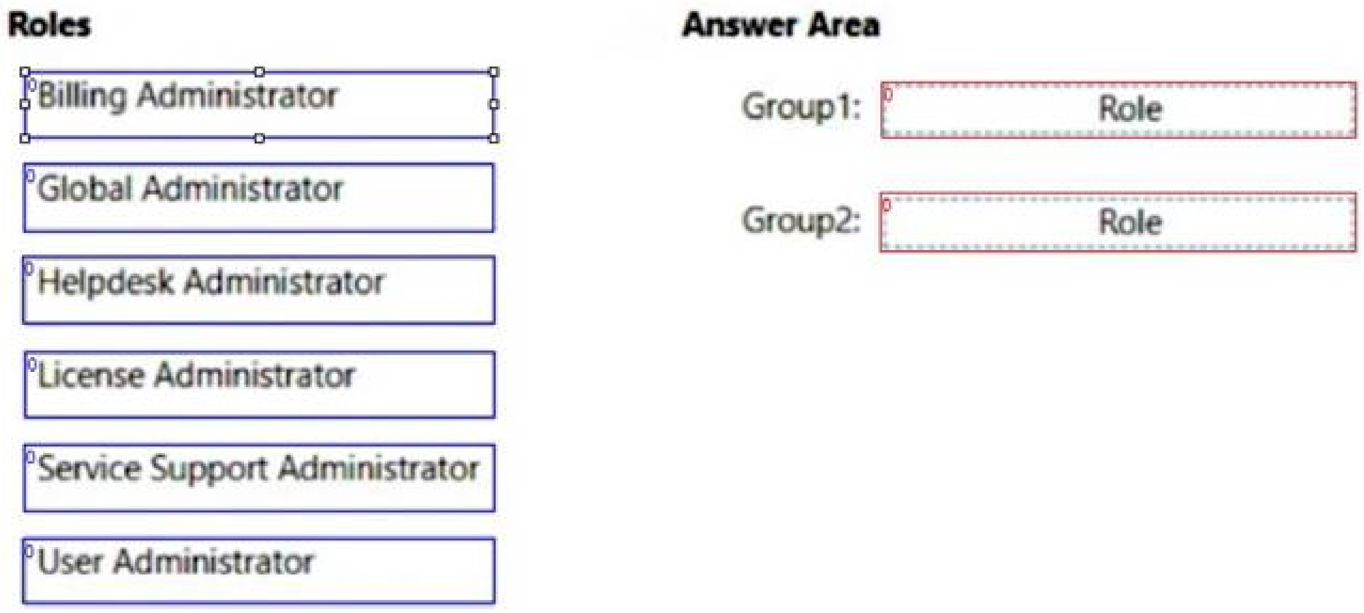
https://www.2passeasy.com/dumps/MS-102/

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.



Roles

- Billing Administrator
- Global Administrator
- Helpdesk Administrator
- License Administrator
- Service Support Administrator
- User Administrator

Answer Area

Group1: Role

Group2: Role

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

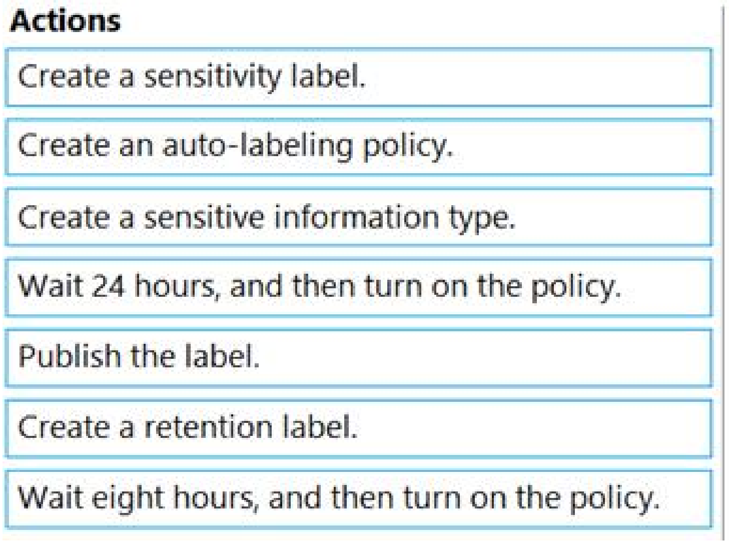
NEW QUESTION 2
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct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

A. Yes
B. No

Answer: B

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

NEW QUESTION 3
DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You need to automatically label the documents on Site1 that contain credit card numbers. Which three actions should you perform in sequence? To answer, move the appropriate
actions from the list of actions to the answer area and arrange them in the correct order.



Actions

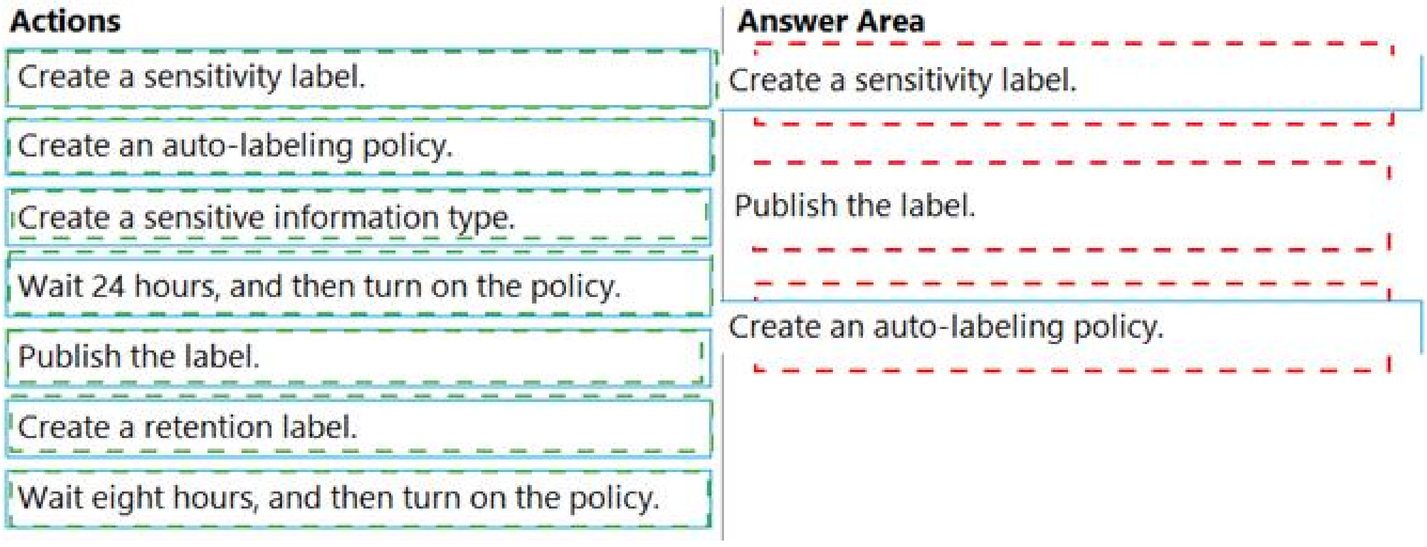
- Create a sensitivity label.
- Create an auto-labeling policy.
- Create a sensitive information type.
- Wait 24 hours, and then turn on the policy.
- Publish the label.
- Create a retention label.
- Wait eight hours, and then turn on the policy.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



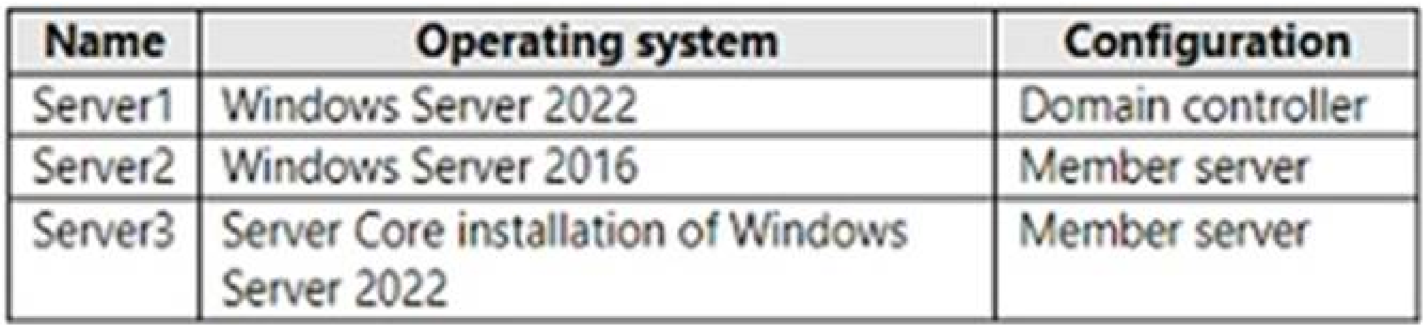
Actions

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

Answer Area

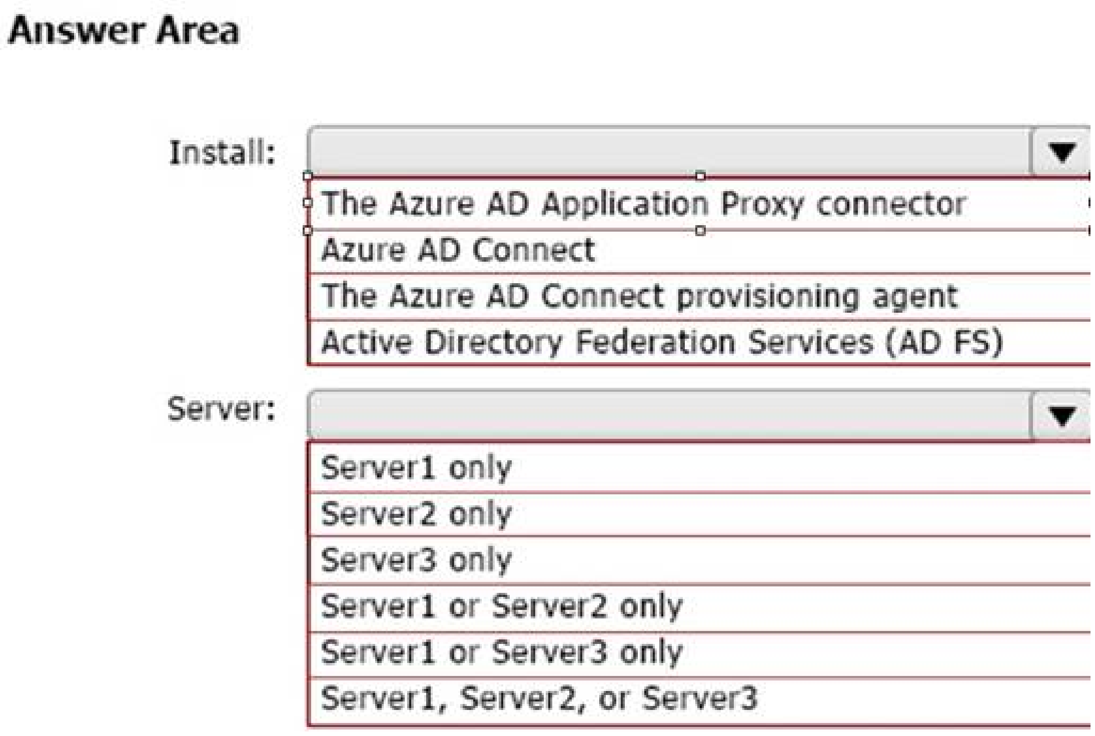
- Create a sensitivity label.
- Publish the label.
- Create an auto-labeling policy.

NEW QUESTION 4
HOTSPOT - (Topic 6)
HOTSPOT
Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.



Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.
You need to implement Azure AD Connect cloud sync.
What should you install first and on which server? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

Install:

- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:

- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: The Azure AD Connect provisioning agent Install the Azure AD Connect provisioning agent
How is Azure AD Connect cloud sync different from Azure AD Connect sync?
With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.
Box 2: Server1 or Server2 only.
Cloud provisioning agent requirements include:
* An on-premises server for the provisioning agent with Windows 2016 or later.
This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.
Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.

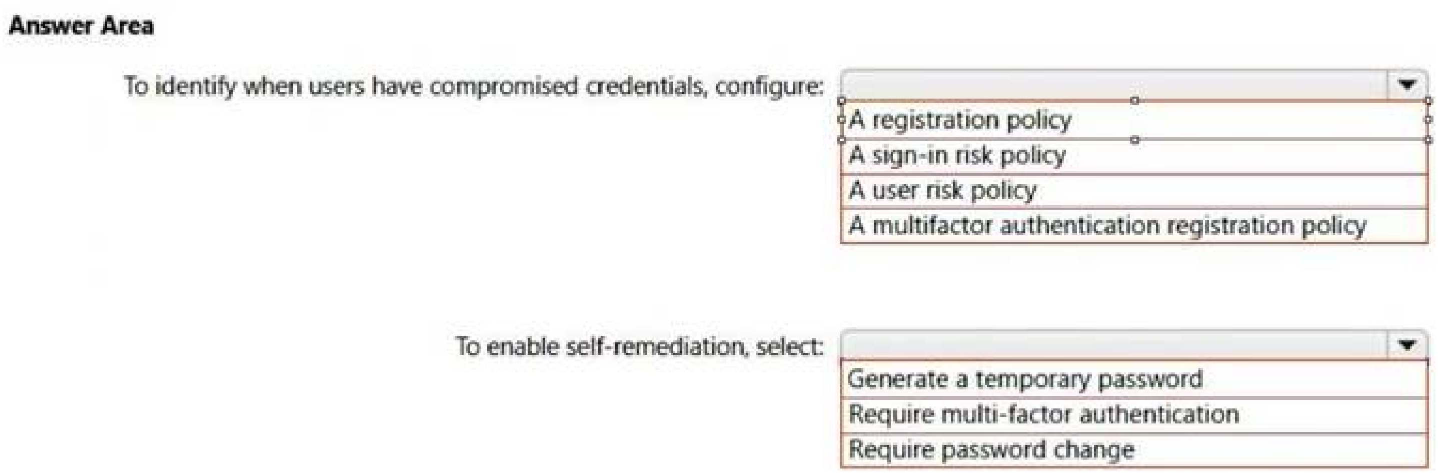
NEW QUESTION 5
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.
You need to remove User1 from the Restricted entities list. What should you use?

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

Answer: D

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

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



Answer Area

To identify when users have compromised credentials, configure:

- A registration policy
- A sign-in risk policy
- A user risk policy
- A multifactor authentication registration policy

To enable self-remediation, select:

- Generate a temporary password
- Require multi-factor authentication
- Require password change

A. Mastered
B. Not Mastered

Answer: A

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

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

A. Yes
B. No

Answer: B

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

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

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

Answer: B

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

NEW QUESTION 9
- (Topic 6)
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 10
- (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

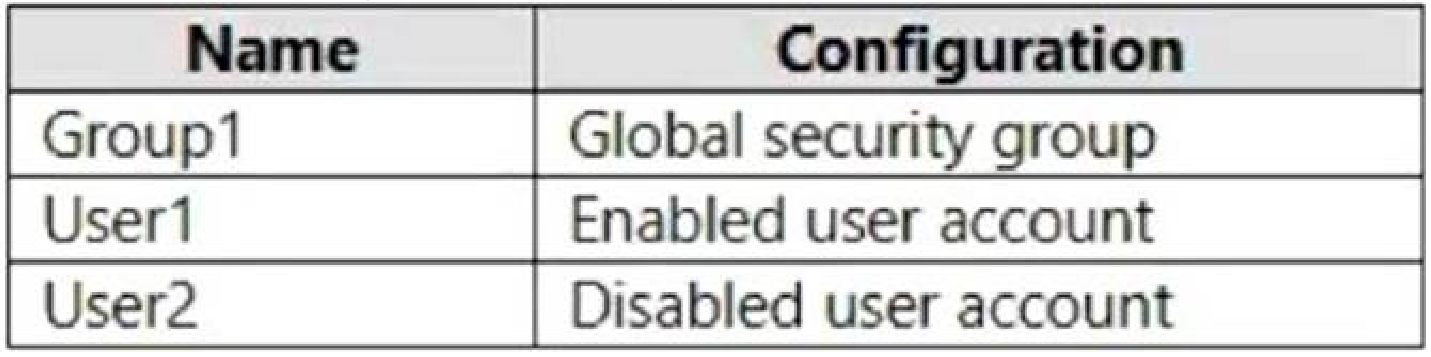
NEW QUESTION 10
- (Topic 6)
You have a Microsoft 365 subscription.
You register two applications named App1 and App2 to Azure AD.
You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

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 13
- (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?

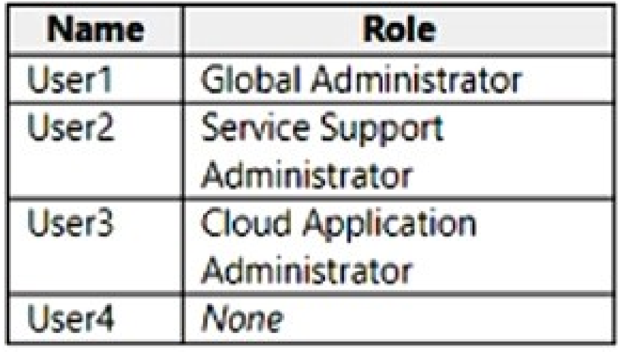
A. Group1 only
B. User1 and User2 only
C. Group1 and User1 only
D. Group1, User1, and User2

Answer: D

Explanation:

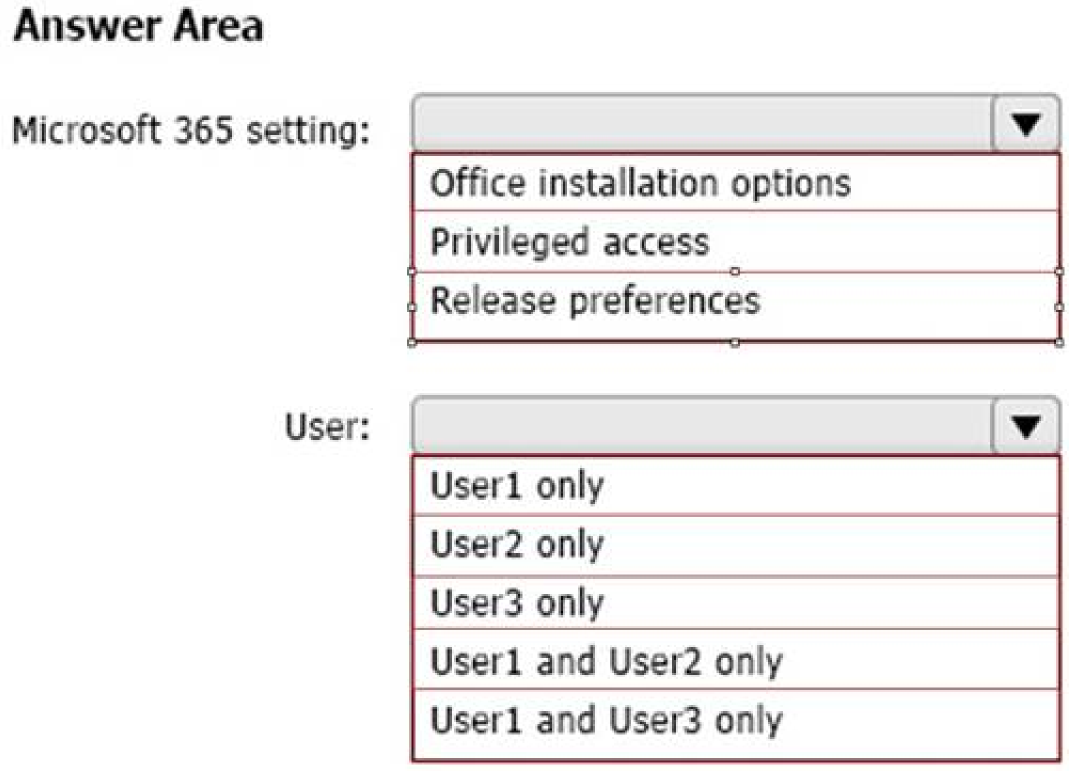
Disabled accounts
Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.
The assumption 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 18
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



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

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



Answer Area

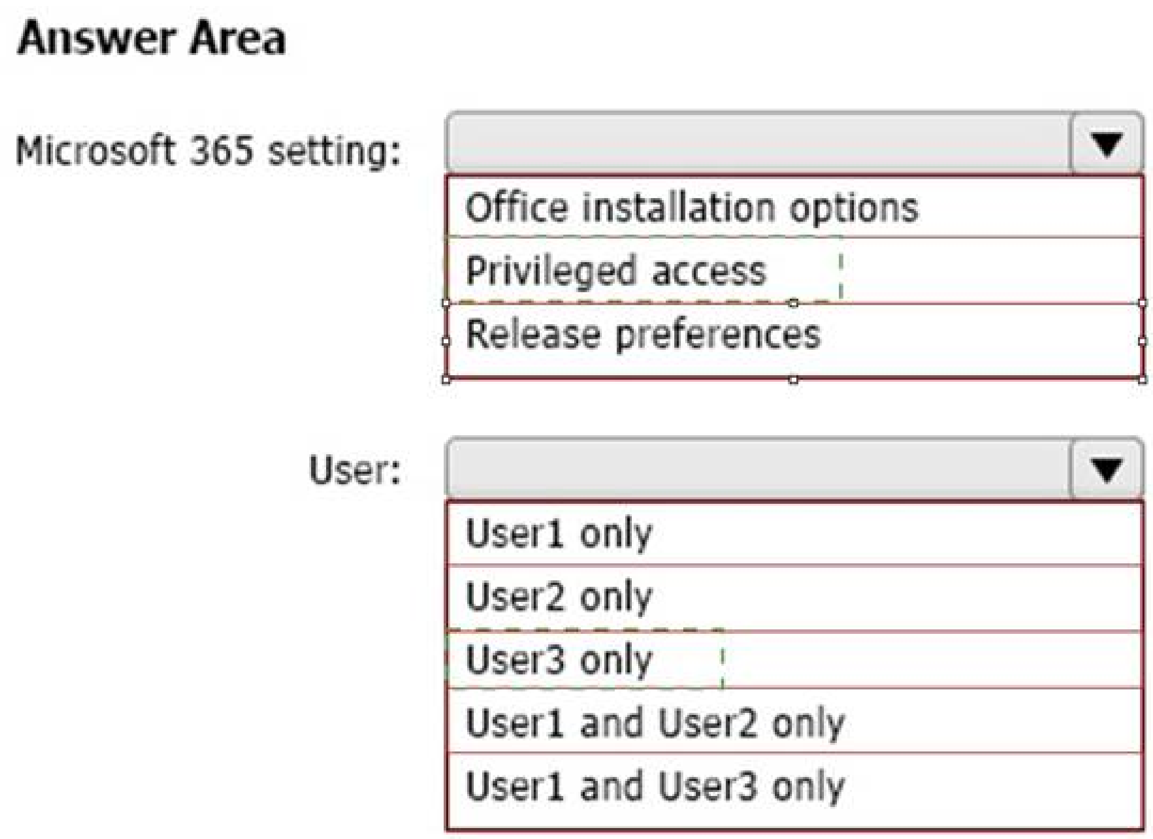
Microsoft 365 setting:
- Office installation options
- Privileged access
- Release preferences

User:
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:

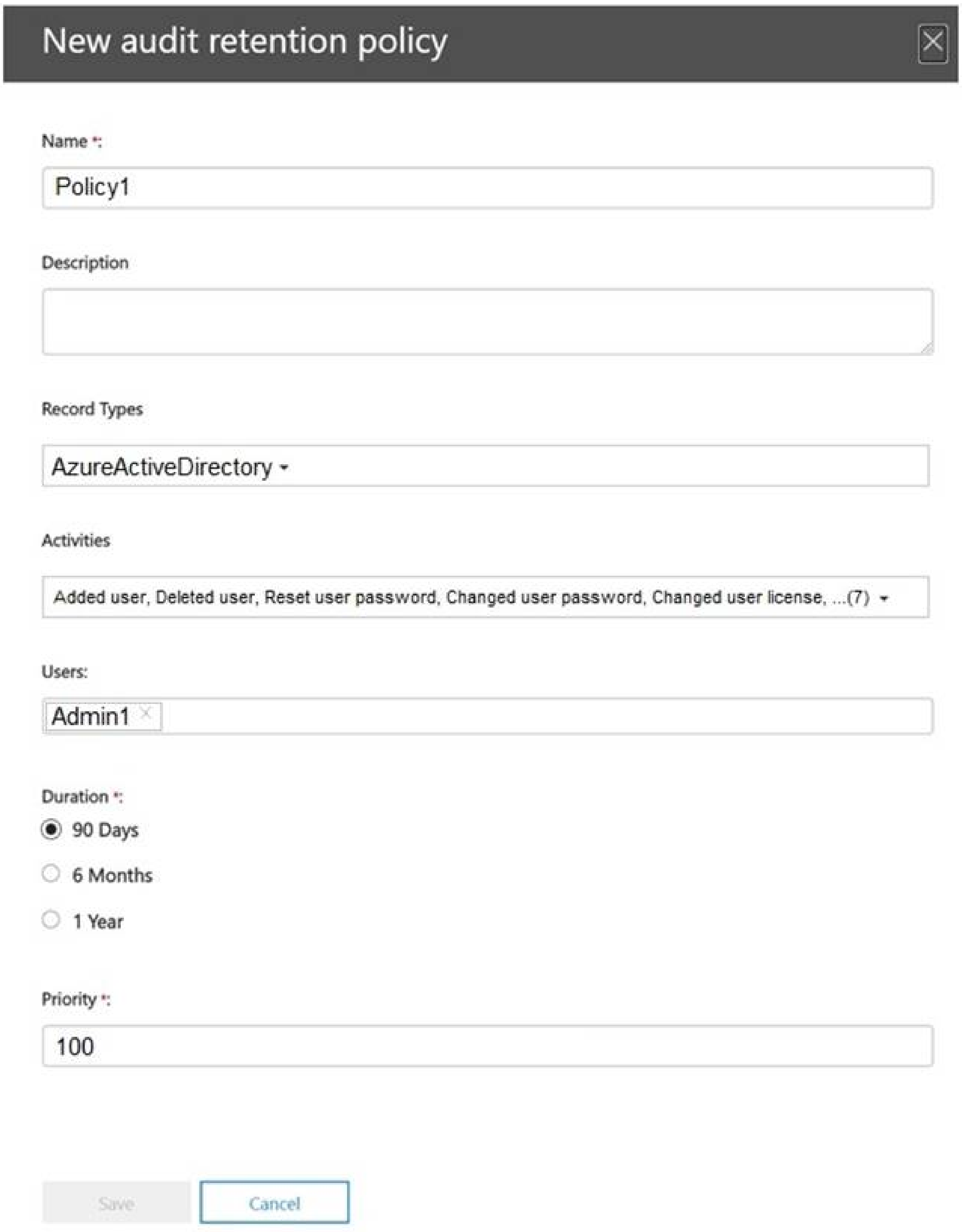


Answer Area

Microsoft 365 setting:
- Office installation options
- Privileged access
- Release preferences

User:
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

NEW QUESTION 20
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains two users named Admin1 and Admin2.
All users are assigned a Microsoft 365 Enterprise E5 license and auditing is turned on.
You create the audit retention policy shown in the exhibit. (Click the Exhibit tab.)



New audit retention policy

Name *:
Policy1

Description

Record Types
AzureActiveDirectory

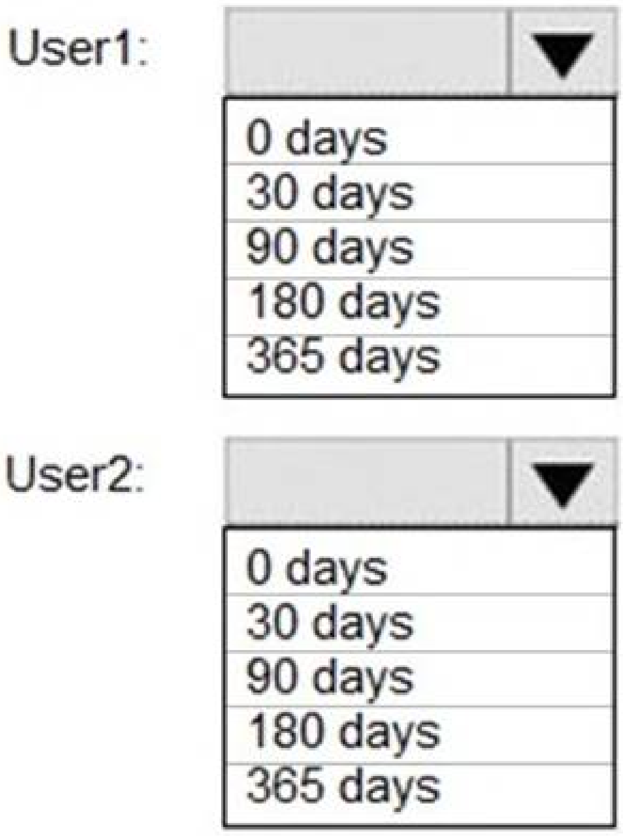
Activities
Added user, Deleted user, Reset user password, Changed user password, Changed user license, ...(7)

Users:
Admin1

Duration *:
● 90 Days
○ 6 Months
○ 1 Year

Priority *:
100

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



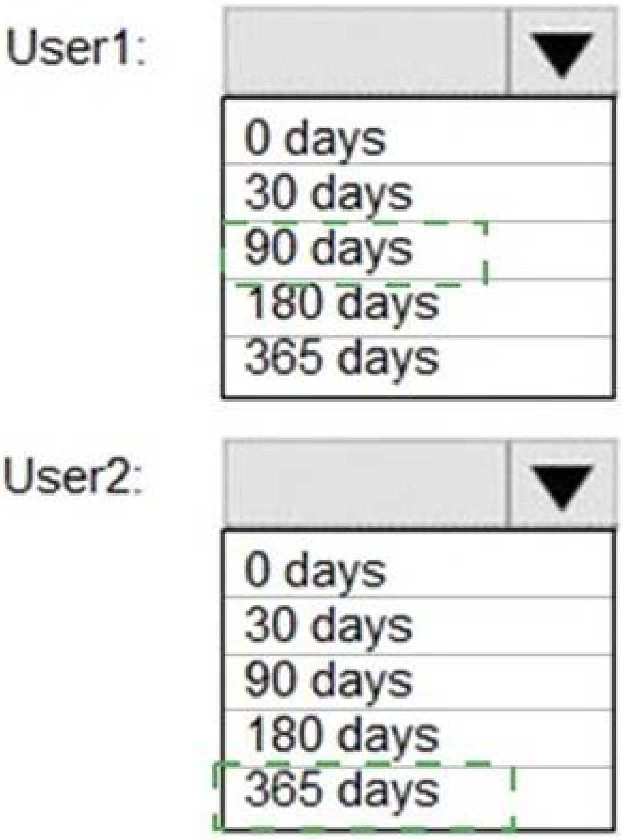
User1:
- 0 days
- 30 days
- 90 days
- 180 days
- 365 days

User2:
- 0 days
- 30 days
- 90 days
- 180 days
- 365 days

A. Mastered
B. Not Mastered

Answer: A

Explanation:



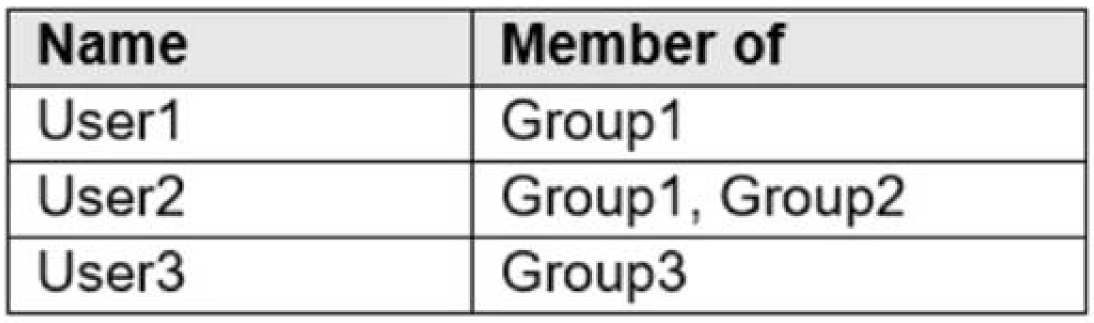
User1:

- 0 days
- 30 days
- [✓ 90 days]
- 180 days
- 365 days

User2:

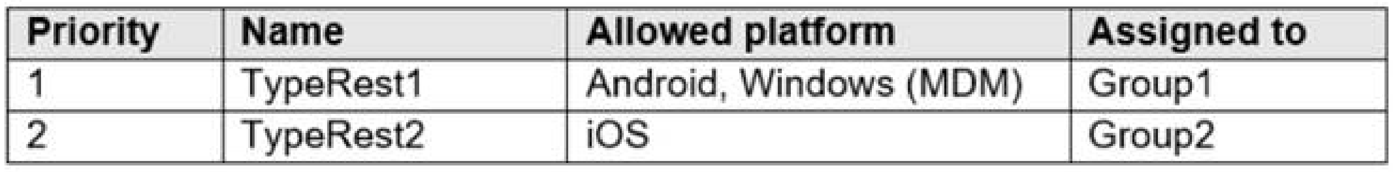
- 0 days
- 30 days
- 90 days
- 180 days
- [✓ 365 days]

NEW QUESTION 25
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription that contains the users in the following table.



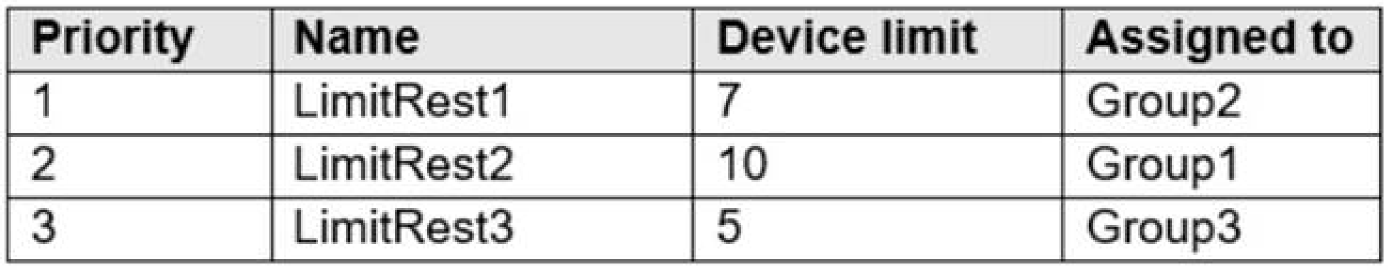
Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

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



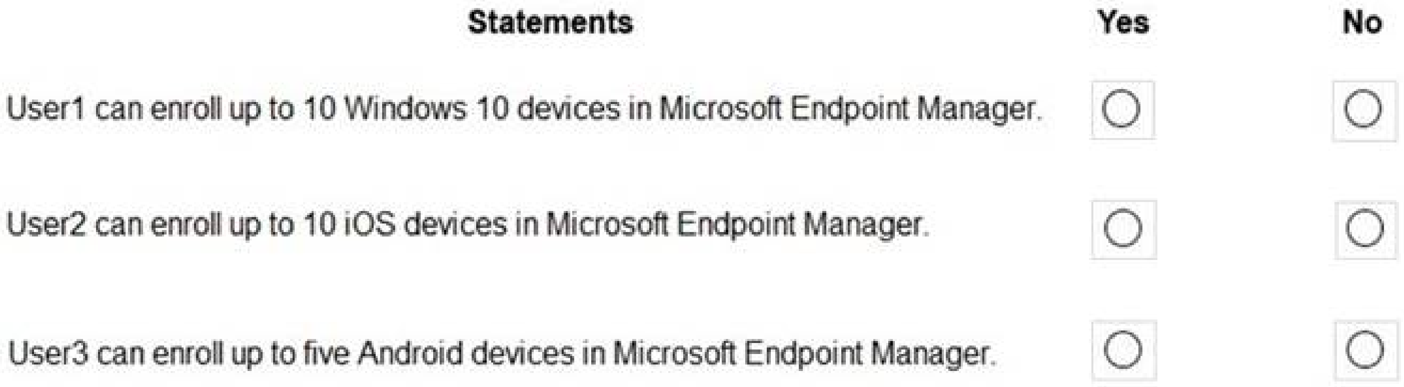
Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

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



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

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



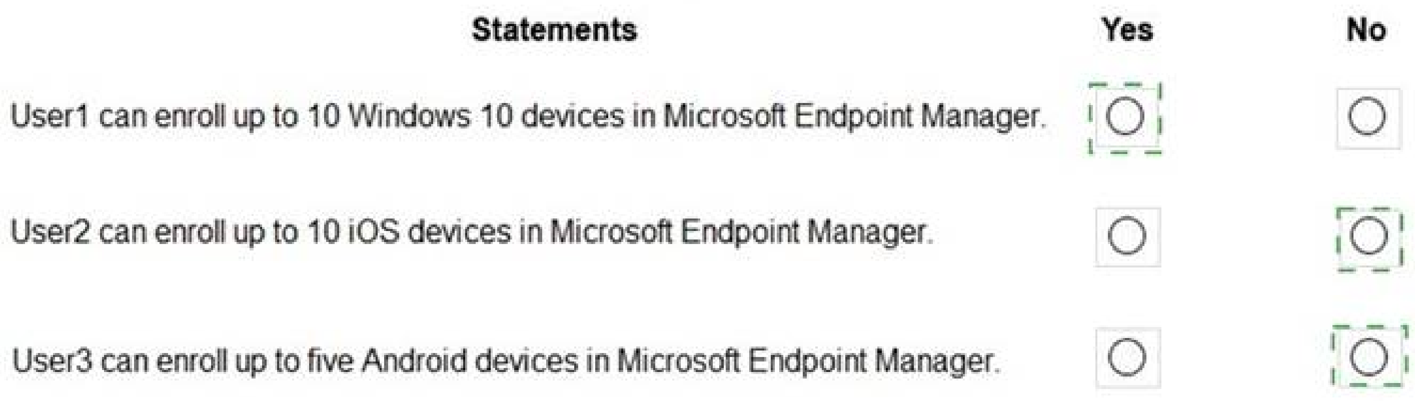
Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

A. Mastered

B. Not Mastered

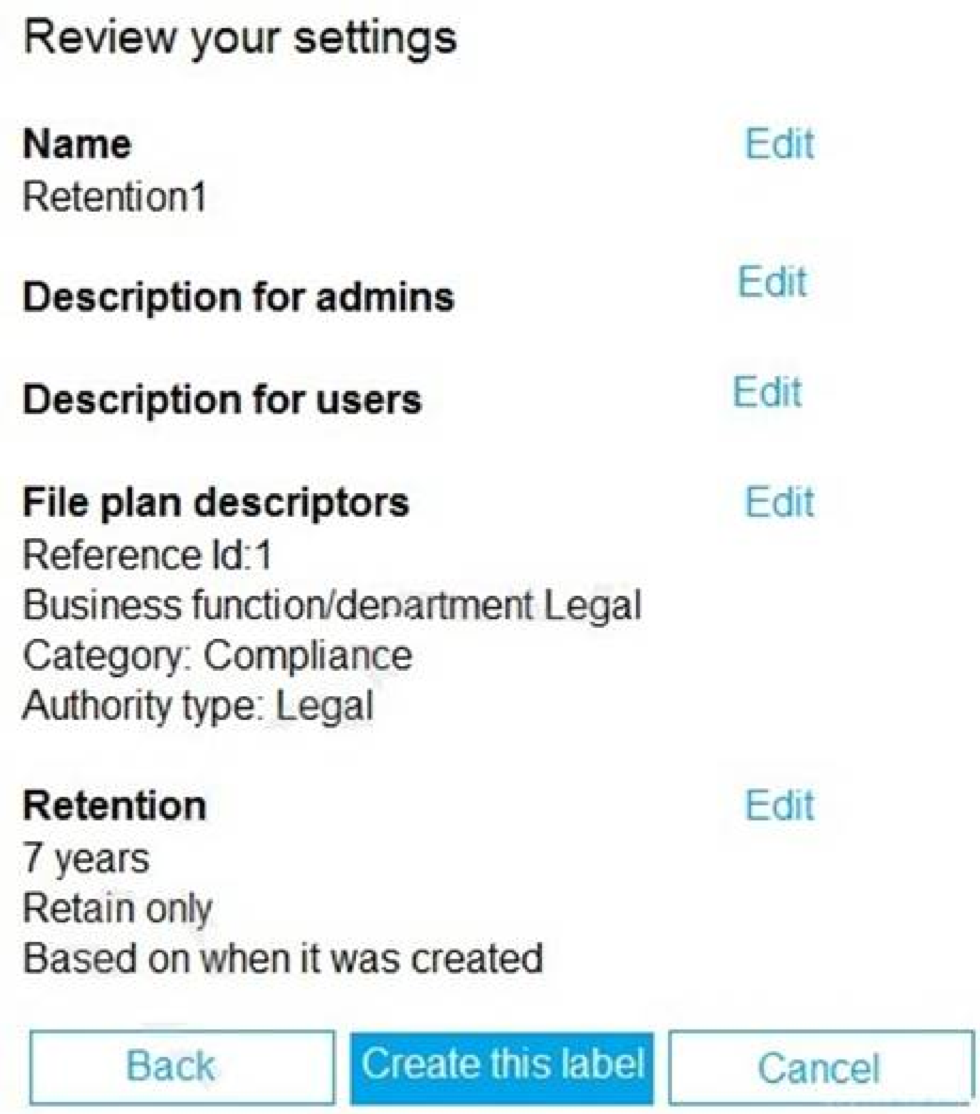
Answer: A

Explanation:



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

NEW QUESTION 27
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You create a retention label named Retention1 as shown in the following exhibit.



Review your settings

Name
Retention1

Description for admins

Description for users

File plan descriptors
Reference Id:1
Business function/denartment Legal
Category: Compliance
Authority type: Legal

Retention
7 years
Retain only
Based on when it was created

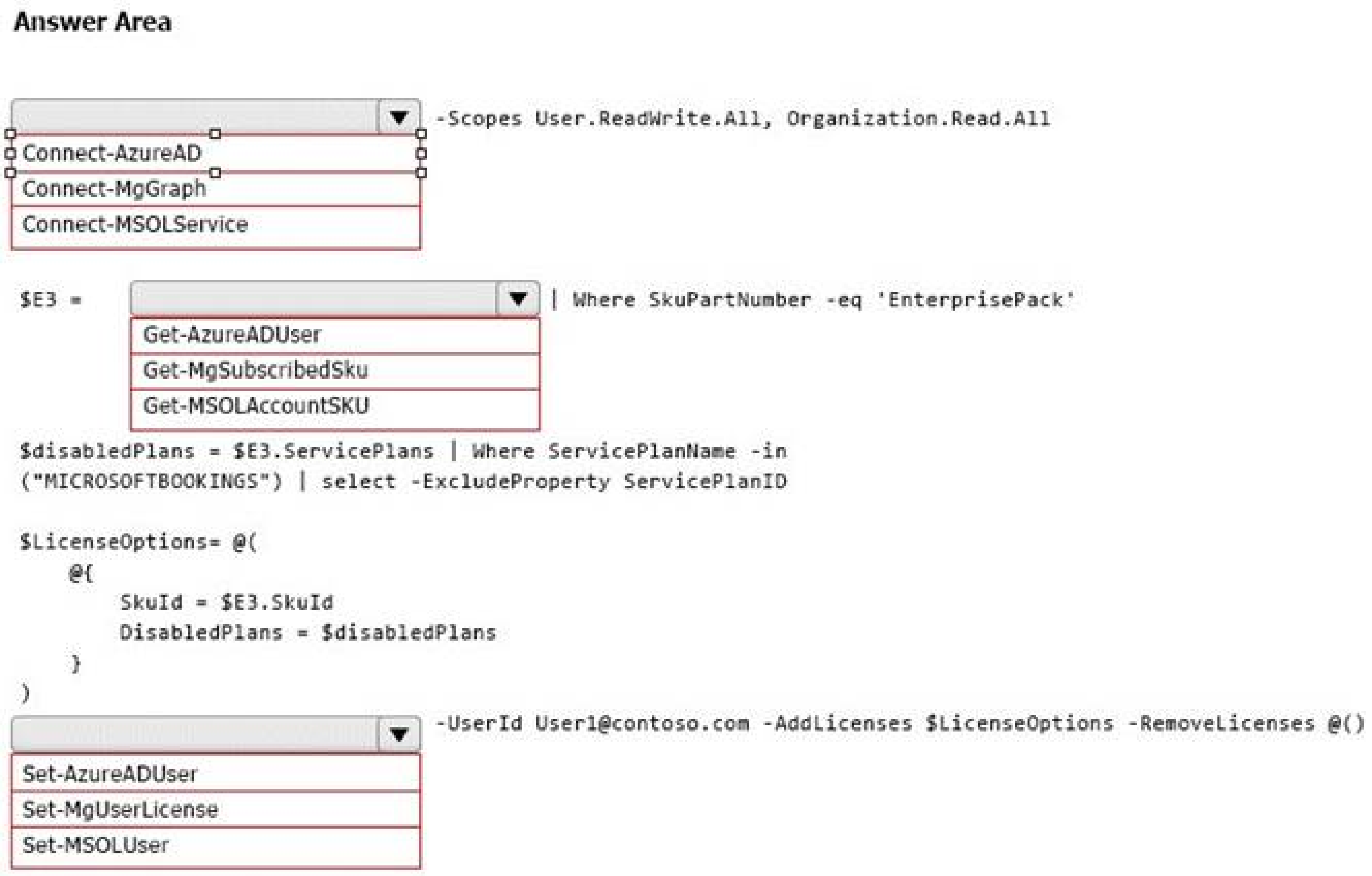
When users attempt to apply Retention1, the label is unavailable. You need to ensure that Retention1 is available to all the users. What should you do?

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

Answer: A

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

NEW QUESTION 28
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

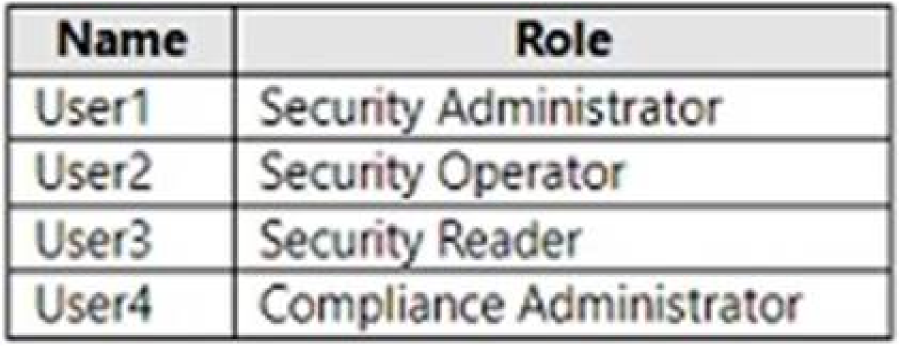
```
[ ▼ ] -Scopes User.ReadWrite.All, Organization.Read.All
  Connect-AzureAD
  Connect-MgGraph
  Connect-MSOLService

$E3 = [ ▼ ] | Where SkuPartNumber -eq 'EnterprisePack'
  Get-AzureADUser
  Get-MgSubscribedSku
  Get-MSOLAccountSKU
$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$LicenseOptions= @(
    @{
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    }
)
[ ▼ ] -UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @()
  Set-AzureADUser
  Set-MgUserLicense
  Set-MSOLUser
```

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 33
- (Topic 6)
You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.



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

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

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

Answer: A

NEW QUESTION 35
- (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 36
- (Topic 6)
Your company has multiple offices.
You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.
You need to ensure that the local administrators can manage only the devices in their respective office.
What should you use?

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

Answer: A

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

NEW QUESTION 39
- (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

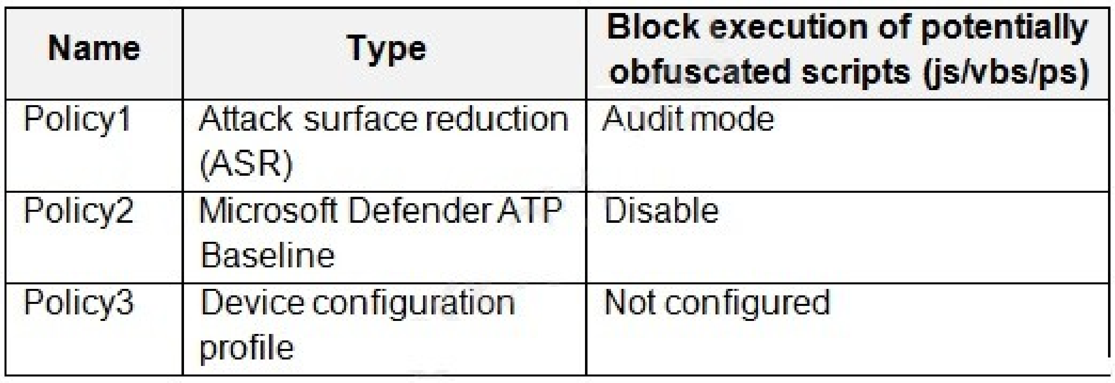
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

NEW QUESTION 41
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365 and contains a mailbox named Mailbox1.
You plan to use Mailbox1 to collect and analyze unfiltered email messages.
You need to ensure that Defender for Office 365 takes no action on any inbound emails delivered to Mailbox1.
What should you do?

A. Configure a retention policy for Mailbox1.
B. Create a mail flow rule.
C. Configure Mailbox! as a SecOps mailbox.
D. Place a litigation hold on Mailbox1.

Answer: D

NEW QUESTION 45
- (Topic 6)
You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.



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

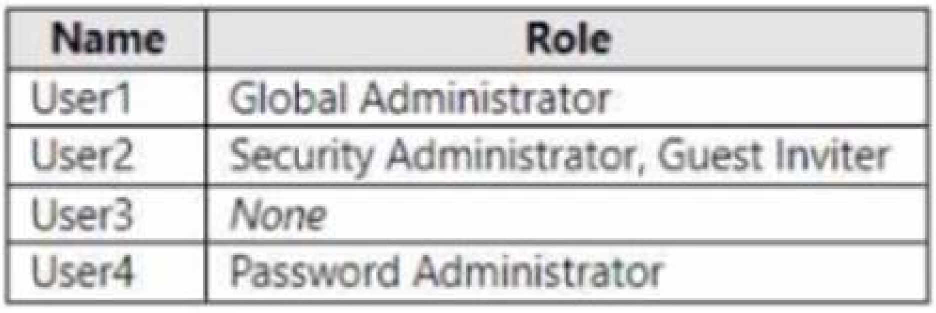
The policies are assigned to Device1.
Which policy settings will be applied to Device1?

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

D. no settings

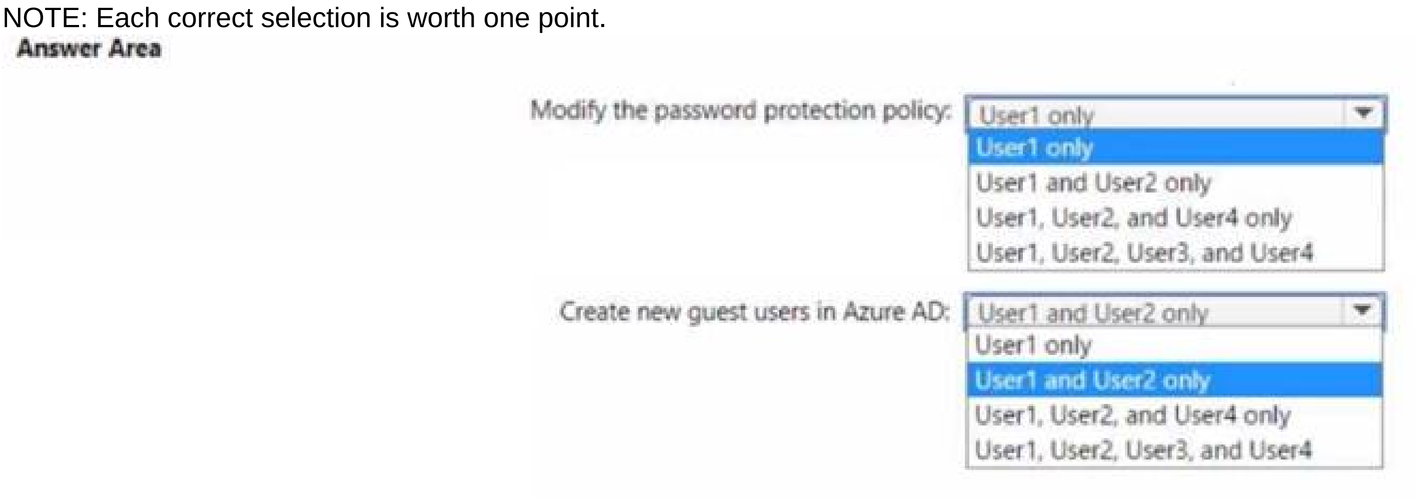
Answer: D

NEW QUESTION 49
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

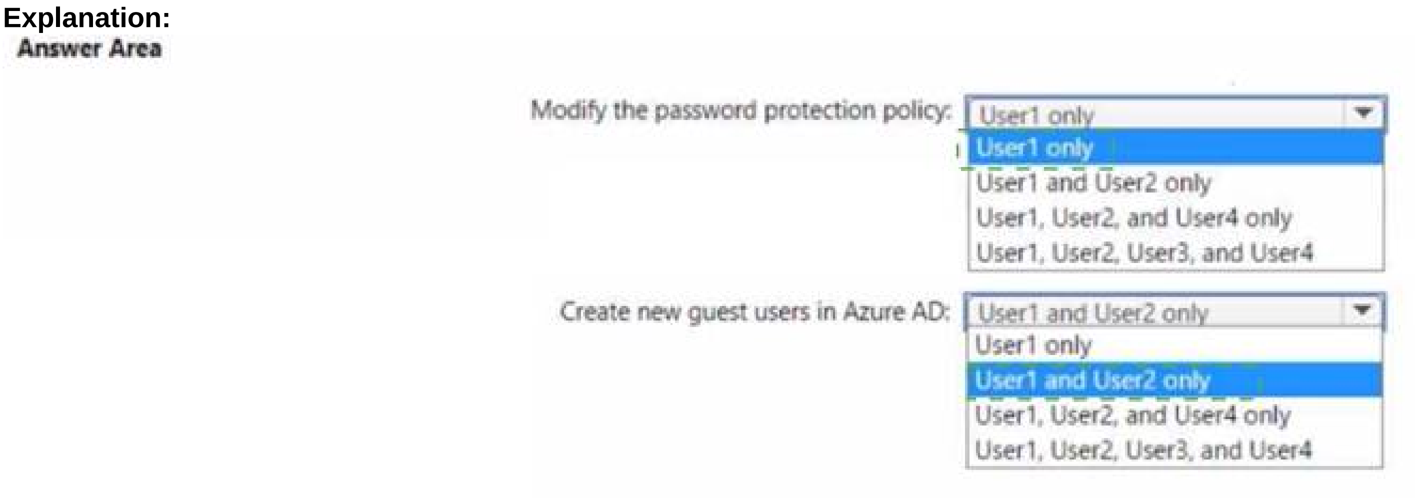
Modify the password protection policy: User1 only
User1 only
User1 and User2 only
User1, User2, and User4 only
User1, User2, User3, and User4

Create new guest users in Azure AD: User1 and User2 only
User1 only
User1 and User2 only
User1, User2, and User4 only
User1, User2, User3, and User4

A. Mastered
B. Not Mastered

Answer: A

Explanation:

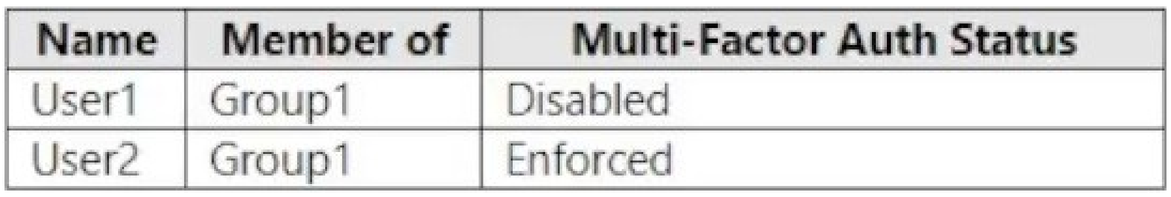


Answer Area

Modify the password protection policy: User1 only
User1 only
User1 and User2 only
User1, User2, and User4 only
User1, User2, User3, and User4

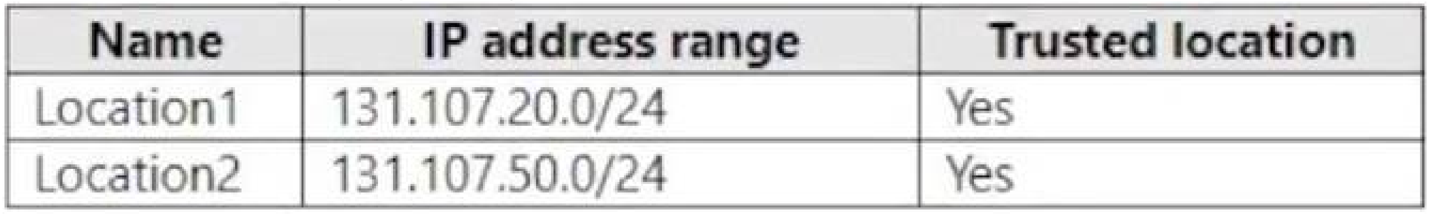
Create new guest users in Azure AD: User1 and User2 only
User1 only
User1 and User2 only
User1, User2, and User4 only
User1, User2, User3, and User4

NEW QUESTION 52
HOTSPOT - (Topic 6)
HOTSPOT
You have an Azure AD tenant named contoso.com that contains the users shown in the following table.



Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1	Enforced

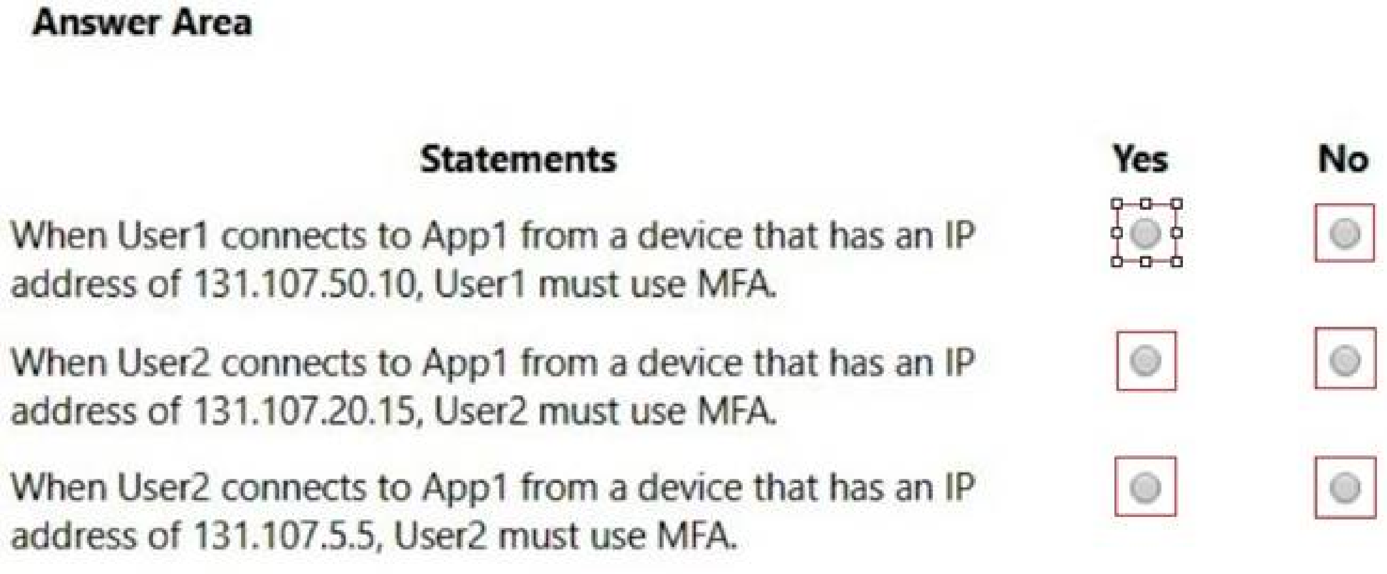
Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs. The tenant contains the named locations shown in the following table.



Name	IP address range	Trusted location
Location1	131.107.20.0/24	Yes
Location2	131.107.50.0/24	Yes

You create a conditional access policy that has the following configurations:
? Users or workload identities assignments: All users
? Cloud apps or actions assignment: App1
? Conditions: Include all trusted locations

? Grant access: Require multi-factor authentication
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

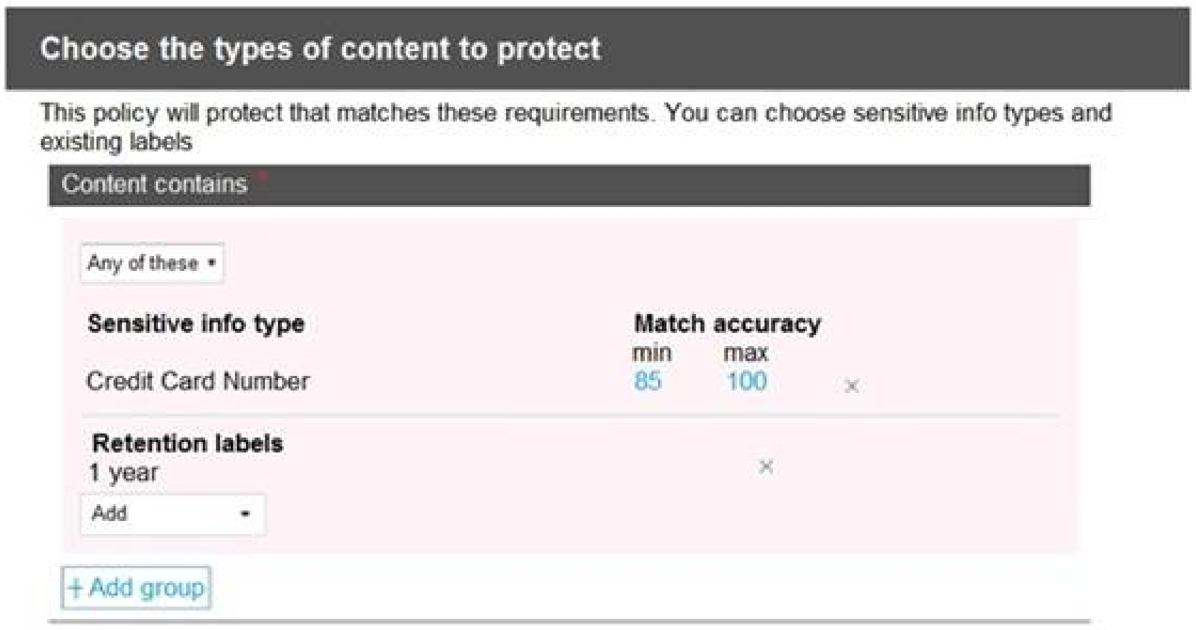
Statements	Yes	No
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
* 131.107.50.10 is in a Trusted Location so the conditional access policy applies. The policy requires MFA. However, User1's MFA status is disabled. The MFA requirement in the conditional access policy will override the user's MFA status of disabled. Therefore, User1 must use MFA.
Box 2: Yes.
* 131.107.20.15 is in a Trusted Location so the conditional access policy applies. The policy requires MFA so User2 must use MFA.
Box 3: No.
IP not from Trusted Location so Policy does not apply, Subnet 131.107.5.5 is not in the range of 131.107.50.0/24

NEW QUESTION 54
HOTSPOT - (Topic 6)
You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.



Choose the types of content to protect

This policy will protect that matches these requirements. You can choose sensitive info types and existing labels

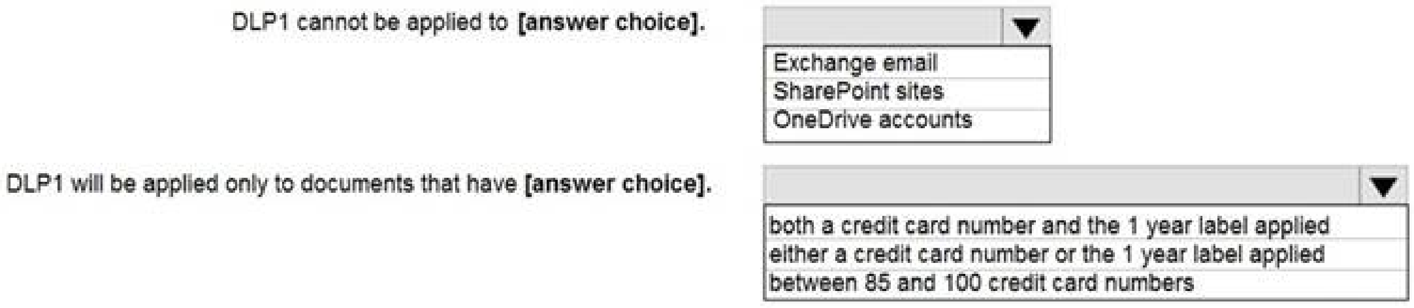
Content contains *

Any of these ▾

Sensitive info type	Match accuracy min	max
Credit Card Number	85	100

Retention labels
1 year

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.



DLP1 cannot be applied to **[answer choice]**.
- Exchange email
- SharePoint sites
- OneDrive accounts

DLP1 will be applied only to documents that have **[answer choice]**.
- both a credit card number and the 1 year label applied
- either a credit card number or the 1 year label applied
- between 85 and 100 credit card numbers

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

NEW QUESTION 58

- (Topic 6)
You have a Microsoft 365 E5 tenant that has sensitivity label support enabled for Microsoft and SharePoint Online.
You need to enable unified labeling for Microsoft 365 groups. Which cmdlet should you run?

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

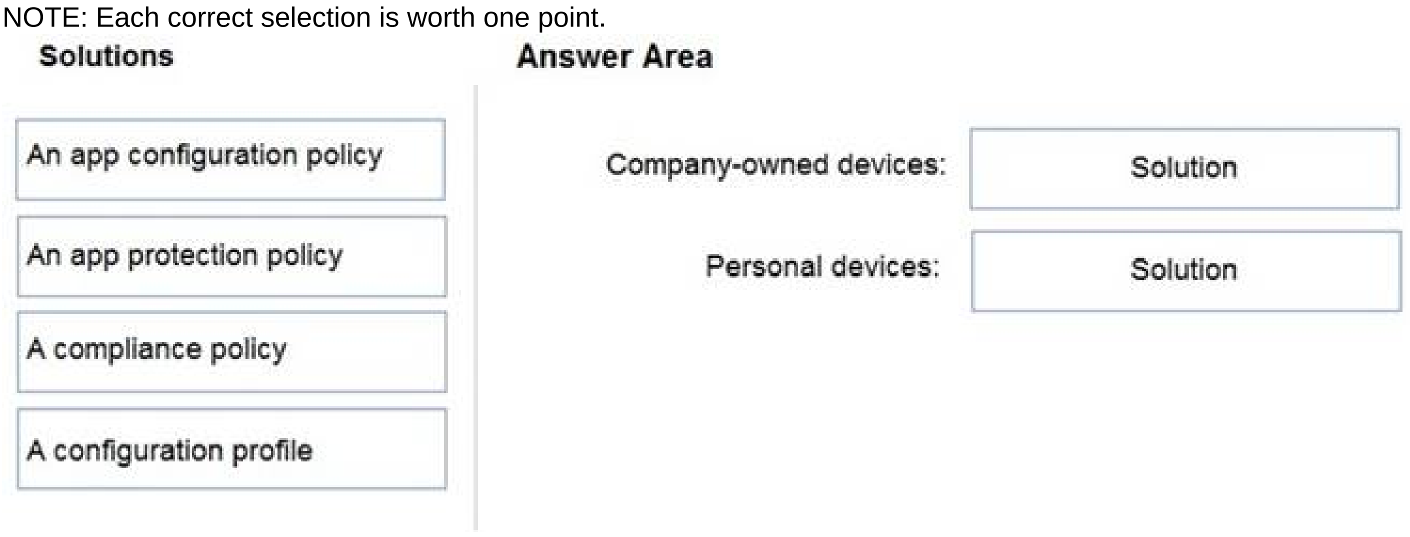
Answer: C

NEW QUESTION 60
- (Topic 6)
Your network contains an Active Directory forest named Contoso. Local. You have a Microsoft 365 subscription.
You plan to implement a directory synchronization solution that will use password hash synchronization.
From the Microsoft 365 admin center, you successfully verify the contoso.com domain name.
You need to prepare the environment for the planned directory synchronization solution. What should you do first?

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

Answer: A

NEW QUESTION 63
DRAG DROP - (Topic 6)
Your company has a Microsoft 365 E5 tenant.
Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.
You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.
What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

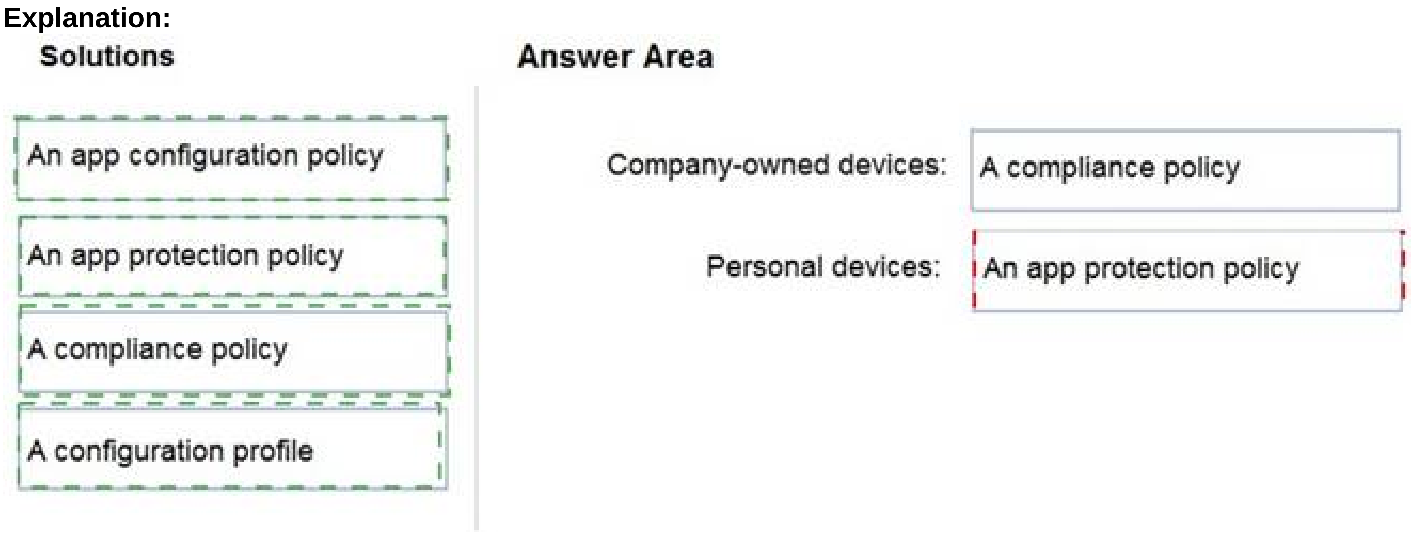


Company-owned devices: Solution
Personal devices: Solution

A. Mastered
B. Not Mastered

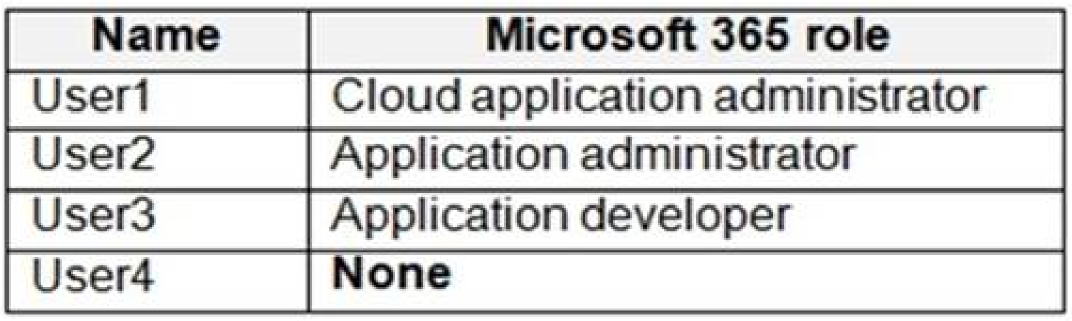
Answer: A

Explanation:



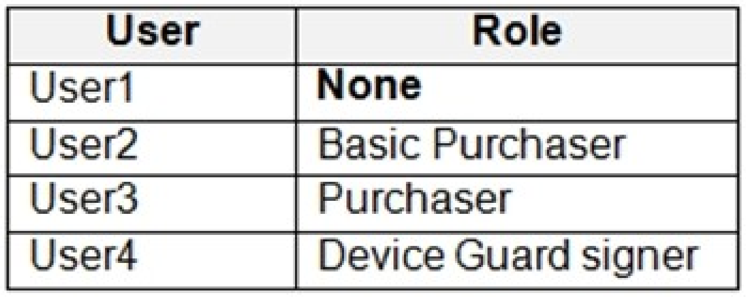
Company-owned devices: A compliance policy
Personal devices: An app protection policy

NEW QUESTION 68
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.



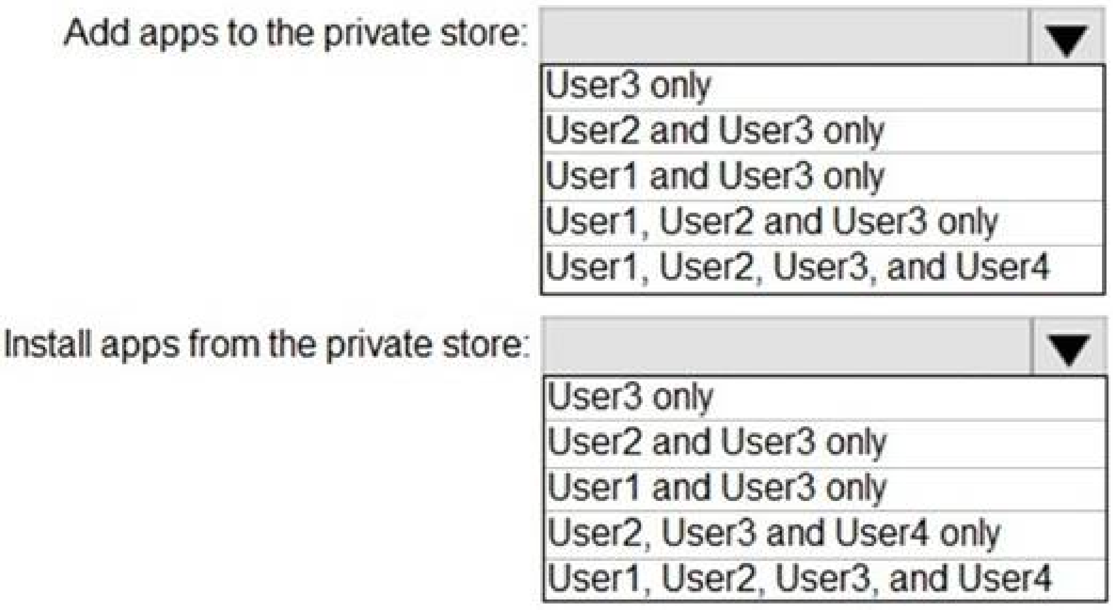
Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	None

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.



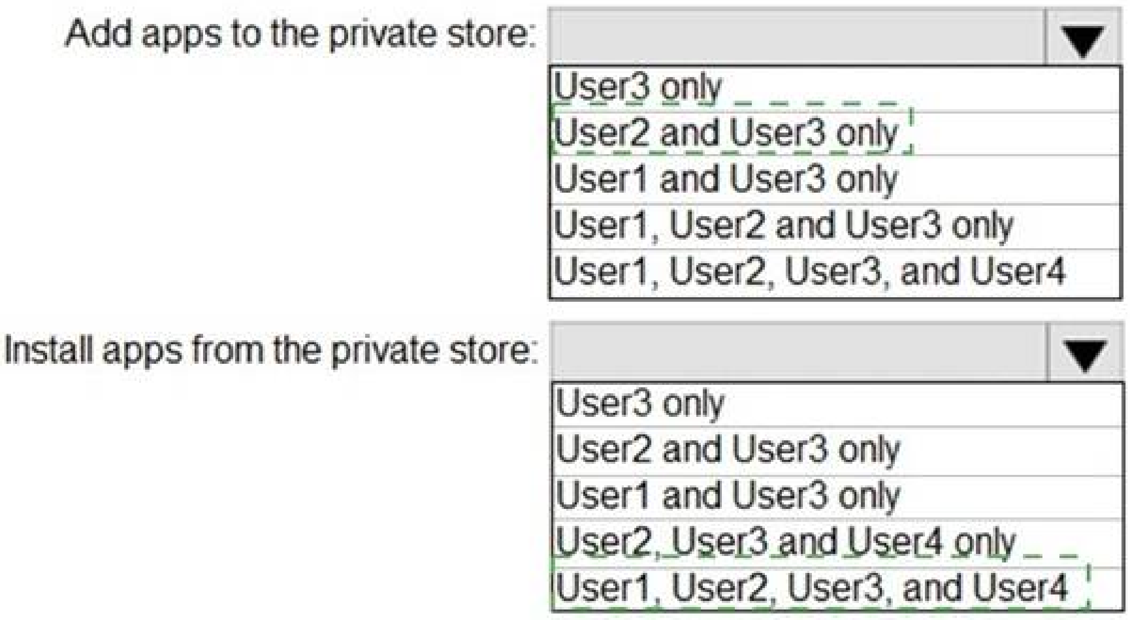
Add apps to the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

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

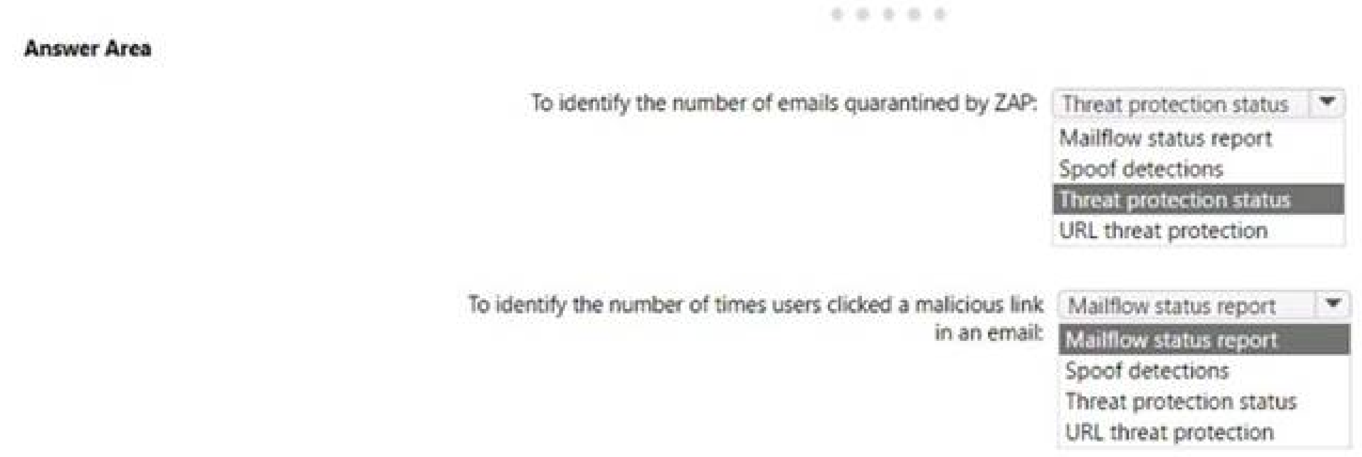
Explanation:



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]

NEW QUESTION 71
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.



Answer Area

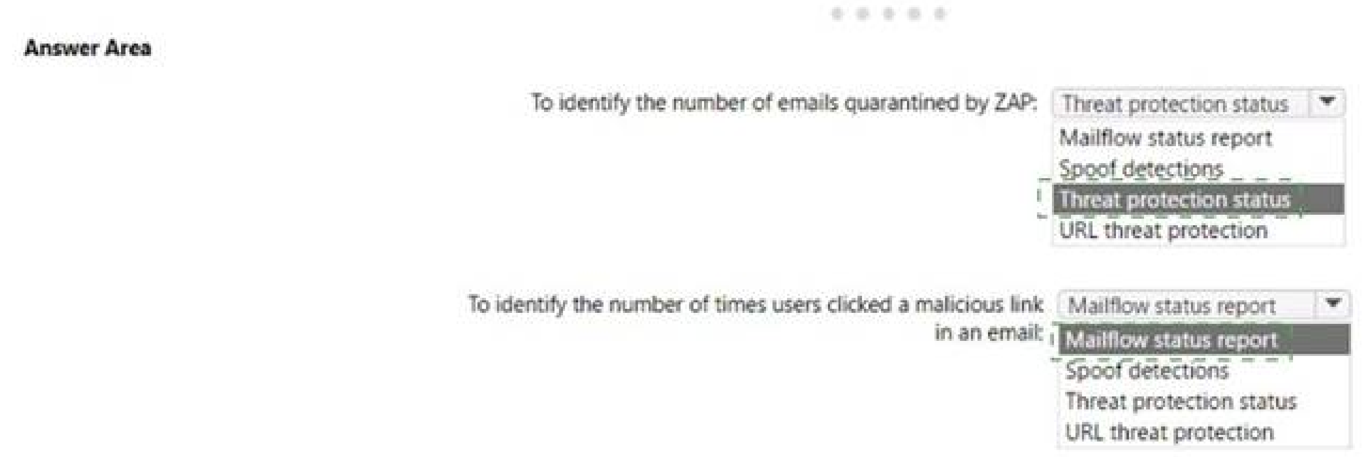
To identify the number of emails quarantined by ZAP: Threat protection status

To identify the number of times users clicked a malicious link in an email: Mailflow status report

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

To identify the number of emails quarantined by ZAP: Threat protection status

To identify the number of times users clicked a malicious link in an email: Mailflow status report

NEW QUESTION 74
- (Topic 6)
You have a Microsoft 365 subscription.
You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.
To which location can the policy be applied?

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

Answer: B

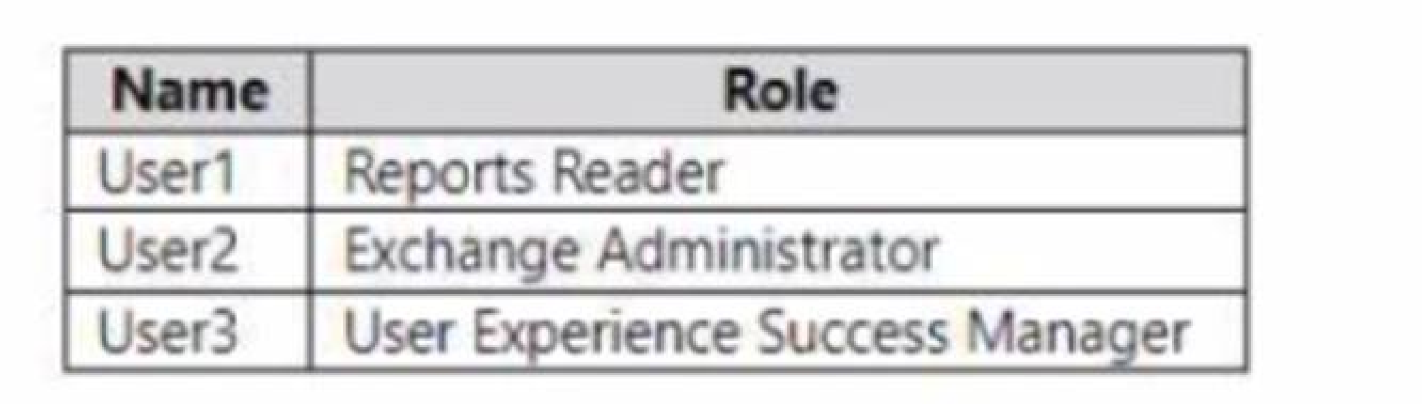
NEW QUESTION 78
- (Topic 6)
You have a Microsoft 365 E5 subscription.
From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.
What is the longest time range that can be included in the report?

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

Answer: C

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

NEW QUESTION 80
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



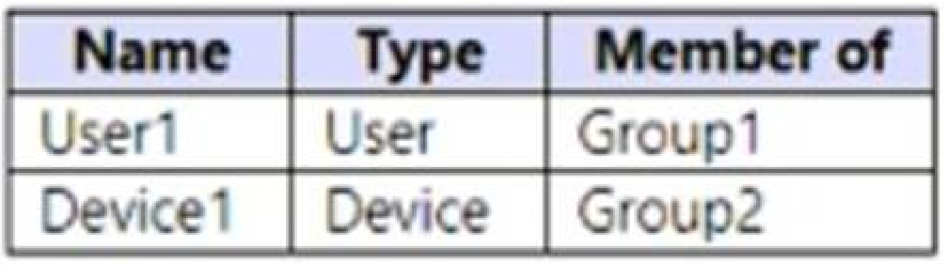
Name	Role
User1	Reports Reader
User2	Exchange Administrator
User3	User Experience Success Manager

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

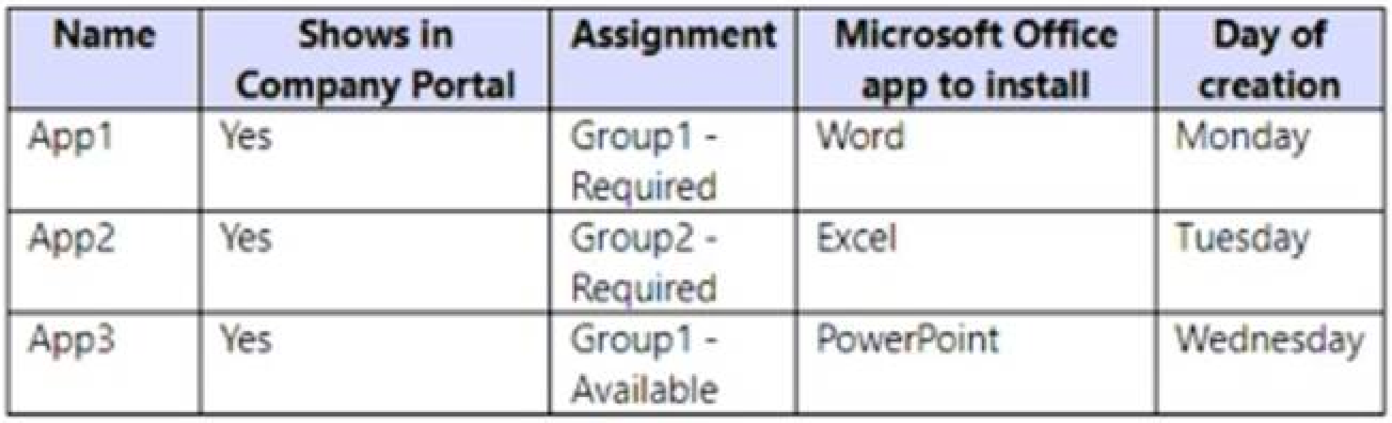
Answer: E

NEW QUESTION 83
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft intune. The subscription contains the resources shown in the following table.



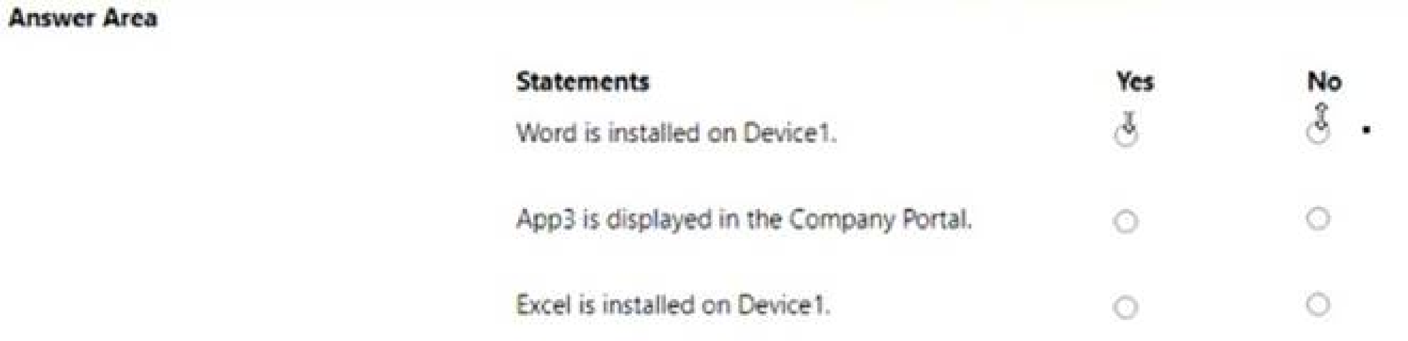
Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

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



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

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



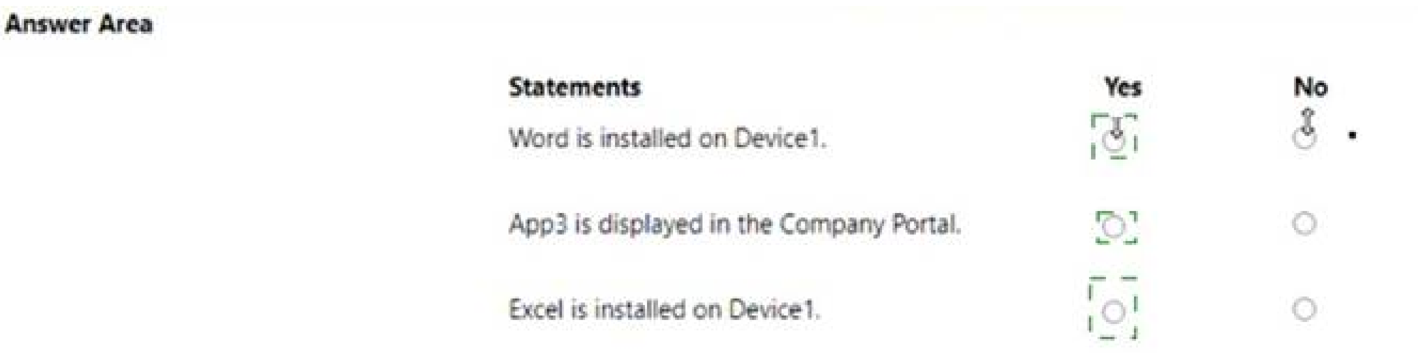
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



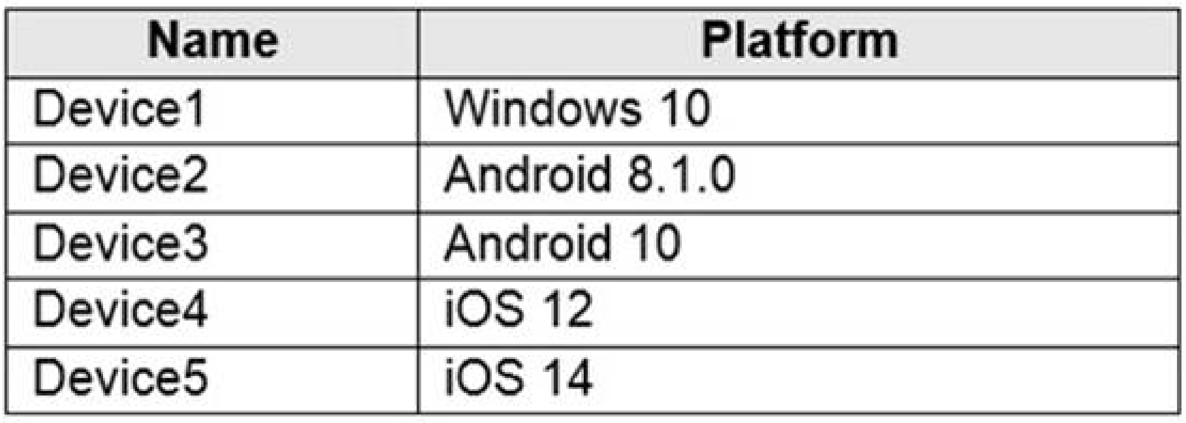
Answer Area

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

NEW QUESTION 86

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.



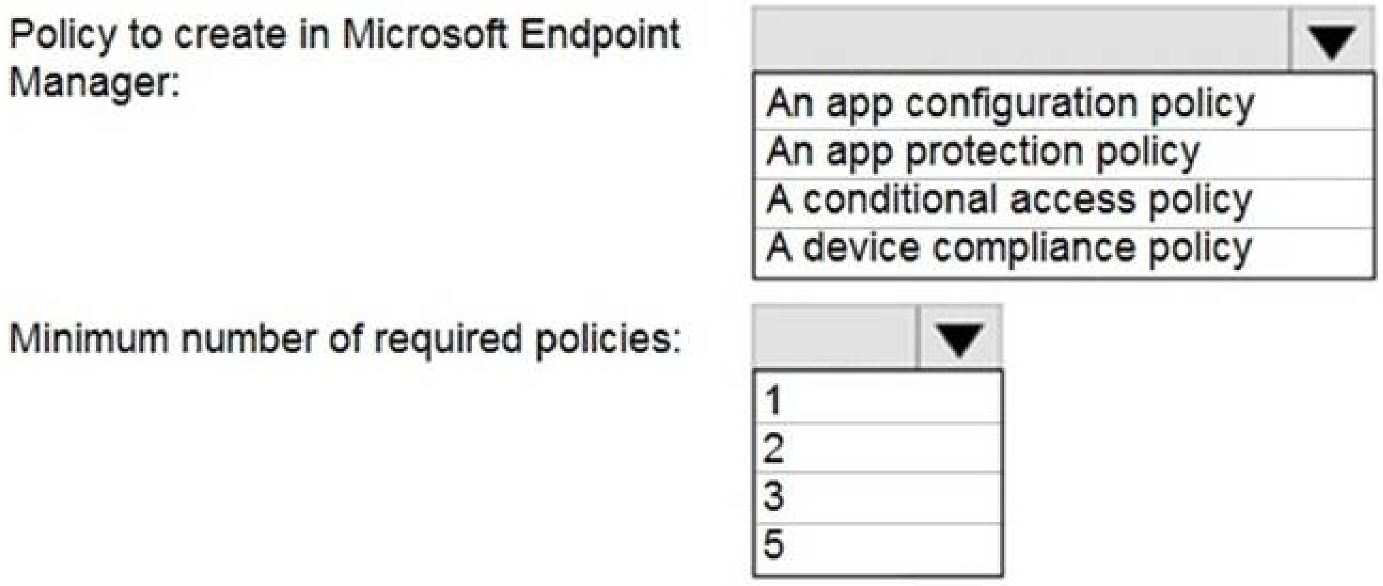
Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



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

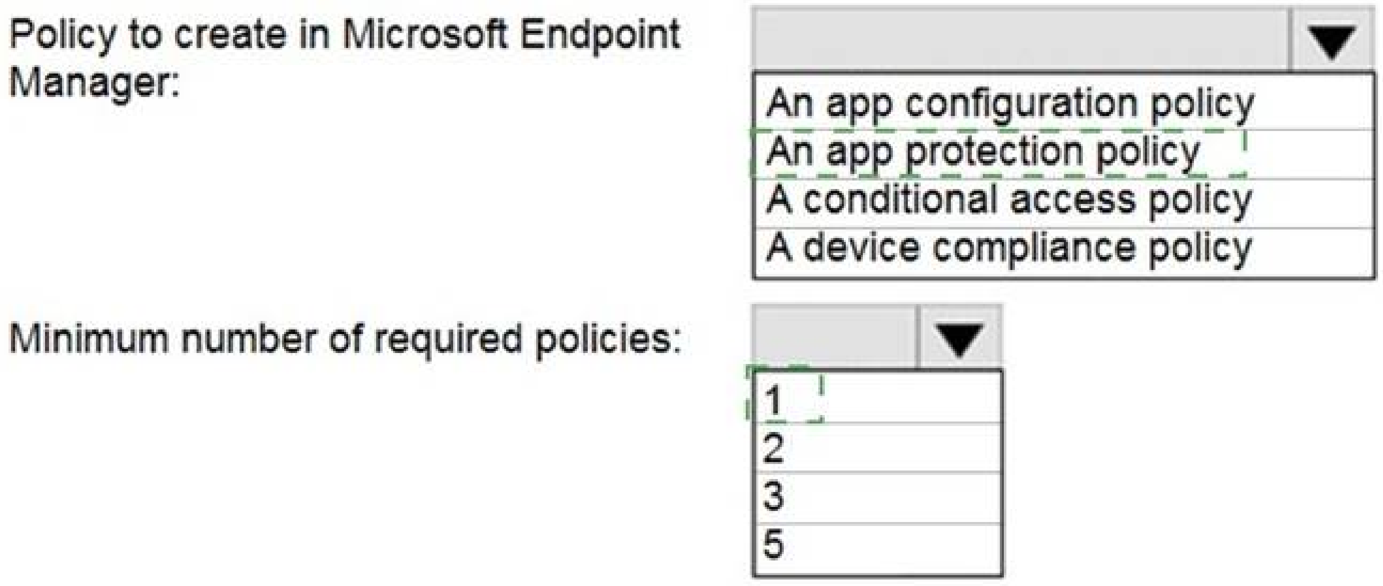
Minimum number of required policies:
- 1
- 2
- 3
- 5

A. Mastered

B. Not Mastered

Answer: A

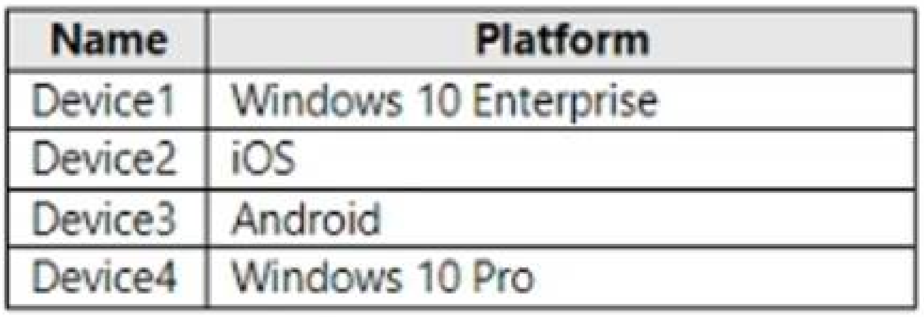
Explanation:



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

Minimum number of required policies:
- [✓ 1]
- 2
- 3
- 5

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



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

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

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

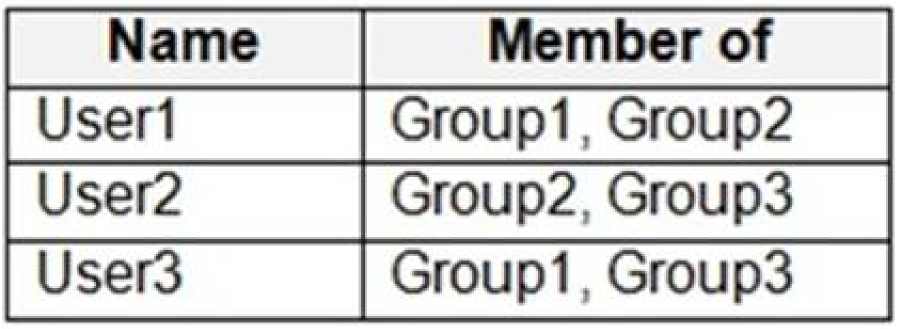
Answer: A

NEW QUESTION 94
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goats. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. You deploy a Microsoft Entra tenant.
Another administrator configures the domain to synchronize to the Microsoft Entra tenant.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.
You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.
Solution: From Microsoft Entra Connect, you modify the filtering settings. Does this meet the goal?

A. Yes
B. No

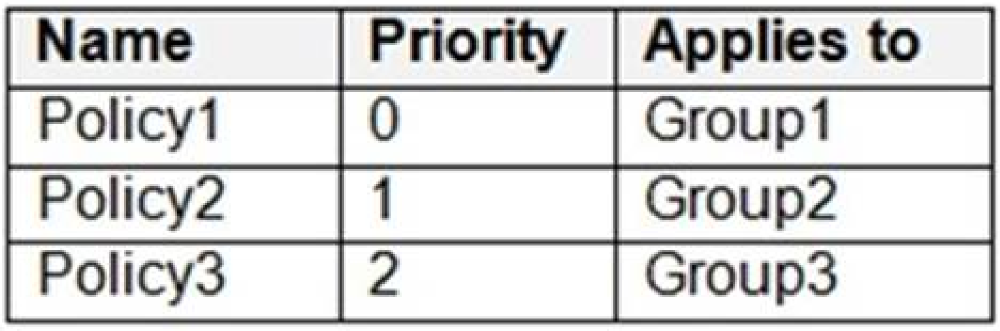
Answer: B

NEW QUESTION 96
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



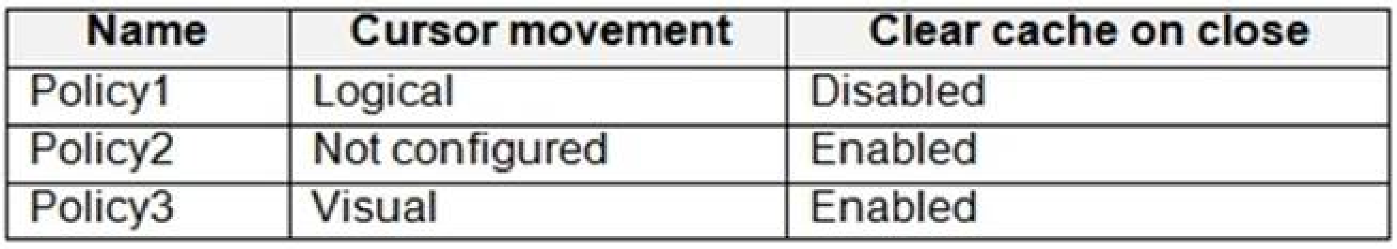
Name	Member of
User1	Group1, Group2
User2	Group2, Group3
User3	Group1, Group3

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



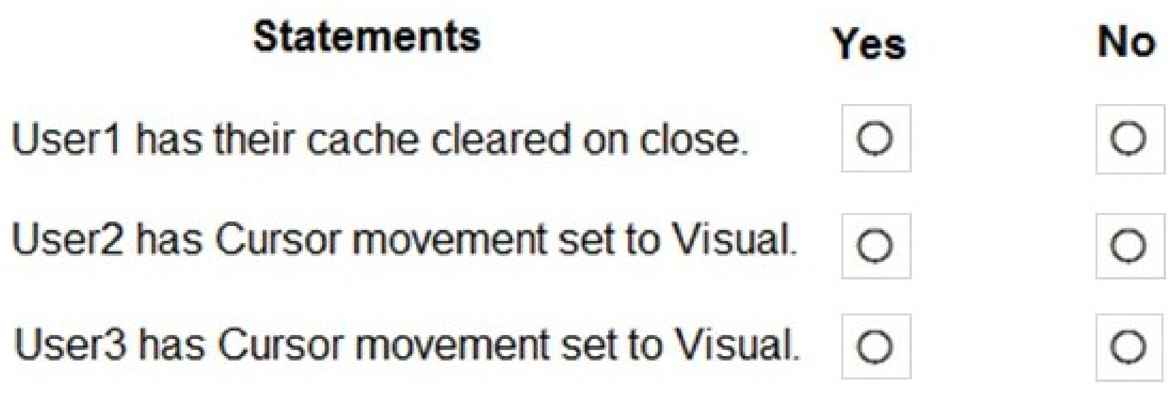
Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

The policies use the settings shown in the following table.



Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

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

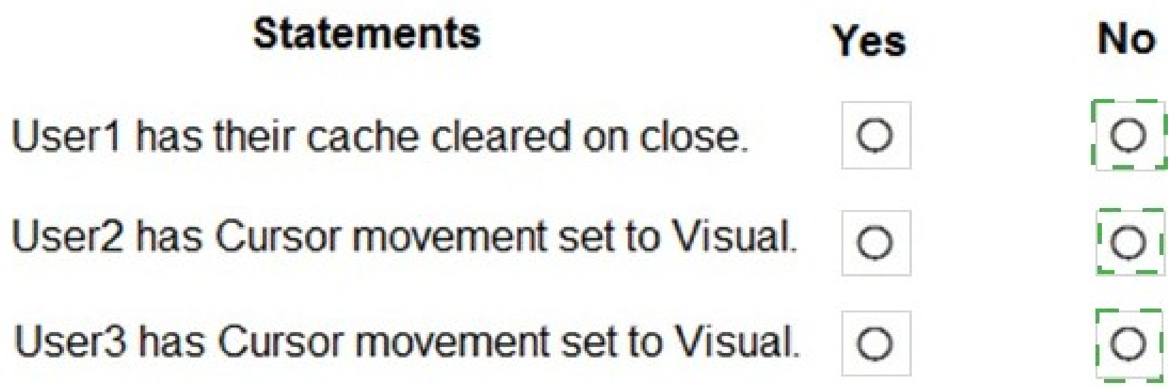


Statements	Yes	No
User1 has their cache cleared on close.	○	○
User2 has Cursor movement set to Visual.	○	○
User3 has Cursor movement set to Visual.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Statements	Yes	No
User1 has their cache cleared on close.	○	[✓ ○]
User2 has Cursor movement set to Visual.	○	[✓ ○]
User3 has Cursor movement set to Visual.	○	[✓ ○]

NEW QUESTION 98
- (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

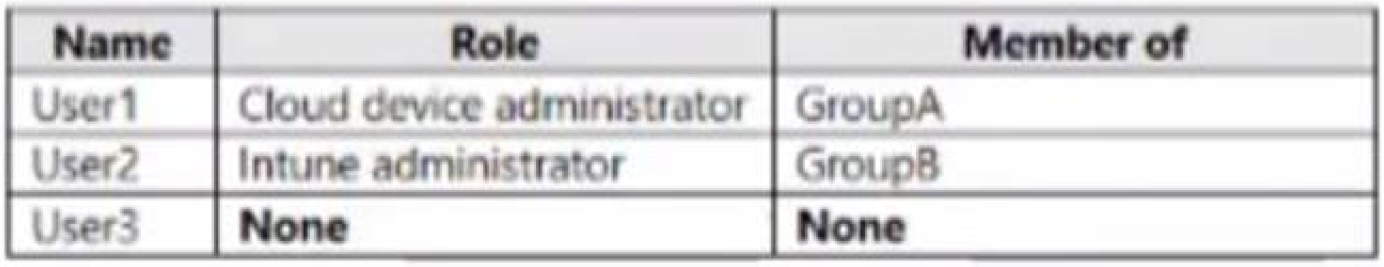
Explanation:
A: Classifiers
This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that 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 100
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You onboard all devices to Microsoft Defender for Endpoint
You need to use Defender for Endpoint to block access to a malicious website at www.contoso.com.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

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

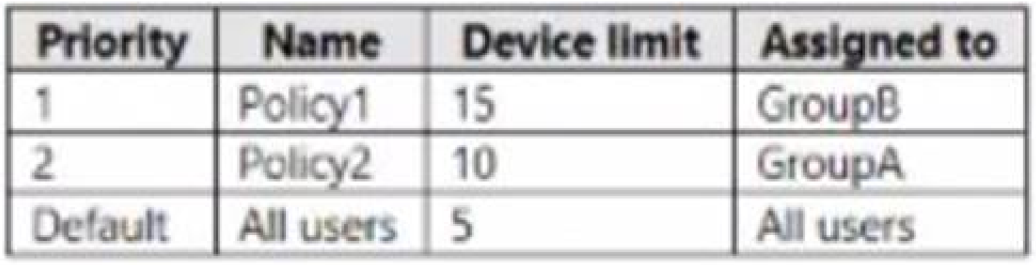
Answer: AC

NEW QUESTION 101
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.



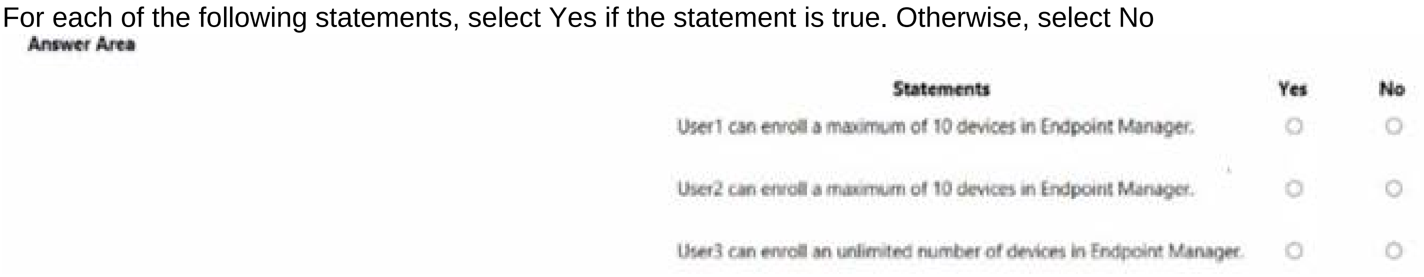
Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	None	None

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



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

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



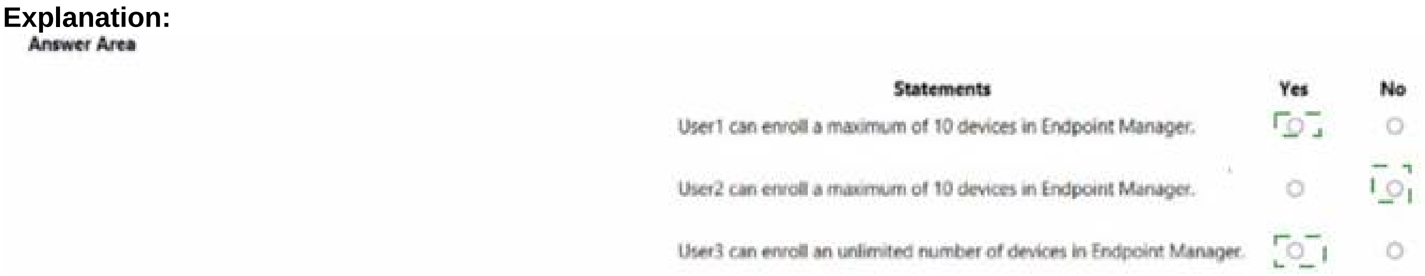
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

NEW QUESTION 105
- (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

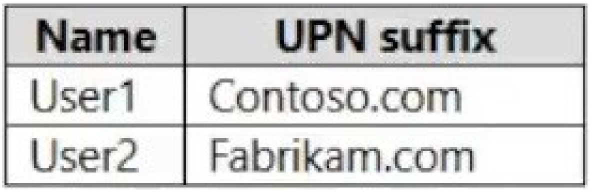
NEW QUESTION 108
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.
All the devices in your organization are onboarded to Microsoft Defender for Endpoint.
You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.
What should you do?

A. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
B. From Alerts queue, create a suppression rule and assign an alert.
C. From Advanced hunting, create a query and a detection rule.
D. From the Microsoft Purview compliance portal, create an audit log search.

Answer: C

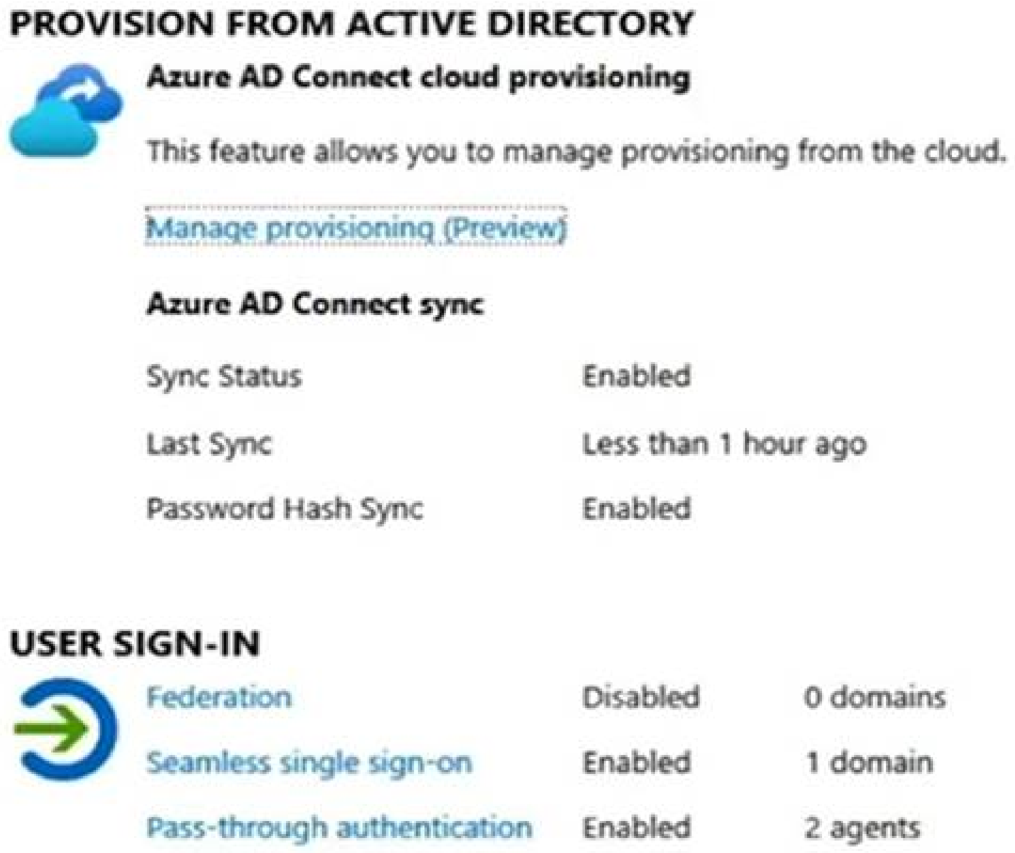
NEW QUESTION 112
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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.)



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

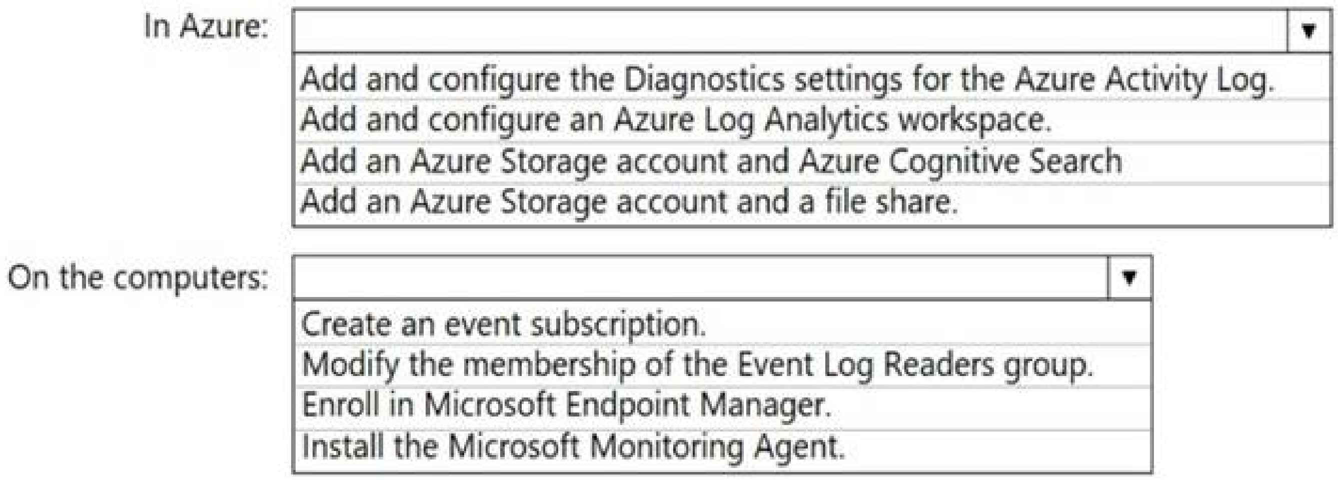
User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet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

A. Yes
B. No

Answer: A

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

NEW QUESTION 116
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.



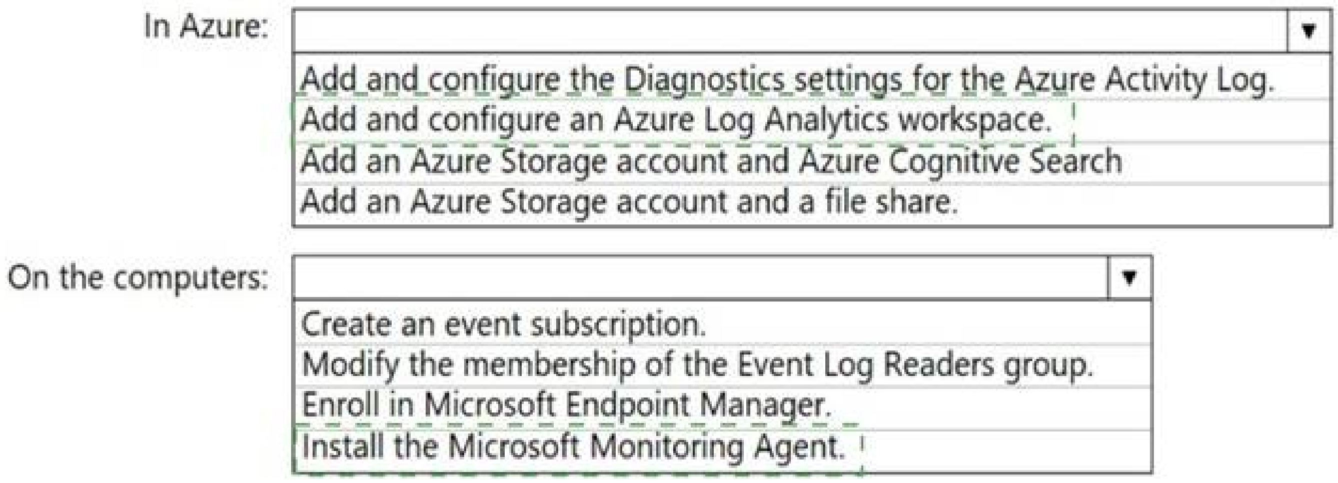
In Azure: ▼
- Add and configure the Diagnostics settings for the Azure Activity Log.
- Add and configure an Azure Log Analytics workspace.
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

On the computers: ▼
- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- Install the Microsoft Monitoring Agent.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



In Azure: ▼

Add and configure the Diagnostics settings for the Azure Activity Log.
[✓ Add and configure an Azure Log Analytics workspace.]
Add an Azure Storage account and Azure Cognitive Search
Add an Azure Storage account and a file share.

On the computers: ▼

Create an event subscription.
Modify the membership of the Event Log Readers group.
Enroll in Microsoft Endpoint Manager.
[✓ Install the Microsoft Monitoring Agent.]

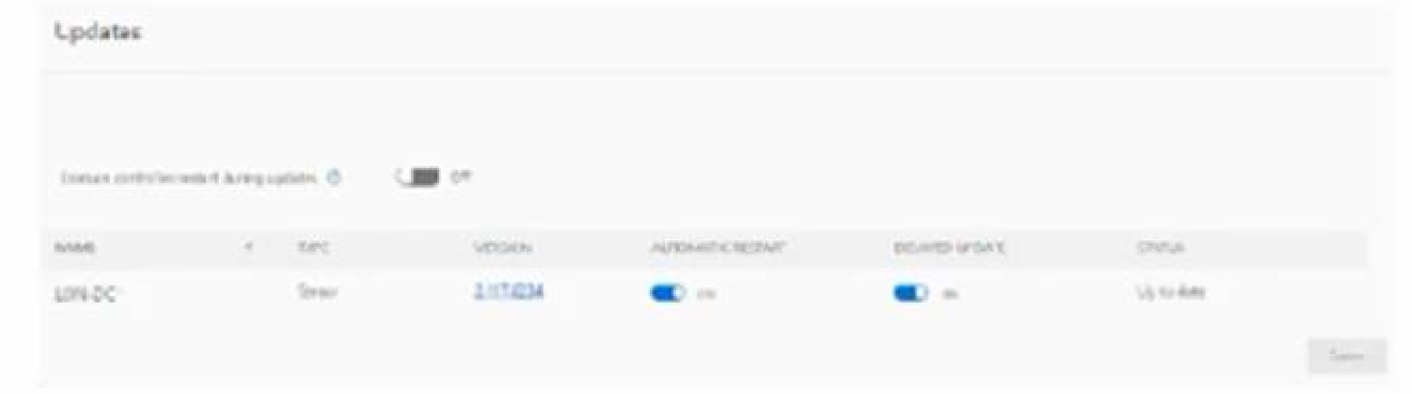
NEW QUESTION 117
- (Topic 6)
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.
Where can you store data from the LinkedIn connector?

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

Answer: C

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

NEW QUESTION 118
- (Topic 6)
You implement Microsoft Azure Advanced Threat Protection (Azure ATP). You have an Azure ATP sensor configured as shown in the following exhibit.



Updates

[illegible] Off

NAME	TYPE	VERSION	AUTOMATIC RESTART	DELAYED UPDATE	STATUS
LON-DC	Sensor	[illegible]	On	On	Up to date

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

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

Answer: B

NEW QUESTION 121
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 security center. Which Microsoft service source will appear on the Incidents page of the Microsoft 365
security center?

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

Answer: A

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

NEW QUESTION 124
- (Topic 6)

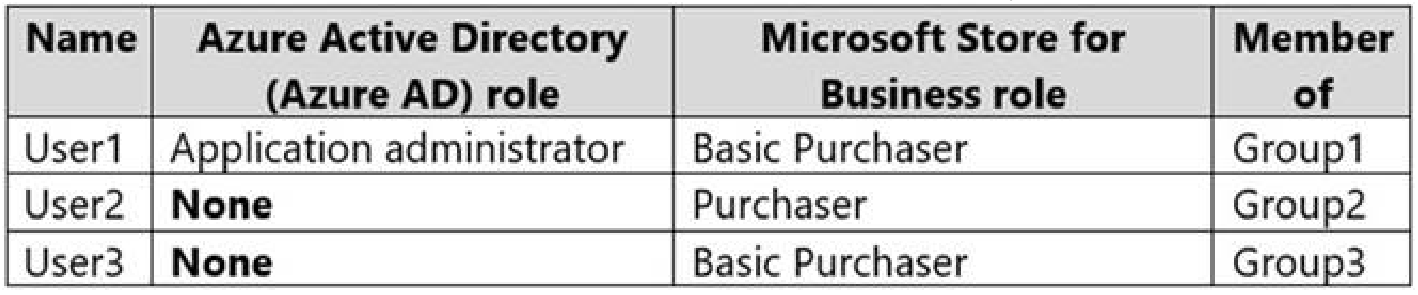
Your network contains an on-premises Active Directory domain named contoso.com.
For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.
You plan to sync contoso.com to an Azure AD tenant.
You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.
What should you include in the recommendation?

A. pass-through authentication
B. conditional access policies
C. password synchronization
D. Azure AD Identity Protection policies

Answer: A

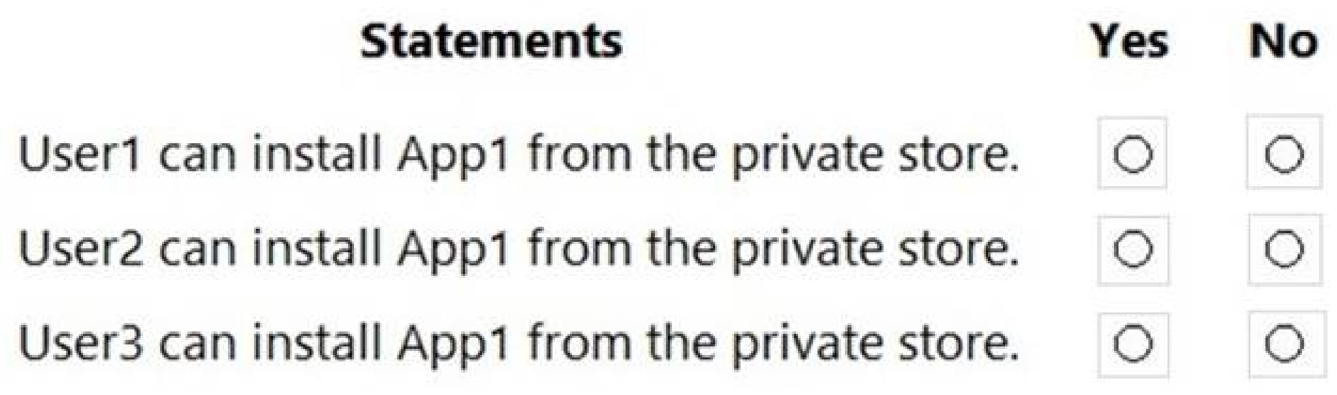
Explanation:
Reference:
https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

NEW QUESTION 125
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.

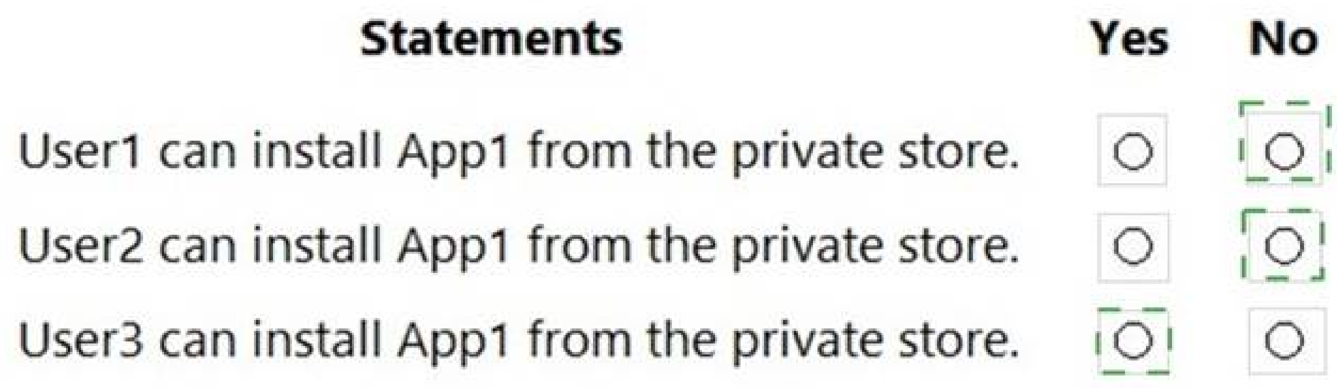


Statements	Yes	No
User1 can install App1 from the private store.	○	○
User2 can install App1 from the private store.	○	○
User3 can install App1 from the private store.	○	○

A. Mastered
B. Not Mastered

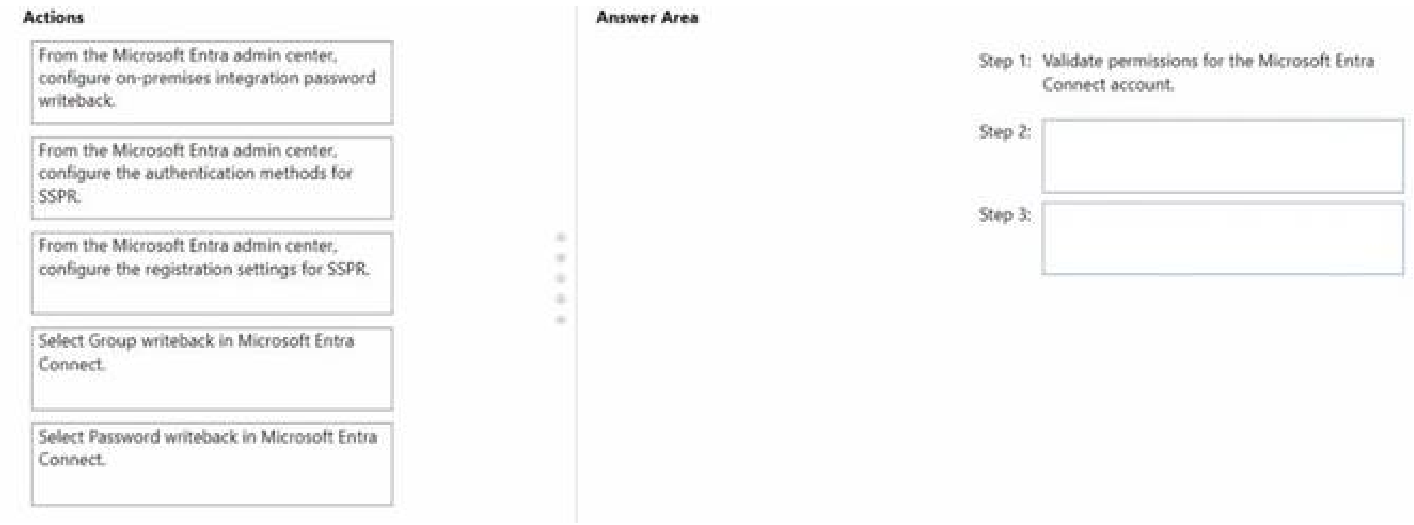
Answer: A

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 126
DRAG DROP - (Topic 6)
You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.
All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.
You plan to implement self-service password reset (SSPR).
You need to ensure that when a user resets or changes a password, the password syncs with AD DS.
Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Actions

From the Microsoft Entra admin center, configure on-premises integration password writeback.

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

Answer Area

Step 1: Validate permissions for the Microsoft Entra Connect account.

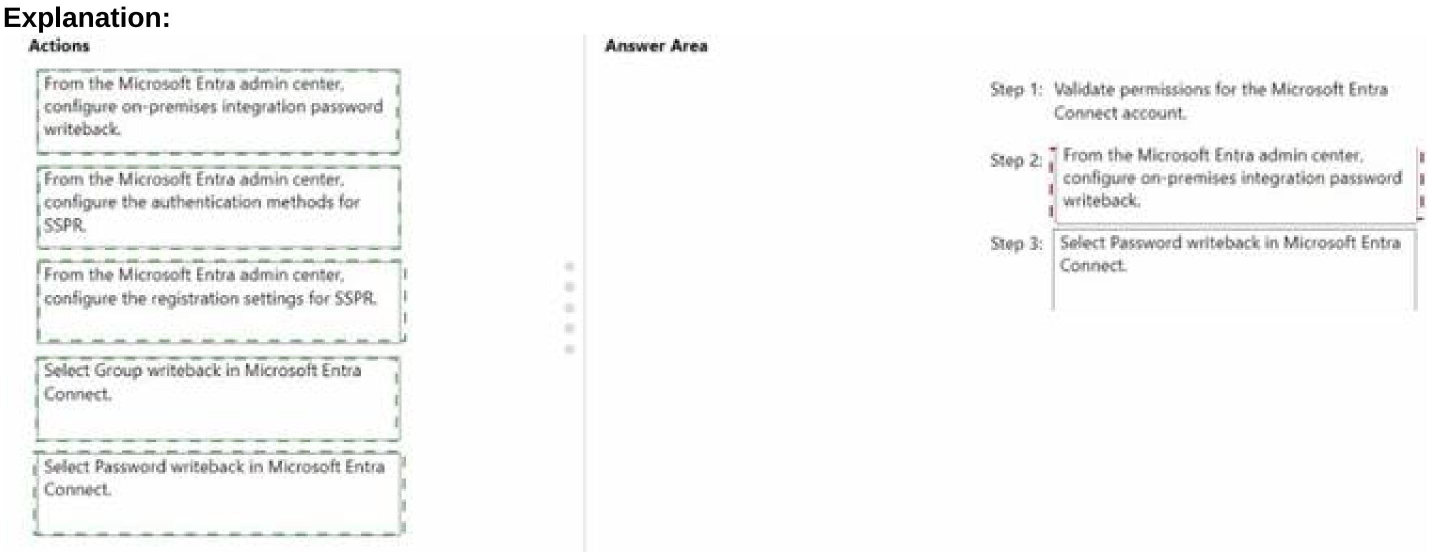
Step 2:

Step 3:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

From the Microsoft Entra admin center, configure on-premises integration password writeback.

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

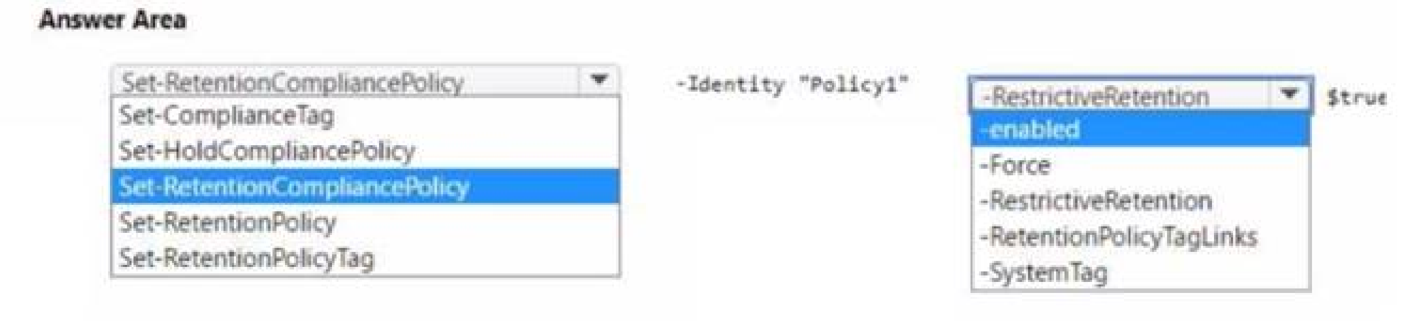
Answer Area

Step 1: Validate permissions for the Microsoft Entra Connect account.

Step 2: From the Microsoft Entra admin center, configure on-premises integration password writeback.

Step 3: Select Password writeback in Microsoft Entra Connect.

NEW QUESTION 128
HOTSPOT - (Topic 6)
From the Microsoft Purview compliance portal, you create a retention policy named Policy 1.
You need to prevent all users from disabling the policy or reducing the retention period. How should you configure the Azure PowerShell command? To answer select the
appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



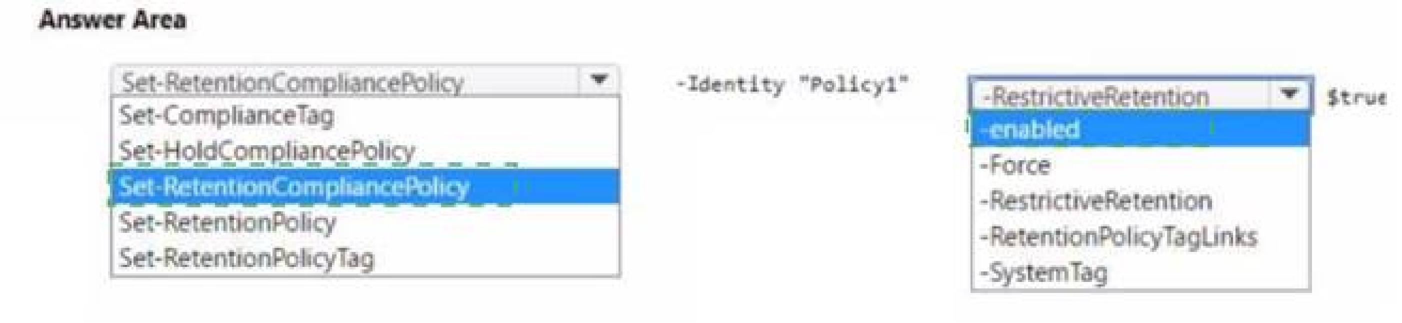
Answer Area

`Set-RetentionCompliancePolicy -Identity "Policy1" -RestrictiveRetention $true`

A. Mastered
B. Not Mastered

Answer: A

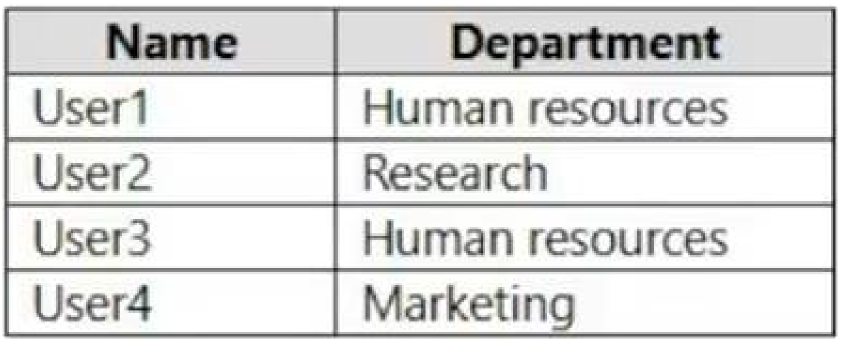
Explanation:



Answer Area

`Set-RetentionCompliancePolicy -Identity "Policy1" -RestrictiveRetention $true`

NEW QUESTION 132
- (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

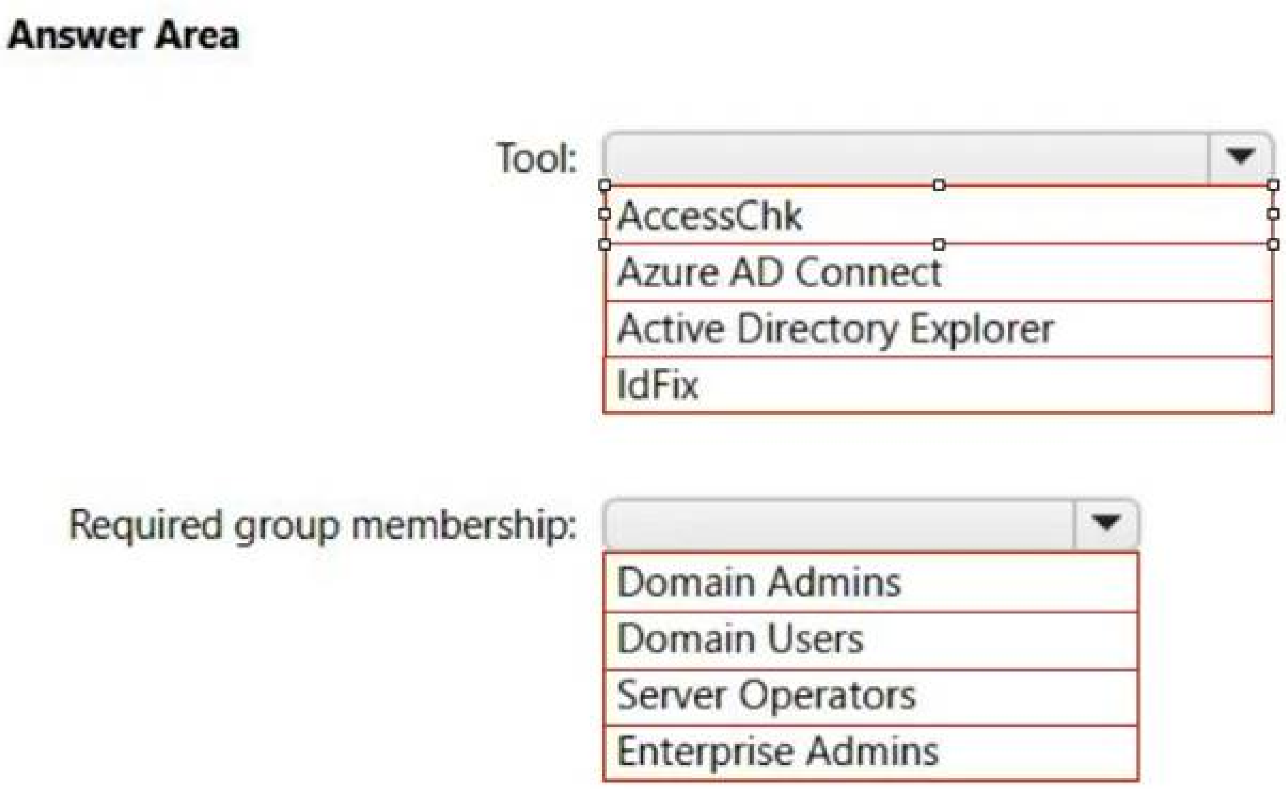
Explanation:
One for all users, one for the research department, and one for the marketing department.
Note: What are Deployment Groups?
With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. 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 135
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the
Security administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 137
HOTSPOT - (Topic 6)
HOTSPOT
Your network contains an on-premises Active Directory domain. You have a Microsoft 365 E5 subscription.
You plan to implement directory synchronization.
You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.
What should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

Tool:
- AccessChk
- Azure AD Connect
- Active Directory Explorer
- IdFix

Required group membership:
- Domain Admins
- Domain Users
- Server Operators
- Enterprise Admins

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: IdFix
Query and fix invalid object attributes with the IdFix tool
Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft 365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization tools such as Azure AD Connect and Azure AD Connect cloud sync. The focus of IdFix is to enable you to accomplish this task in a simple, expedient fashion.
The IdFix tool provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Window’s Server AD forests in preparation for deployment to Microsoft 365. The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow you to successfully synchronize users, contacts, and groups from on-premises Active Directory into Microsoft 365. Note: IdFix might identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be synchronized to the cloud, the product group recommends that these errors be corrected.
Incorrect:
* AccessChk
Box 2: Enterprise Admins
IdFix permissions requirements
The user account that you use to run IdFix must have read and write access to the AD DS domain.
If you aren’t sure if your user account meets these requirements, and you’re not sure how to check, you can still download and run IdFix. If your user account doesn’t have the right permissions, IdFix will simply display an error when you try to run it.
* Enterprise Admins
The Enterprise Admins group exists only in the root domain of an Active Directory forest of domains. The group is a Universal group if the domain is in native mode. The group is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, like adding child domains.
Incorrect:
* Domain Admins
Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that's created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.
* Server Operator
Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer. Any service that accesses the system has the Service identity.
* Domain Users - too few permissions
The Domain Users group includes all user accounts in a domain. When you create a user account in a domain, it's automatically added to this group.

NEW QUESTION 142
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
You need to assign the Security Administrator role. Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp

NEW QUESTION 145
- (Topic 6)
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.
Does this meet the goal?

A. Yes
B. No

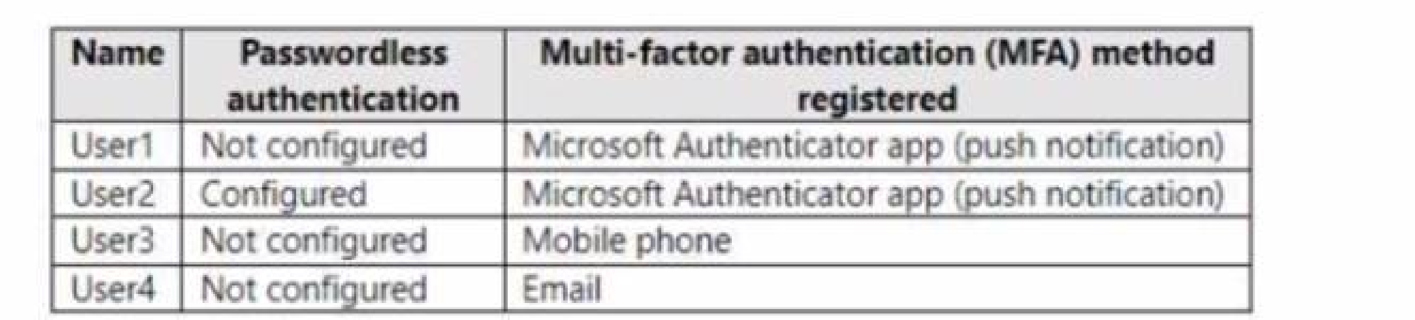
Answer: A

NEW QUESTION 148
- (Topic 6)
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant includes a user named User1.
You enable Azure AD Identity Protection.
You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.
To which role should you add User1?

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

Answer: A

NEW QUESTION 151
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



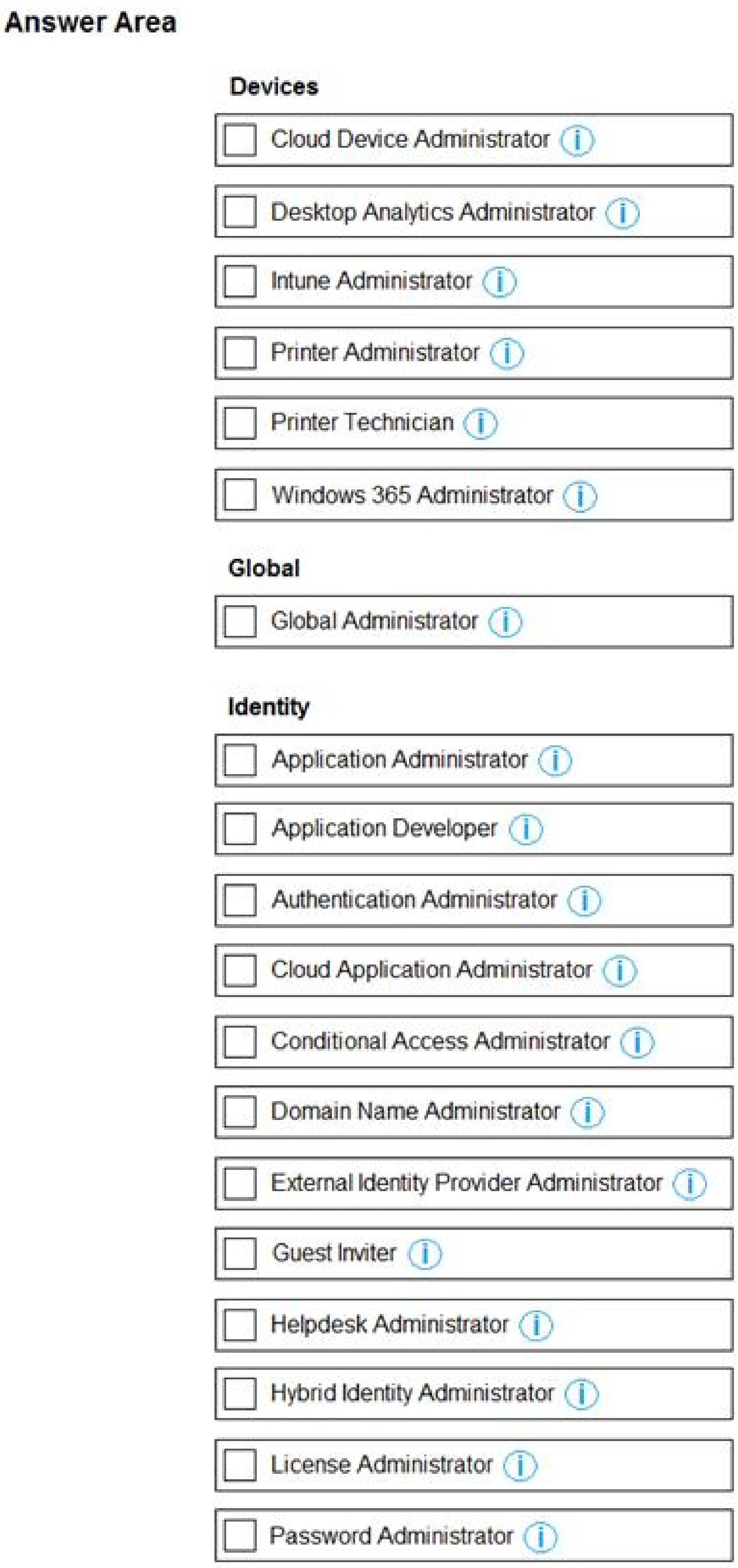
Name	Passwordless authentication	Multi-factor authentication (MFA) method registered
User1	Not configured	Microsoft Authenticator app (push notification)
User2	Configured	Microsoft Authenticator app (push notification)
User3	Not configured	Mobile phone
User4	Not configured	Email

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 156
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 ⓘ

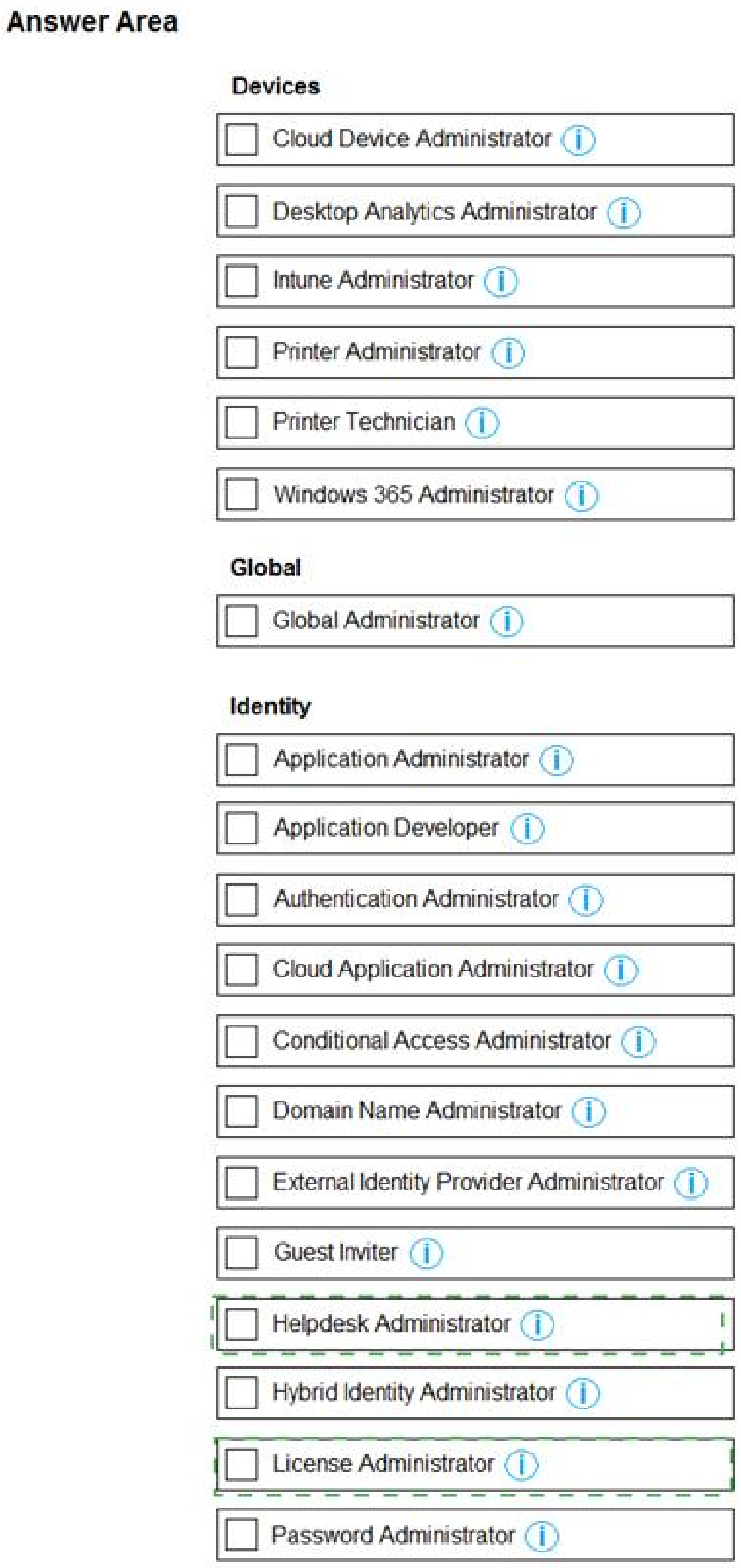
Identity

- □ 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 157
- (Topic 6)
You have Windows 10 devices that are managed by using Microsoft Endpoint Manager. You need to configure the security settings in Microsoft Edge.
What should you create in Microsoft Endpoint Manager?

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

Answer: C

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

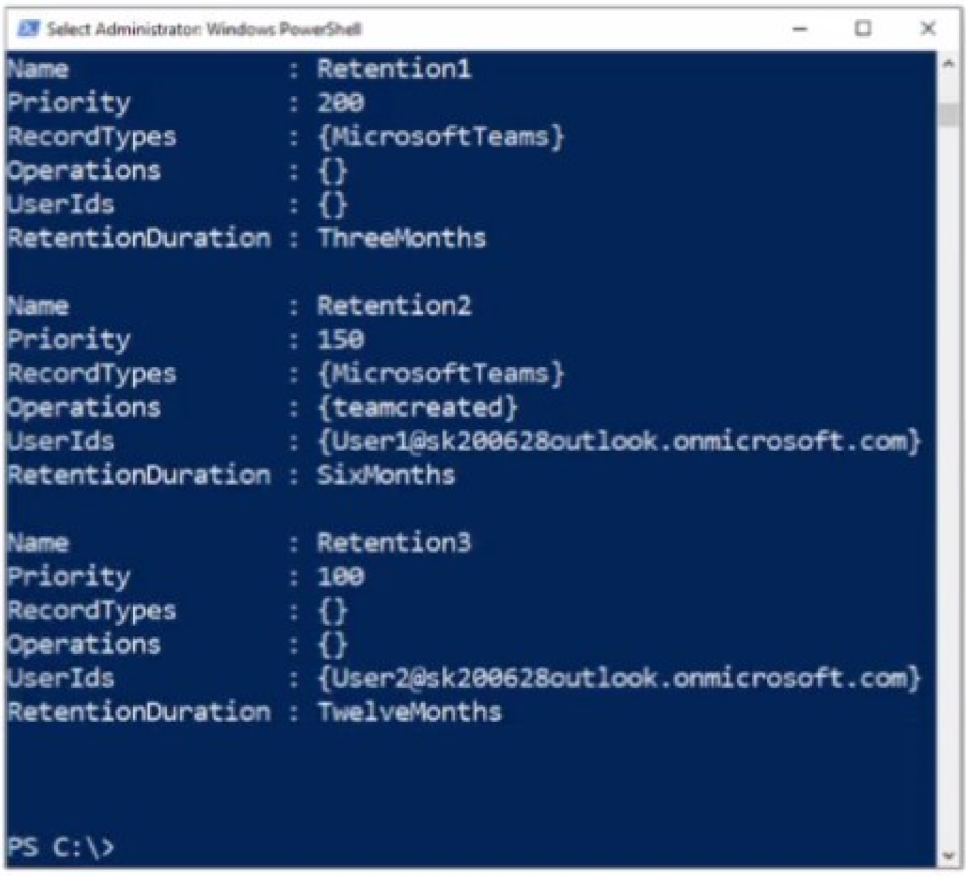
NEW QUESTION 159
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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

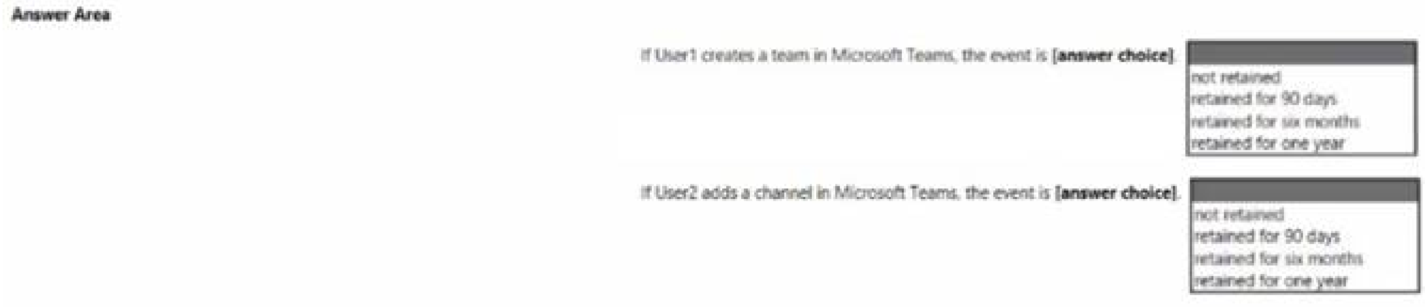
Answer: B

NEW QUESTION 160
HOTSPOT - (Topic 6)
You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.



```
Name              : Retention1
Priority          : 200
RecordTypes       : {MicrosoftTeams}
Operations        : {}
UserIds           : {}
RetentionDuration : ThreeMonths

Name              : Retention2
Priority          : 150
RecordTypes       : {MicrosoftTeams}
Operations        : {teamcreated}
UserIds           : {User1@sk200628outlook.onmicrosoft.com}
RetentionDuration : SixMonths

Name              : Retention3
Priority          : 100
RecordTypes       : {}
Operations        : {}
UserIds           : {User2@sk200628outlook.onmicrosoft.com}
RetentionDuration : TwelveMonths


PS C:\>
```

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

If User1 creates a team in Microsoft Teams, the event is [**answer choice**].

not retained
retained for 90 days
retained for six months
retained for one year

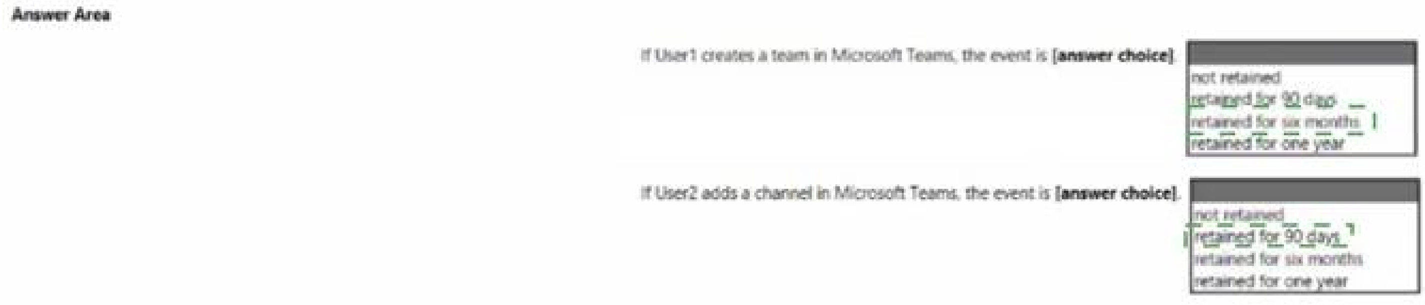
If User2 adds a channel in Microsoft Teams, the event is [**answer choice**].

not retained
retained for 90 days
retained for six months
retained for one year

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

If User1 creates a team in Microsoft Teams, the event is [**answer choice**].

not retained
retained for 90 days
retained for six months
retained for one year

If User2 adds a channel in Microsoft Teams, the event is [**answer choice**].

not retained
retained for 90 days
retained for six months
retained for one year

NEW QUESTION 164
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it as a result these questions will not appear in the review screen.
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

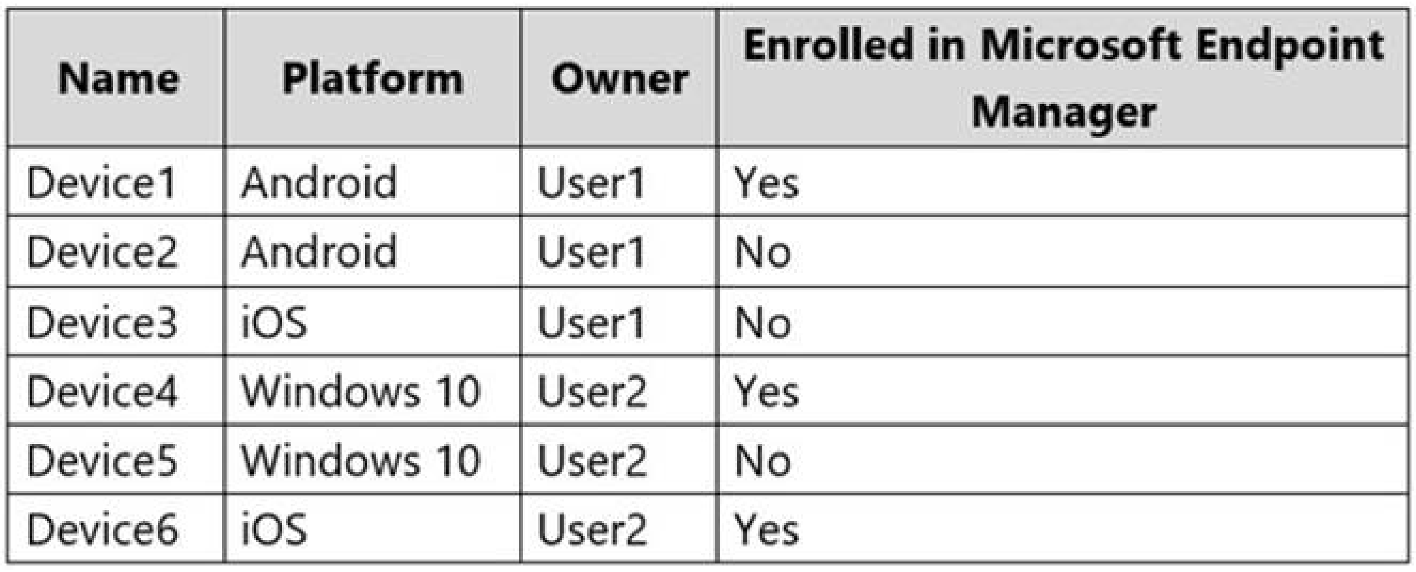
Answer: B

NEW QUESTION 168
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.
Which two policies can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 171
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users have the devices shown in the following table.



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

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

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

Answer: C

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

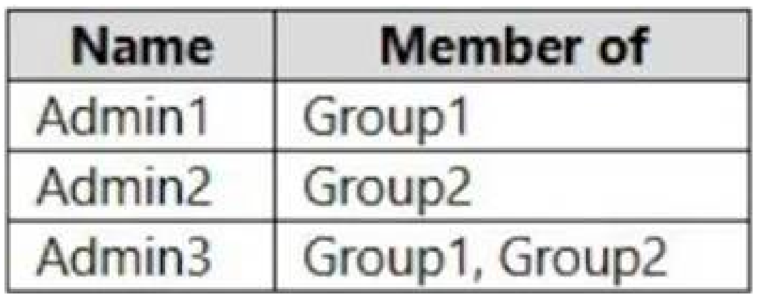
NEW QUESTION 175
- (Topic 6)
You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:
• Windows 10
• Android
• OS
On which devices can you configure the Endpoint DLP policies?

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

Answer: D

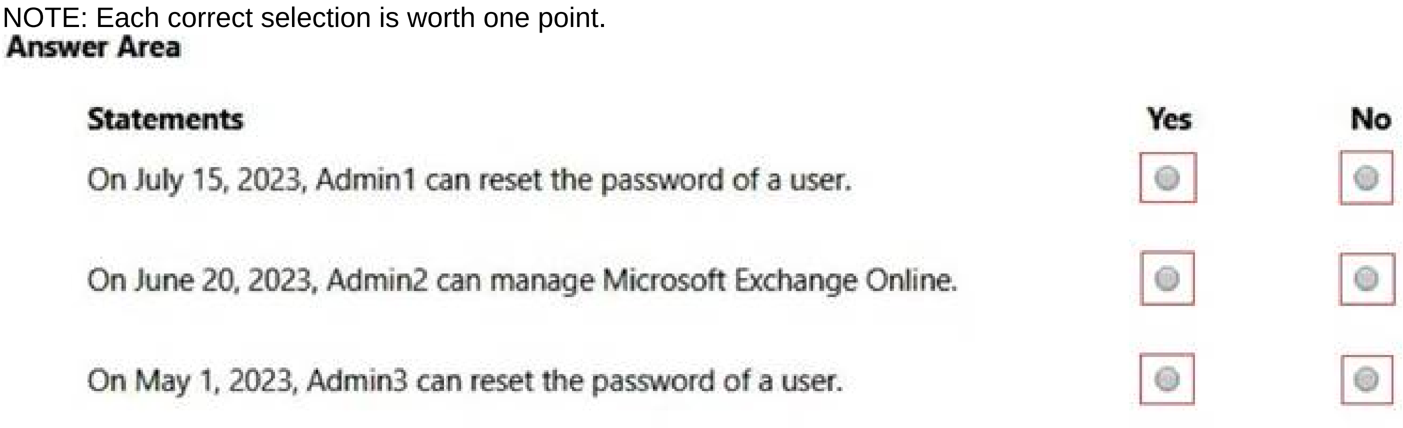
Explanation:
Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions,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

NEW QUESTION 179
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:
? Scope type: Directory
? Selected members: Group1
? Assignment type: Active
? Assignment starts: Mar 15, 2023
? Assignment ends: Aug 15, 2023
You add the following assignment for the Exchange Administrator role:
? Scope type: Directory
? Selected members: Group2
? Assignment type: Eligible
? Assignment starts: Jun 15, 2023
? Assignment ends: Oct 15, 2023
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer Area

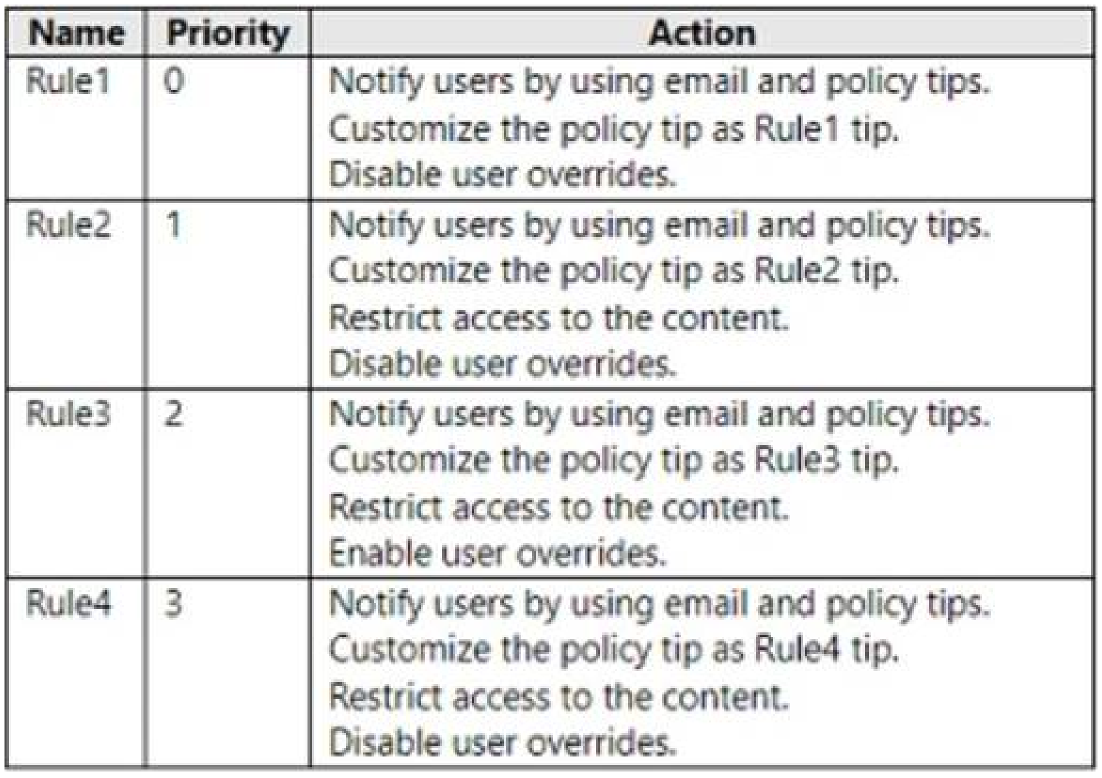
Statements	Yes	No
On July 15, 2023, Admin1 can reset the password of a user.	○	○
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	○	○
On May 1, 2023, Admin3 can reset the password of a user.	○	○

A. Mastered
B. Not Mastered

Answer: A

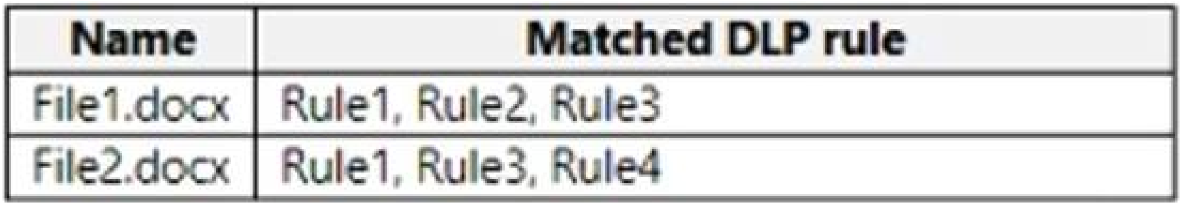
Explanation:
Box 1: Yes
Admin1 is member of Group1.
The User Administrator role assignment has Group1 as a member. The assignment type: Active
July 15, 2023 is with the assignment period.
A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.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

NEW QUESTION 183
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.



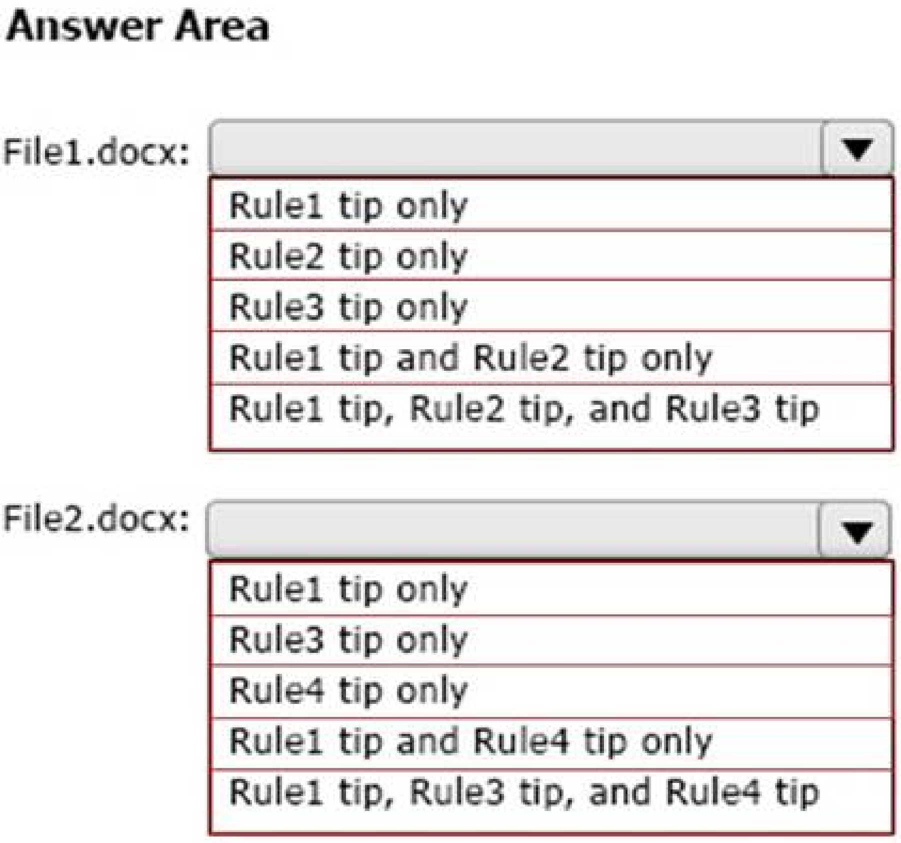
Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users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

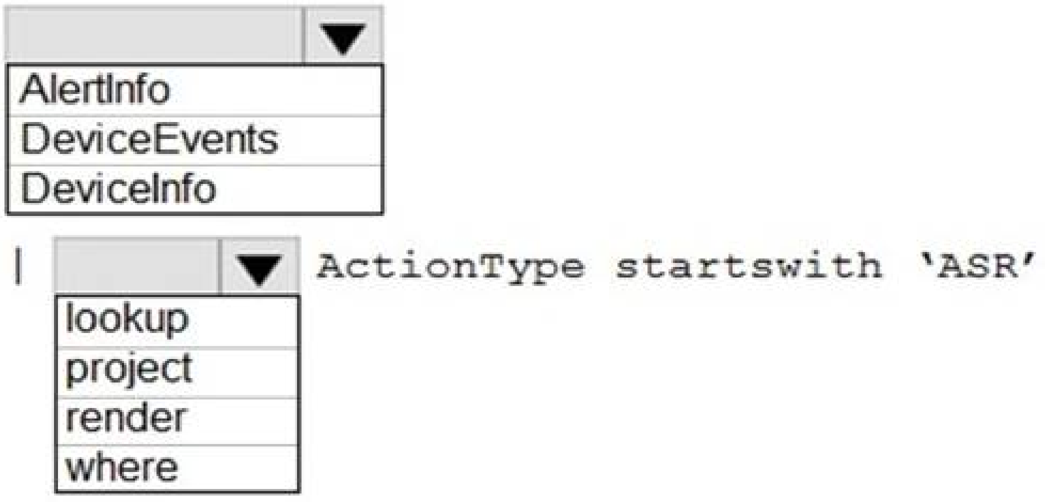
A. Mastered
B. Not Mastered

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 188
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices. You plan to attack surface reduction (ASR) rules for the Windows 10 devices.
You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.
You need to find the ASR rules that match the activities on the devices.
How should you complete the Kusto query? To answer, select the appropriate options in

the answer area.
NOTE: Each correct selection is worth one point.



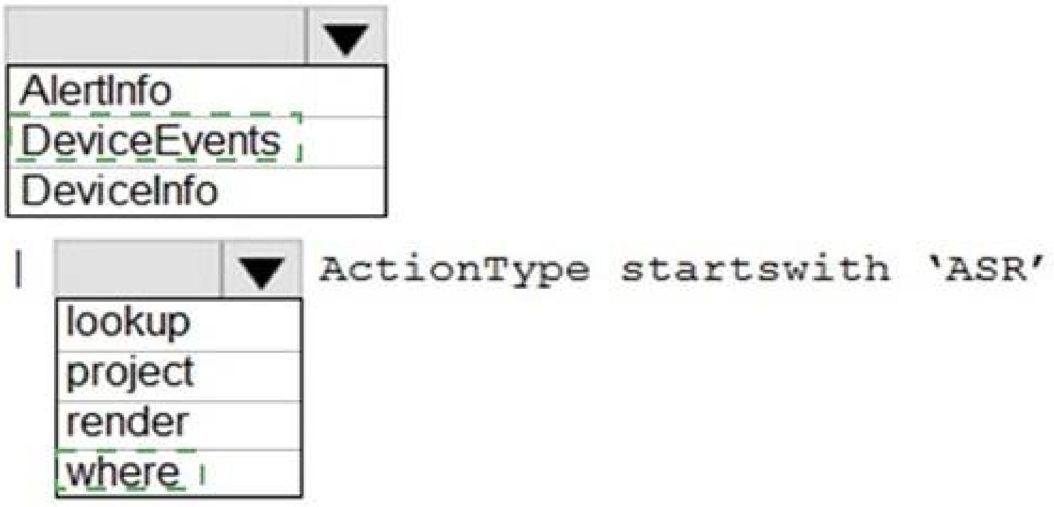
AlertInfo
DeviceEvents
DeviceInfo

| lookup / project / render / where ActionType startswith 'ASR'

A. Mastered
B. Not Mastered

Answer: A

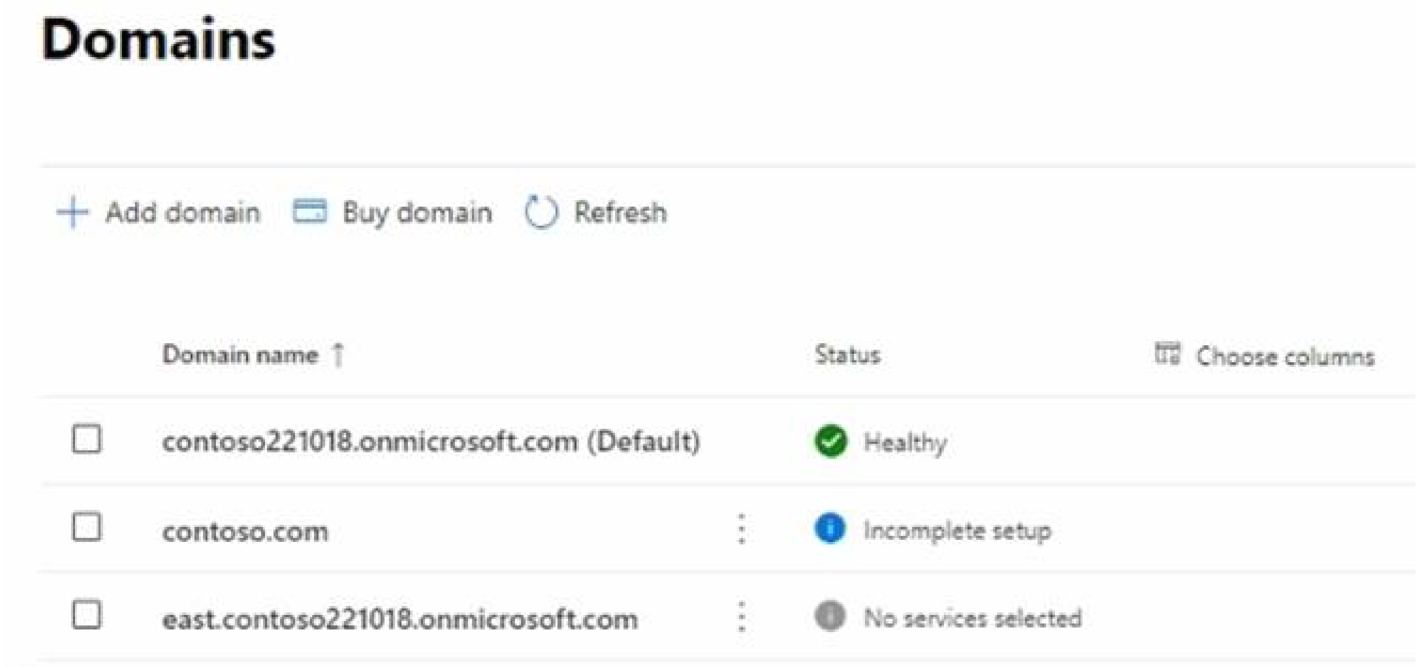
Explanation:



AlertInfo
DeviceEvents
DeviceInfo

| lookup / project / render / where ActionType startswith 'ASR'

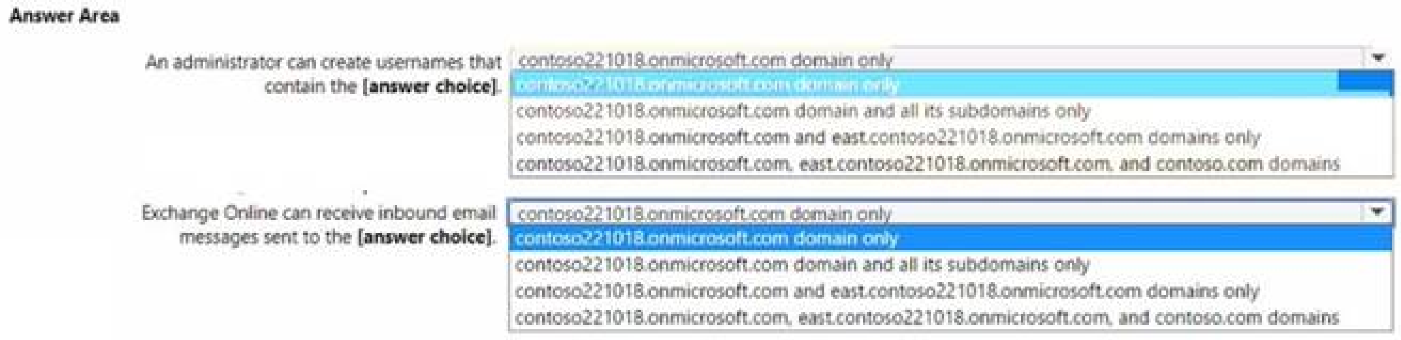
NEW QUESTION 193
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 subscription That contains the domains shown in the following exhibit.



Domains

Domain name ↑	Status
contoso221018.onmicrosoft.com (Default)	✓ Healthy
contoso.com	Incomplete setup
east.contoso221018.onmicrosoft.com	No services selected

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

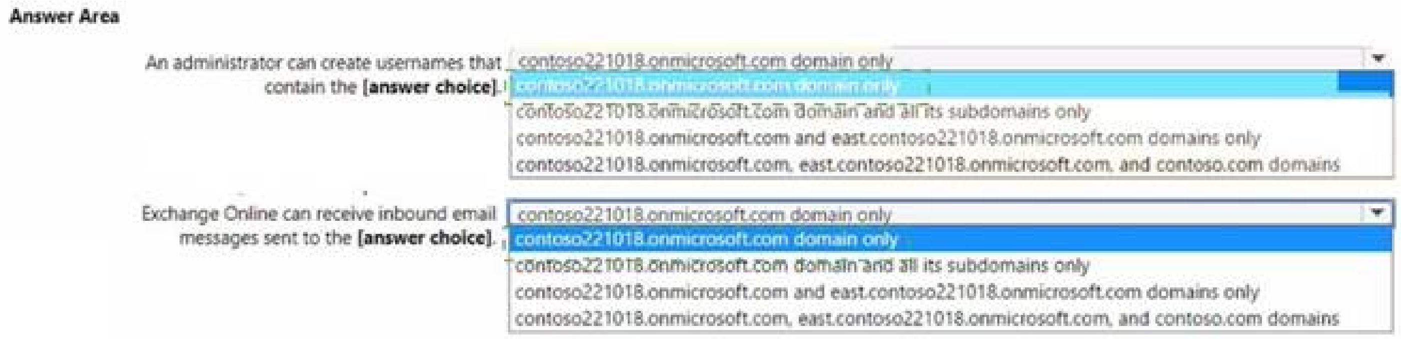
An administrator can create usernames that contain the **[answer choice]**.
- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain and all its subdomains only
- contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
- contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

Exchange Online can receive inbound email messages sent to the **[answer choice]**.
- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain and all its subdomains only
- contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
- contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

An administrator can create usernames that contain the **[answer choice]**.

- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain and all its subdomains only
- contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
- contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

Exchange Online can receive inbound email messages sent to the **[answer choice]**.

- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain and all its subdomains only
- contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
- contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

NEW QUESTION 194

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription.

All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.

You need to configure Defender for Endpoint to meet the following requirements:

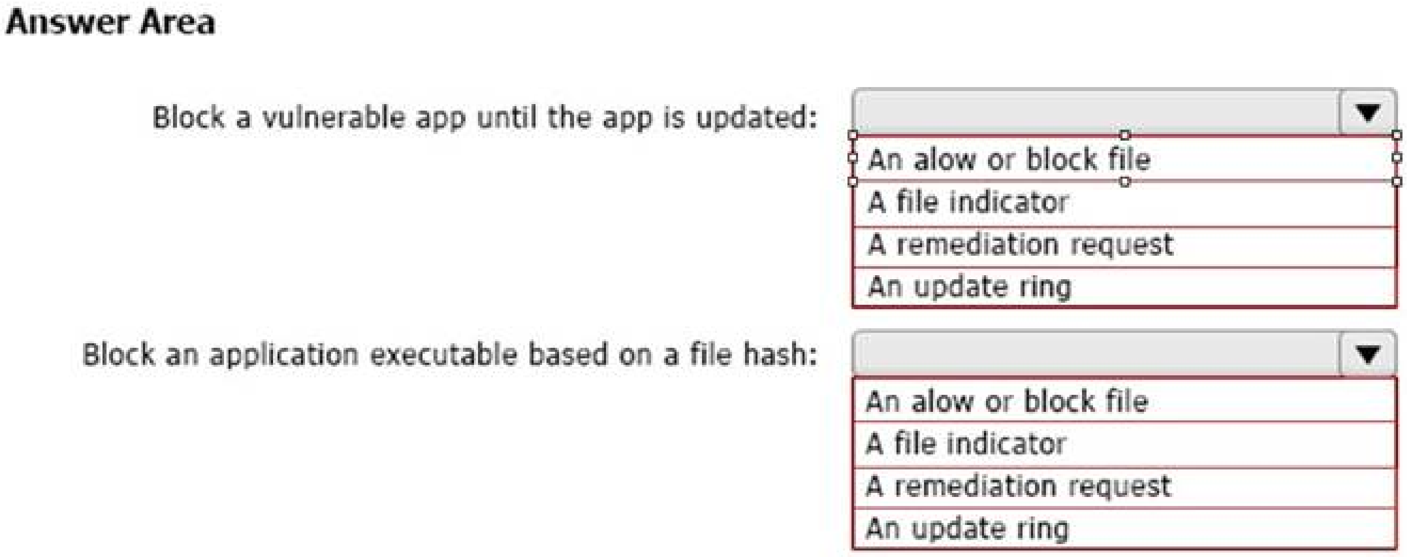
? Block a vulnerable app until the app is updated.

? Block an application executable based on a file hash.

The solution must minimize administrative effort.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

Block a vulnerable app until the app is updated:

- An alow or block file
- A file indicator
- A remediation request
- An update ring

Block an application executable based on a file hash:

- An alow or block file
- A file indicator
- A remediation request
- An update ring

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: A remediation request

Block a vulnerable app until the app is updated.

Block vulnerable applications

How to block vulnerable applications

? Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.

? Select a security recommendation to see a flyout with more information.

? Select Request remediation.

? Select whether you want to apply the remediation and mitigation to all device groups or only a few.

? Select the remediation options on the Remediation request page. The remediation options are software update, software uninstall, and attention required.

? Pick a Remediation due date and select Next.

? Under Mitigation action, select Block or Warn. Once you submit a mitigation action, it is immediately applied.

? Review the selections you made and Submit request. On the final page you can

choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.

Box 2: A file indicator

Block an application executable based on a file hash.

While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.

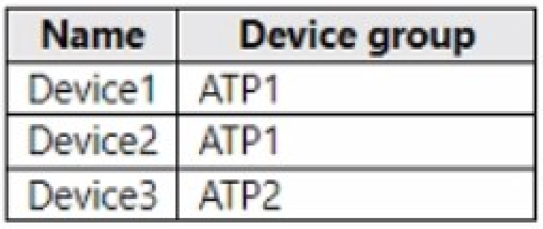
The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

NEW QUESTION 195

HOTSPOT - (Topic 6)

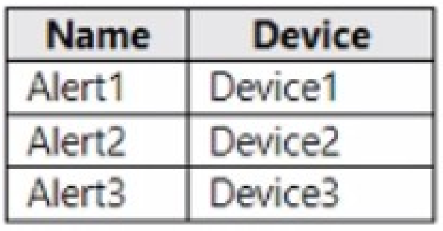
Your company uses Microsoft Defender for Endpoint.

The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.



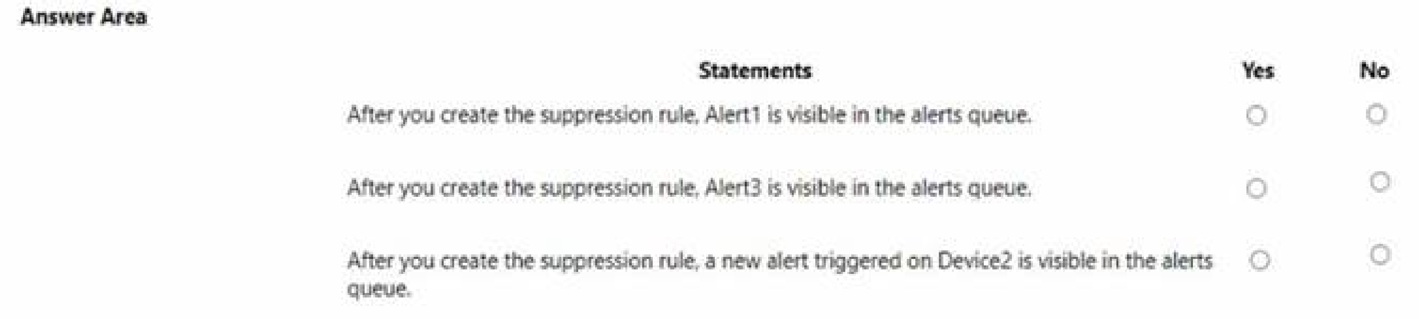
Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

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



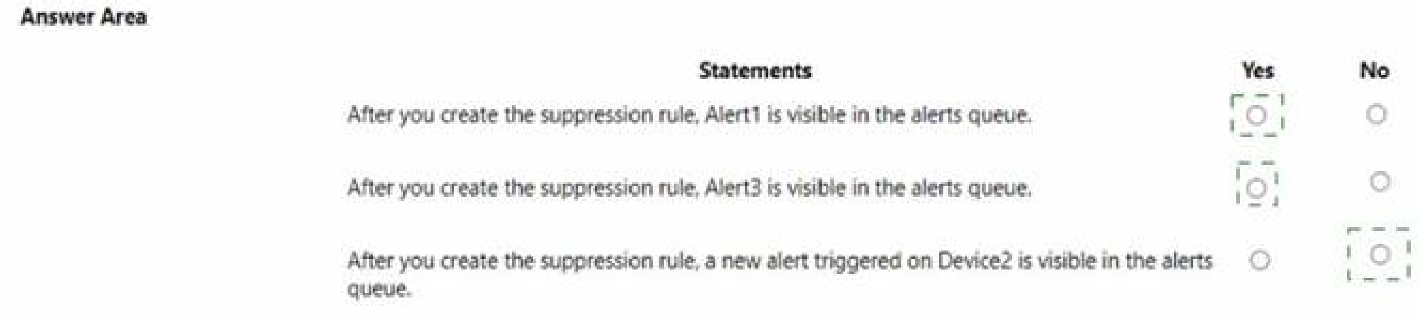
Answer Area

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.	○	[✓ ○]

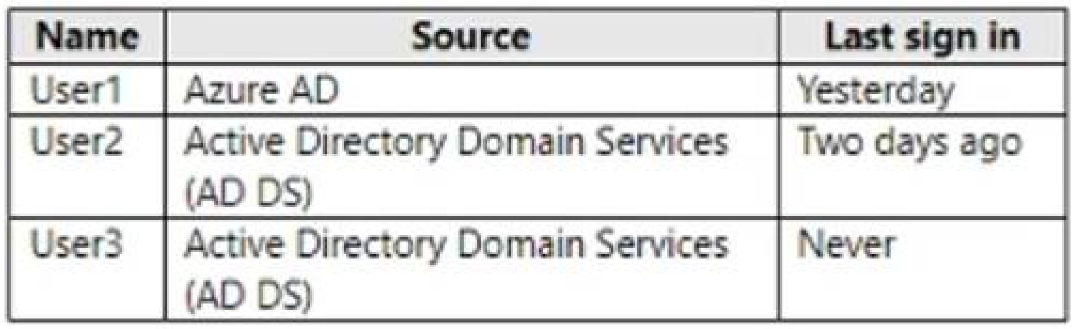
NEW QUESTION 198
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 203
- (Topic 6)
You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.



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

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

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

Answer: D

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

NEW QUESTION 208
- (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

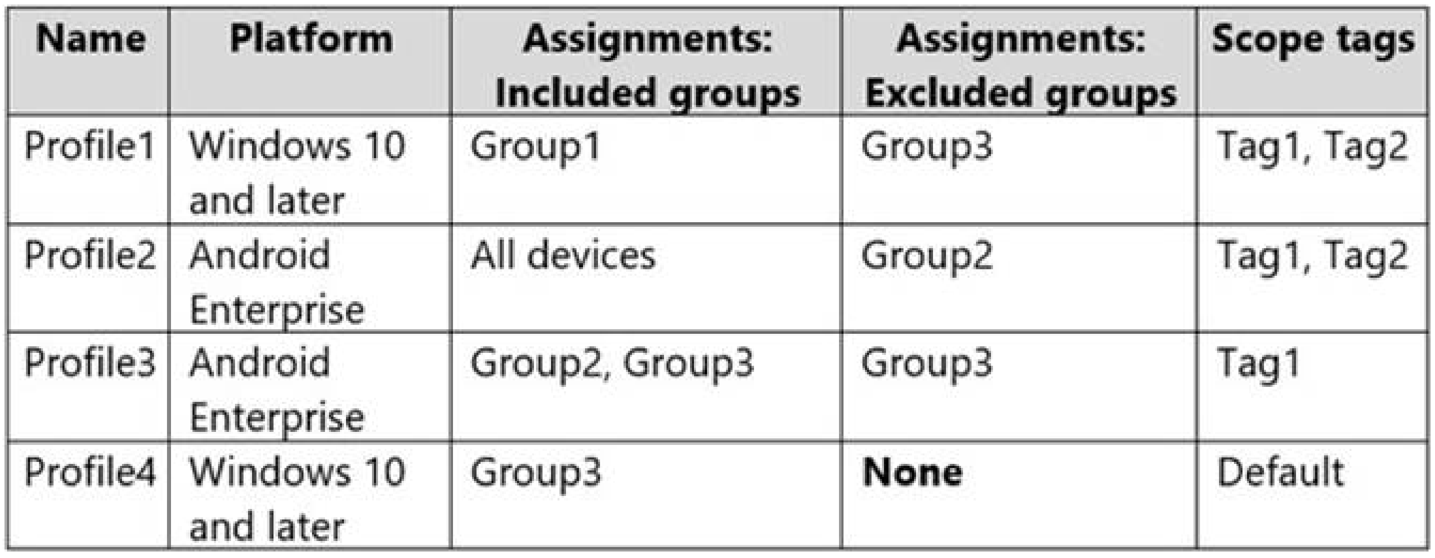
Explanation:
Reference:
https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

NEW QUESTION 209
- (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

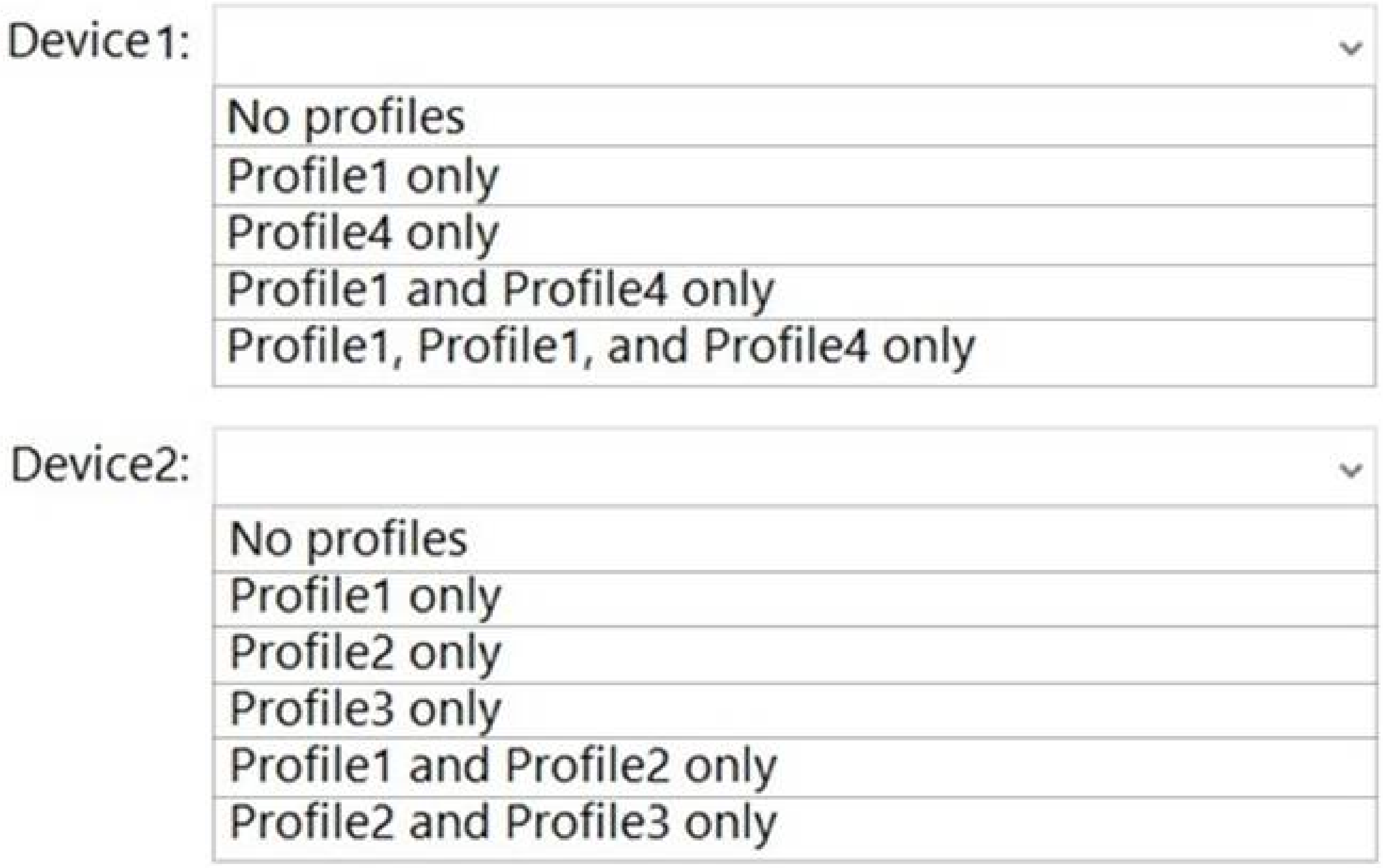
Answer: B

NEW QUESTION 211
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.



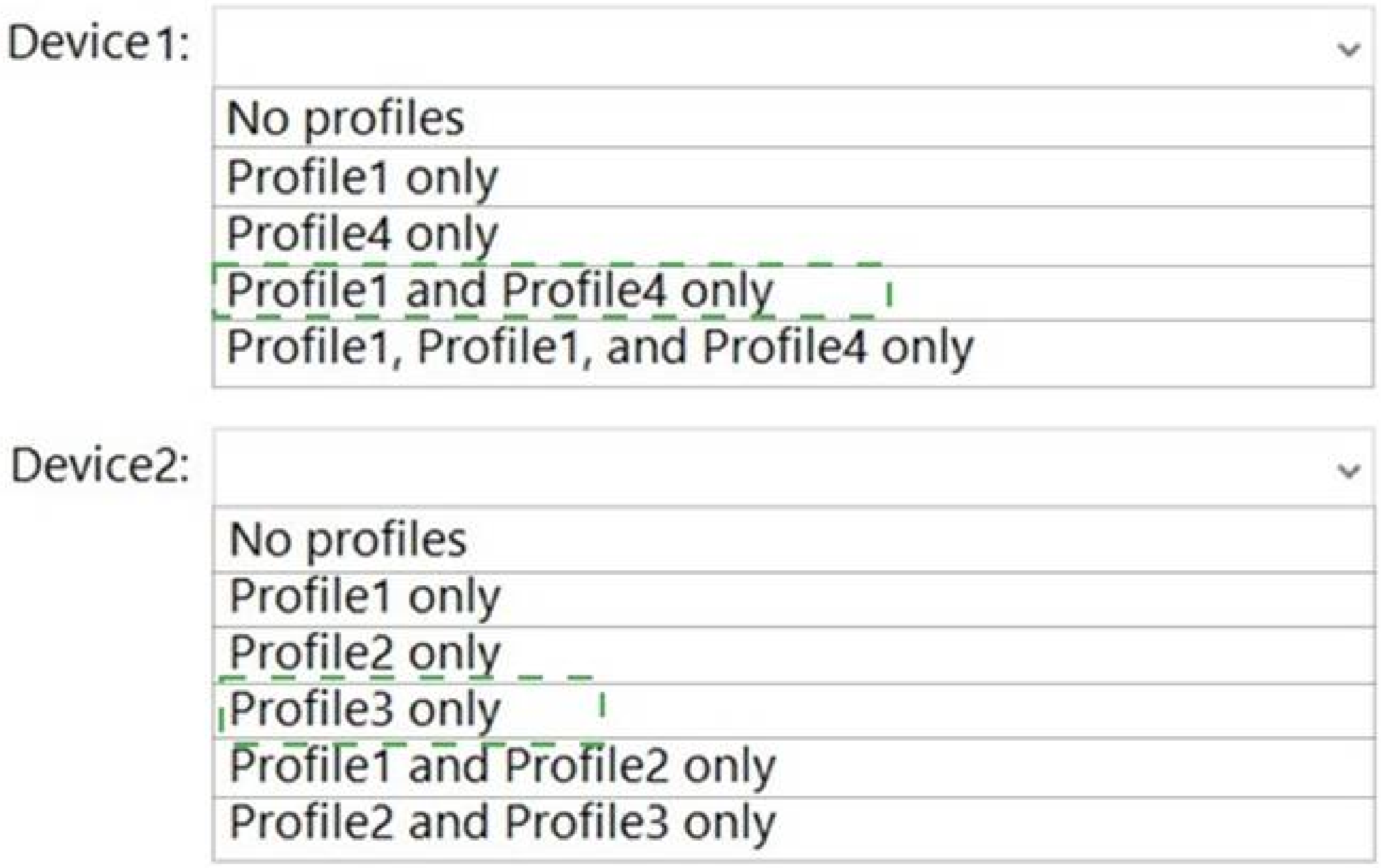
Device1:
No profiles
Profile1 only
Profile4 only
Profile1 and Profile4 only
Profile1, Profile1, and Profile4 only

Device2:
No profiles
Profile1 only
Profile2 only
Profile3 only
Profile1 and Profile2 only
Profile2 and Profile3 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:

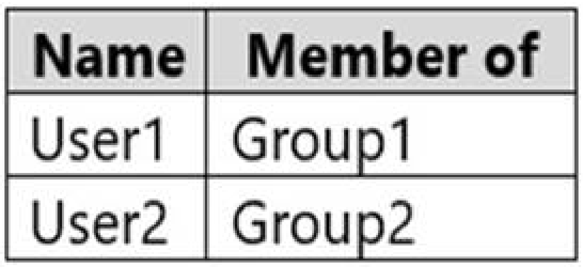


Device1:
No profiles
Profile1 only
Profile4 only
[✓ Profile1 and Profile4 only]
Profile1, Profile1, and Profile4 only

Device2:
No profiles
Profile1 only
Profile2 only
[✓ Profile3 only]
Profile1 and Profile2 only
Profile2 and Profile3 only

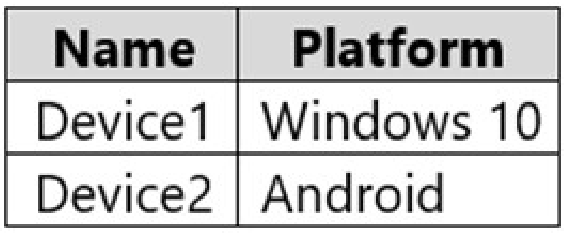
NEW QUESTION 215

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



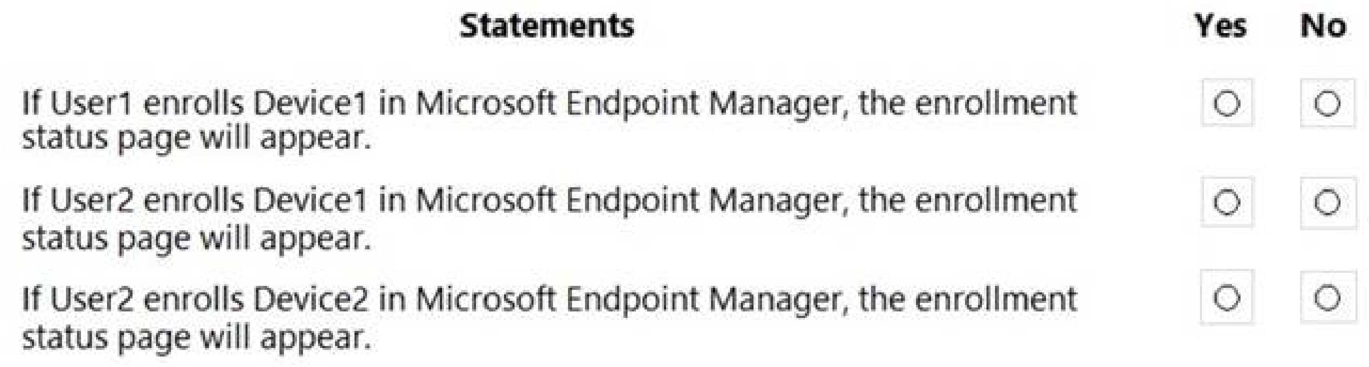
Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:
? Show app and profile configuration progress: Yes
? Allow users to collect logs about installation errors: Yes
? Only show page to devices provisioned by out-of-box experience (OOBE): No
? Assignments: Group2
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

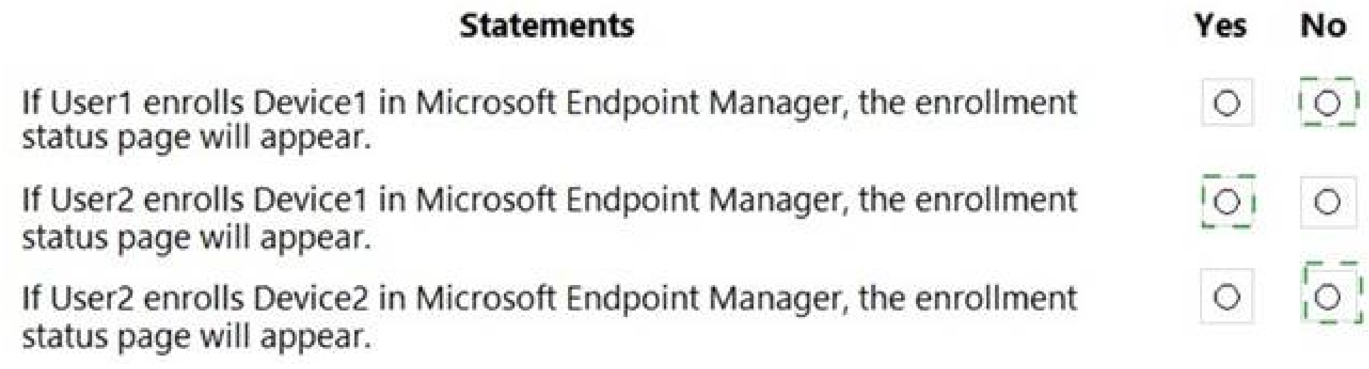


Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page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

A. Mastered
B. Not Mastered

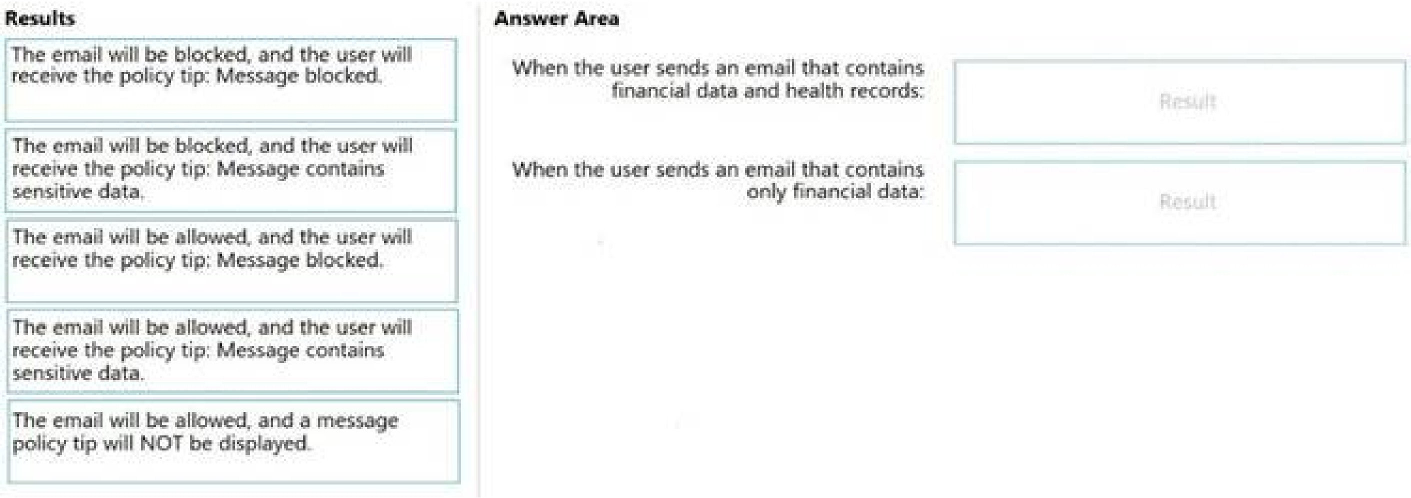
Answer: A

Explanation:



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

NEW QUESTION 216
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 subscription.
In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:
? Block emails that contain financial data.
? Display the following policy tip text: Message blocked.
From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:
? Use the following location: Exchange email.
? Display the following policy tip text: Message contains sensitive data.
? When a user sends an email, notify the user if the email contains health records.
What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Results

- The email will be blocked, and the user will receive the policy tip: Message blocked.
- The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.
- The email will be allowed, and the user will receive the policy tip: Message blocked.
- The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.
- The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records: Result

When the user sends an email that contains only financial data: Result

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked. If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.
Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

NEW QUESTION 218
- (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 223
- (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

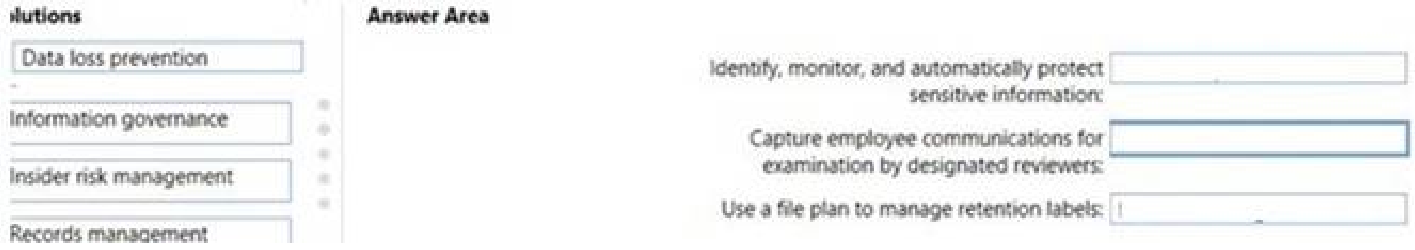
Answer: B

NEW QUESTION 225
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 E5 tenant.
You need to implement compliance solutions that meet the following requirements:

- Use a file plan to manage retention labels.
- Identify, monitor, and automatically protect sensitive information.
- Capture employee communications for examination by designated reviewers.

Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



lutions

- Data loss prevention
- Information governance
- Insider risk management
- Records management

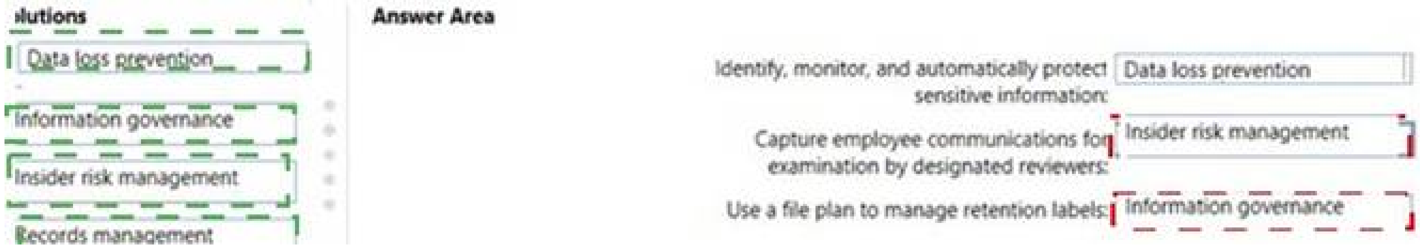
Answer Area

Identify, monitor, and automatically protect sensitive information:	
Capture employee communications for examination by designated reviewers:	
Use a file plan to manage retention labels:	

A. Mastered
B. Not Mastered

Answer: A

Explanation:



lutions

- Data loss prevention
- Information governance
- Insider risk management
- Records management

Answer Area

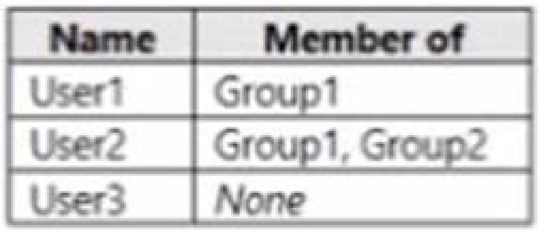
Identify, monitor, and automatically protect sensitive information:	Data loss prevention
Capture employee communications for examination by designated reviewers:	Insider risk management
Use a file plan to manage retention labels:	Information governance

NEW QUESTION 229

HOTSPOT - (Topic 6)

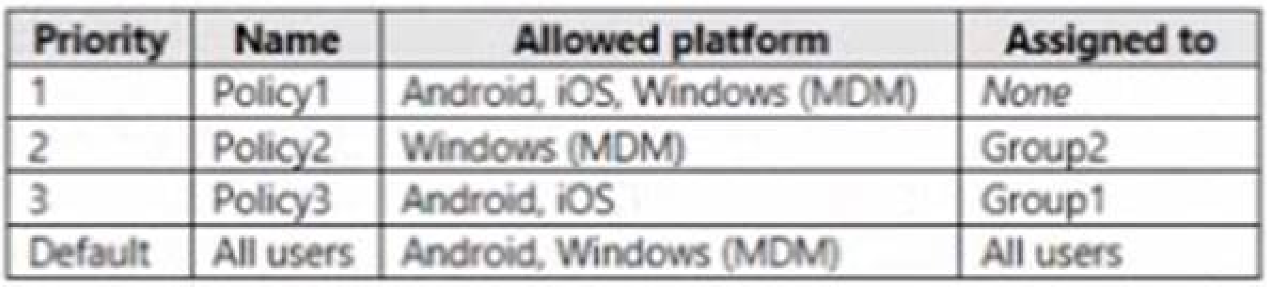
You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

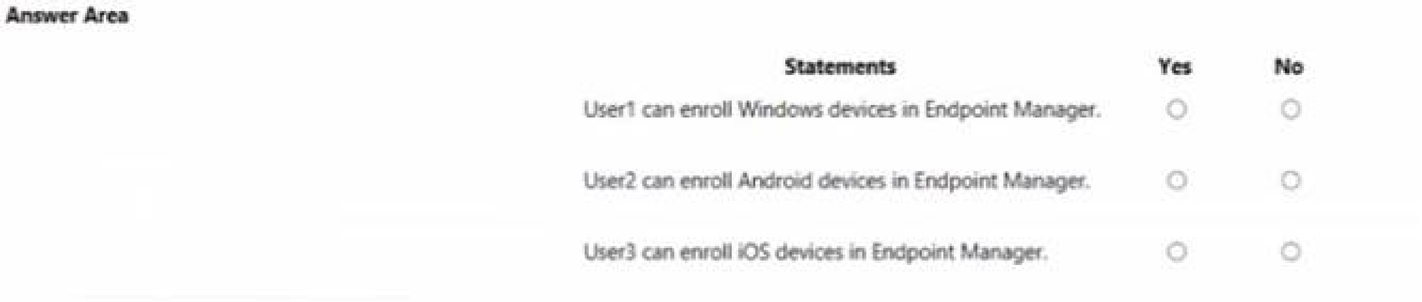


Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

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



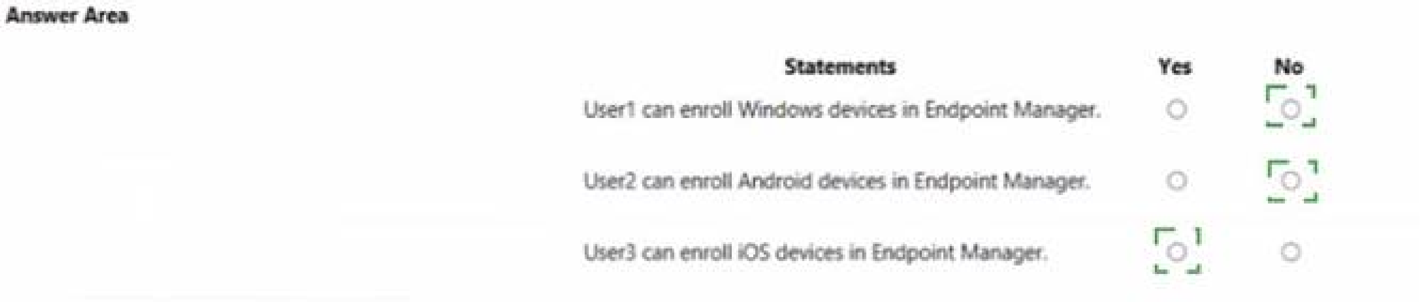
Answer Area

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 232

- (Topic 6)

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

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

Answer: C

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

NEW QUESTION 236
- (Topic 6)
You have a Microsoft 365 tenant.
Company policy requires that all Windows 10 devices meet the following minimum requirements:
? Require complex passwords.
? Require the encryption of data storage devices.
? Have Microsoft Defender Antivirus real-time protection enabled.
You need to prevent devices that do not meet the requirements from accessing resources in the tenant.
Which two components should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: BD

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

NEW QUESTION 237
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP).
You need to create a detection exclusion in Azure ATP. Which tool should you use?

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

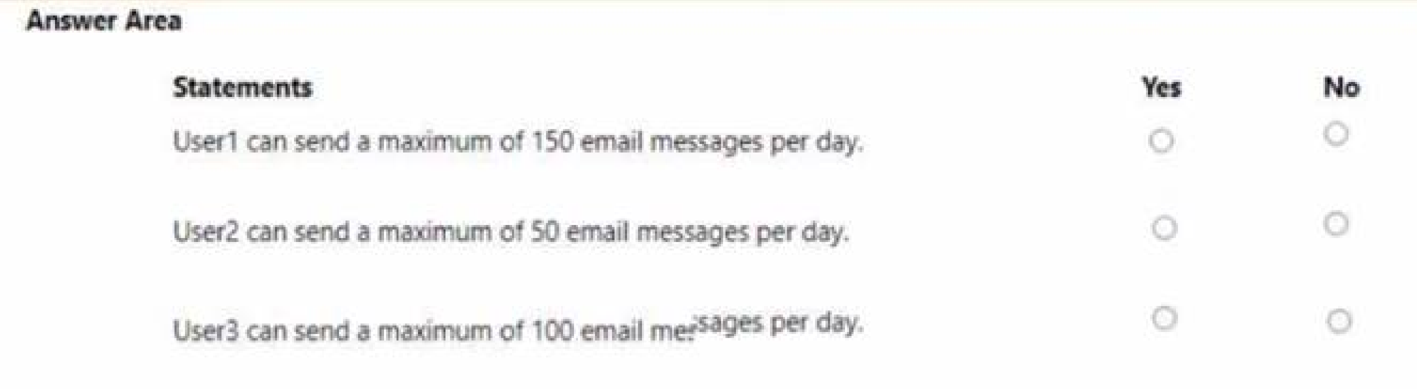
Answer: D

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

NEW QUESTION 240
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.
The subscription has the following two anti-spam policies:
• Name: AntiSpam1
• Priority: 0
• Induce these users, groups and domains o Users: User3
o Groups: Group!
• Exclude these users, groups and domains o Groups: Group2
• Message limits
o Set a daily message limit 100
• Name: AntiSpam2
• Priority: 1

- Include these users, groups and domains o Users: User! o Groups: Group2
- Exclude these users, groups and domains o Users: User3
- Message limits

o Set a daily message limit 50
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



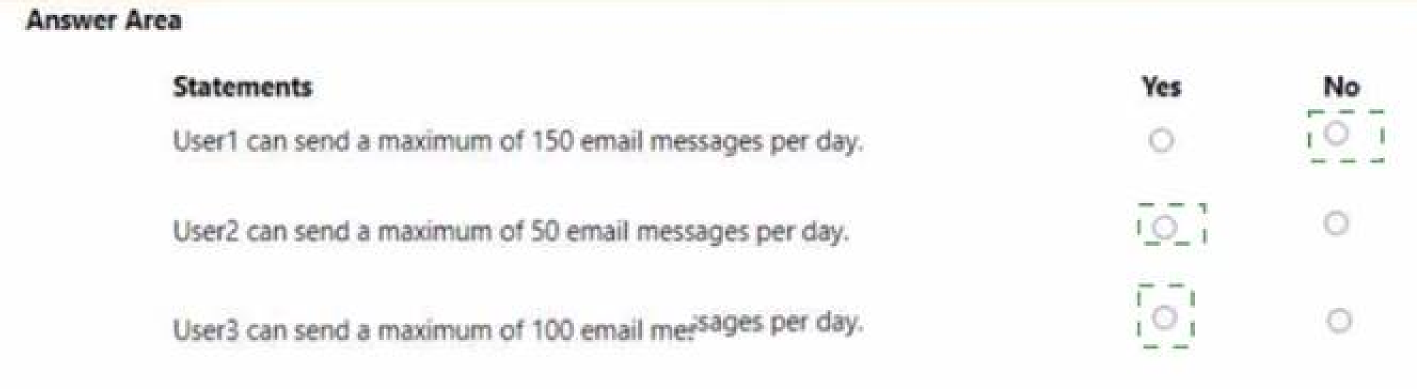
Answer Area

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	○	○
User2 can send a maximum of 50 email messages per day.	○	○
User3 can send a maximum of 100 email messages per day.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

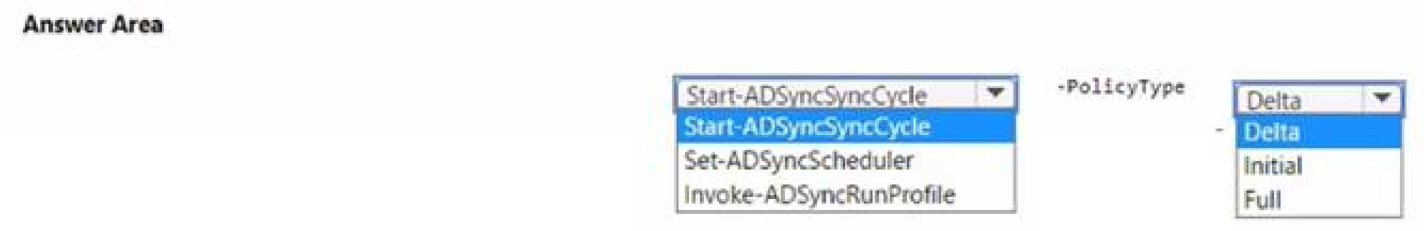
Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	○	[✓ ○]
User2 can send a maximum of 50 email messages per day.	[✓ ○]	○
User3 can send a maximum of 100 email messages per day.	[✓ ○]	○

NEW QUESTION 245
- (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 248
HOTSPOT - (Topic 6)
Your network contains an Active Directory domain and an Azure AD tenant.
You implement directory synchronization for all 10.000 users in the organization. You automate the creation of 100 new user accounts.
You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.
Which command should you run? To answer, select the appropriate options in the answer area.



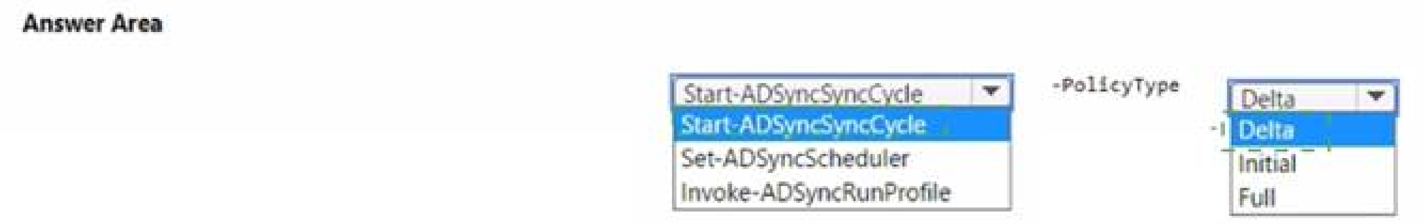
Answer Area

Start-ADSyncSyncCycle ▼ -PolicyType Delta ▼

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Start-ADSyncSyncCycle ▼ -PolicyType Delta ▼

NEW QUESTION 252
- (Topic 6)
You have a new Microsoft 365 E5 tenant.
You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.
What should you do first?

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

Answer: A

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

NEW QUESTION 257
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview policies to meet the following requirements: Identify documents that are stored in Microsoft Teams and SharePoint that contain
Personally Identifiable Information (PII). Report on shared documents that contain PII. What should you create?

A. a data loss prevention (DLP) policy
B. a retention policy
C. an alert policy
D. a Microsoft Defender for Cloud Apps policy

Answer: A

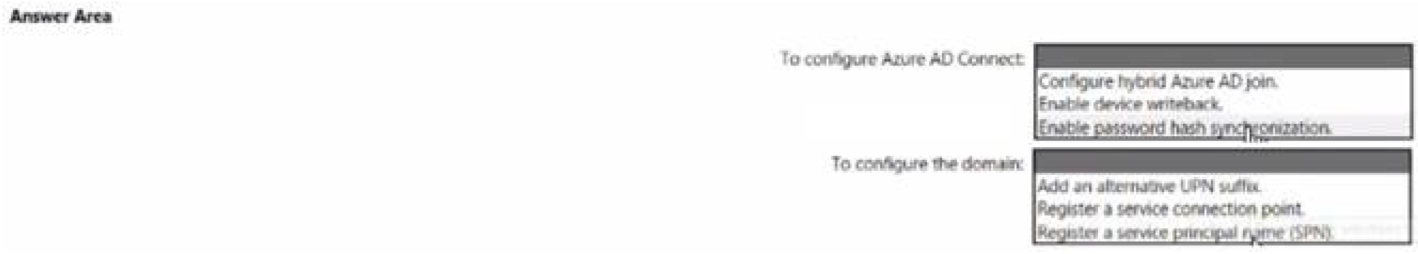
Explanation:
Demonstrate data protection
Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.
There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.
In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.
? From the Security & Compliance tab of your browser, click Home.
? Click Data loss prevention > Policy.
? Click + Create a policy.
? In Start with a template or create a custom policy, click Custom > Custom policy > Next.
? In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b. Description: Protect the personally identifiable information of European citizens
? Etc.
Reference:
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-test-environment

NEW QUESTION 262
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:
• Support KQL for querying data.
• Retain report data for at least one year.
What should you include in the recommendation?

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

Answer: D

NEW QUESTION 264
HOTSPOT - (Topic 6)
Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD) Password hash synchronization is disabled.
You plan to implement co-management.
You need to configure Azure AD Connect and the domain to support co-management. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

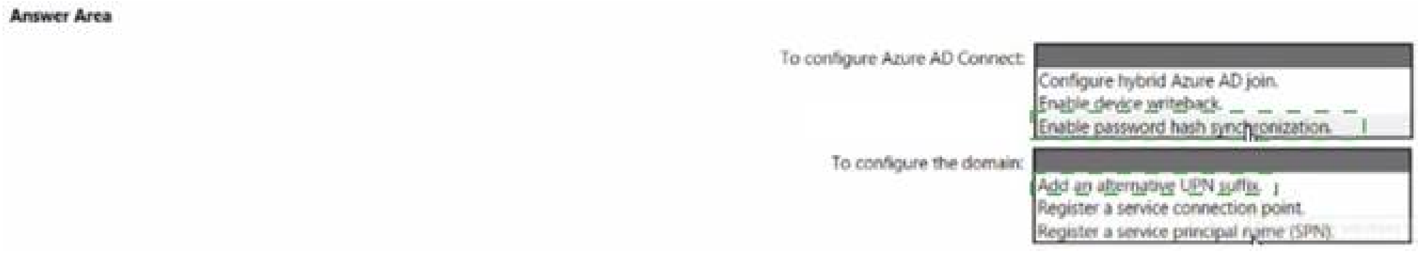
To configure Azure AD Connect:
- Configure hybrid Azure AD join.
- Enable device writeback.
- Enable password hash synchronization.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

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

NEW QUESTION 268
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.
You need to implement passwordless authentication. The solution must support all the devices.
Which authentication method should you use?

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

Answer: C

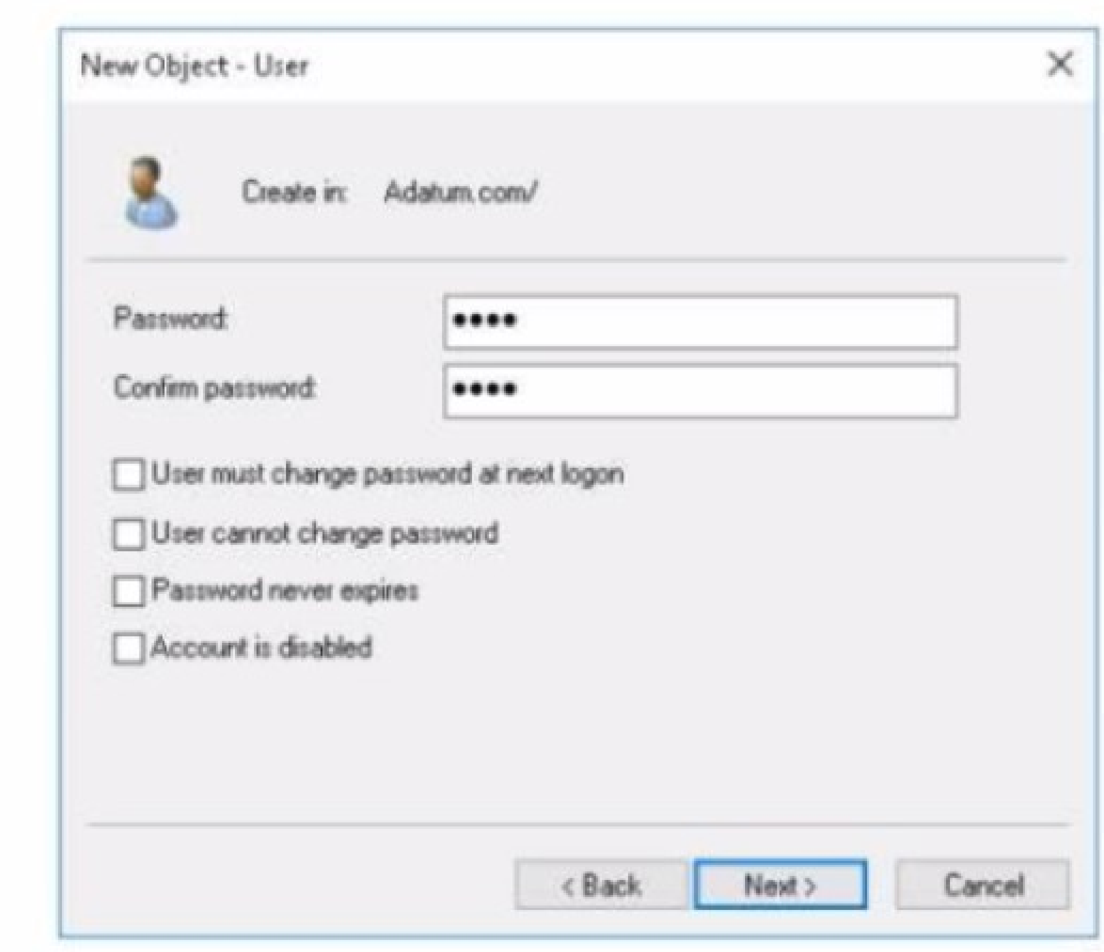
NEW QUESTION 269
- (Topic 6)
You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.
Company policy requires that the devices have the following configurations:
? Require complex passwords.
? Require the encryption of removable data storage devices.
? Have Microsoft Defender Antivirus real-time protection enabled.
You need to configure the devices to meet the requirements.
What should you use?

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

Answer: B

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

NEW QUESTION 274
HOTSPOT - (Topic 6)
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure AD by using the Azure AD Connect Express Settings.
Password write back is disabled.
You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.



New Object - User

Create in: Adatum.com/

Password: ••••

Confirm password: ••••

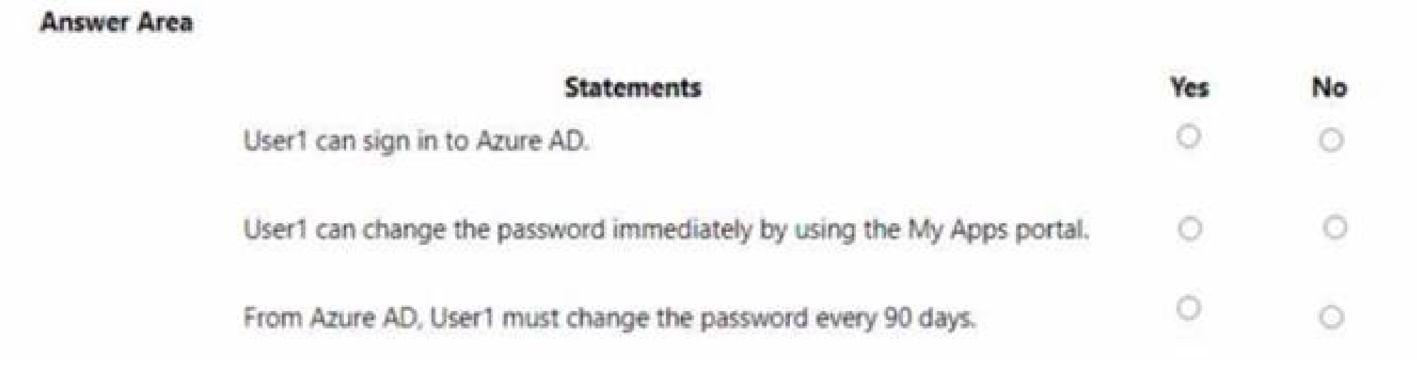
□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

The Azure AD password policy is configured as shown in the following exhibit. Password policy
Set the password policy for all users in your organization. Days before passwords expire 90
Days before a user is notified about 14 expiration
You confirm that User1 is synced to Azure AD.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



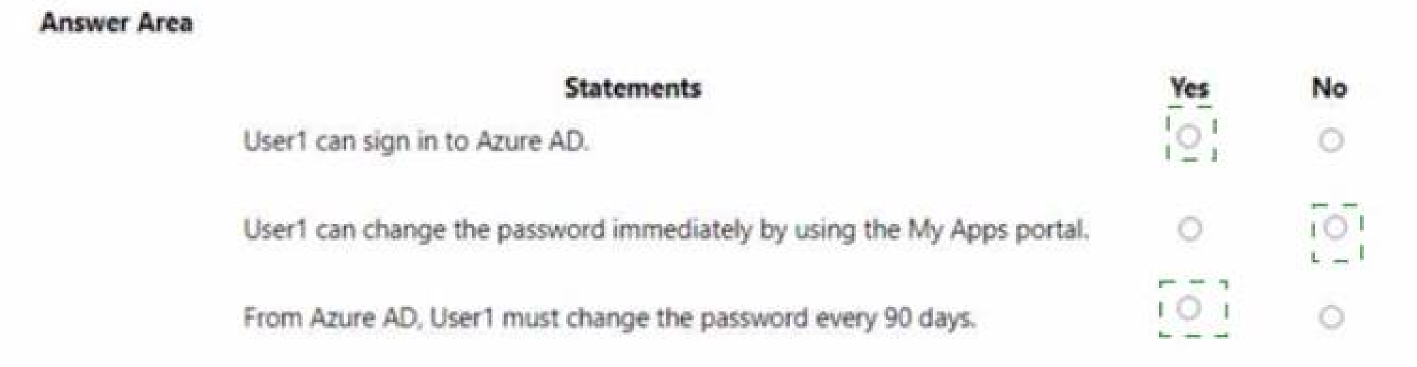
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

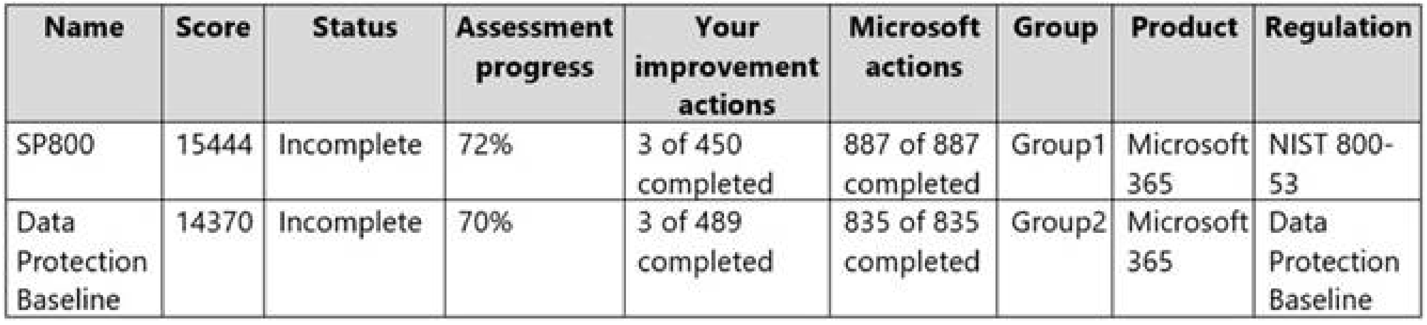
Explanation:



Answer Area

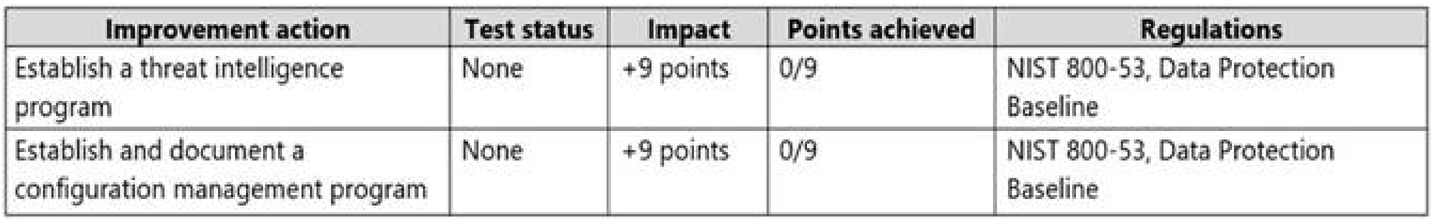
Statements	Yes	No
User1 can sign in to Azure AD.	[✓ ○]	○
User1 can change the password immediately by using the My Apps portal.	○	[✓ ○]
From Azure AD, User1 must change the password every 90 days.	[✓ ○]	○

NEW QUESTION 279
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).
The tenant has two Compliance Manager assessments as shown in the following table.



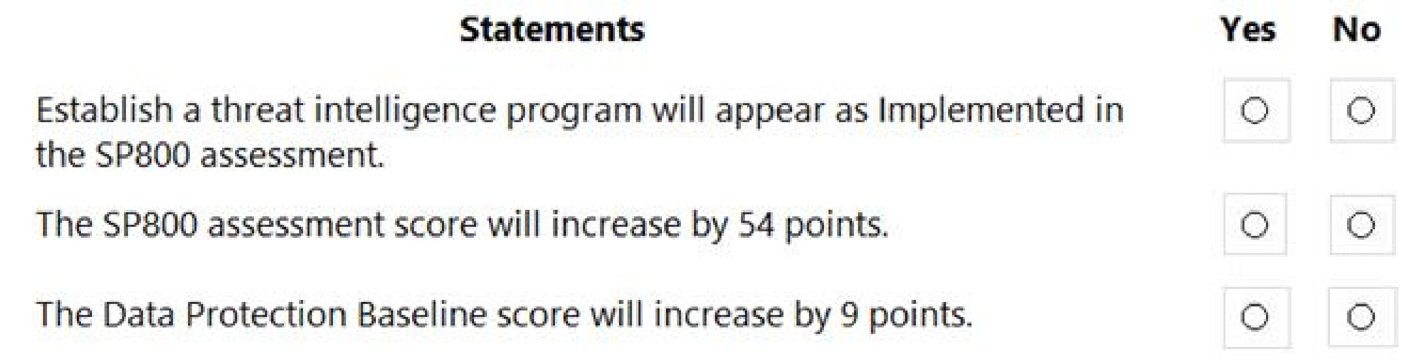
Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft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

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



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

You perform the following actions:
? For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.
? Enable multi-factor authentication (MFA) for all users.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

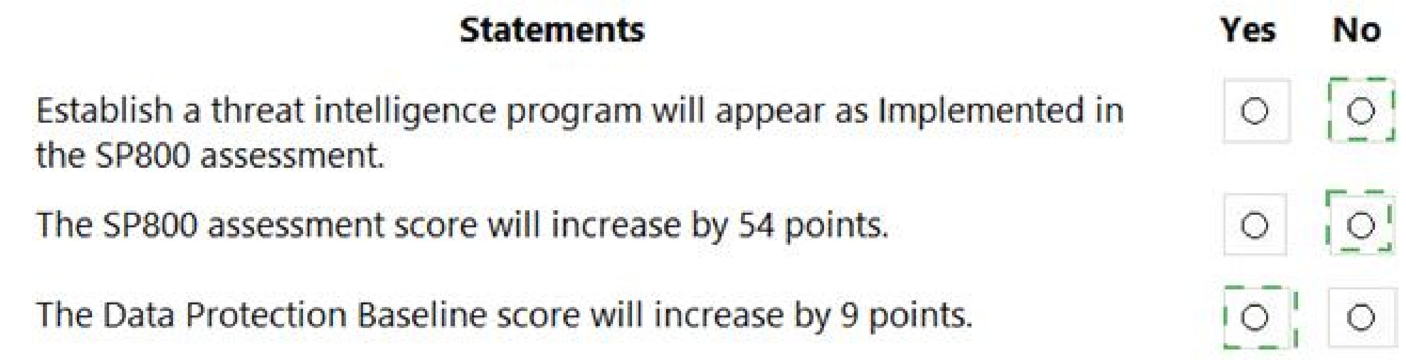


Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

A. Mastered
B. Not Mastered

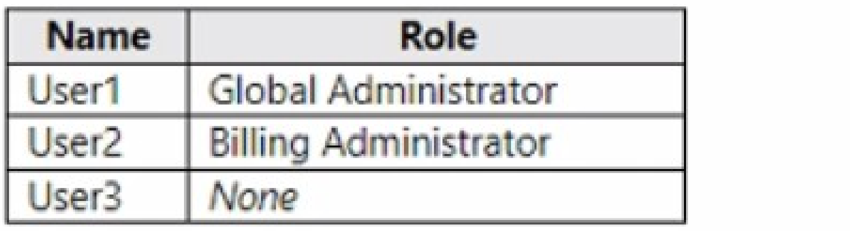
Answer: A

Explanation:



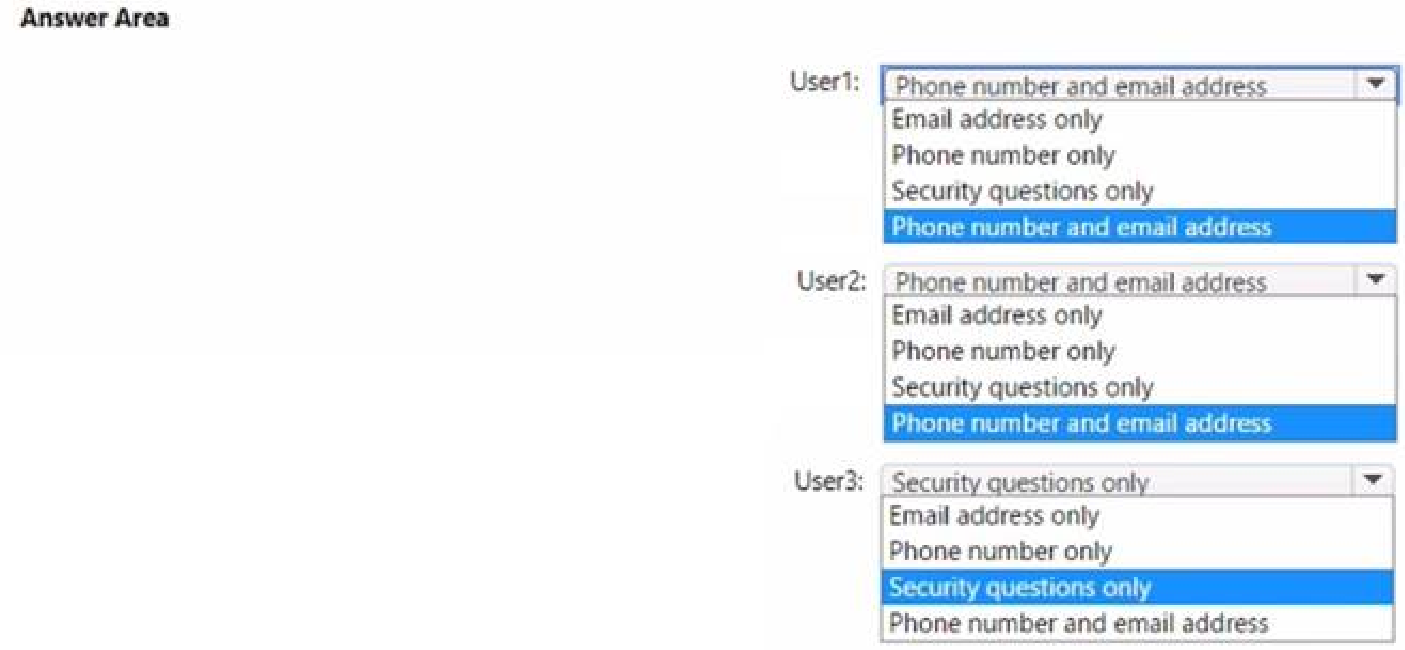
Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	[✓ ○]
The SP800 assessment score will increase by 54 points.	○	[✓ ○]
The Data Protection Baseline score will increase by 9 points.	[✓ ○]	○

NEW QUESTION 282
HOTSPOT - (Topic 6)
You have an Azure AD tenant that contains the users shown in the following table.



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

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



Answer Area

User1: Phone number and email address
- Email address only
- Phone number only
- Security questions only
- [✓ Phone number and email address]

User2: Phone number and email address
- Email address only
- Phone number only
- Security questions only
- [✓ Phone number and email address]

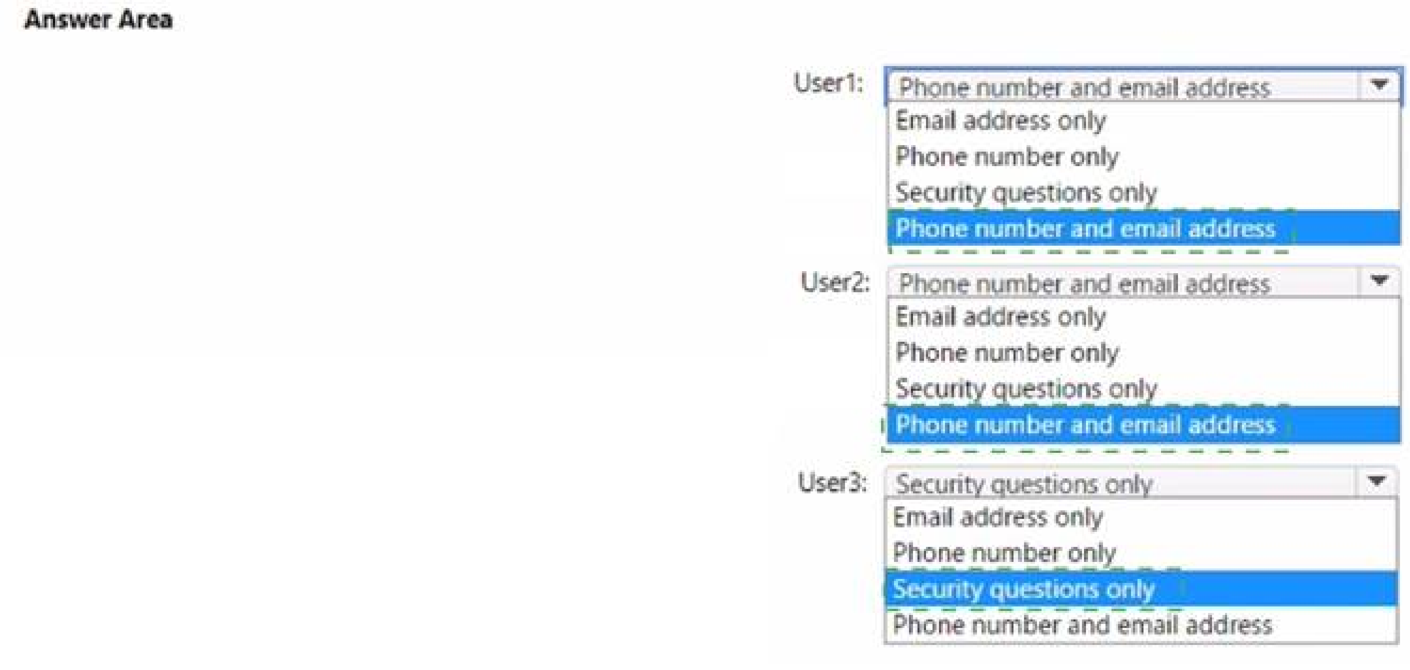
User3: Security questions only
- Email address only
- Phone number only
- [✓ Security questions only]
- Phone number and email address

A. Mastered

B. Not Mastered

Answer: A

Explanation:



Answer Area

User1: Phone number and email address
- Email address only
- Phone number only
- Security questions only
- Phone number and email address

User2: Phone number and email address
- Email address only
- Phone number only
- Security questions only
- Phone number and email address

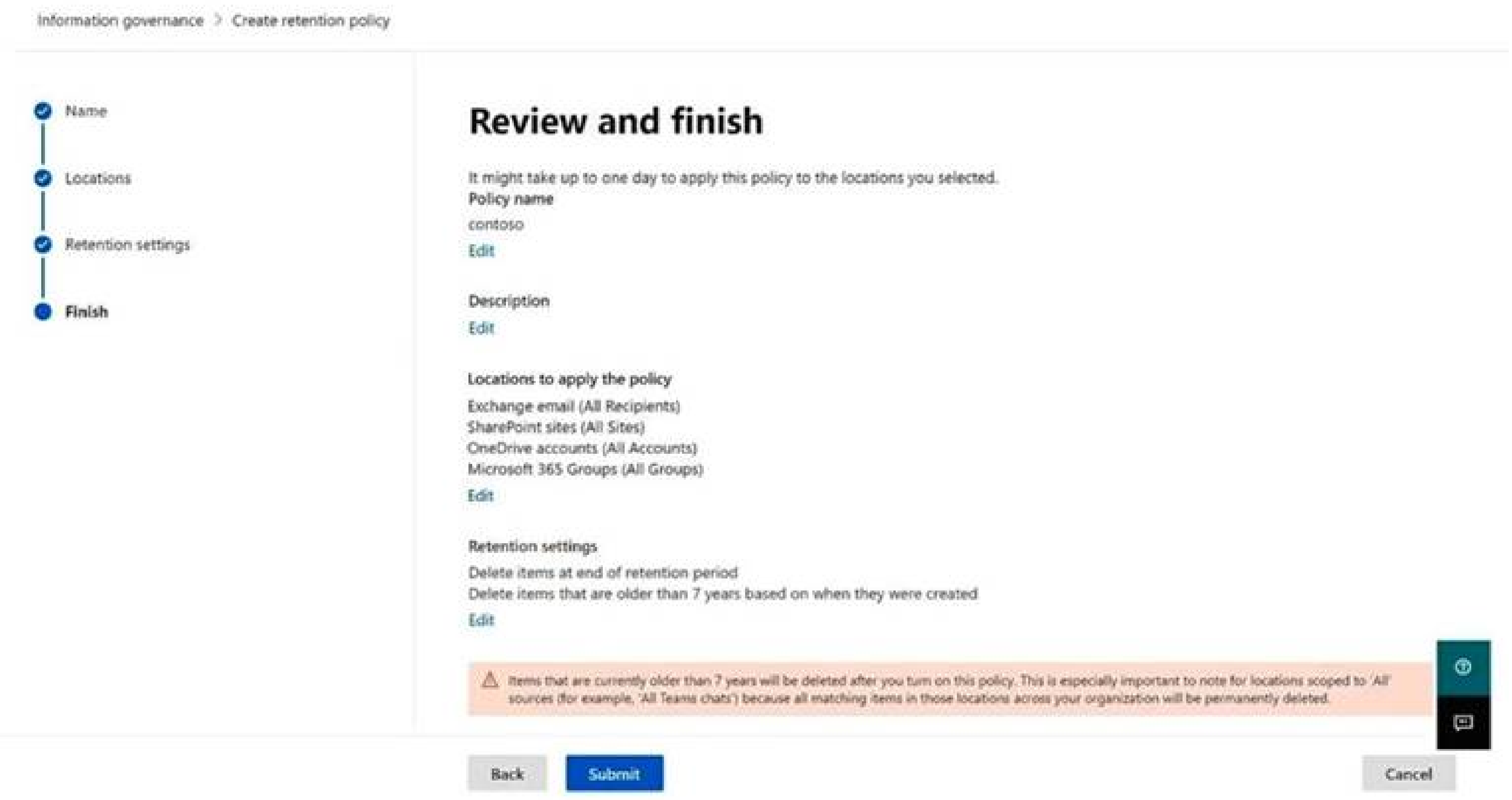
User3: Security questions only
- Email address only
- Phone number only
- Security questions only
- Phone number and email address

NEW QUESTION 285
- (Topic 6)
You purchase a new computer that has Windows 10, version 21H1 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

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

Answer: C

NEW QUESTION 287
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 tenant.
You plan to create a retention policy as shown in the following exhibit.



Information governance > Create retention policy

Review and finish

It might take up to one day to apply this policy to the locations you selected.

Policy name
contoso
Edit

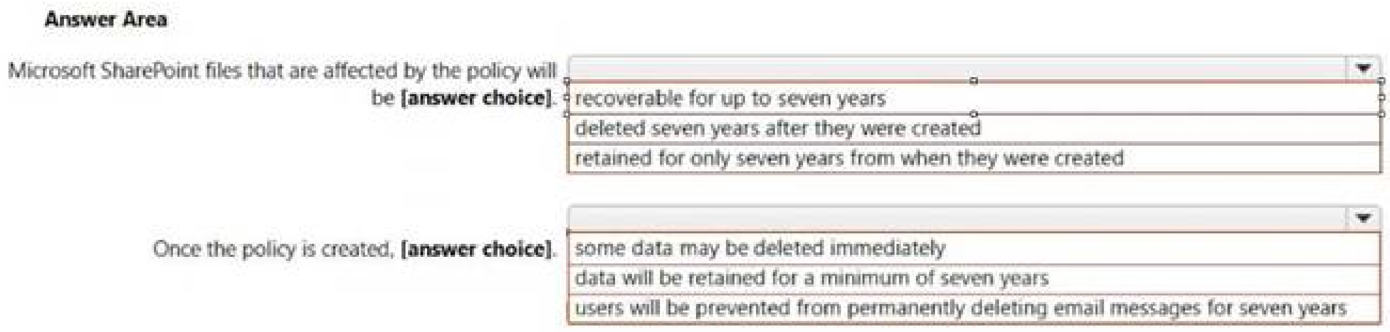
Description
Edit

Locations to apply the policy
Exchange email (All Recipients)
SharePoint sites (All Sites)
OneDrive accounts (All Accounts)
Microsoft 365 Groups (All Groups)
Edit

Retention settings
Delete items at end of retention period
Delete items that are older than 7 years based on when they were created
Edit

Items that are currently older than 7 years will be deleted after you turn on this policy. This is especially important to note for locations scoped to 'All' sources (for example, 'All Teams chats') because all matching items in those locations across your organization will be permanently deleted.

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



Answer Area

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

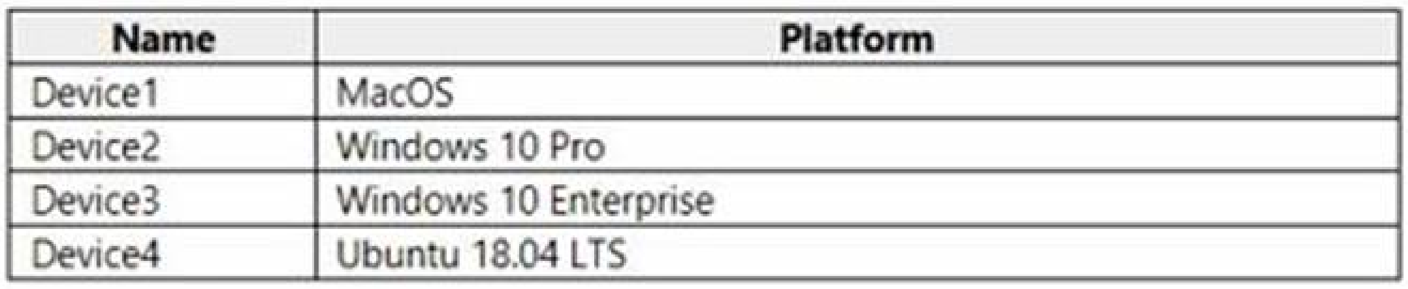
Once the policy is created, **[answer choice]**.
- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 288
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.



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

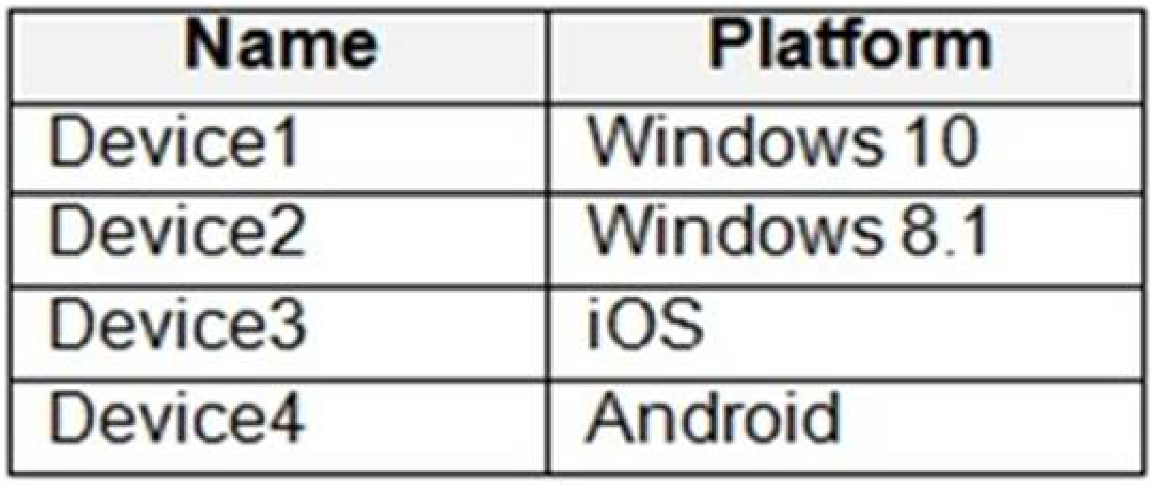
You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?

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

Answer: C

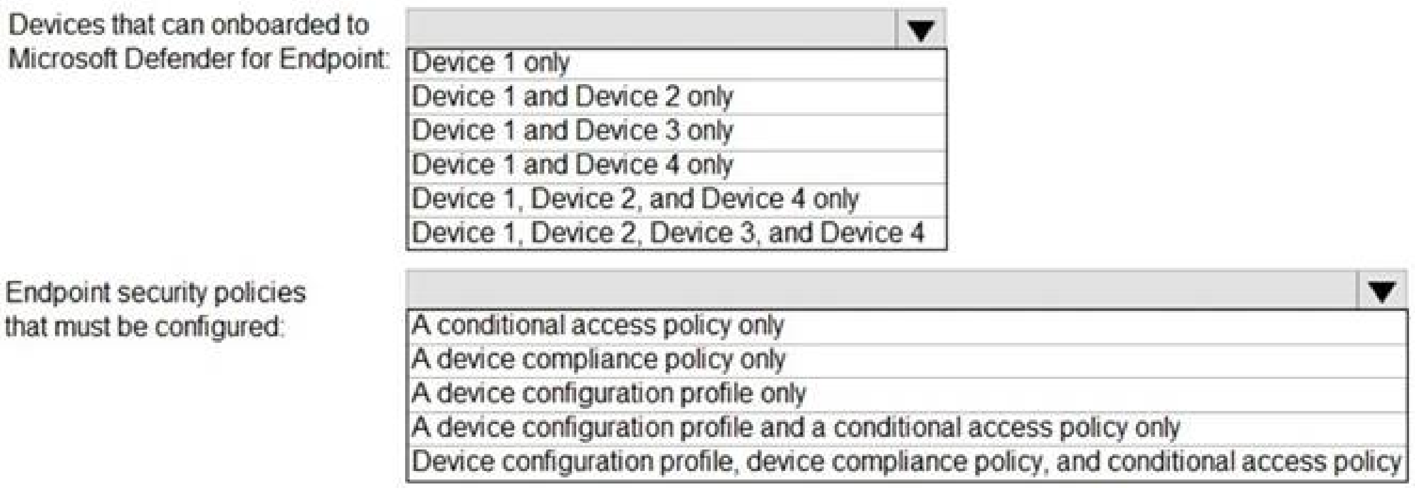
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements

NEW QUESTION 293
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.



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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, table Description automatically generated with medium confidence

NEW QUESTION 297
- (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

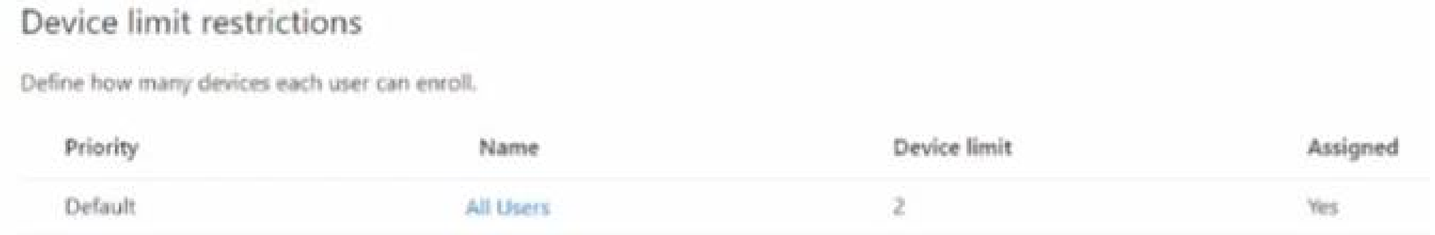
Answer: C

NEW QUESTION 301
- (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 305
HOTSPOT - (Topic 6)
You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.
In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

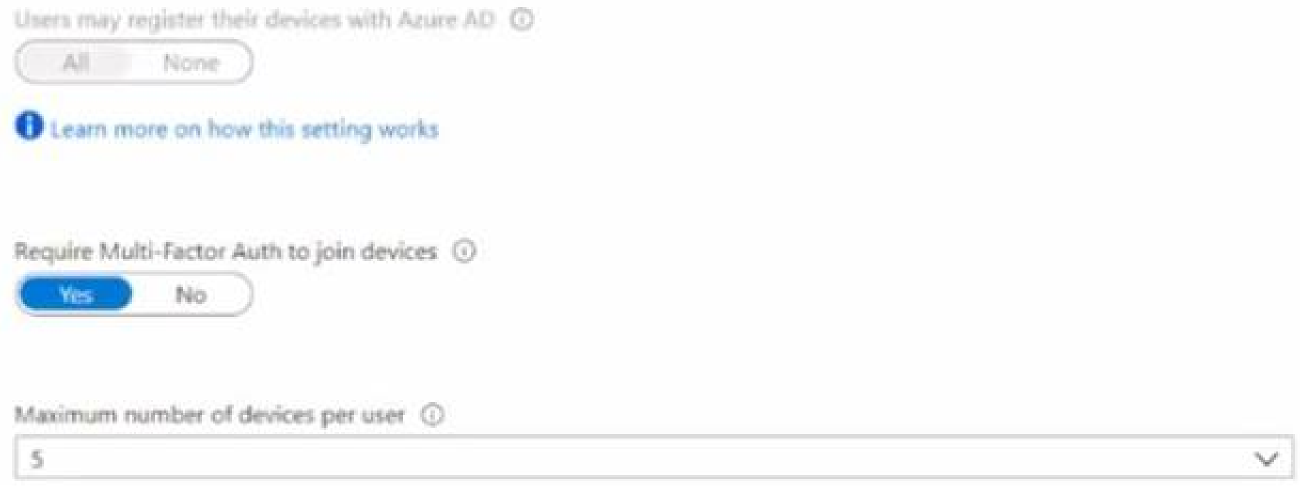


Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

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

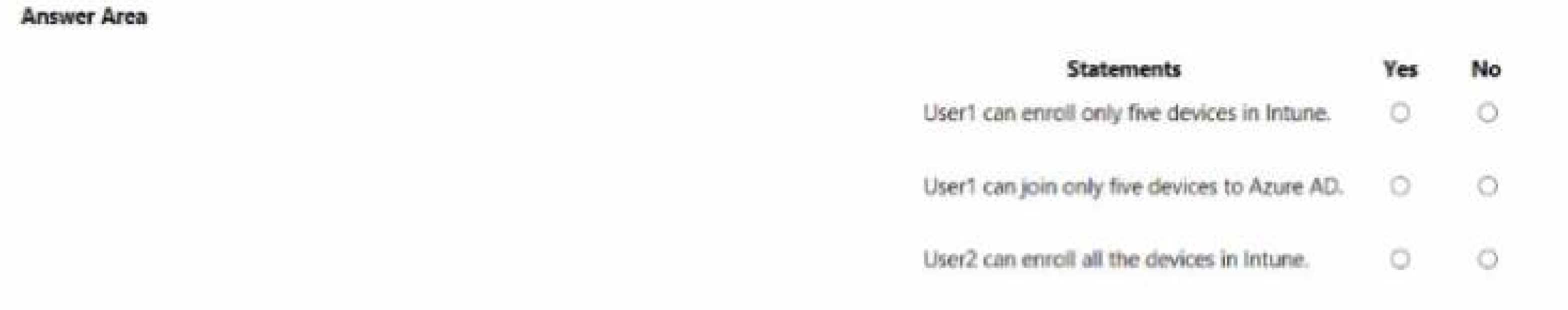


Users may register their devices with Azure AD ⓘ
All | None
ⓘ Learn more on how this setting works

Require Multi-Factor Auth to join devices ⓘ
Yes | No

Maximum number of devices per user ⓘ
5

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



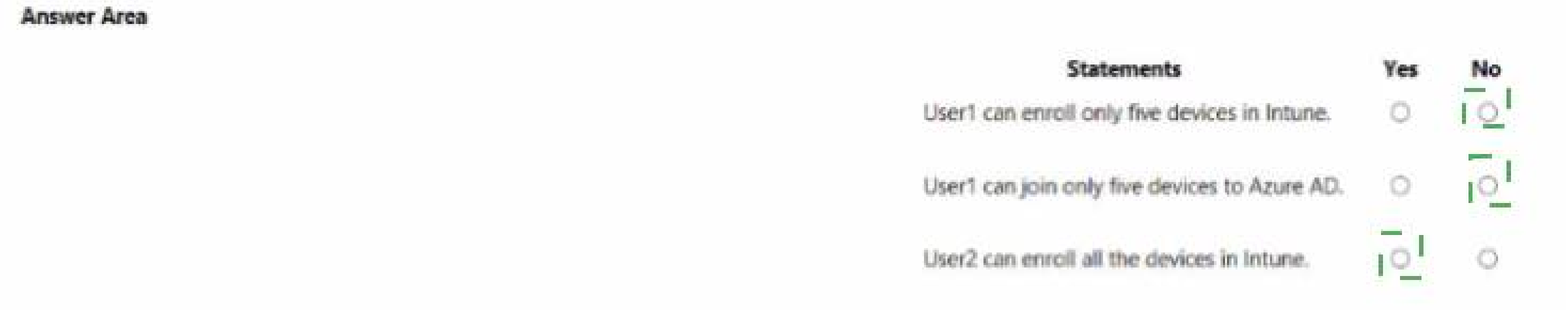
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

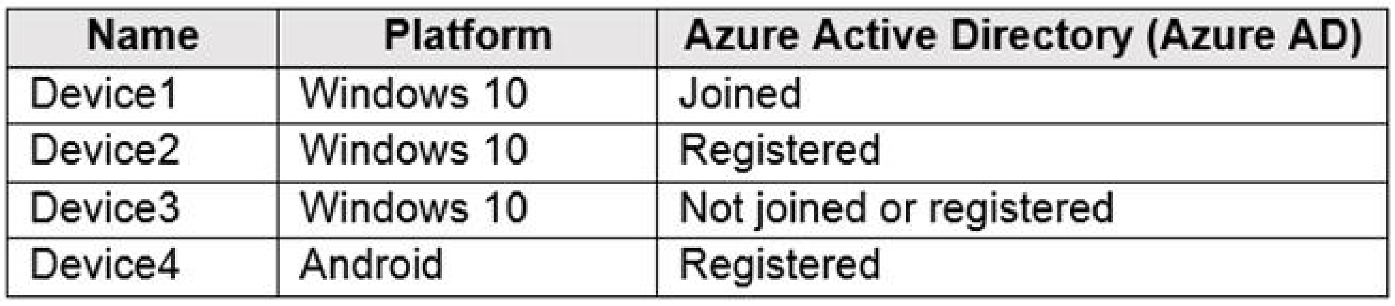
Explanation:



Answer Area

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

NEW QUESTION 307
- (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

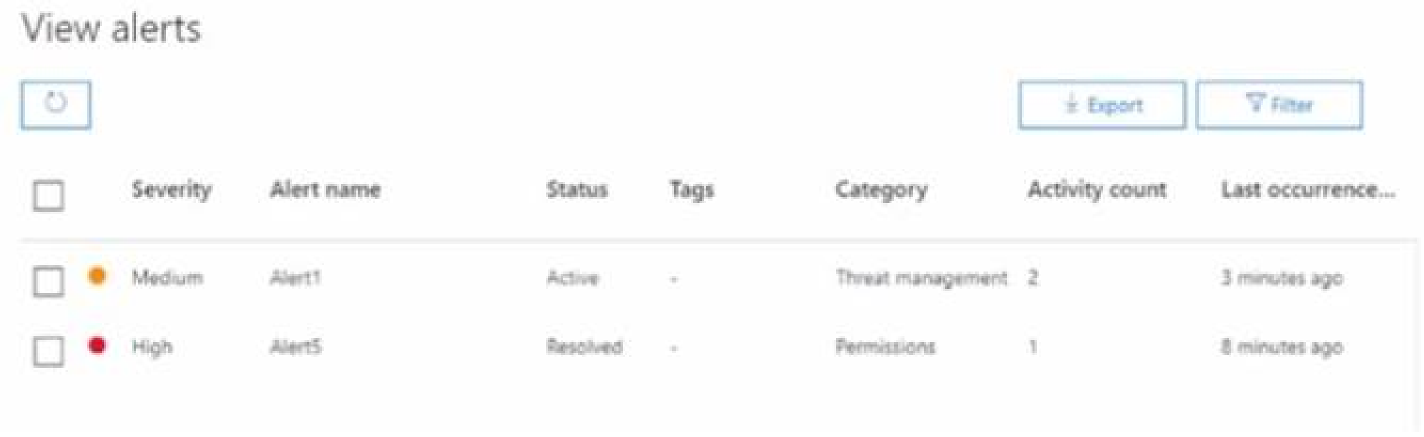
You plan to review device startup performance issues by using Endpoint analytics. Which devices can you monitor by using Endpoint analytics?

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

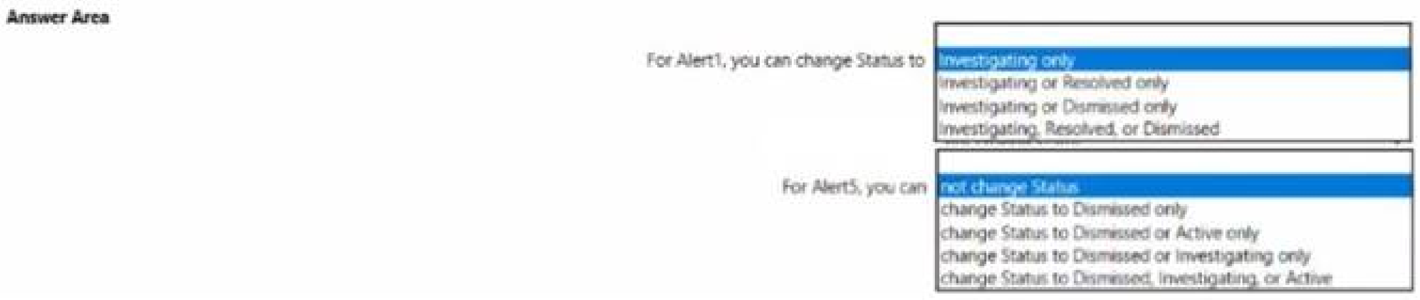
NEW QUESTION 308
HOTSPOT - (Topic 6)
You have a Microsoft 365 ES tenant.
You have the alerts shown in the following exhibit.



View alerts

□	Severity	Alert name	Status	Tags	Category	Activity count	Last occurrence...
□	● Medium	Alert1	Active	-	Threat management	2	3 minutes ago
□	● High	Alert5	Resolved	-	Permissions	1	8 minutes ago

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

For Alert1, you can change Status to

- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

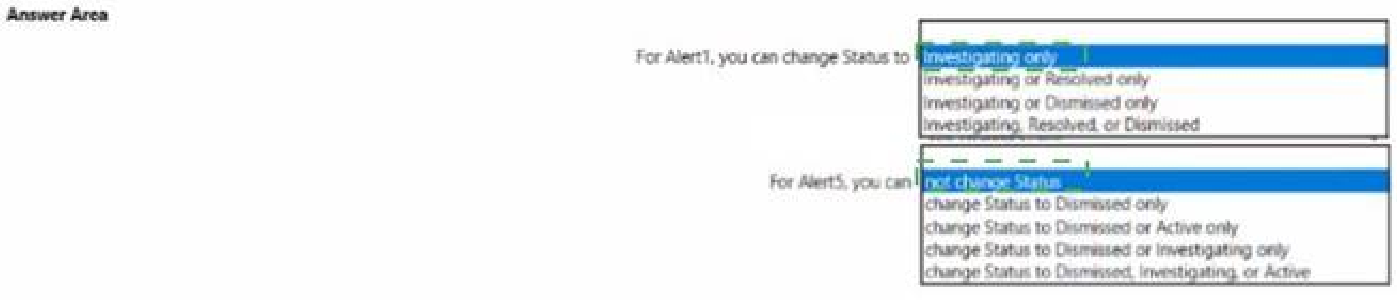
For Alert5, you can

- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

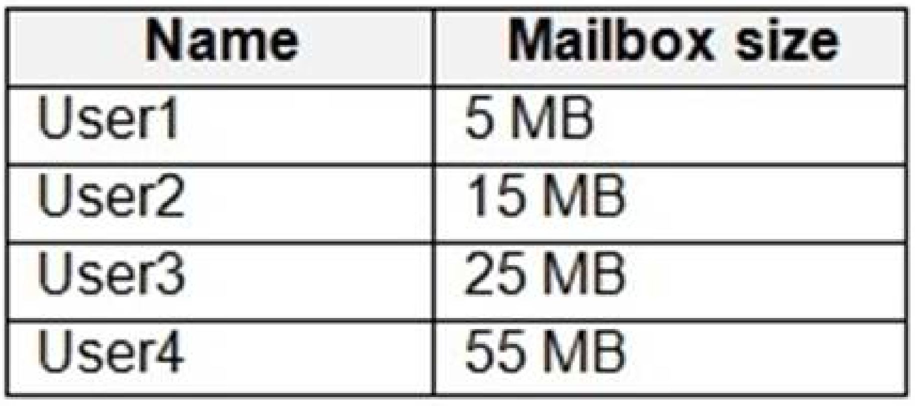
For Alert1, you can change Status to

- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

For Alert5, you can

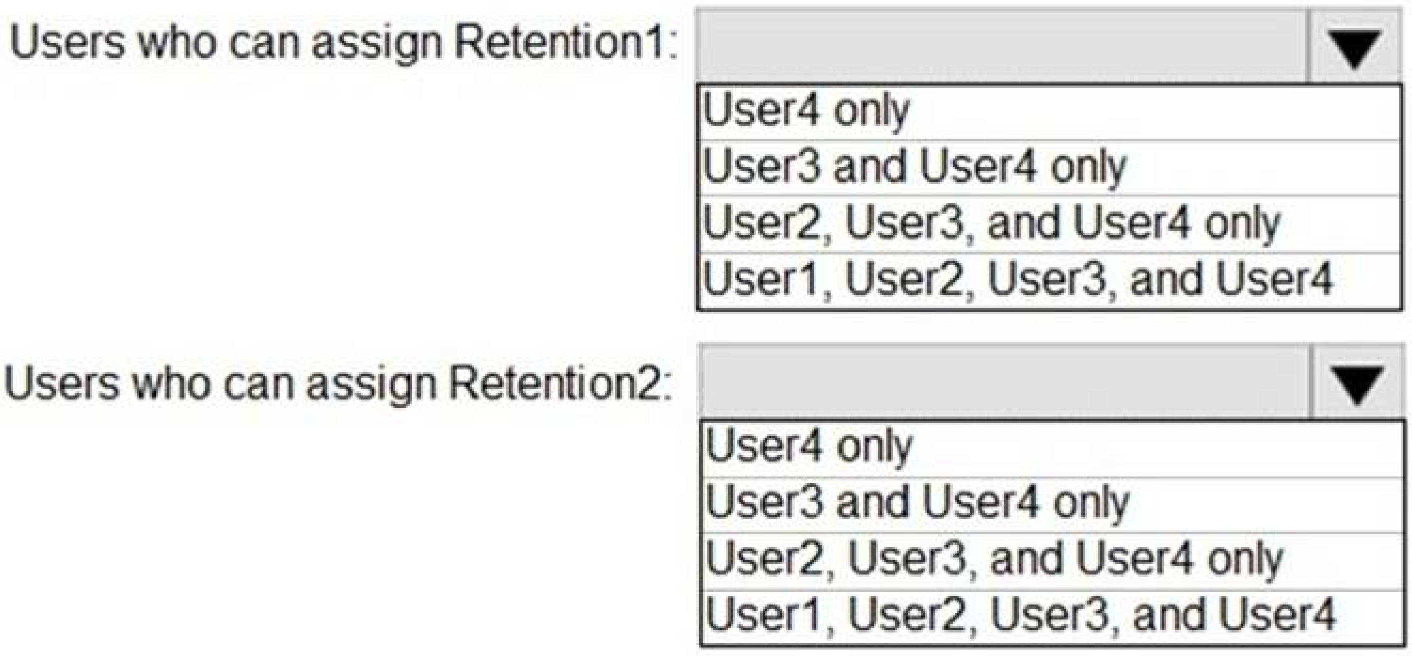
- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active

NEW QUESTION 311
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



Name	Mailbox size
User1	5 MB
User2	15 MB
User3	25 MB
User4	55 MB

You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email.
You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2.
Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Users who can assign Retention1:

- User4 only
- User3 and User4 only
- User2, User3, and User4 only
- User1, User2, User3, and User4

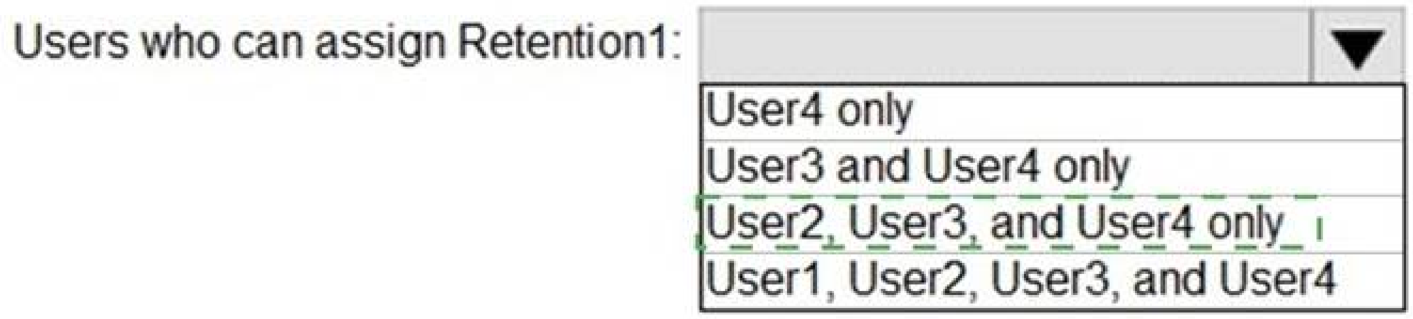
Users who can assign Retention2:

- User4 only
- User3 and User4 only
- User2, User3, and User4 only
- User1, User2, User3, and User4

A. Mastered
B. Not Mastered

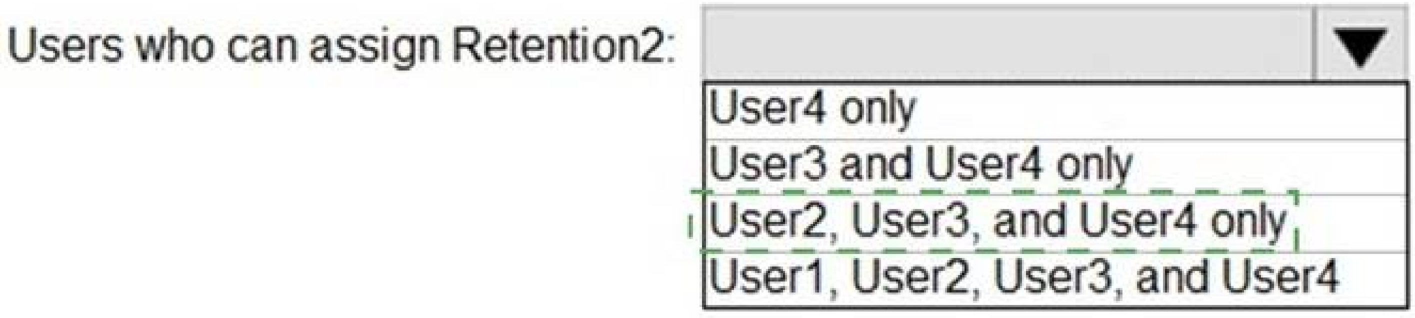
Answer: A

Explanation:



Users who can assign Retention1: ▼

- User4 only
- User3 and User4 only
- User2, User3, and User4 only
- User1, User2, User3, and User4



Users who can assign Retention2: ▼

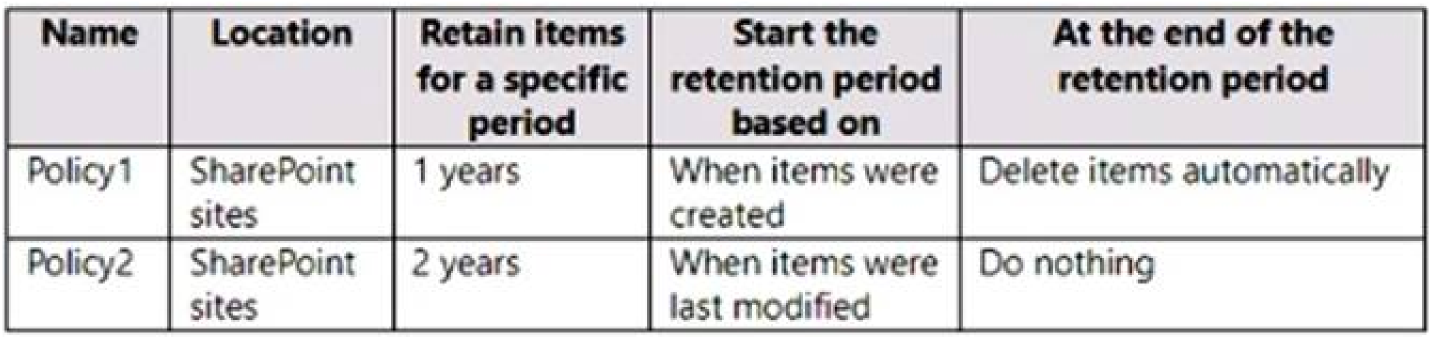
- User4 only
- User3 and User4 only
- User2, User3, and User4 only
- User1, User2, User3, and User4

NEW QUESTION 312

- (Topic 6)

You have a Microsoft 365 subscription.

You have the retention policies shown in the following table.



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

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx.

File1.docx was created on January 1, 2022 and last modified on January 31,2022. The file was NOT modified again.

When will File1.docx be deleted automatically?

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

Answer: D

Explanation:

Retention wins over deletion. Note:

Explanation for the four different principles:

* 1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system- initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.

* 2. Etc. Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

NEW QUESTION 317

DRAG DROP - (Topic 6)

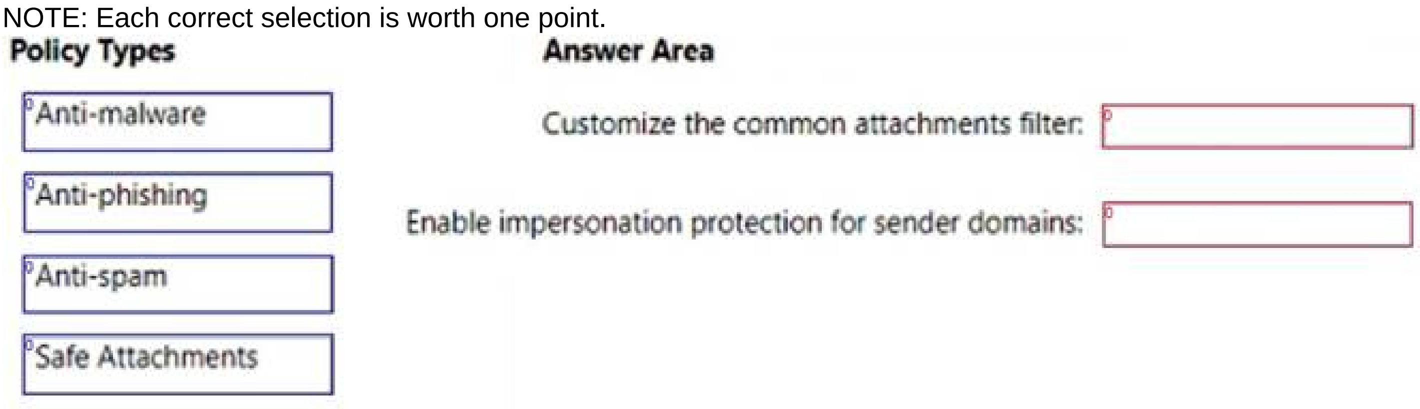
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. You need to configure policies to meet the following requirements:

? Customize the common attachments filter.

? Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type 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.



Policy Types

- Anti-malware
- Anti-phishing
- Anti-spam
- Safe Attachments

Answer Area

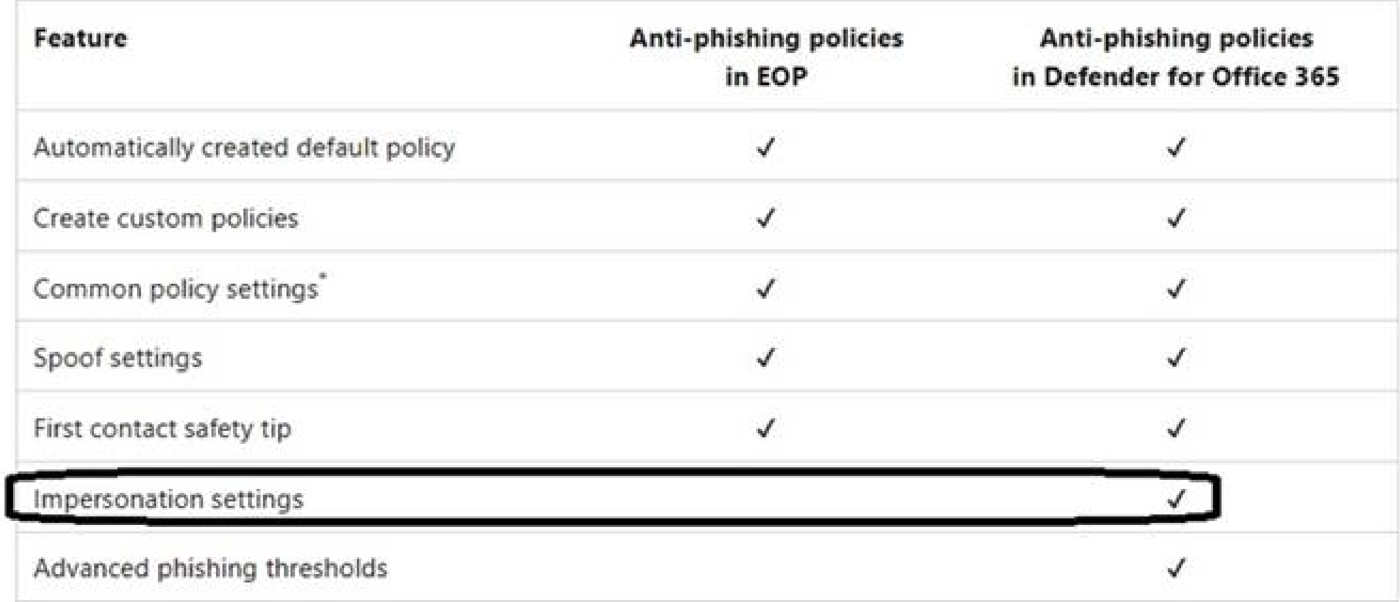
Customize the common attachments filter:

Enable impersonation protection for sender domains:

A. Mastered
B. Not Mastered

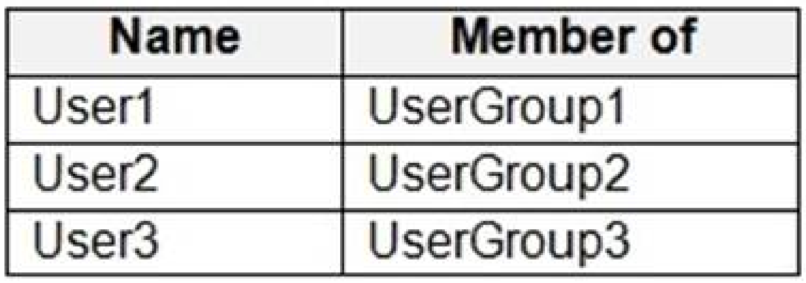
Answer: A

Explanation:
Box 1: Anti-malware
Customize the common attachments filter. See step 5 below.
* 1. Use the Microsoft 365 Defender portal to create anti-malware policies
In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & Collaboration > Policies & Rules > Threat policies > Anti-Malware in the Policies section. To go directly to the Anti-malware page, use https://security.microsoft.com/antimalwarev2
* 2. On the Anti-malware page, select Create to open the new anti-malware policy wizard. On the Name your policy page, configure these settings:
Name: Enter a unique, descriptive name for the policy. Description: Enter an optional description for the policy.
* 3. When you're finished on the Name your policy page, select Next.
* 4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions)
* 5. On the Protection settings page, configure the following settings: Protection settings section:
Enable the common attachments filter: If you select this option, messages with the specified attachments are treated as malware and are automatically quarantined. You can modify the list by clicking Customize file types and selecting or deselecting values in the list.
* 6. Etc.
Box 2: Anti-phishing
Enable impersonation protection for sender domains. Anti-phishing policies in Microsoft 365
The high-level differences between anti-phishing policies in EOP and anti-phishing policies in Defender for Office 365 are described in the following table:



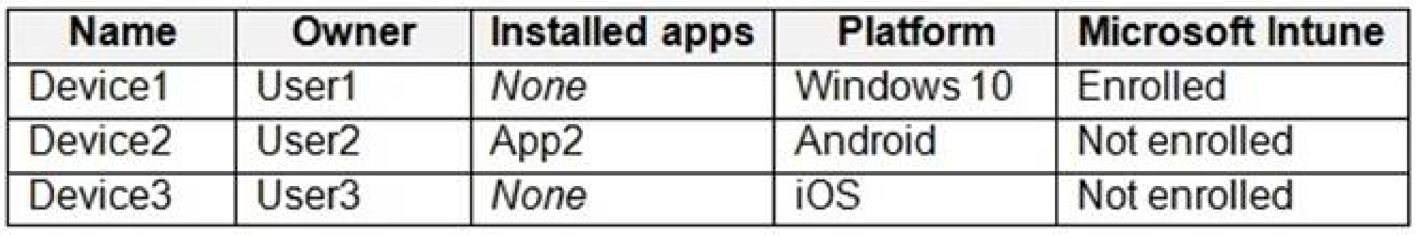
Feature	Anti-phishing policies in EOP	Anti-phishing policies in Defender for Office 365
Automatically created default policy	✓	✓
Create custom policies	✓	✓
Common policy settings*	✓	✓
Spoof settings	✓	✓
First contact safety tip	✓	✓
Impersonation settings		✓
Advanced phishing thresholds		✓

NEW QUESTION 318
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.



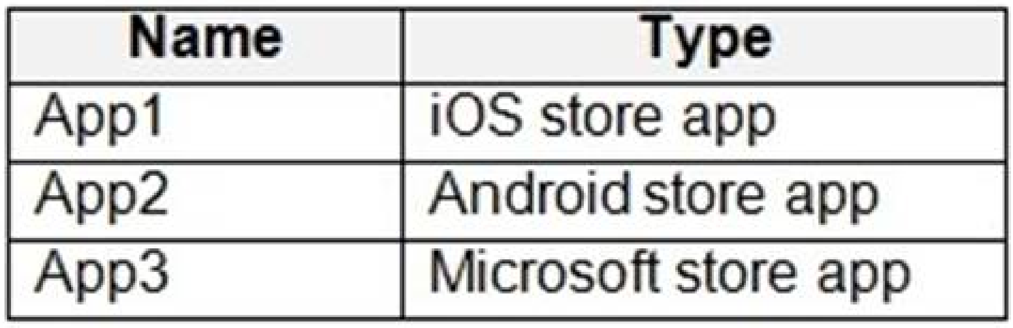
Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.



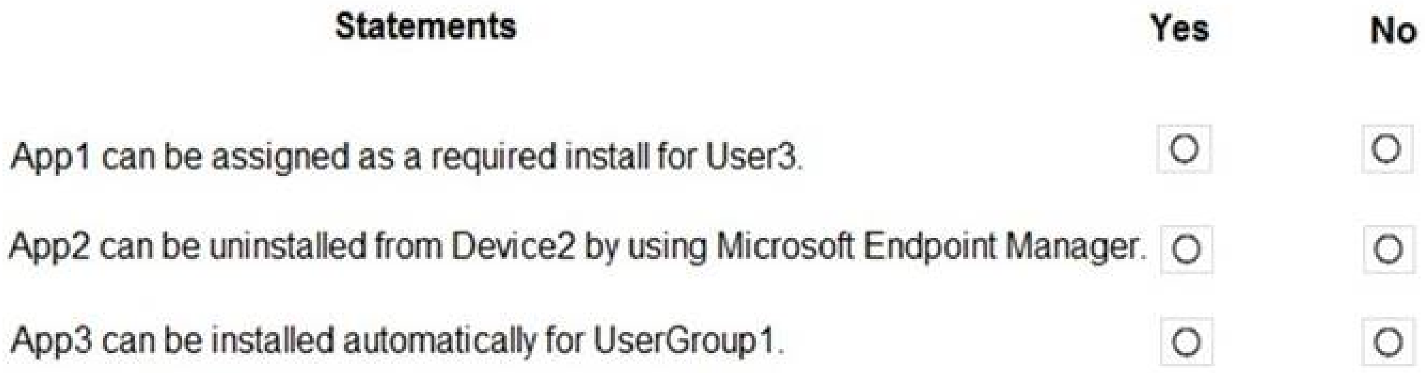
Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	*None*	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	*None*	iOS	Not enrolled

You have the apps shown in the following table.



Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the users.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

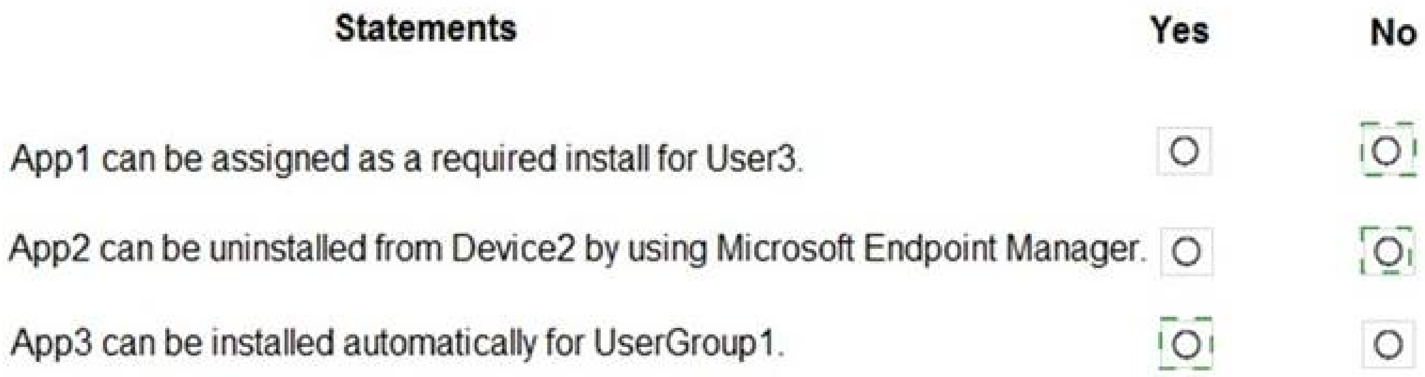


Statements	Yes	No
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



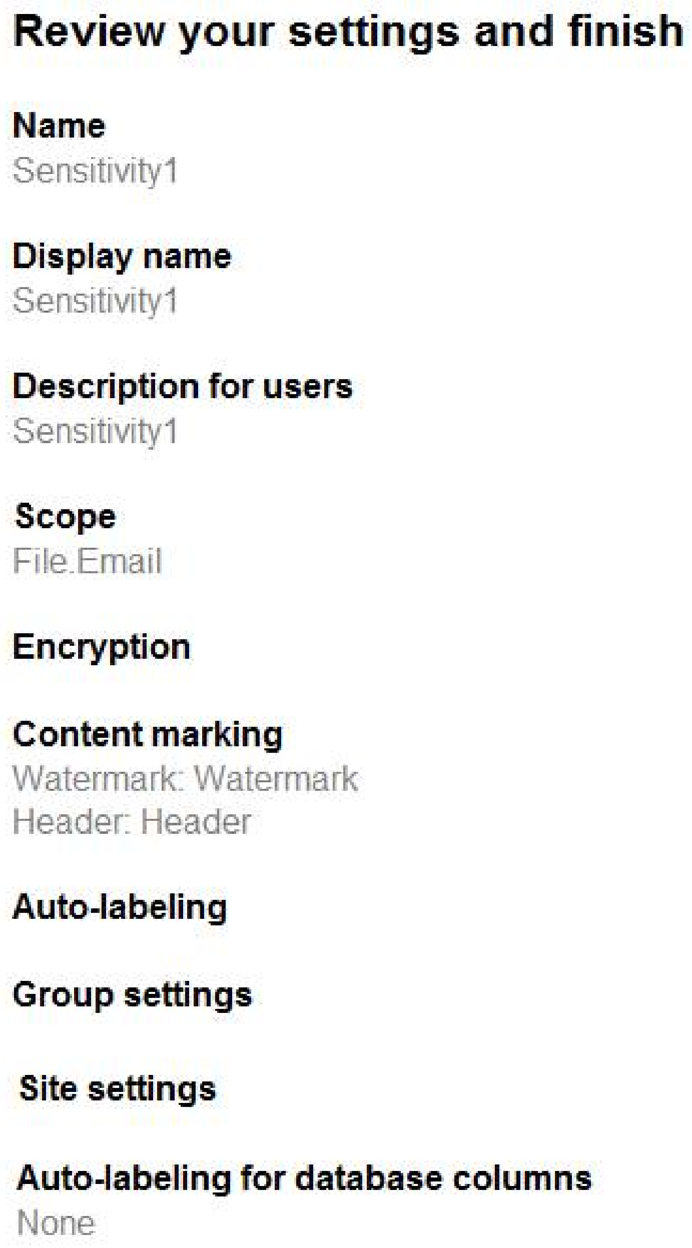
Statements	Yes	No
App1 can be assigned as a required install for User3.	○	[✓ ○]
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	[✓ ○]
App3 can be installed automatically for UserGroup1.	[✓ ○]	○

NEW QUESTION 319
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?

A. From the Cloud App Security admin center, select Users and accounts.
B. From the Microsoft 365 security center, view the Threat tracker.
C. From the Microsoft 365 admin center, view the Security & compliance report.
D. From the Azure Active Directory admin center, view the Risky sign-ins report.

Answer: A

NEW QUESTION 321
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant.
You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)



Review your settings and finish

Name
Sensitivity1

Display name
Sensitivity1

Description for users
Sensitivity1

Scope
File.Email

Encryption

Content marking
Watermark: Watermark
Header: Header

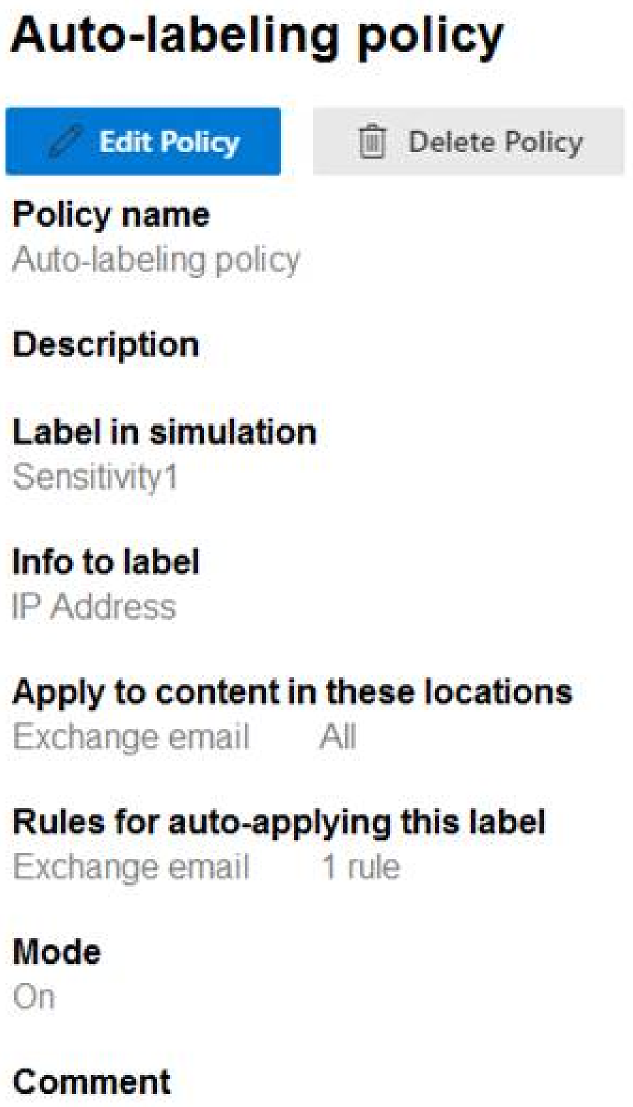
Auto-labeling

Group settings

Site settings

Auto-labeling for database columns
None

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



Auto-labeling policy

Policy name
Auto-labeling policy

Description

Label in simulation
Sensitivity1

Info to label
IP Address

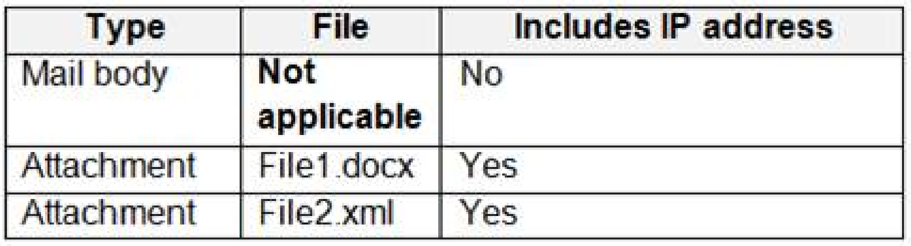
Apply to content in these locations
Exchange email All

Rules for auto-applying this label
Exchange email 1 rule

Mode
On

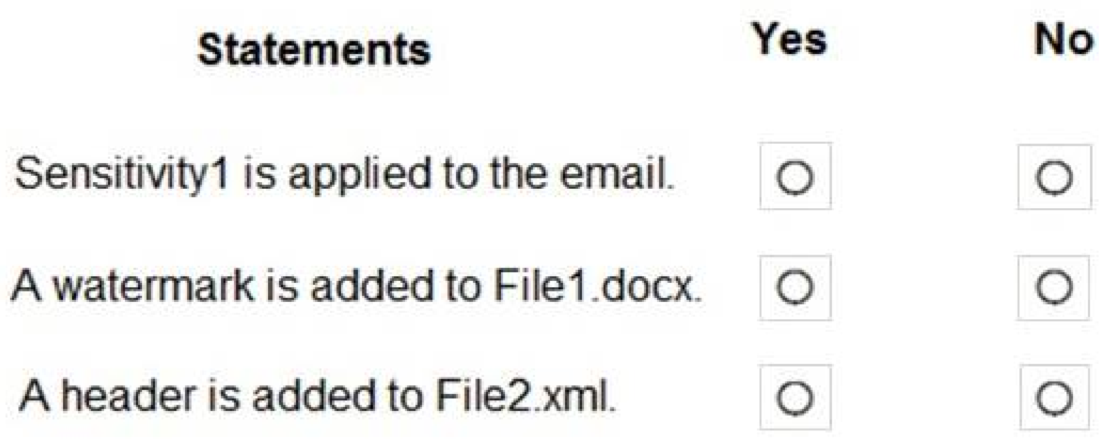
Comment

A user sends an email that contains the components shown in the following table.



Type	File	Includes IP address
Mail body	**Not applicable**	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

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

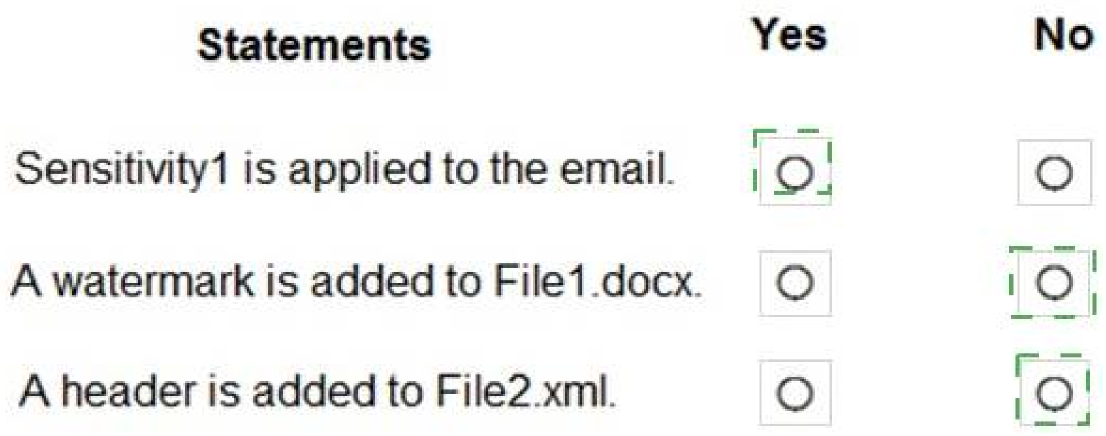


Statements	Yes	No
Sensitivity1 is applied to the email.	○	○
A watermark is added to File1.docx.	○	○
A header is added to File2.xml.	○	○

A. Mastered
B. Not Mastered

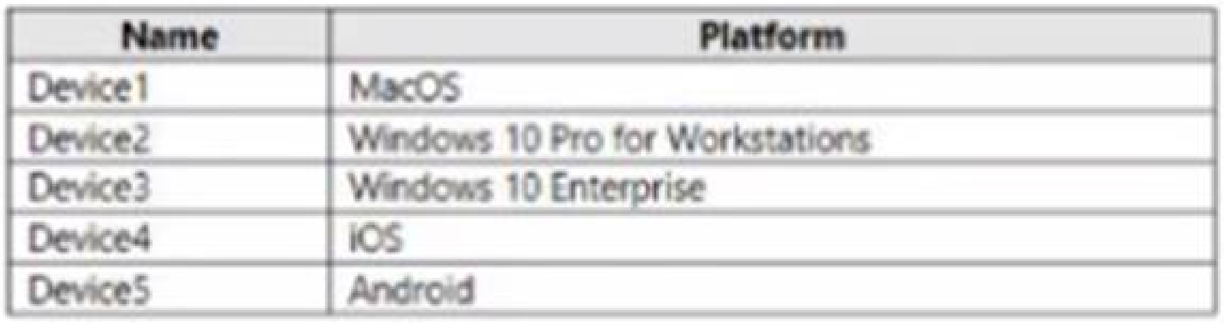
Answer: A

Explanation:



Statements	Yes	No
Sensitivity1 is applied to the email.	[✓ ○]	○
A watermark is added to File1.docx.	○	[✓ ○]
A header is added to File2.xml.	○	[✓ ○]

NEW QUESTION 324
- (Topic 6)
You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.



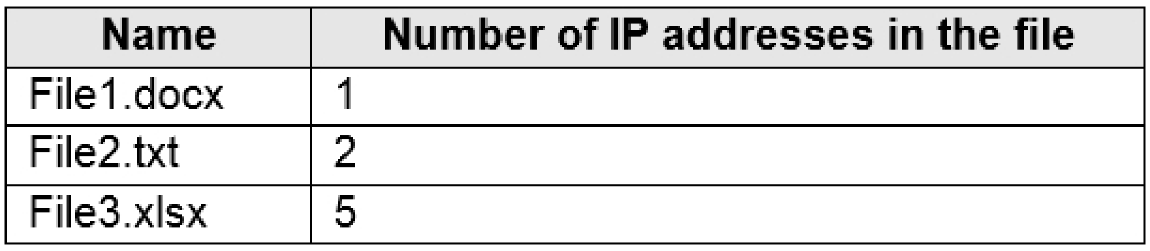
Name	Platform
Device1	MacOS
Device2	Windows 10 Pro for Workstations
Device3	Windows 10 Enterprise
Device4	iOS
Device5	Android

You plan to enable VPN access for the devices.
What is the minimum number of configuration policies required?

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

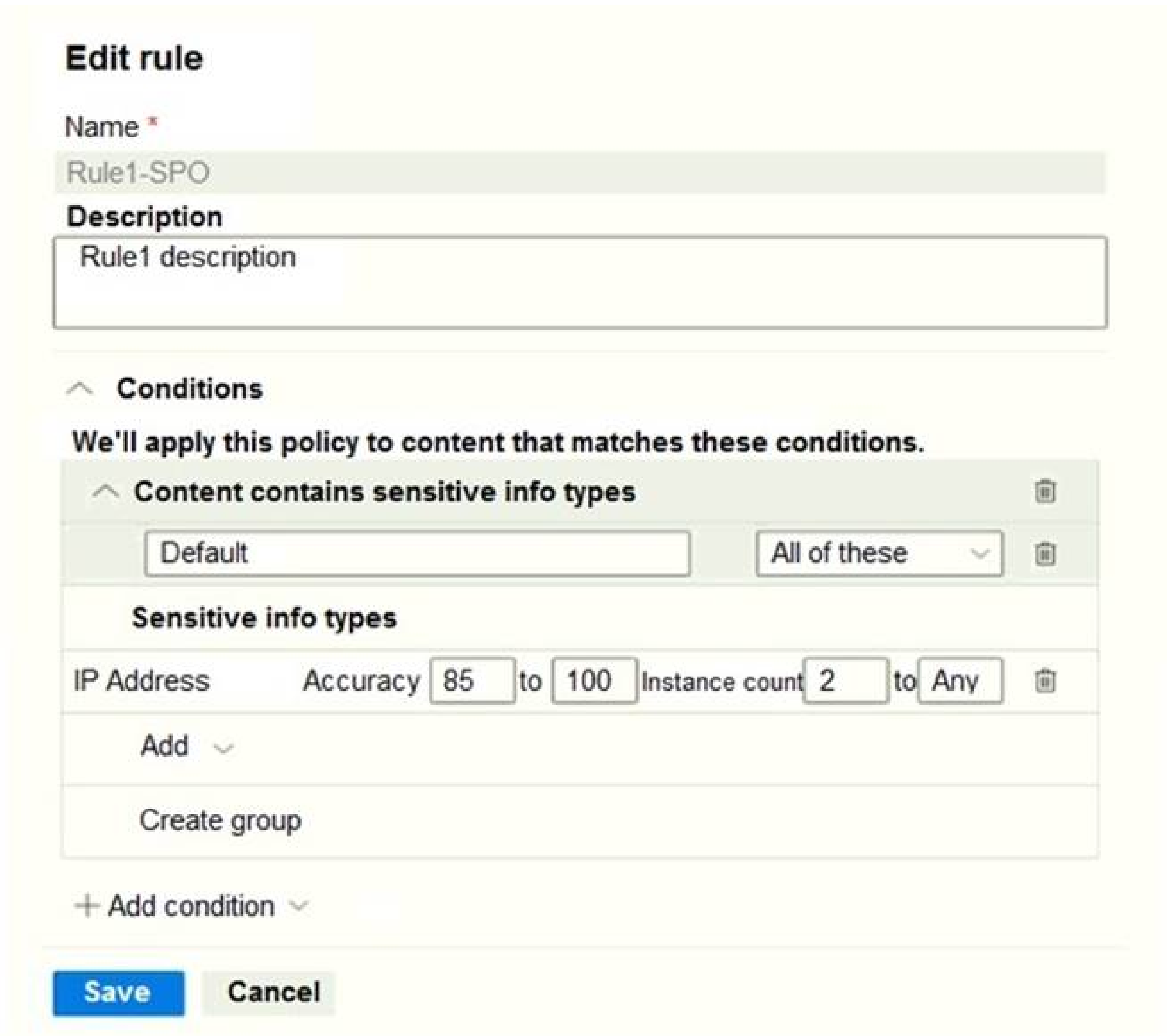
Answer: D

NEW QUESTION 325
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.



Edit rule

Name *

Rule1-SPO

Description

Rule1 description

Conditions

We'll apply this policy to content that matches these conditions.

Content contains sensitive info types

Default — All of these

Sensitive info types

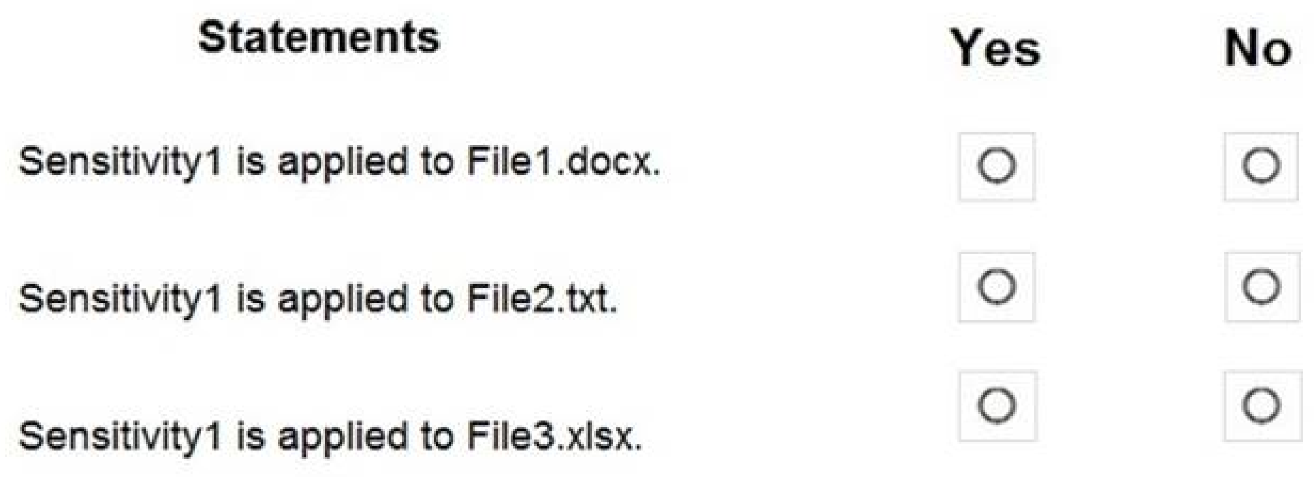
IP Address	Accuracy	85	to	100	Instance count	2	to	Any

Add

Create group

+ Add condition

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

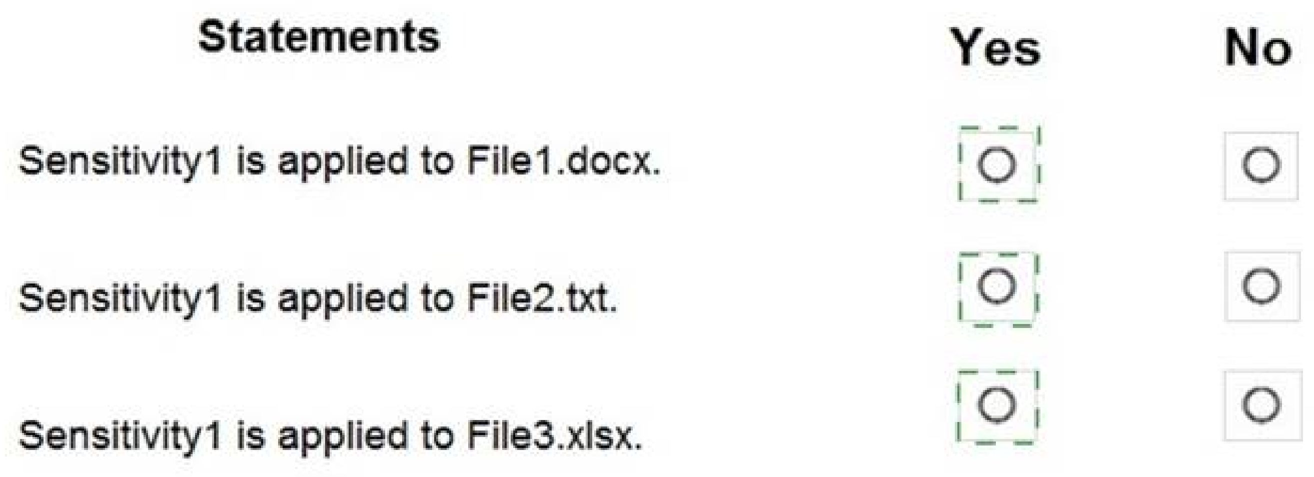


Statements	Yes	No
Sensitivity1 is applied to File1.docx.	○	○
Sensitivity1 is applied to File2.txt.	○	○
Sensitivity1 is applied to File3.xlsx.	○	○

A. Mastered
B. Not Mastered

Answer: A

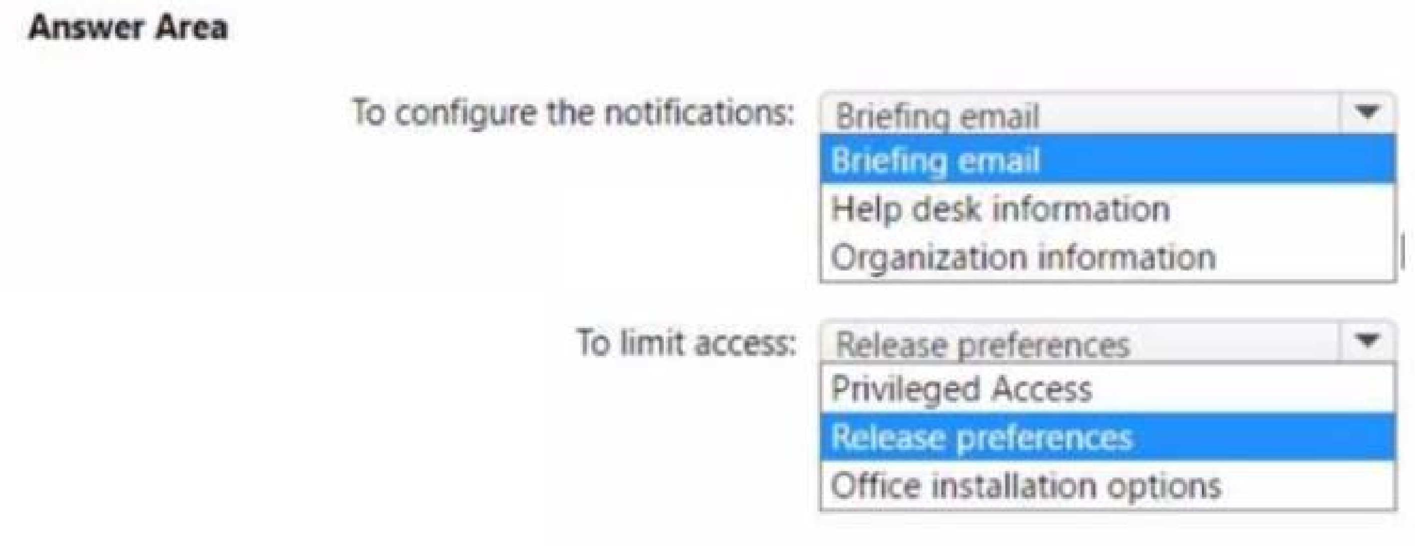
Explanation:



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

NEW QUESTION 326
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

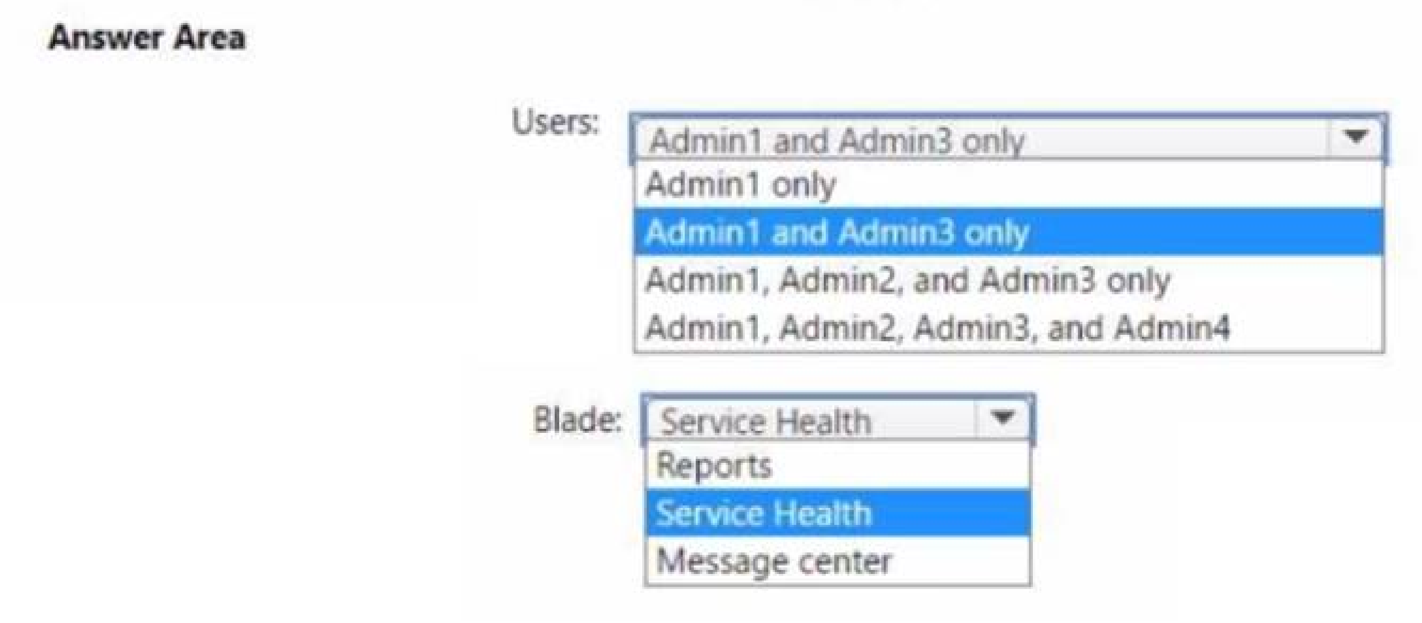
To configure the notifications: Briefing email
- Briefing email
- Help desk information
- Organization information

To limit access: Release preferences
- Privileged Access
- Release preferences
- Office installation options

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 330
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.



Answer Area

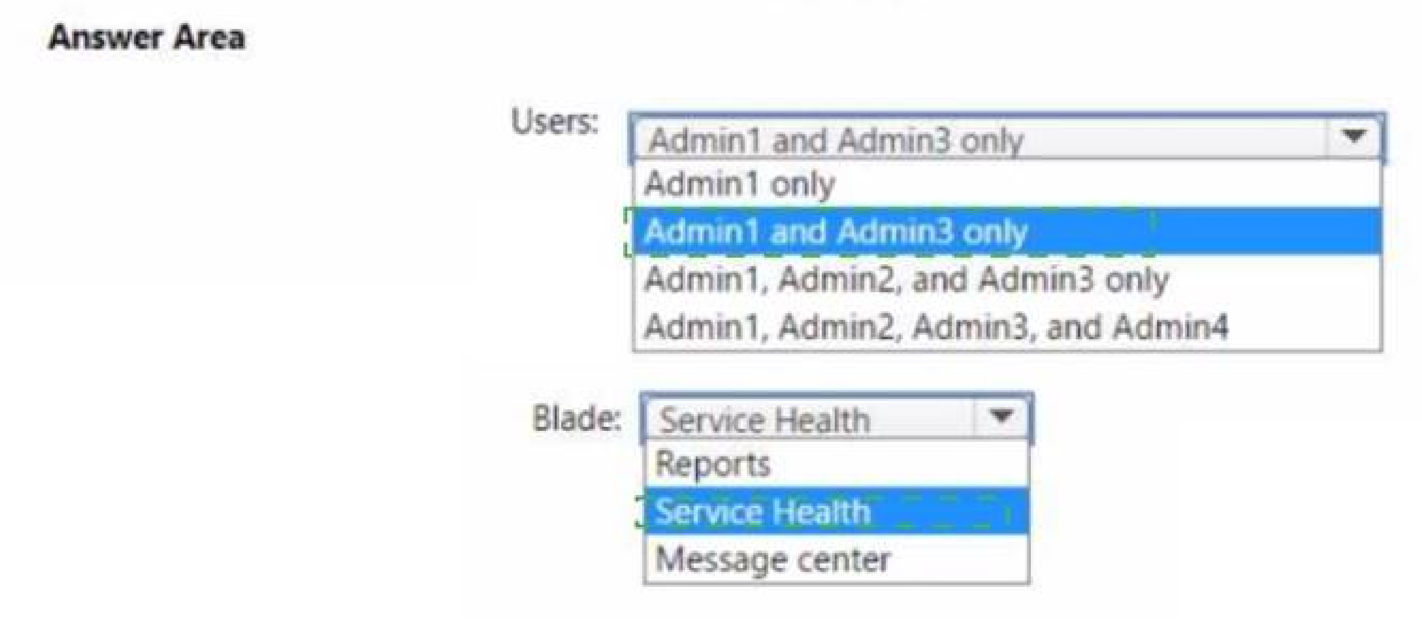
Users: Admin1 and Admin3 only
- Admin1 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Blade: Service Health
- Reports
- Service Health
- Message center

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Users: Admin1 and Admin3 only
- Admin1 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Blade: Service Health
- Reports
- Service Health
- Message center

NEW QUESTION 335
- (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 336
- (Topic 4)
Which role should you assign to User1?
Available Choices (select all choices that are correct)

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

Answer: C

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

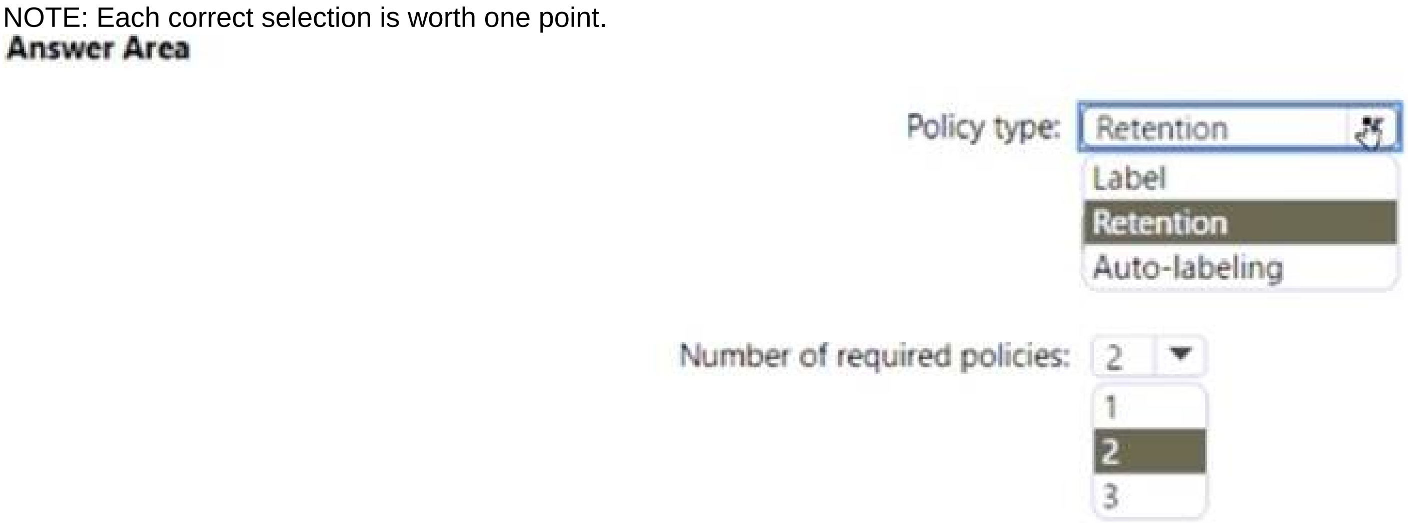
NEW QUESTION 341
- (Topic 4)
You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.
Which authentication strategy should you implement for the pilot projects?

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 346
HOTSPOT - (Topic 3)
You need to configure the information governance settings to meet the technical requirements.
Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

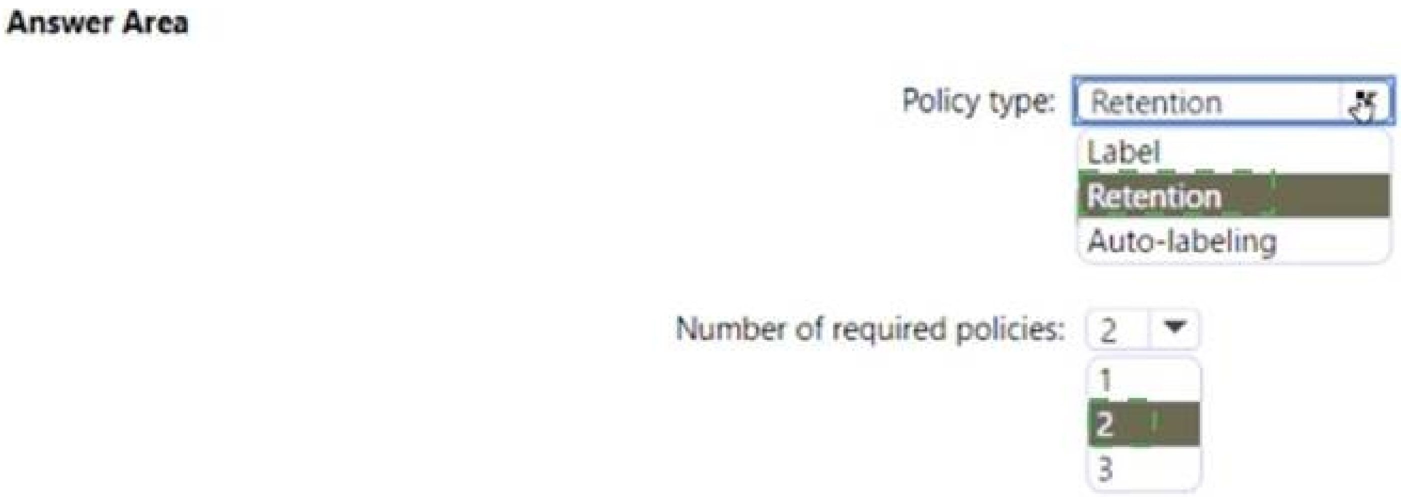
Policy type: Retention

Number of required policies: 2

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

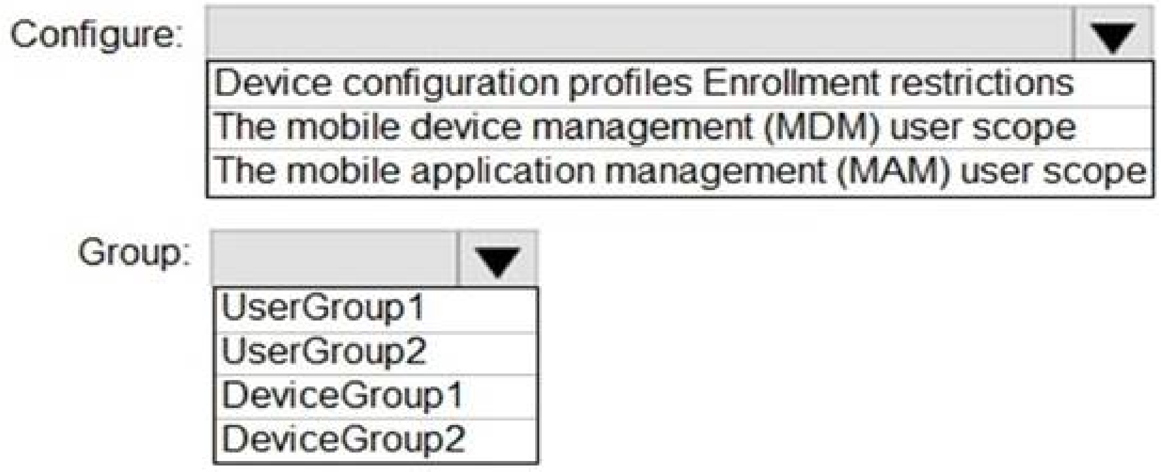
Policy type: Retention

Label
[✓ Retention]
Auto-labeling

Number of required policies: 2

1
[✓ 2]
3

NEW QUESTION 351
HOTSPOT - (Topic 3)
You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.
What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



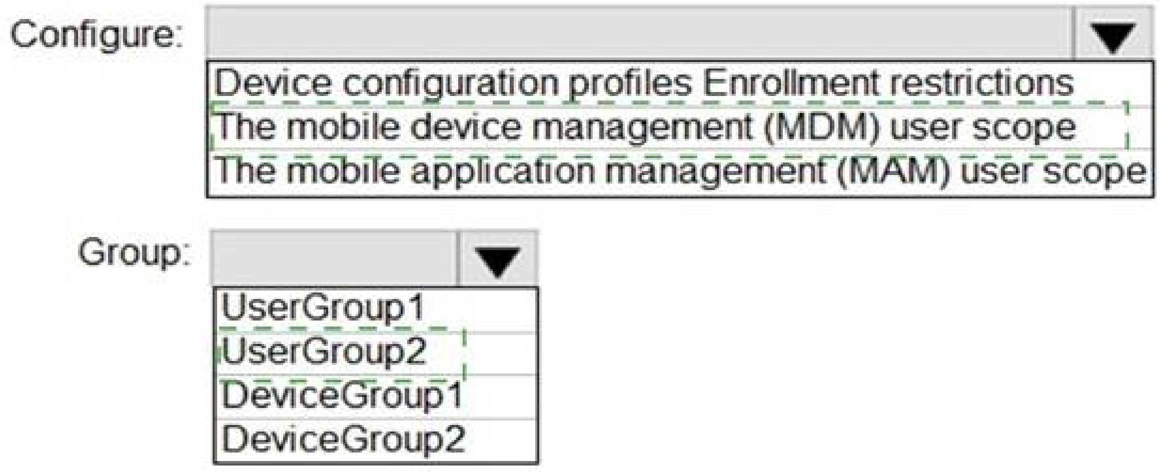
Configure:
Device configuration profiles Enrollment restrictions
The mobile device management (MDM) user scope
The mobile application management (MAM) user scope

Group:
UserGroup1
UserGroup2
DeviceGroup1
DeviceGroup2

A. Mastered
B. Not Mastered

Answer: A

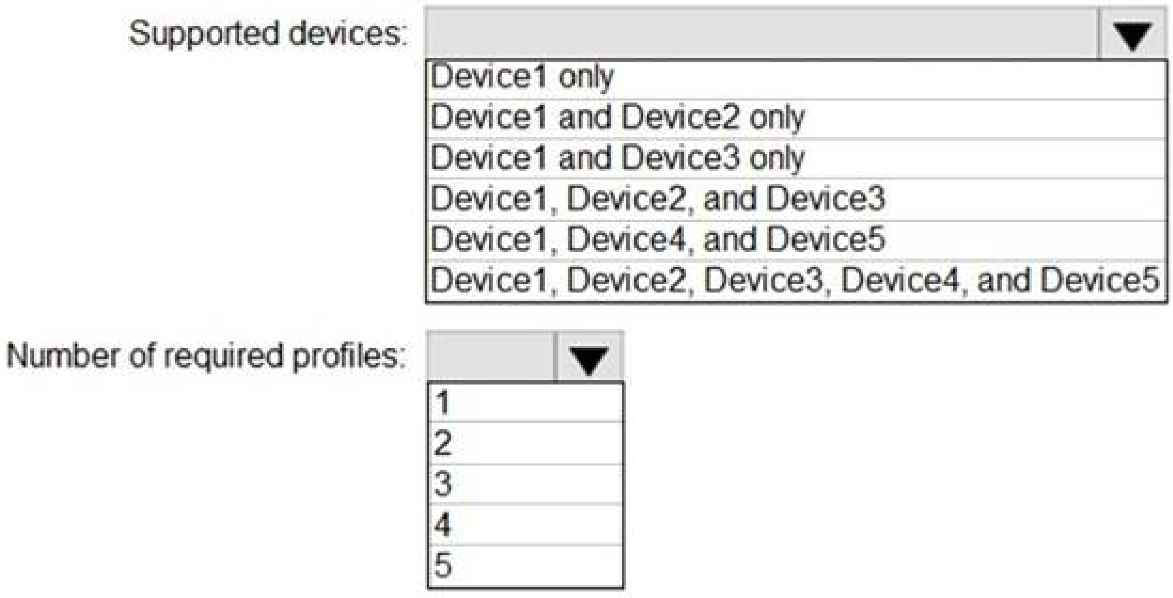
Explanation:



Configure:
Device configuration profiles Enrollment restrictions
[✓ The mobile device management (MDM) user scope]
The mobile application management (MAM) user scope

Group:
UserGroup1
[✓ UserGroup2]
DeviceGroup1
DeviceGroup2

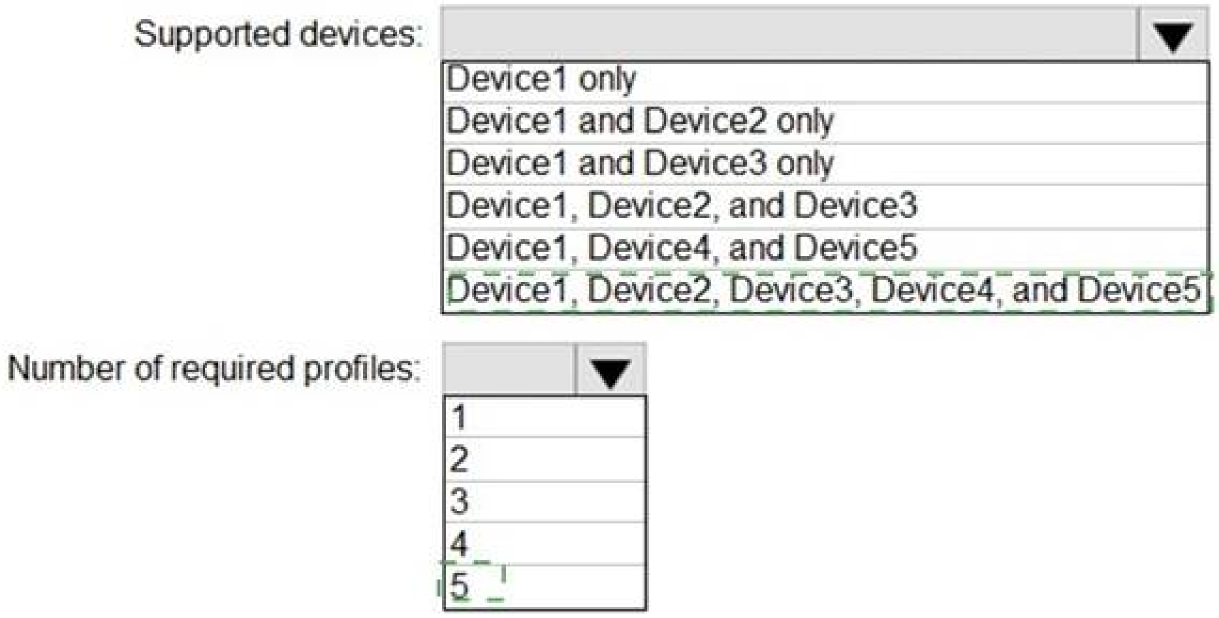
NEW QUESTION 353
HOTSPOT - (Topic 3)
You plan to implement the endpoint protection device configuration profiles to support the planned changes.
You need to identify which devices will be supported, and how many profiles you should implement.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.


Supported devices:
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3
Device1, Device4, and Device5
Device1, Device2, Device3, Device4, and Device5
Number of required profiles:
1
2
3
4
5

A. Mastered
B. Not Mastered

Answer: A

Explanation:


Supported devices:
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3
Device1, Device4, and Device5
Device1, Device2, Device3, Device4, and Device5
Number of required profiles:
1
2
3
4
5

NEW QUESTION 357
- (Topic 2)
You need to meet the technical requirement for the EU PII data. What should you create?

A. a retention policy from the Security & Compliance admin center.
B. a retention policy from the Exchange admin center
C. a data loss prevention (DLP) policy from the Exchange admin center
D. a data loss prevention (DLP) policy from the Security & Compliance admin center

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies
EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

NEW QUESTION 358
- (Topic 1)
On which server should you use the Defender for identity sensor?

A. Server1
B. Server2
C. Server3
D. Server4
E. Servers5

Answer: A

Explanation:
However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

NEW QUESTION 360

......