Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (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 2
- (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 3
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft 365 compliance policies to meet the following requirements:
? Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
? Report on shared documents that contain PII.
What should you create?

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

Answer: B

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

NEW QUESTION 4
- (Topic 6)
Your company has a Microsoft 365 E5 tenant that contains a user named User1. You review the company’s compliance score.
You need to assign the following improvement action to User1:Enable self-service password reset.
What should you do first?

A. From Compliance Manager, turn off automated testing.
B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

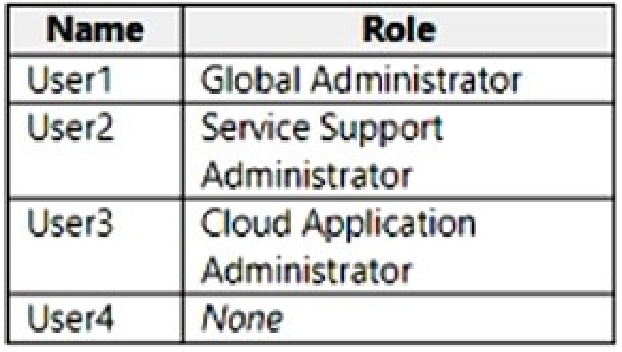
Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide

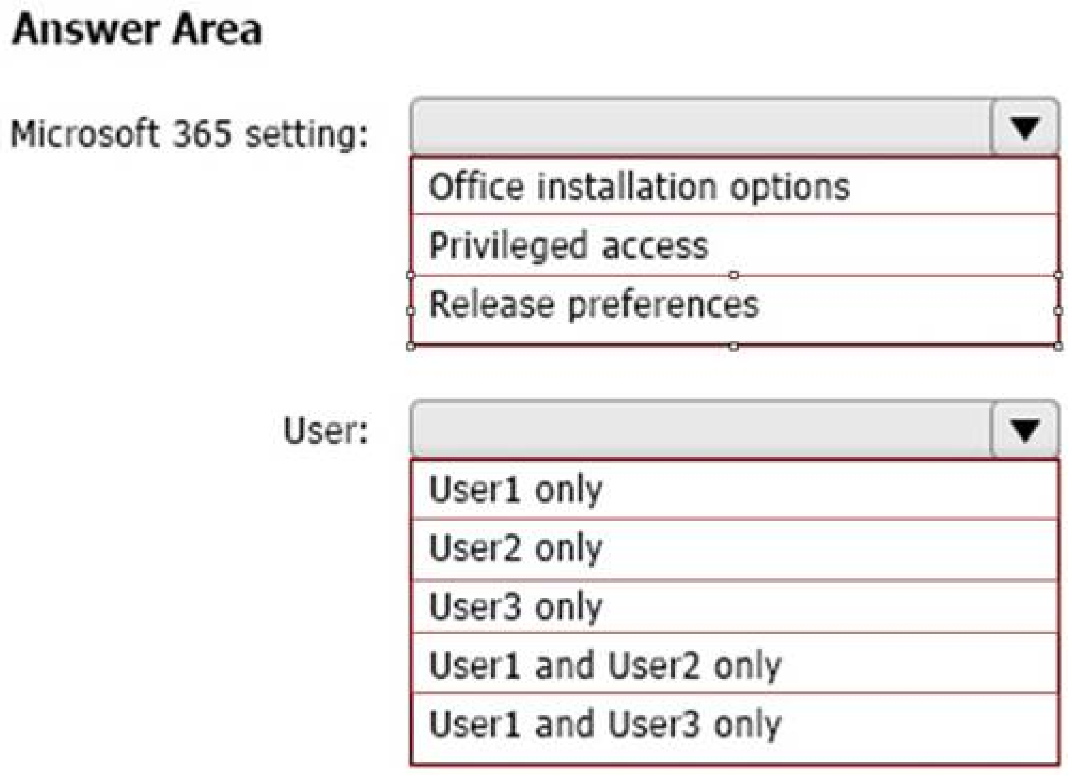
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

NEW QUESTION 5
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

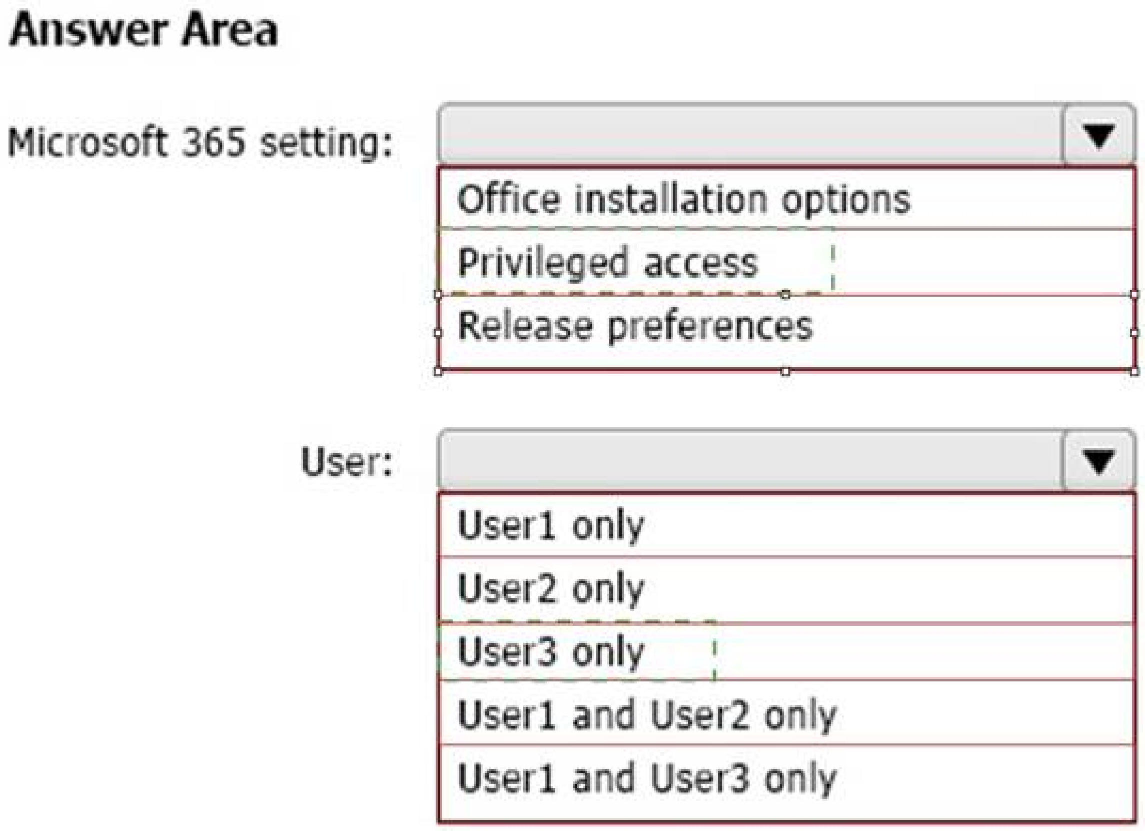
Microsoft 365 setting:
- Office installation options
- Privileged access
- Release preferences

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



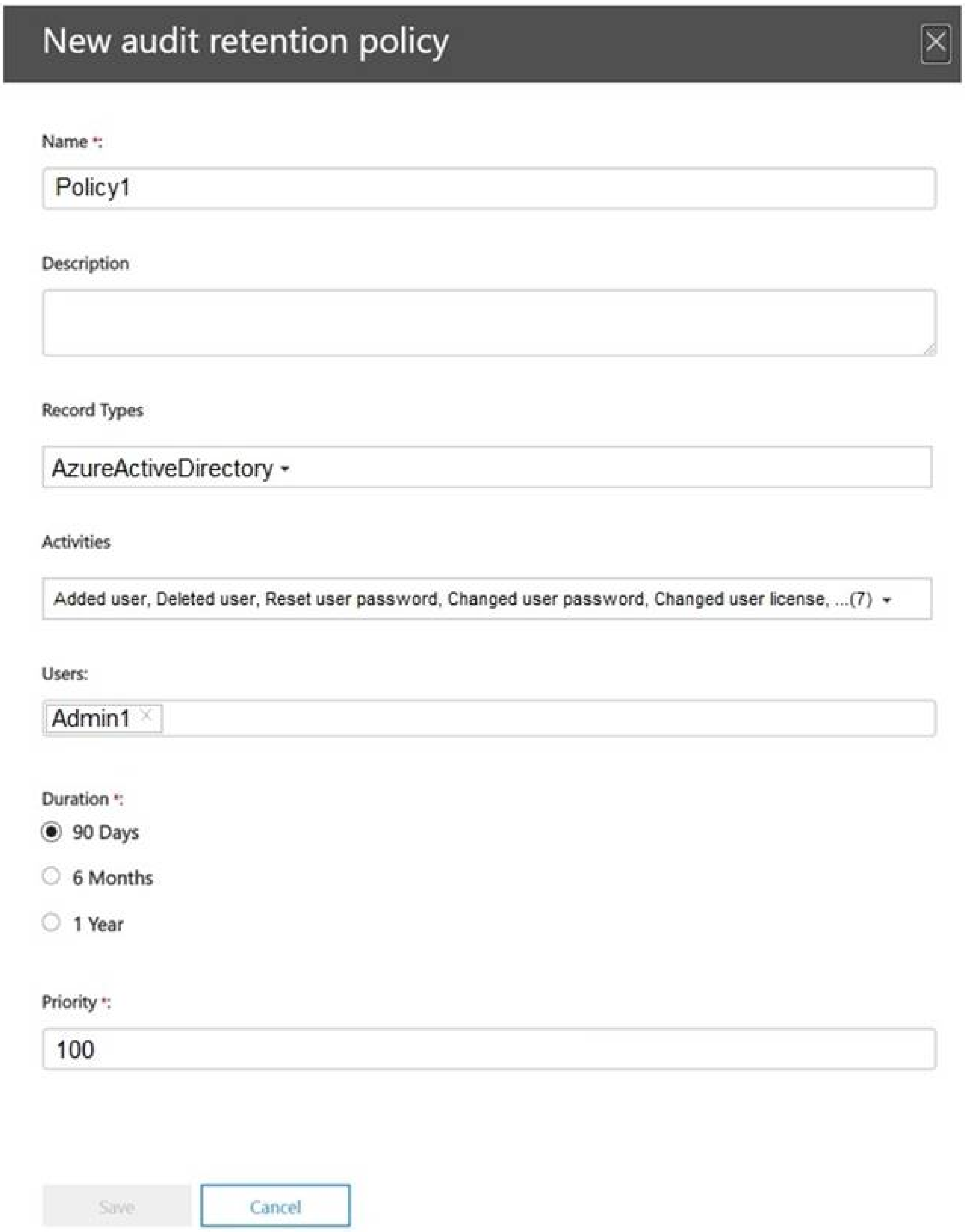
Answer Area

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 6
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

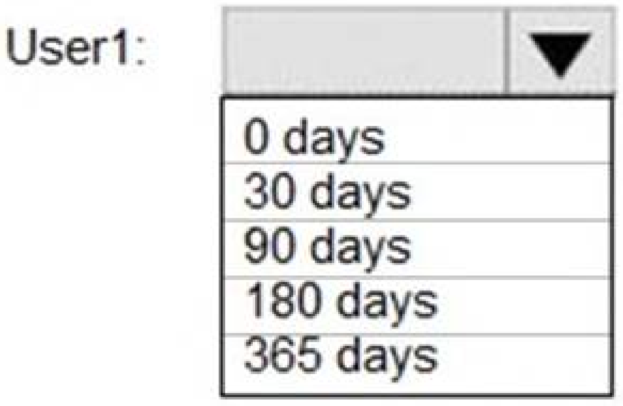
Activities: Added user, Deleted user, Reset user password, Changed user password, Changed user license, ...(7)

Users: Admin1

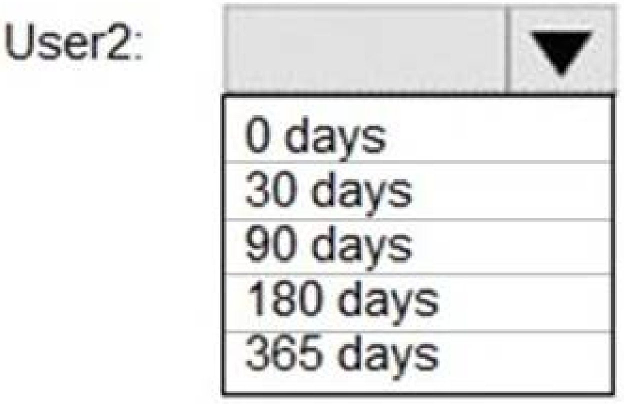
Duration *:
● 90 Days
○ 6 Months
○ 1 Year

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

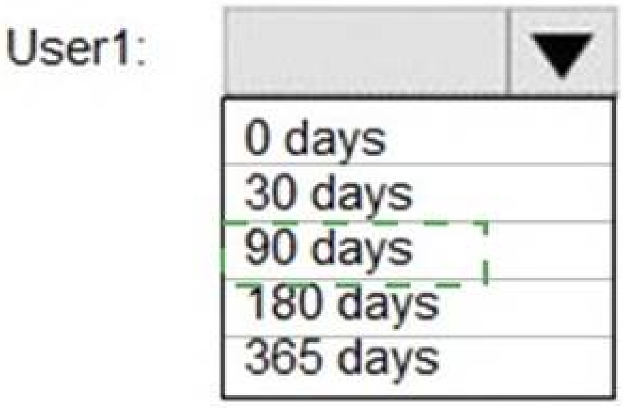

User2:

0 days
30 days
90 days
180 days
365 days

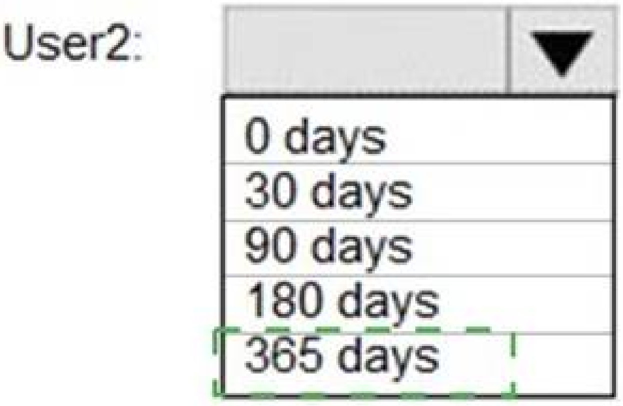
A. Mastered
B. Not Mastered

Answer: A

Explanation:

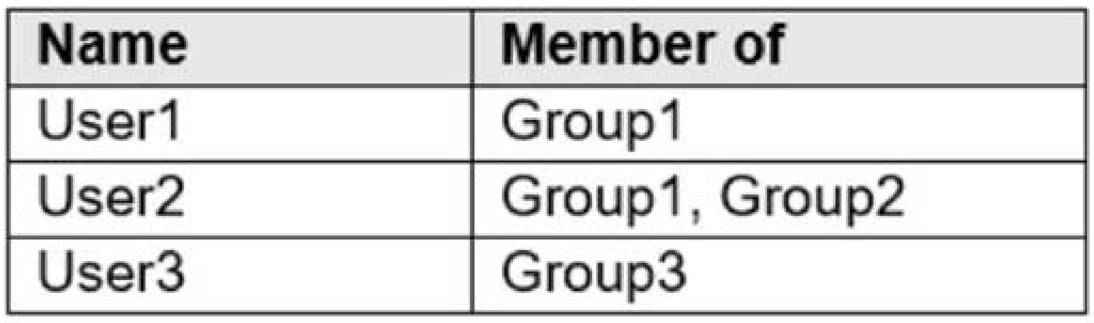

User1:

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


User2:

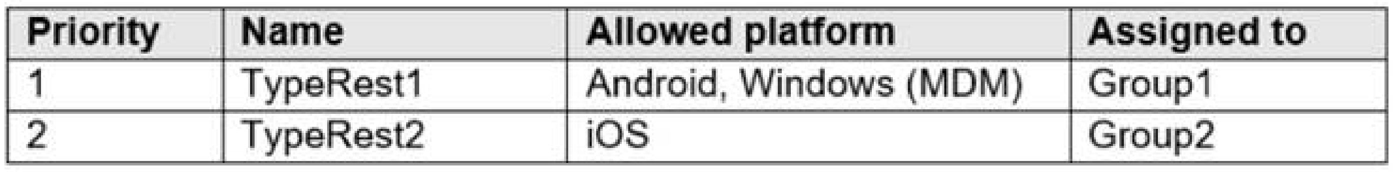
0 days
30 days
90 days
180 days
[✓ 365 days]

NEW QUESTION 7
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription that contains the users in the following table.



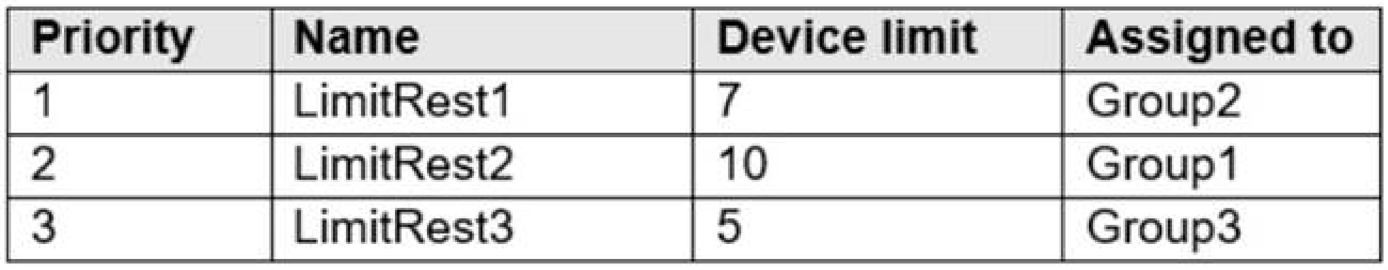
Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

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



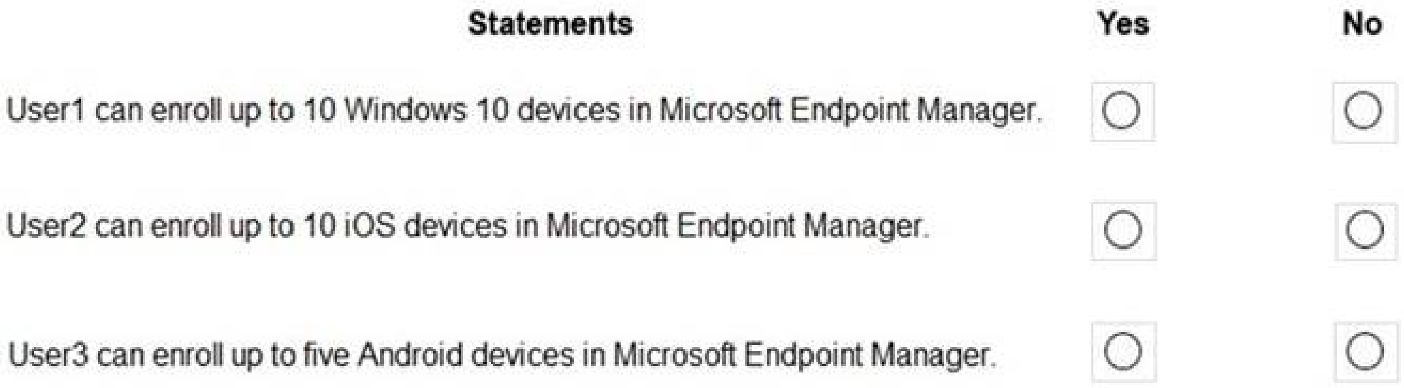
Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

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.

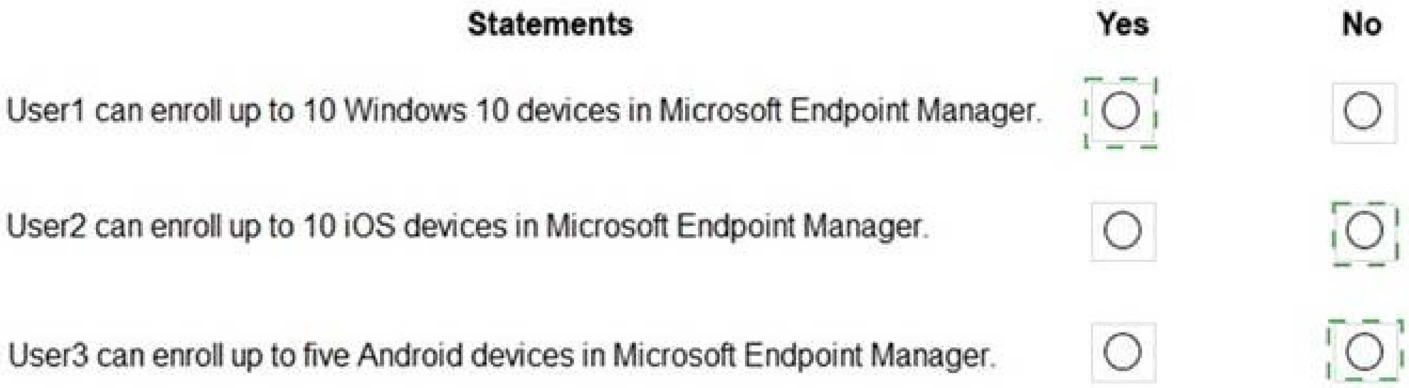


Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



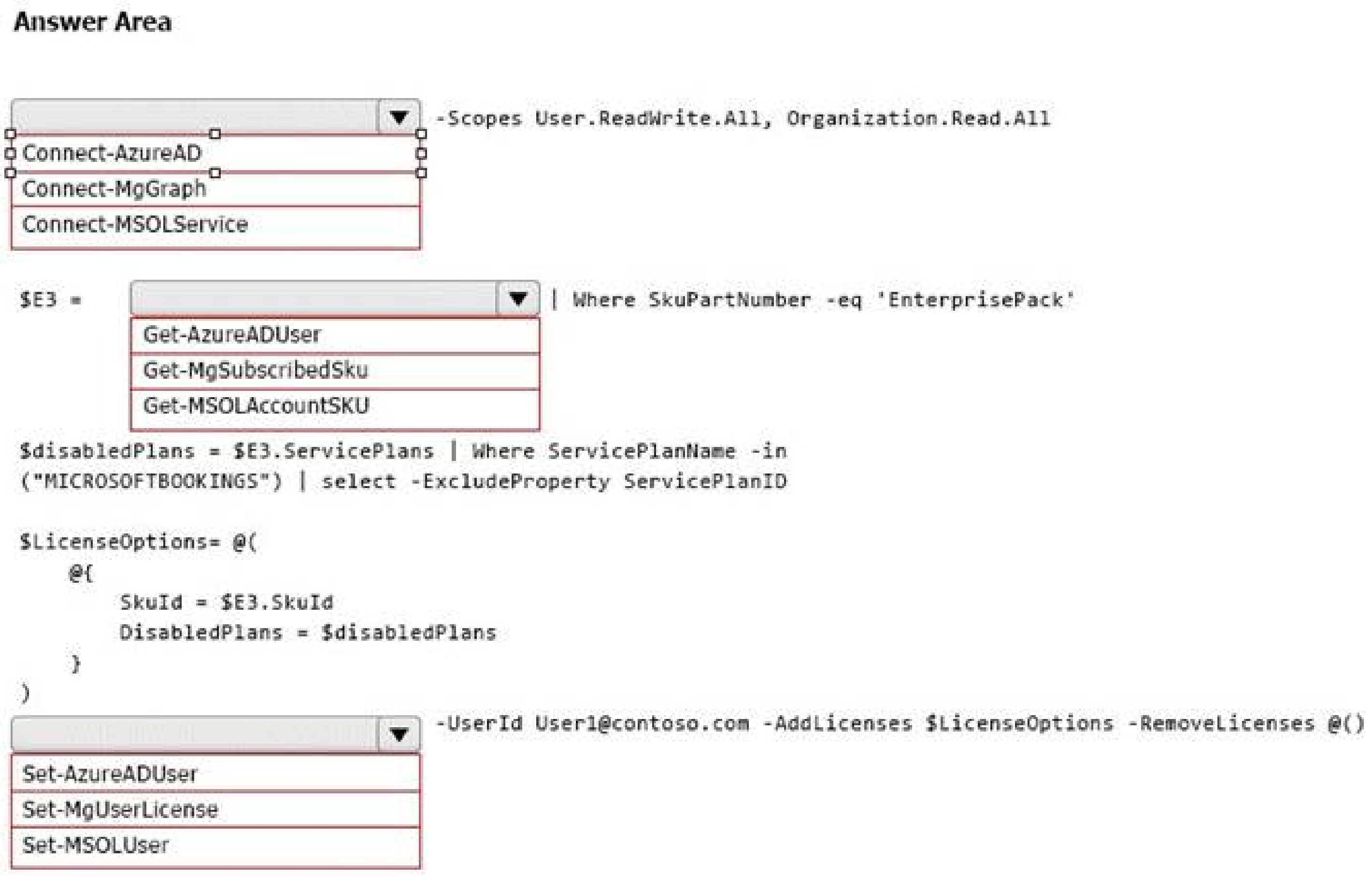
Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	[✓ ○]	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	[✓ ○]
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	[✓ ○]

NEW QUESTION 8
- (Topic 6)
You purchase a new computer that has Windows 10, version 2004 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

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

Answer: B

NEW QUESTION 9
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription.
A user named user1@contoso.com was recently provisioned.
You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

```
-Scopes User.ReadWrite.All, Organization.Read.All
```

```
$E3 =
```

```
| Where SkuPartNumber -eq 'EnterprisePack'
$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$LicenseOptions= @(
    @{
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    }
)
```

```
-UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @()
```

A. Mastered
B. Not Mastered

Answer: A

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

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

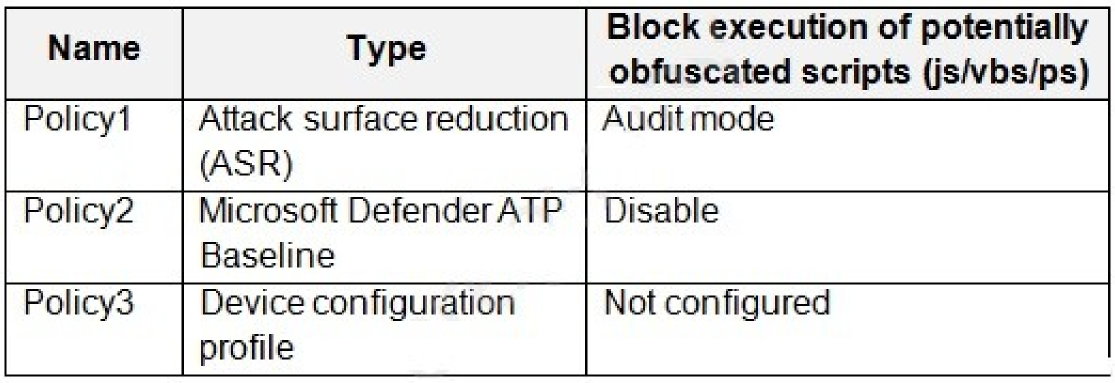
A. Window 10 Pro, version 1909
B. Window 10 Pro, version 2004
C. Window 10 Pro, version 1909

D. Window 10 Enterprise, version 2004

Answer: D

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

NEW QUESTION 11
- (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

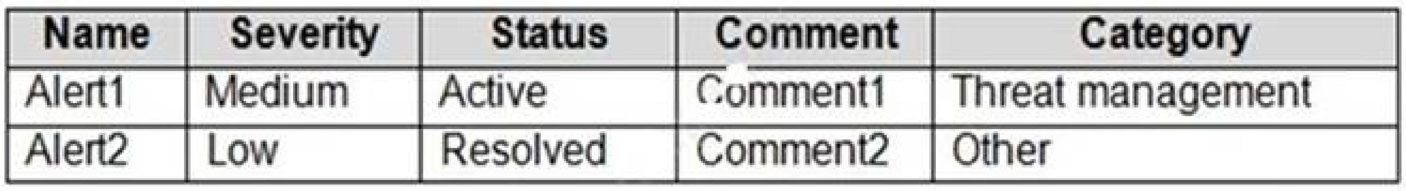
NEW QUESTION 15
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance 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 16
- (Topic 6)
You have a Microsoft 365 subscription that contains the alerts shown in the following table.



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

Which properties of the alerts can you modify?

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

Answer: B

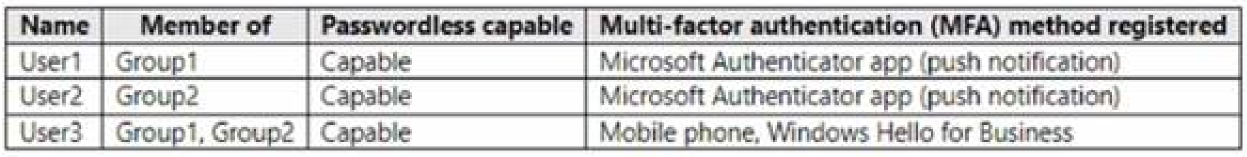
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365-worldwide#limitations

NEW QUESTION 17
- (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

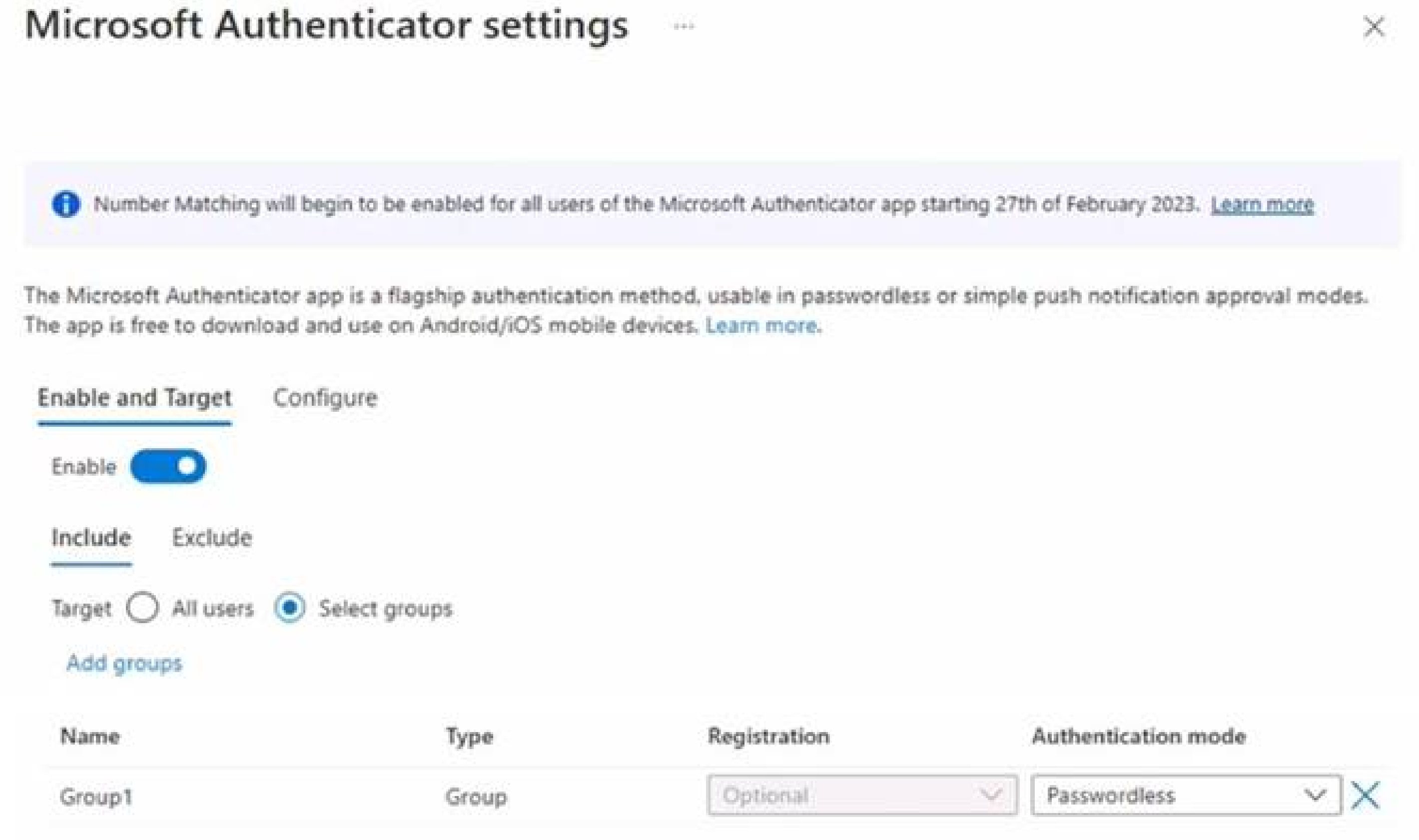
Answer: C

NEW QUESTION 21
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



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

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



Microsoft Authenticator settings

Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. Learn more

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. Learn more.

Enable and Target | Configure

Enable: On

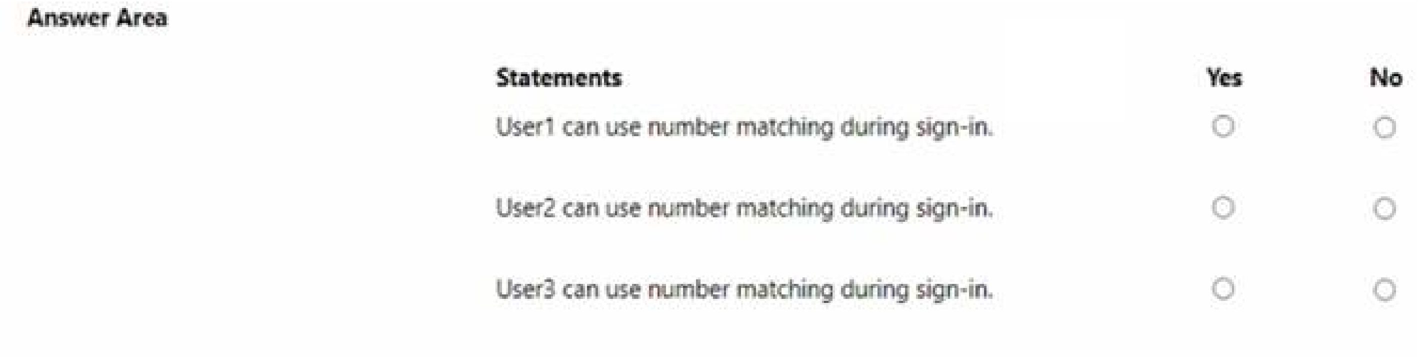
Include | Exclude

Target ○ All users ● Select groups

Add groups

Name	Type	Registration	Authentication mode
Group1	Group	Optional	Passwordless

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



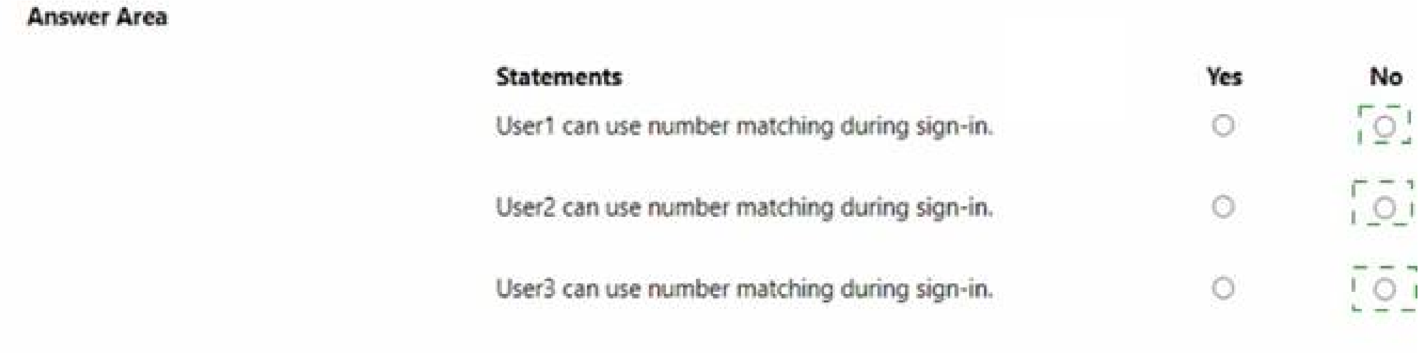
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

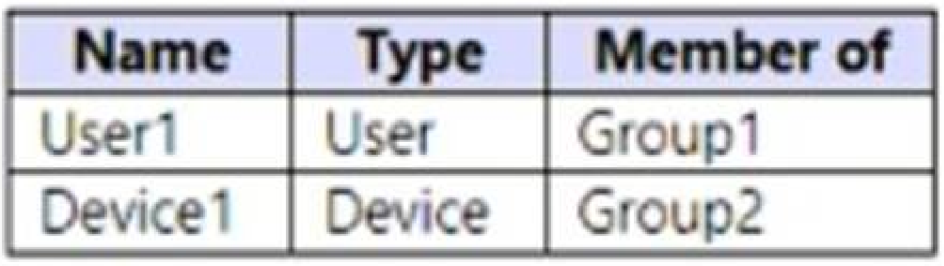
Statements	Yes	No
User1 can use number matching during sign-in.	○	[✓ ○]
User2 can use number matching during sign-in.	○	[✓ ○]
User3 can use number matching during sign-in.	○	[✓ ○]

NEW QUESTION 23
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature. You need to block users from downloading a file named File1.exe.
What should you use?

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

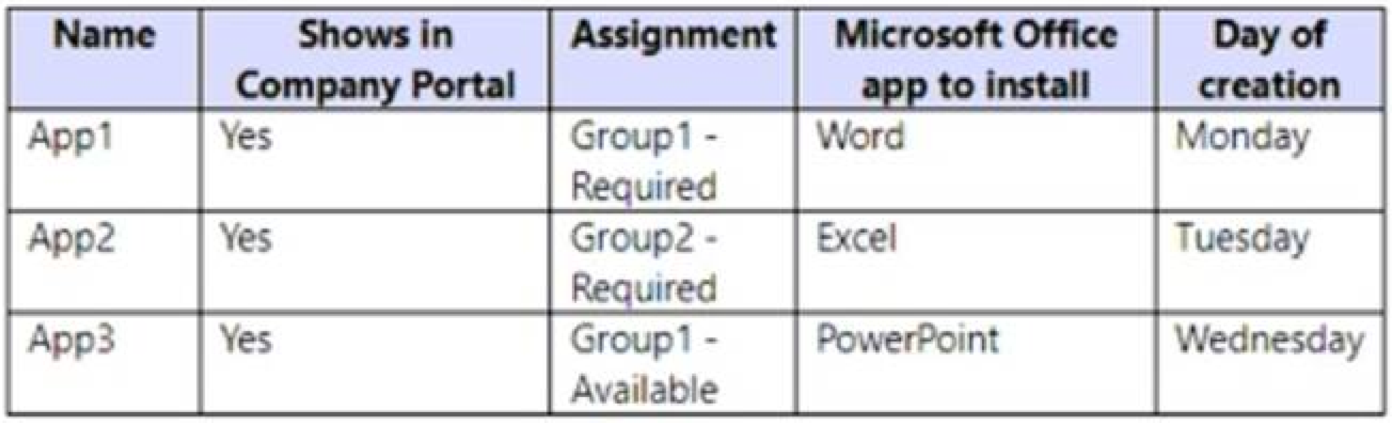
Answer: A

NEW QUESTION 27
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft intune. The subscription contains the resources shown in the following table.



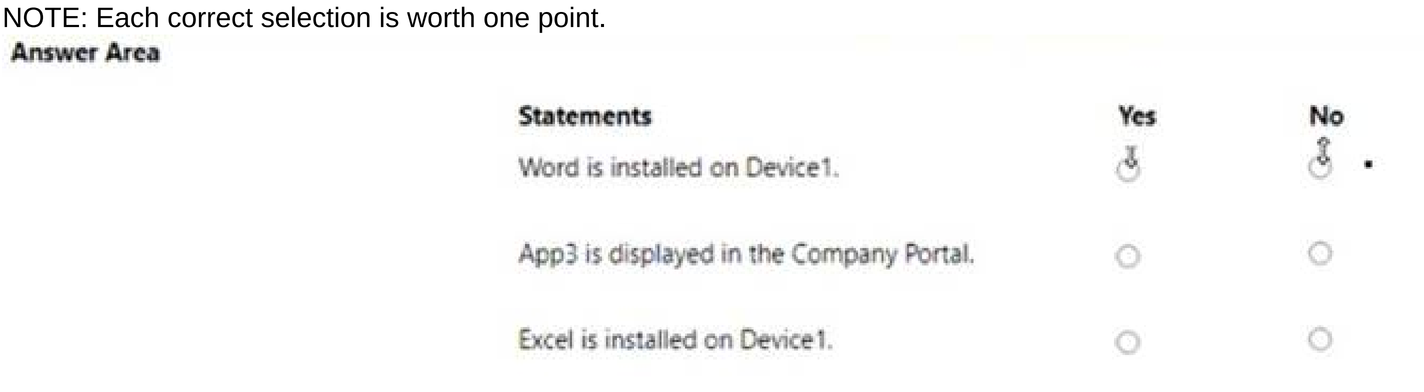
Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

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.



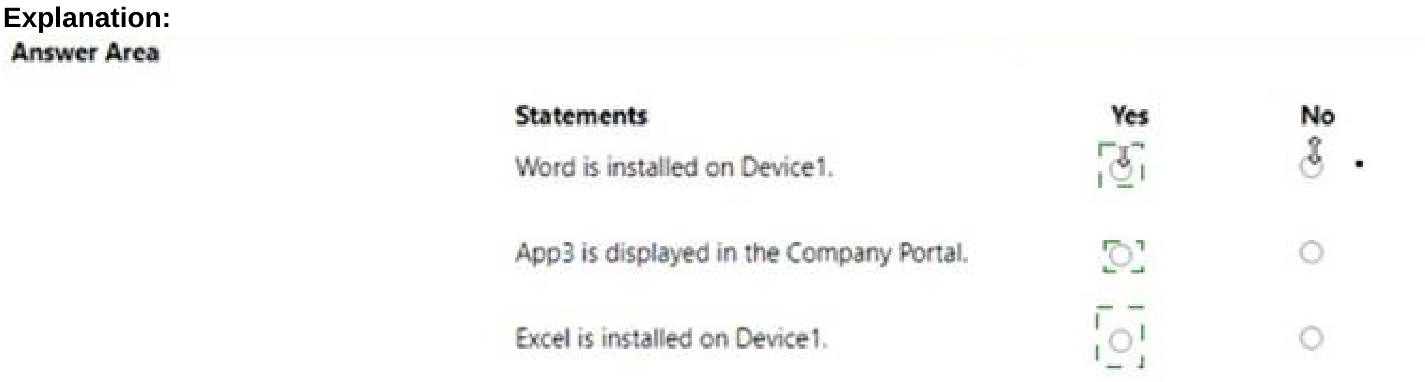
Answer Area

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

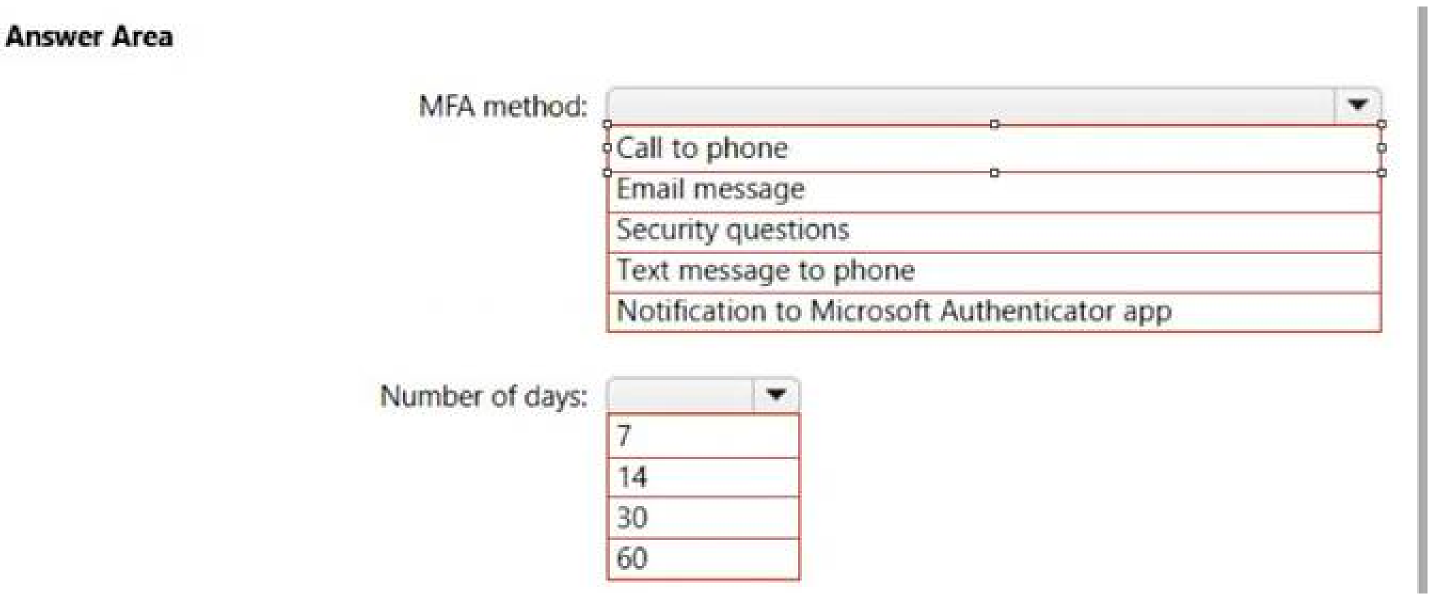
Explanation:



Answer Area

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

NEW QUESTION 32
HOTSPOT - (Topic 6)
HOTSPOT
You have a new Microsoft 365 E5 tenant. Enable Security defaults is set to Yes.
A user signs in to the tenant for the first time.
Which multi-factor authentication (MFA) method can the user use, and how many days does the user have to register for MFA? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

MFA method:
- Call to phone
- Email message
- Security questions
- Text message to phone
- Notification to Microsoft Authenticator app

Number of days:
- 7
- 14
- 30
- 60

A. Mastered
B. Not Mastered

Answer: A

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

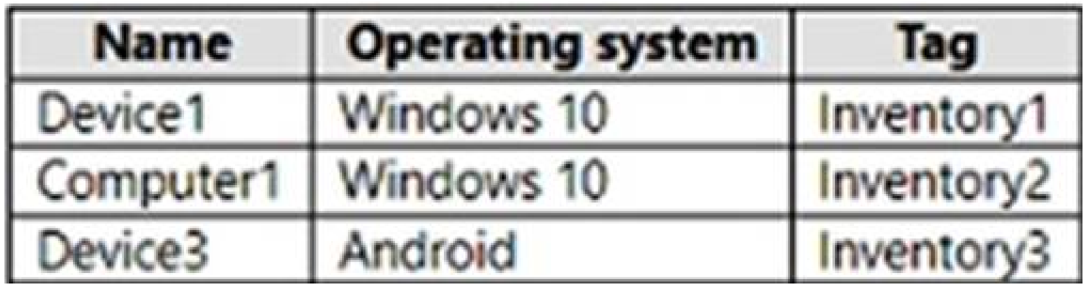
NEW QUESTION 34
- (Topic 6)
You have a Microsoft 365 subscription.
You need to configure a compliance solution that meets the following requirements: Defines sensitive data based on existing data samples
Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint 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

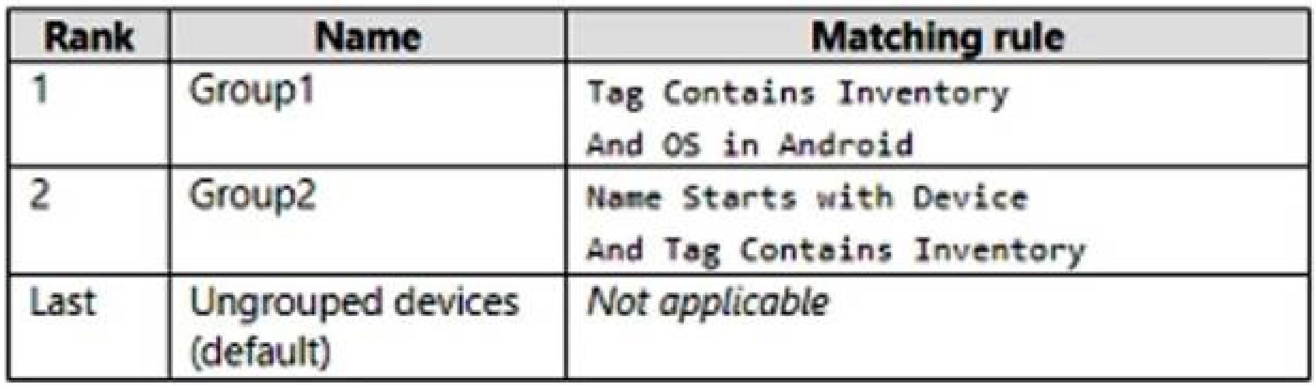
Explanation:
A: Classifiers
This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that 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 36
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.



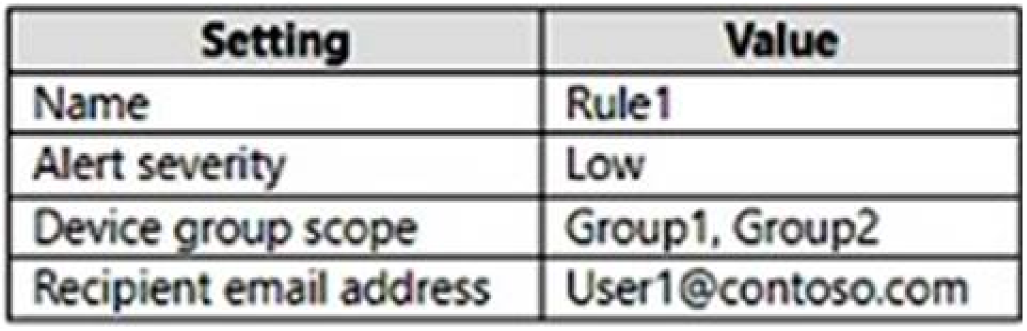
Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

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



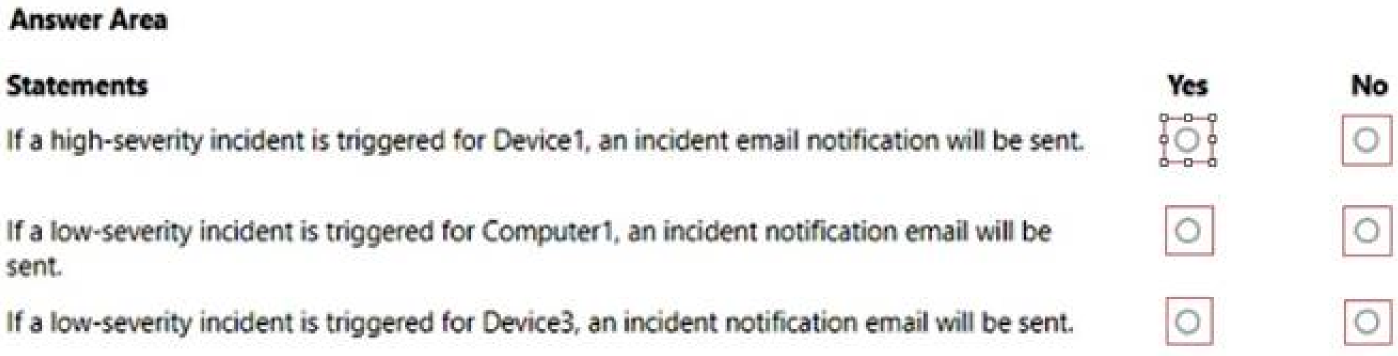
Rank	Name	Matching rule
1	Group1	Tag Contains Inventory And OS in Android
2	Group2	Name Starts with Device And Tag Contains Inventory
Last	Ungrouped devices (default)	*Not applicable*

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



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

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



Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 40
- (Topic 6)
You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.
Devices are onboarded by using Microsoft Defender for Endpoint.
You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.
What should you create first?

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

Answer: B

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

NEW QUESTION 45
- (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 50
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

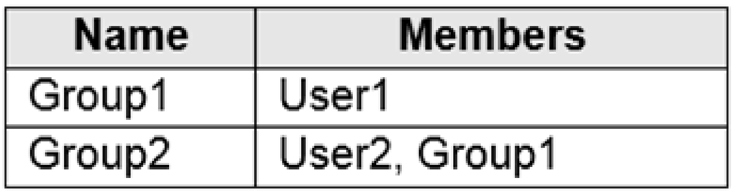
Explanation:
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

NEW QUESTION 52
- (Topic 6)
Your company has on-premises servers and an Azure AD tenant.
Several months ago, the Azure AD Connect Hearth agent was installed on all the servers. You review the health status of all the servers regularly.
Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect Servers list.
You suspect that another administrator removed Server1 from the list. You need to ensure that you can view the health status of Server1.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

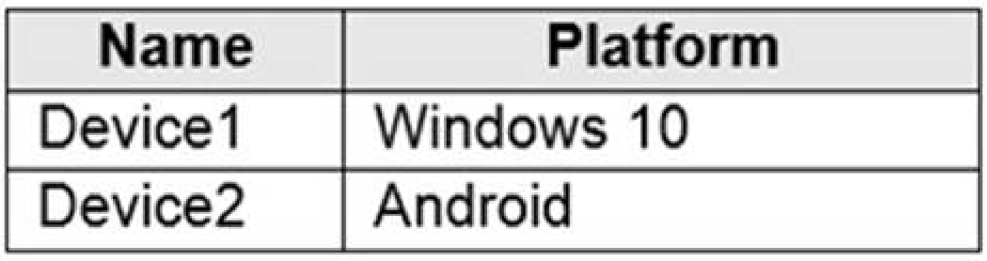
Answer: DE

NEW QUESTION 55
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.



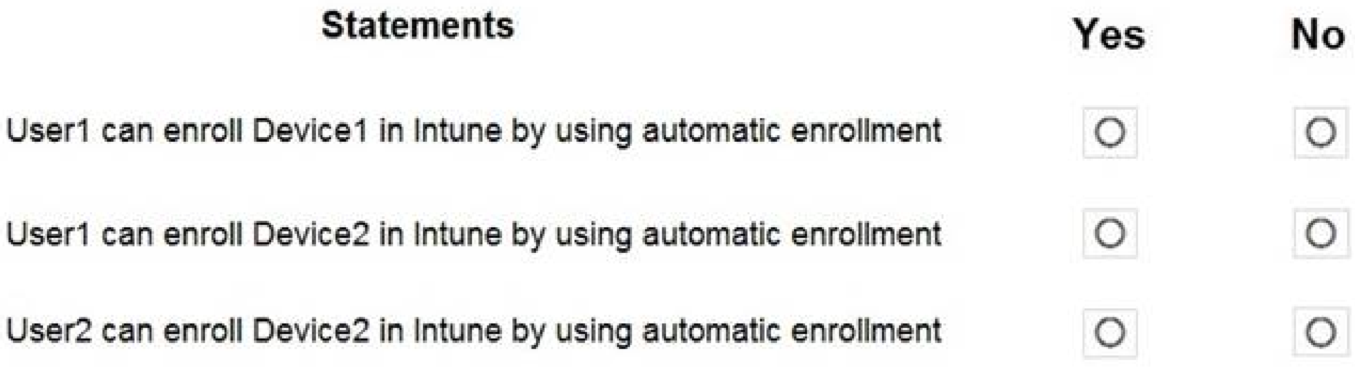
Name	Members
Group1	User1
Group2	User2, Group1

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



Name	Platform
Device1	Windows 10
Device2	Android

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

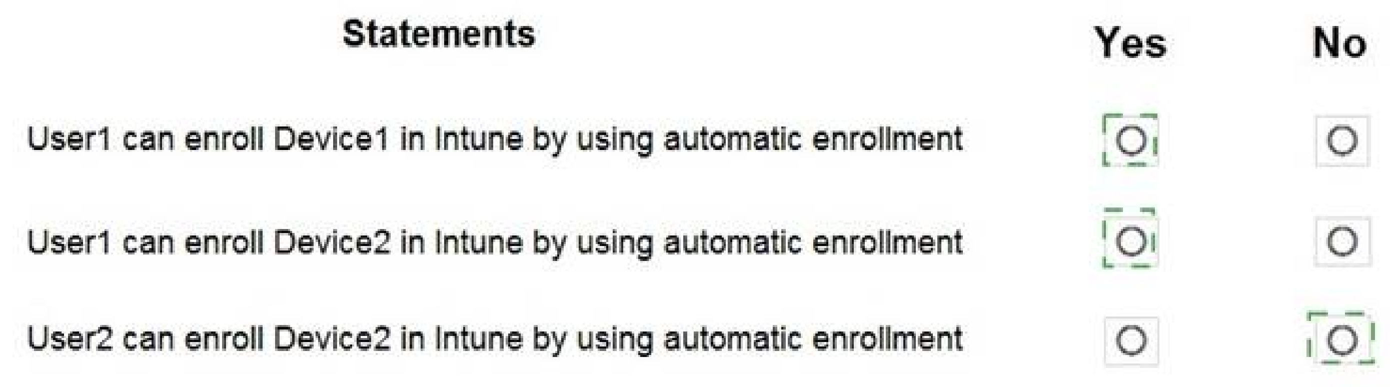


Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

A. Mastered
B. Not Mastered

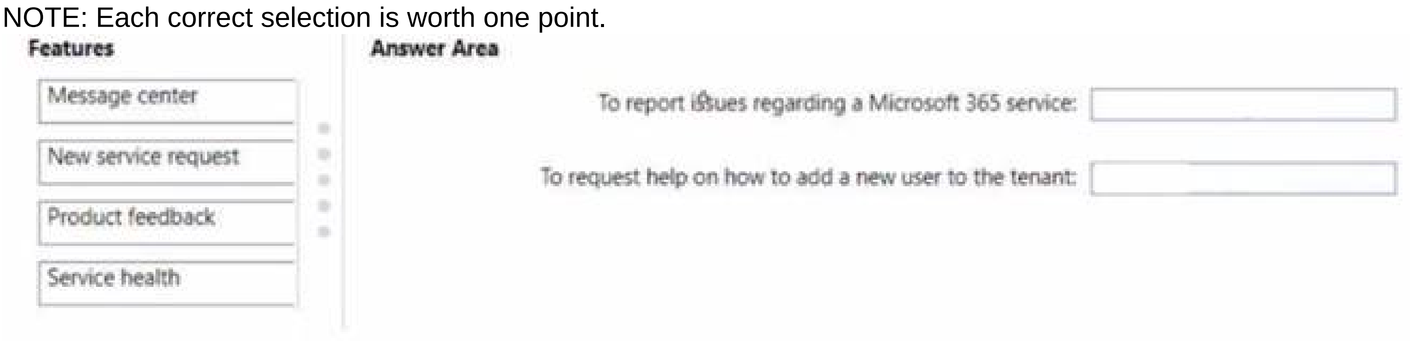
Answer: A

Explanation:



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

NEW QUESTION 60
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You need to meet the following requirements:
• Report a Microsoft 365 service issue.
• Request help on how to add a new user to an Azure AD tenant.
What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



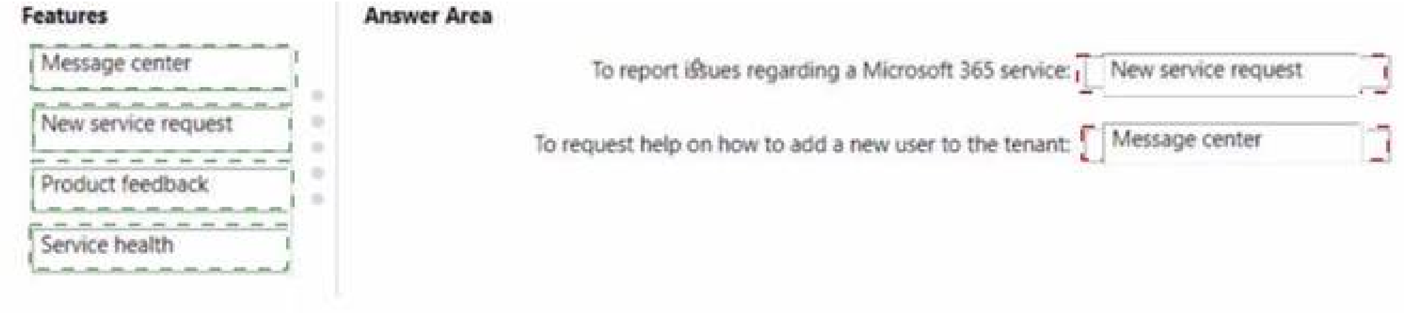
Features
Message center
New service request
Product feedback
Service health

Answer Area
To report issues regarding a Microsoft 365 service:
To request help on how to add a new user to the tenant:

A. Mastered
B. Not Mastered

Answer: A

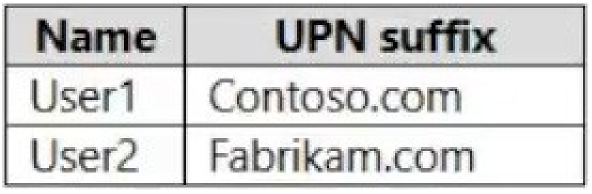
Explanation:



Features
Message center
New service request
Product feedback
Service health

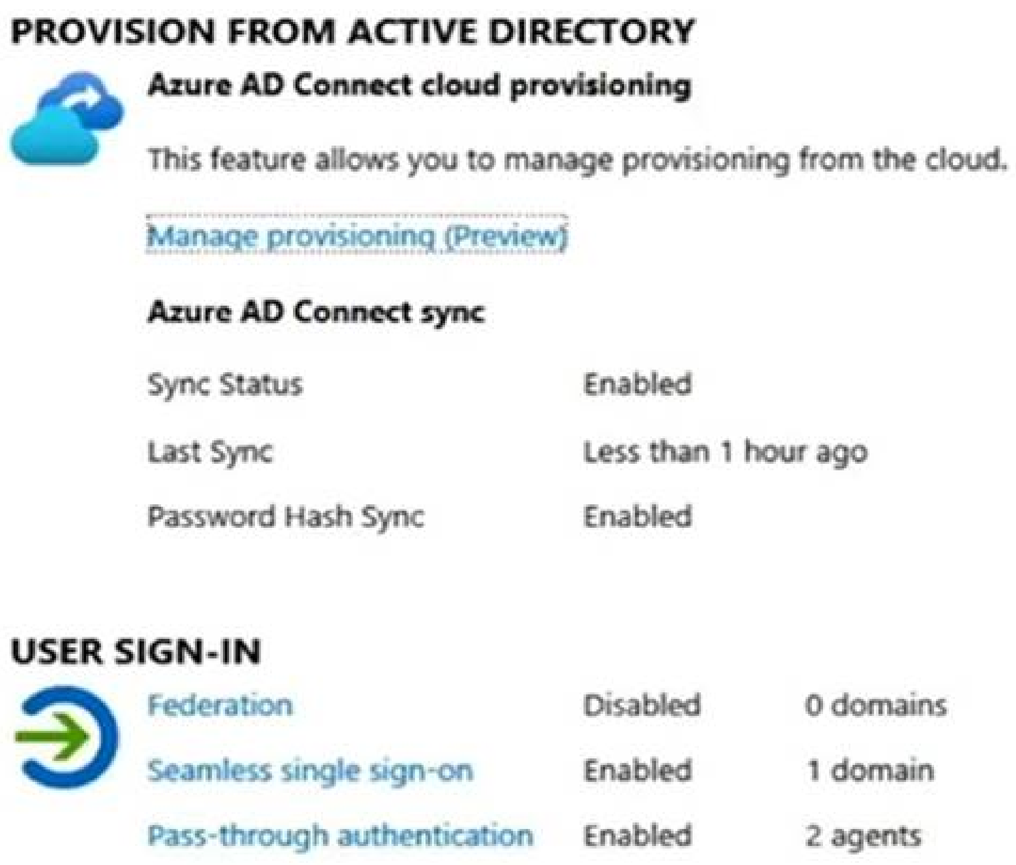
Answer Area
To report issues regarding a Microsoft 365 service: New service request
To request help on how to add a new user to the tenant: Message center

NEW QUESTION 63
- (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 68
- (Topic 6)
Your on-premises network contains an Active Directory domain. You have a Microsoft 365 E5 subscription.
You plan to implement a hybrid configuration that has the following requirements:
• Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources
• Supports the use of Azure AD Identity Protection
You need to configure Azure AD Connect to support the planned implementation. Which two options should you select? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AB

NEW QUESTION 72
- (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?

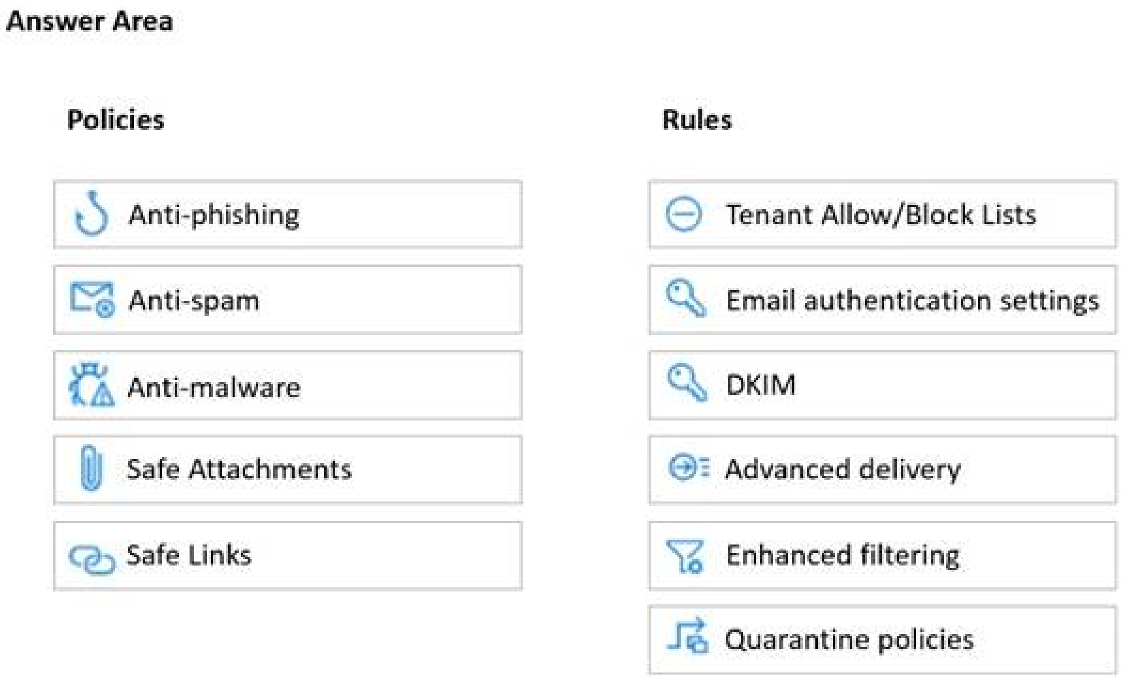
A. a Microsoft OneDrive for Business folder
B. a Microsoft SharePoint Online document library
C. a Microsoft 365 mailbox
D. Azure Files

Answer: C

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

NEW QUESTION 73
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to use a mailbox named Mailbox1 to analyze malicious email messages. You need to configure Microsoft Defender for Office 365 to meet the following requirements:

• Ensure that incoming email is NOT filtered for Mailbox1.
• Detect impersonation and spoofing attacks on all other mailboxes in the subscription. Which two settings should you configure? To answer, select the appropriate settings in the
answer area.



Answer Area

Policies
- Anti-phishing
- Anti-spam
- Anti-malware
- Safe Attachments
- Safe Links

Rules
- Tenant Allow/Block Lists
- Email authentication settings
- DKIM
- Advanced delivery
- Enhanced filtering
- Quarantine policies

A. Mastered
B. Not Mastered

Answer: A

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

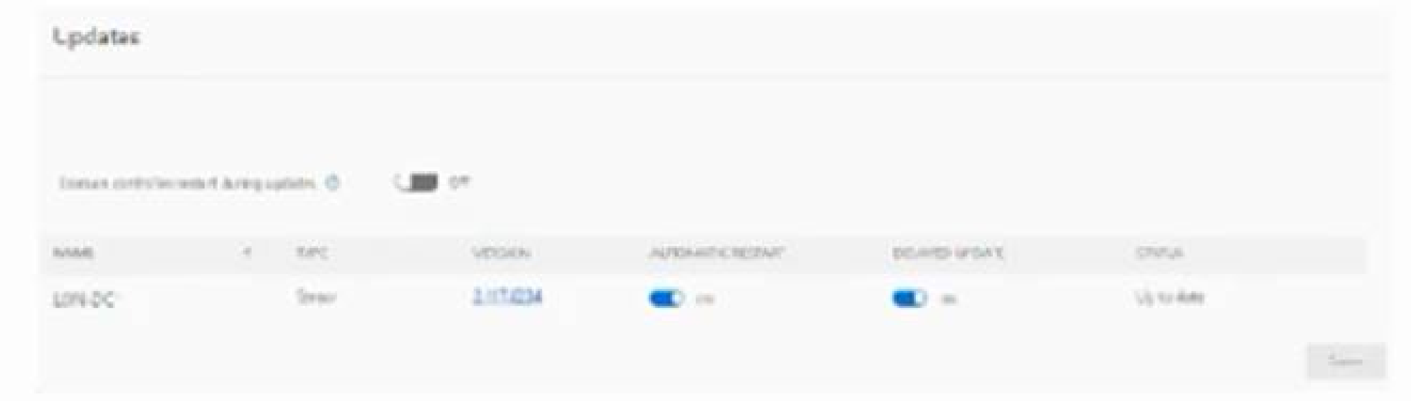
NEW QUESTION 78
- (Topic 6)
You have a Microsoft 365 subscription.
You configure a data loss prevention (DLP) policy.
You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.
You need to prevent the users from bypassing the DLP policy. What should you configure?

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

Answer: D

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

NEW QUESTION 80
- (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

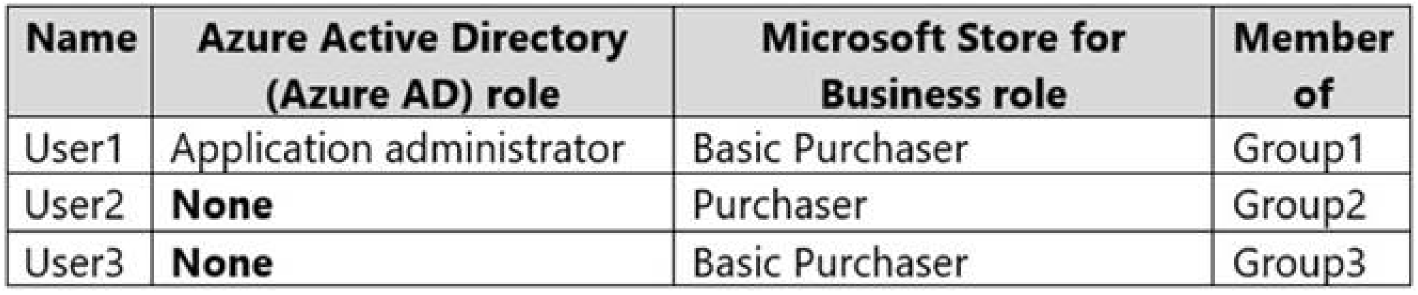
NEW QUESTION 82
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.com.
For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.
You plan to sync contoso.com to an Azure AD tenant.
You need to recommend a solution 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

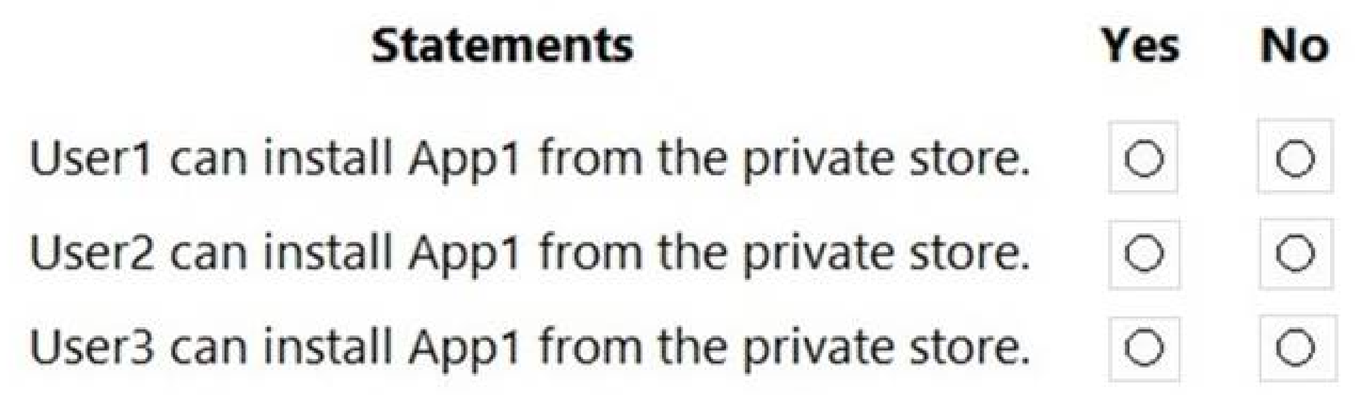
Explanation:
Reference:
https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

NEW QUESTION 86
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.

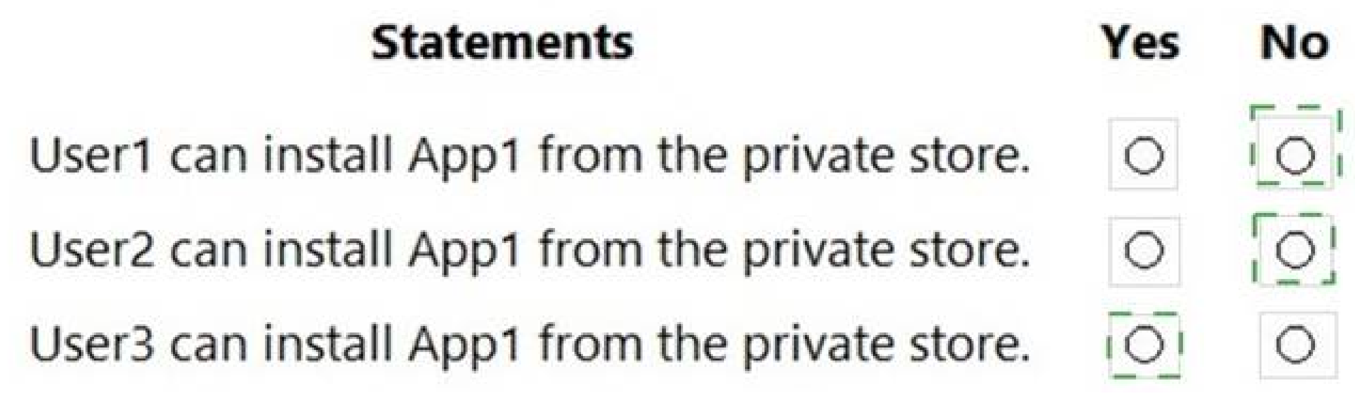


Statements	Yes	No
User1 can install App1 from the private store.	○	○
User2 can install App1 from the private store.	○	○
User3 can install App1 from the private store.	○	○

A. Mastered
B. Not Mastered

Answer: A

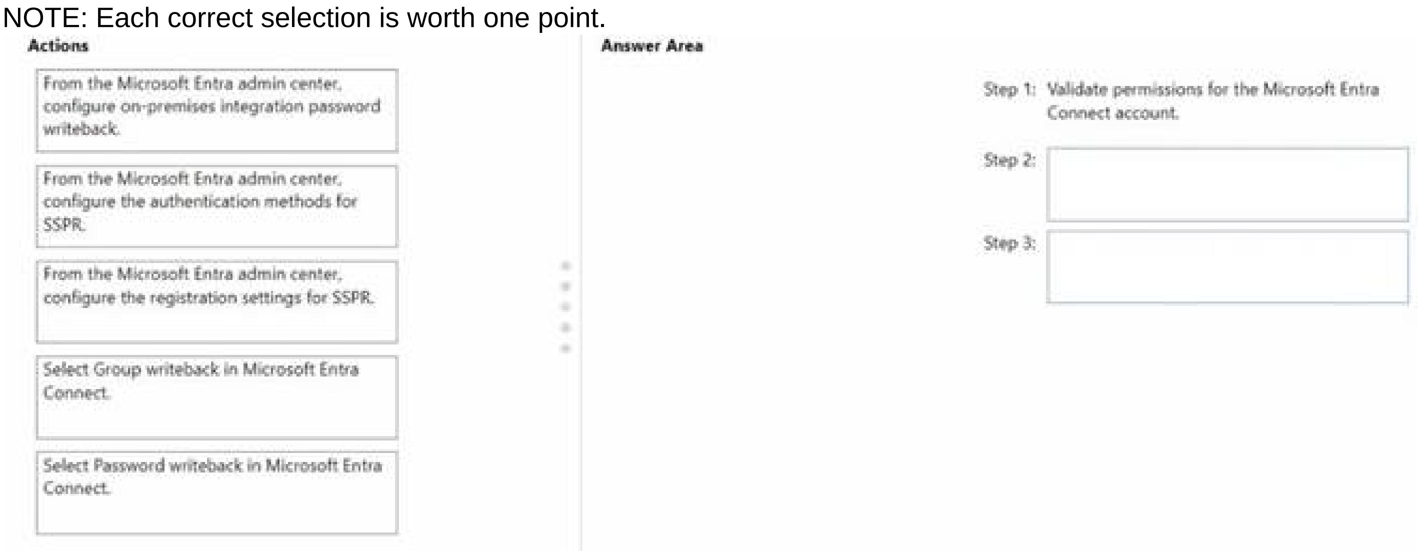
Explanation:



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 88
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.

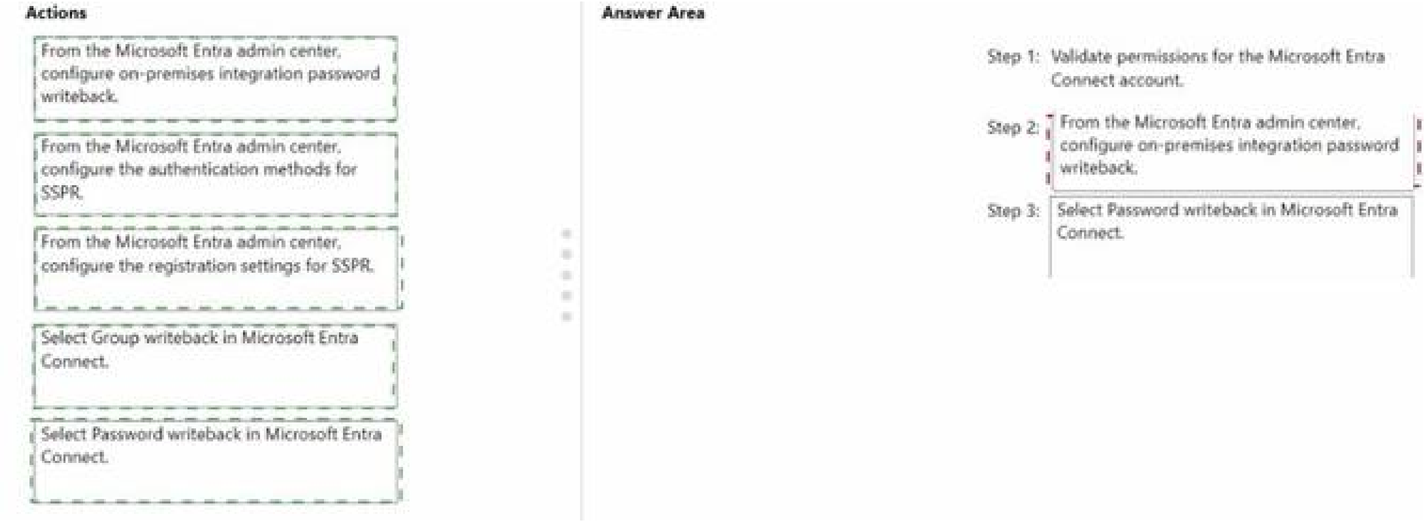
Answer Area

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 89
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You create an account tor a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.
Does this meet the goal?

A. Yes
B. no

Answer: B

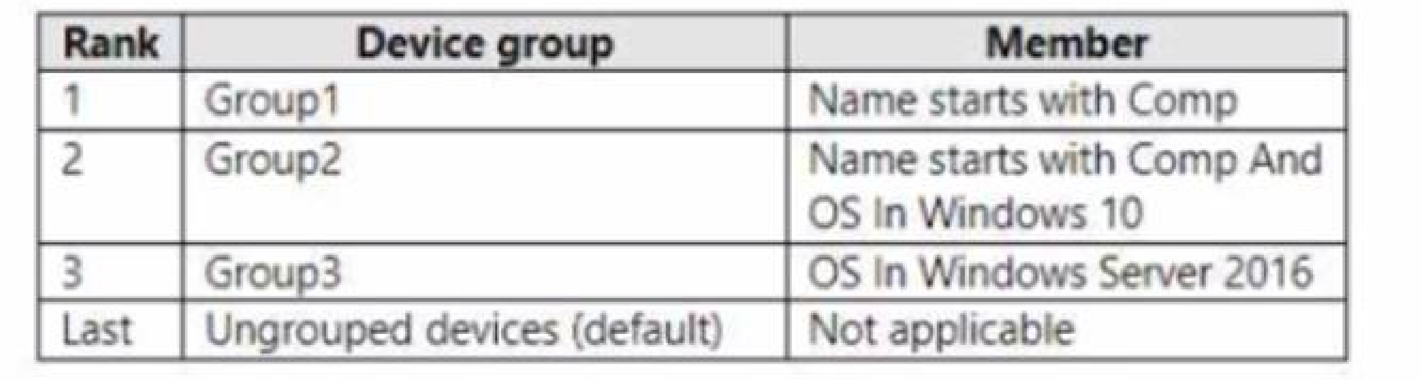
NEW QUESTION 91
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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

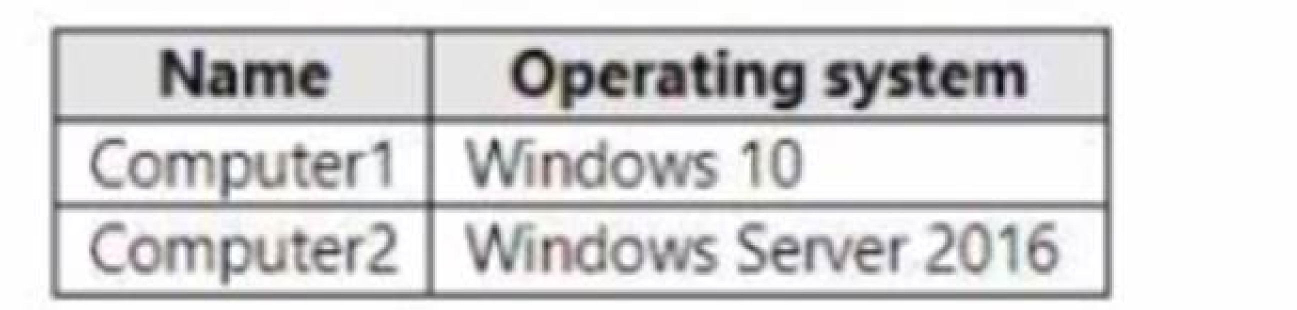
NEW QUESTION 94
HOTSPOT - (Topic 6)

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



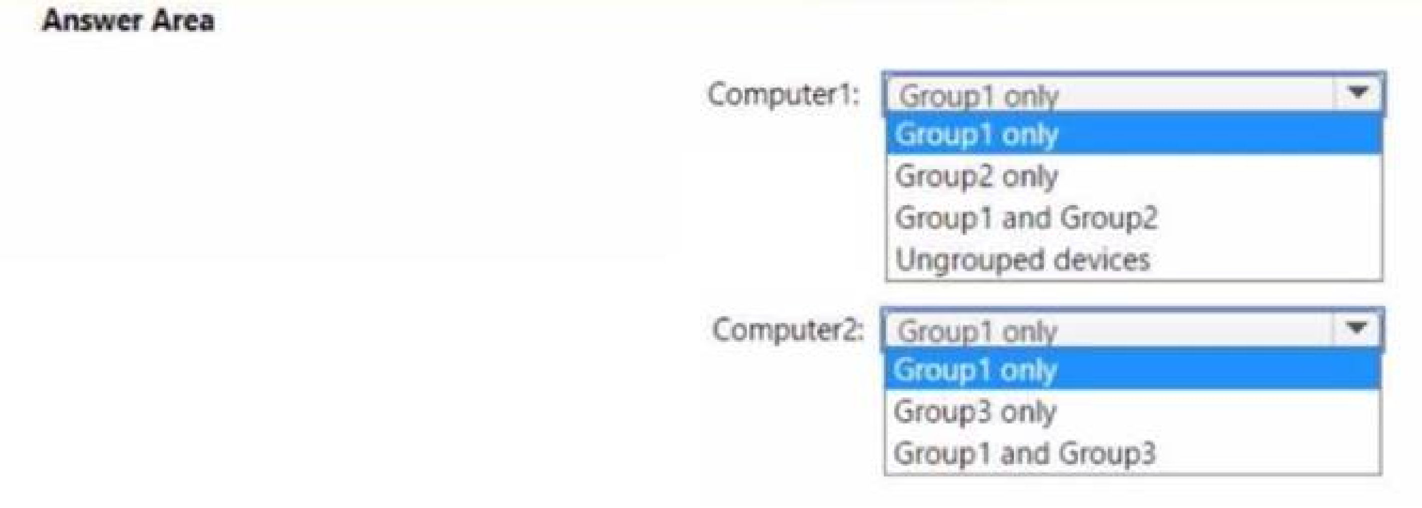
Rank	Device group	Member
1	Group1	Name starts with Comp
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped devices (default)	Not applicable

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



Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

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



Answer Area

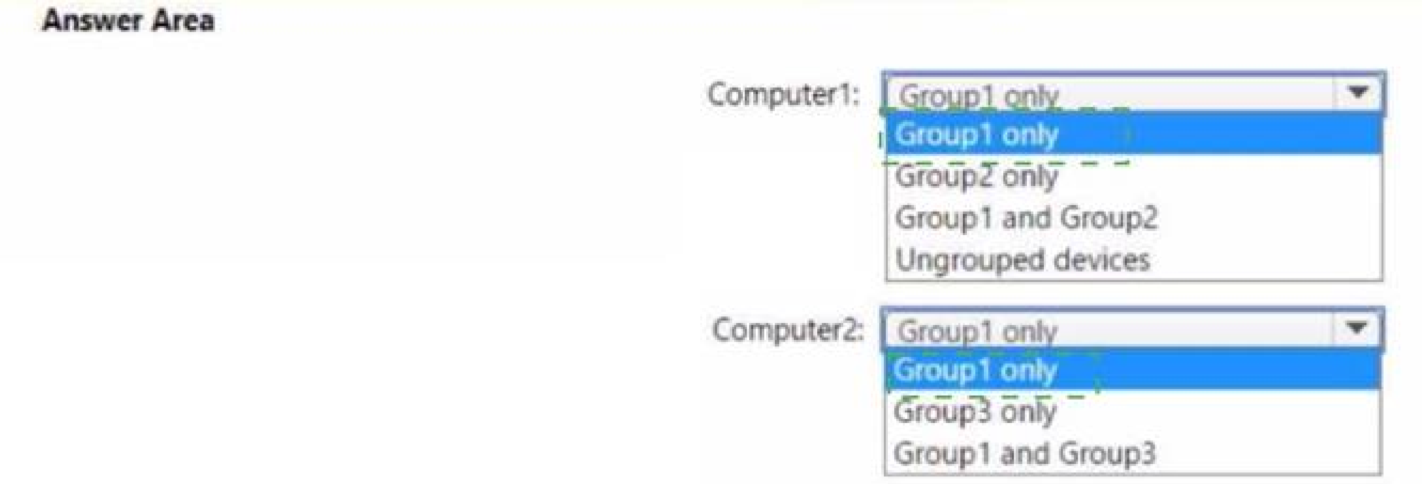
Computer1: Group1 only
- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped devices

Computer2: Group1 only
- Group1 only
- Group3 only
- Group1 and Group3

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Computer1: Group1 only
- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped devices

Computer2: Group1 only
- Group1 only
- Group3 only
- Group1 and Group3

NEW QUESTION 97
- (Topic 6)
You have a Microsoft 365 subscription.
You plan to implement Microsoft Purview Privileged Access Management. Which Microsoft Office 365 workloads support privileged access?

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

Answer: A

Explanation:
Privileged access management
Having standing access by some users to sensitive information or critical network configuration settings in Microsoft Exchange Online is a potential pathway for compromised accounts or internal threat activities. Microsoft Purview Privileged Access Management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. Instead of administrators having constant

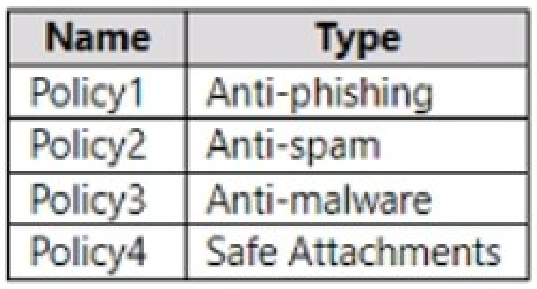
access, just-in-time access rules are implemented for tasks that need elevated permissions. Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.
Note: When will privileged access support Office 365 workloads beyond Exchange? Privileged access management will be available in other Office 365 workloads soon.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access- management-solution-overview
https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management

NEW QUESTION 102
- (Topic 6)
You have a Microsoft 365 E5 subscription. You need to create a mail-enabled contact. Which portal should you use?

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

Answer: A

NEW QUESTION 107
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.



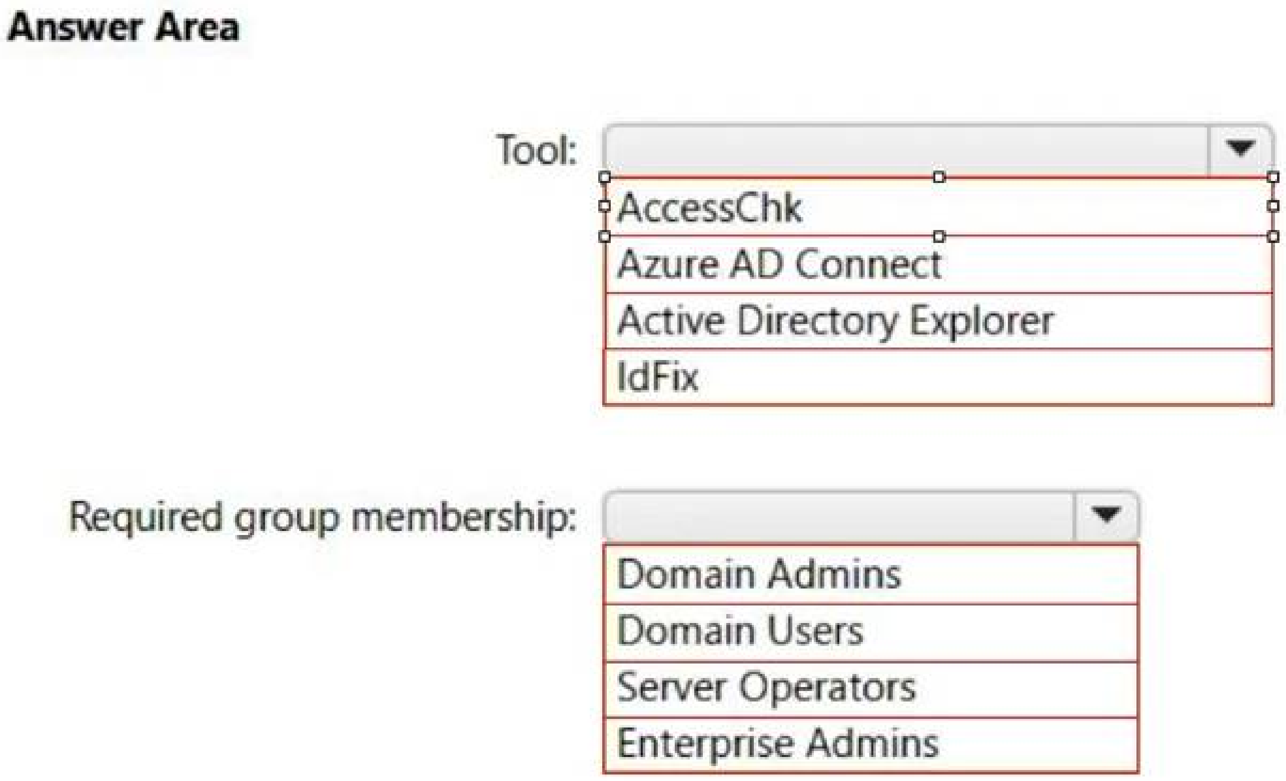
Name	Type
Policy1	Anti-phishing
Policy2	Anti-spam
Policy3	Anti-malware
Policy4	Safe Attachments

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

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

Answer: A

NEW QUESTION 110
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

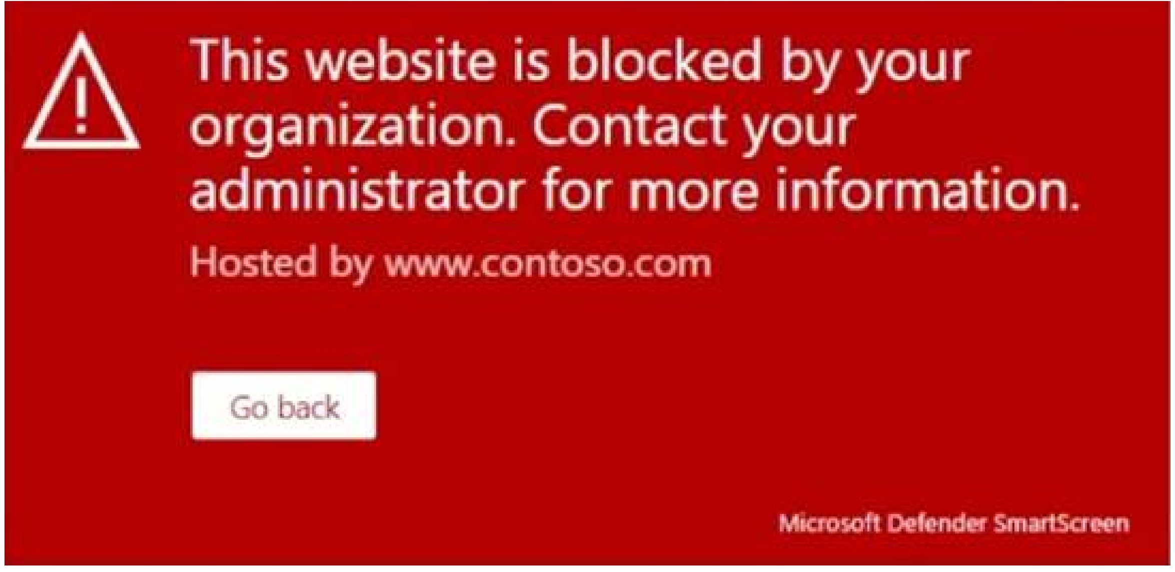
Query and fix invalid object attributes with the IdFix tool
Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft 365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server 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 112
- (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 113
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.



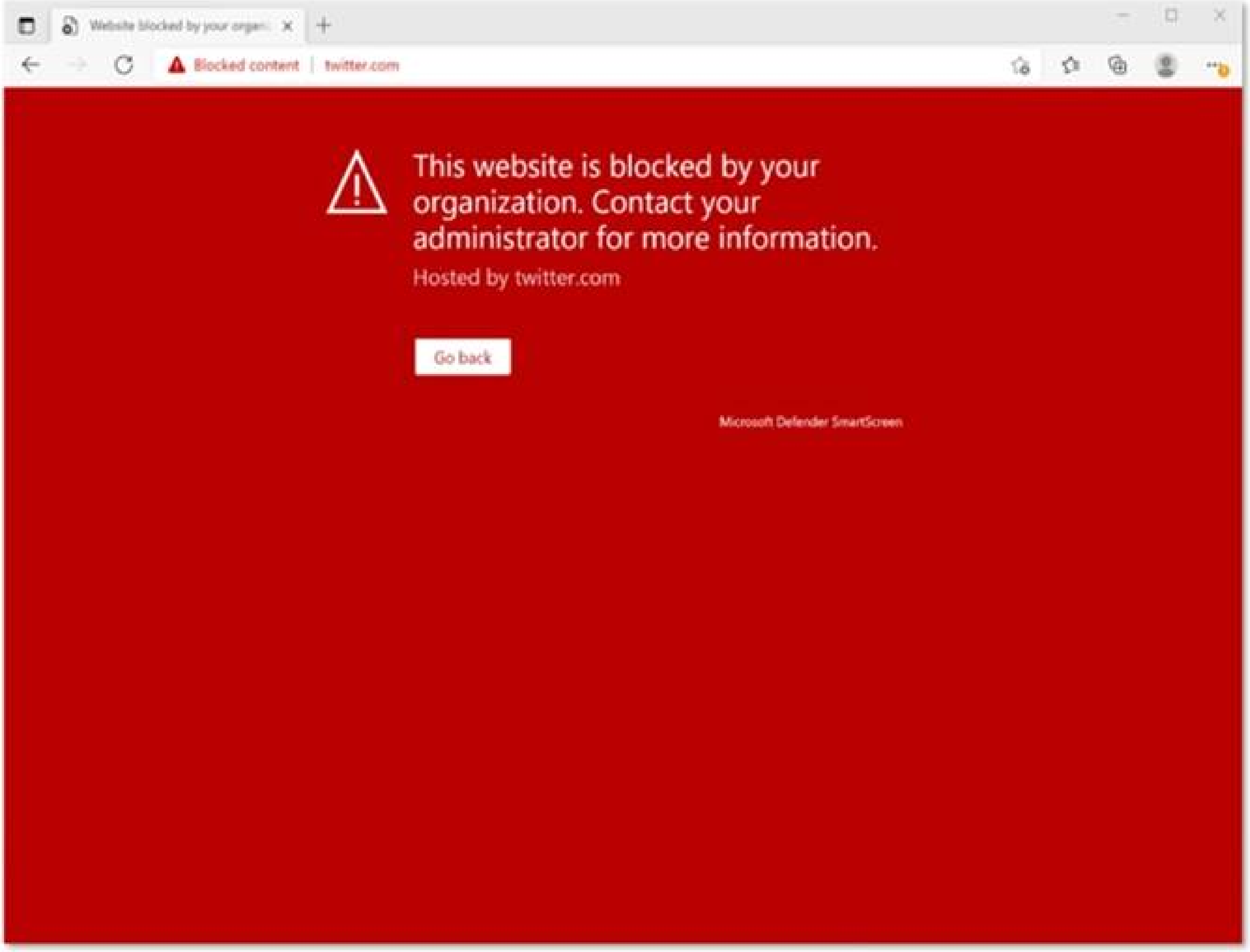
This website is blocked by your organization. Contact your administrator for more information.
Hosted by www.contoso.com

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

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

Answer: E

Explanation:


Website blocked by your organi...
Blocked content | twitter.com
Go back

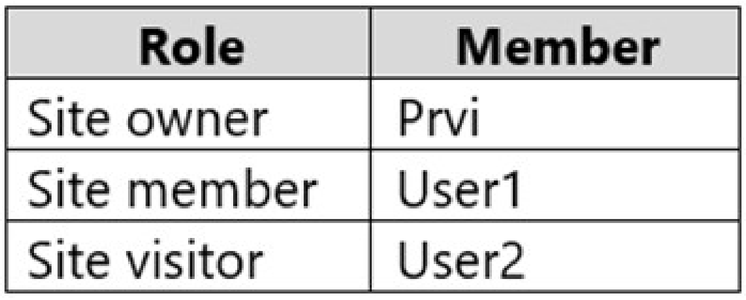
This website is blocked by your organization. Contact your administrator for more information.

Hosted by twitter.com

Microsoft Defender SmartScreen

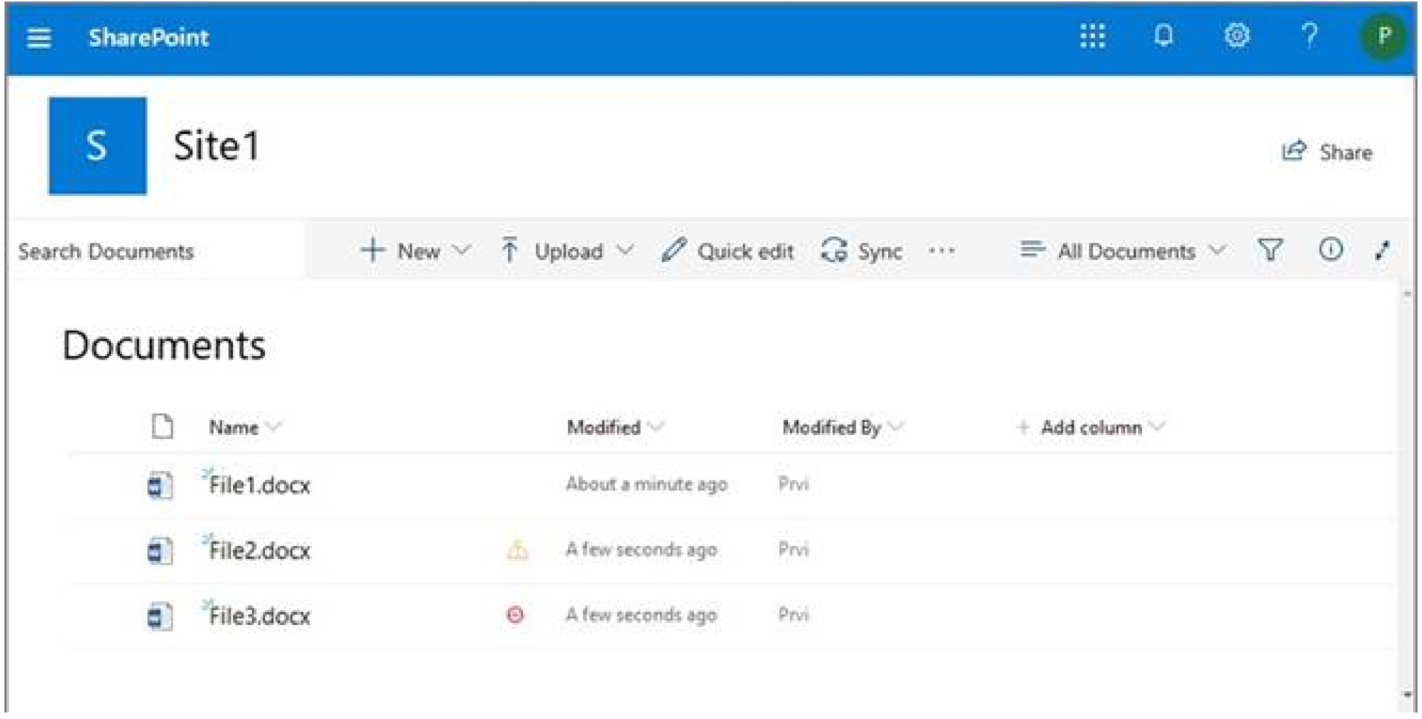
This Website Is Blocked By Your Organization
Custom indicators will block malicious IPs, URLs, and domains. Then, they will display the above message for the user.
Reference: https://jadexstrategic.com/web-protection/

NEW QUESTION 117
HOTSPOT - (Topic 6)
From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.



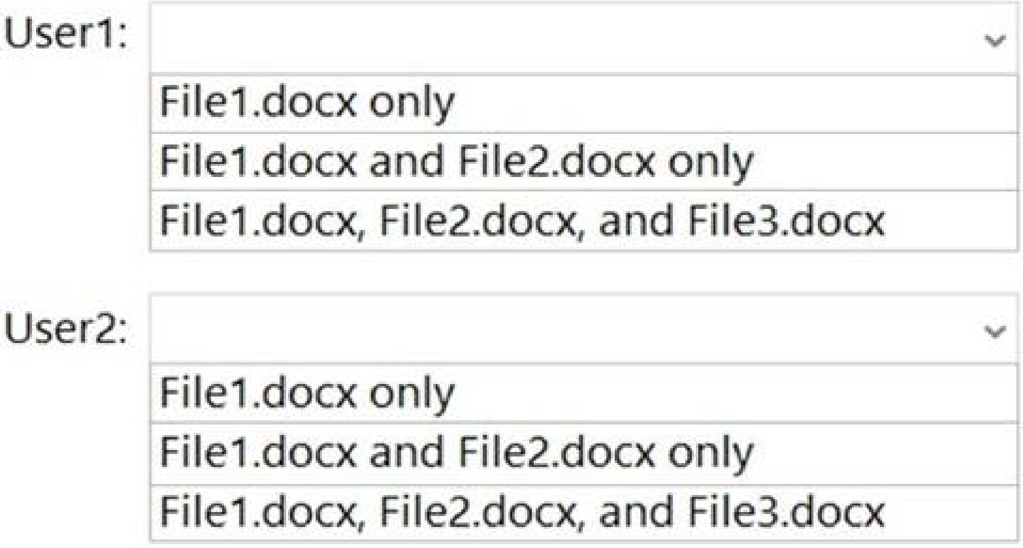
Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

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



Name		Modified	Modified By	Add column
File1.docx		About a minute ago	Prvi	
File2.docx	⚠	A few seconds ago	Prvi	
File3.docx	⊖	A few seconds ago	Prvi	

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



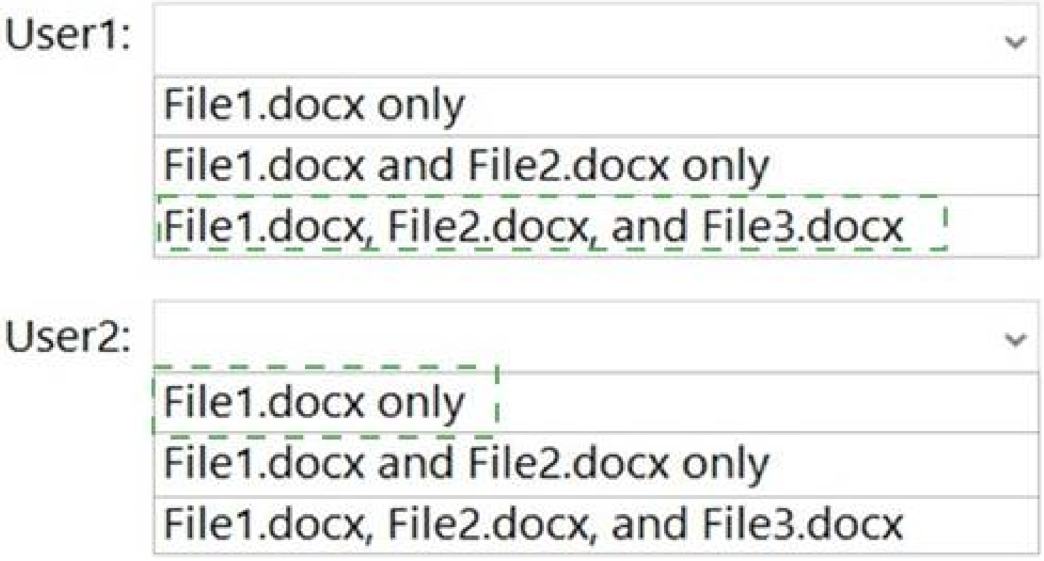
User1:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

A. Mastered
B. Not Mastered

Answer: A

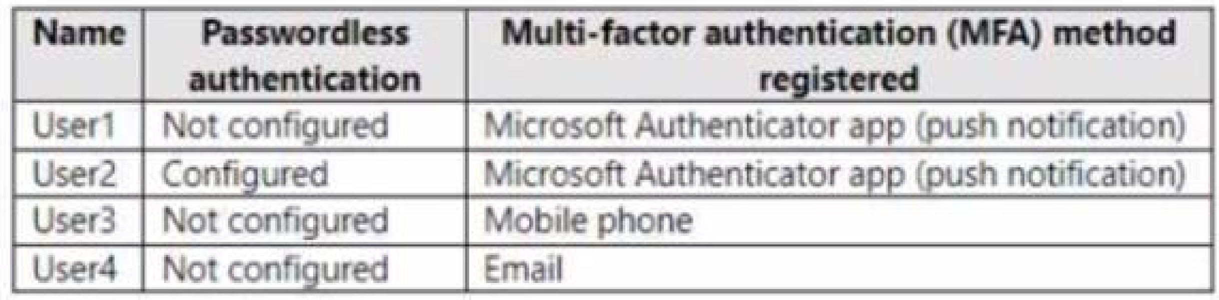
Explanation:



User1:
- File1.docx only
- File1.docx and File2.docx only
- [✓ File1.docx, File2.docx, and File3.docx]

User2:
- [✓ File1.docx only]
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

NEW QUESTION 119
- (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 122
- (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 125
- (Topic 6)
You have a Microsoft 365 subscription that uses Security & Compliance retention policies.
You implement a preservation lock on a retention policy that is assigned to all executive users.
Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point?

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

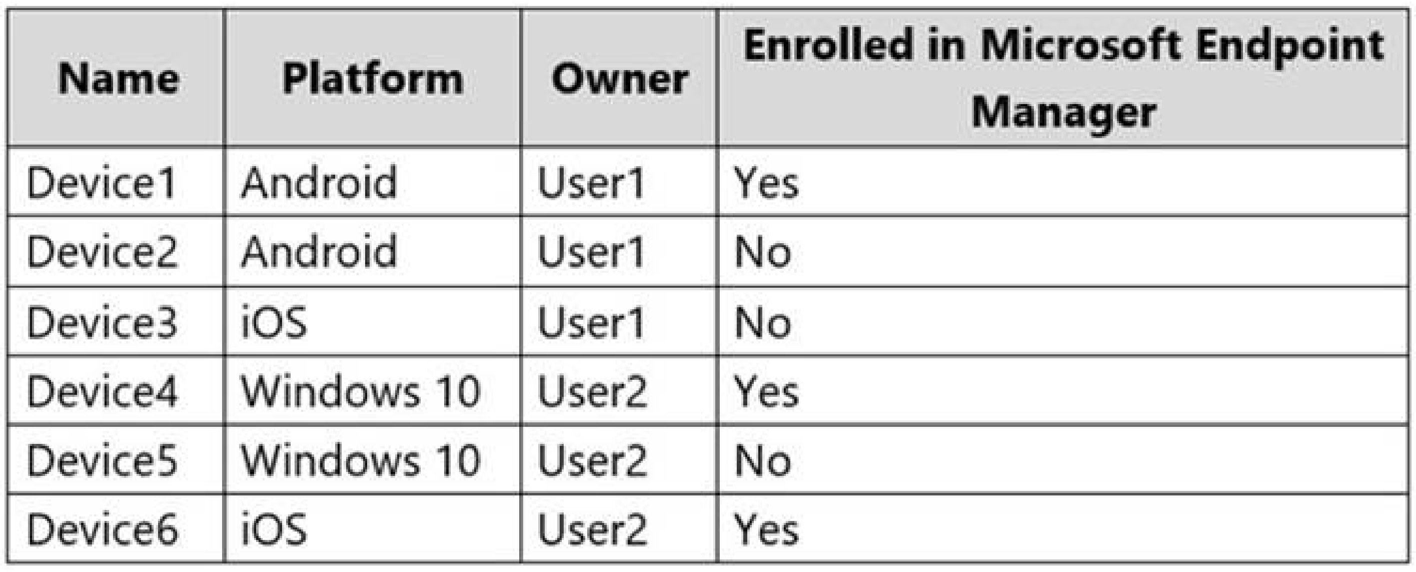
Answer: AB

NEW QUESTION 126
- (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 131
- (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 135
- (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

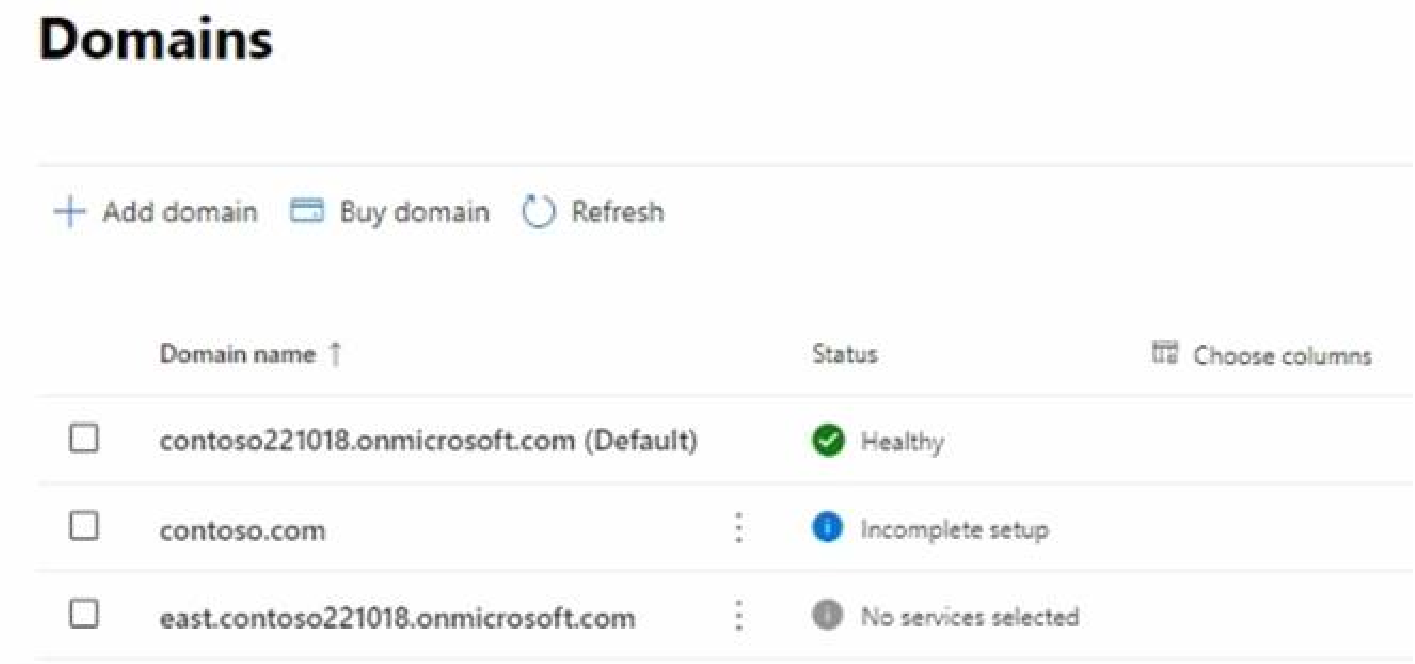
NEW QUESTION 137
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: You run idfix.exe and export the 10 user accounts.
Does this meet the goal?

A. Yes
B. No

Answer: B

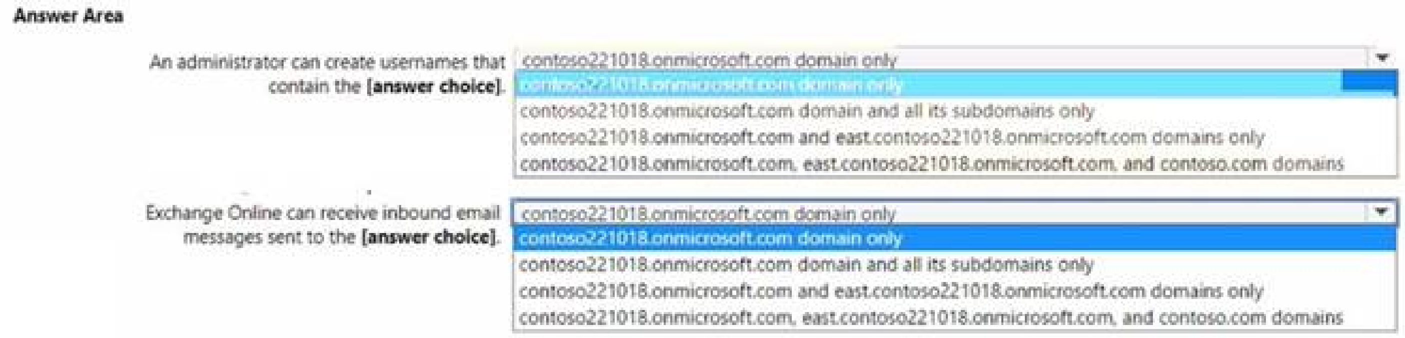
Explanation:
The question states that “all the user account synchronizations completed successfully”. If there were problems with the 10 accounts that needed fixing with idfix.exe, there would have been synchronization errors in Azure AD Connect Health.
It is likely that the 10 user accounts are being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

NEW QUESTION 140
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

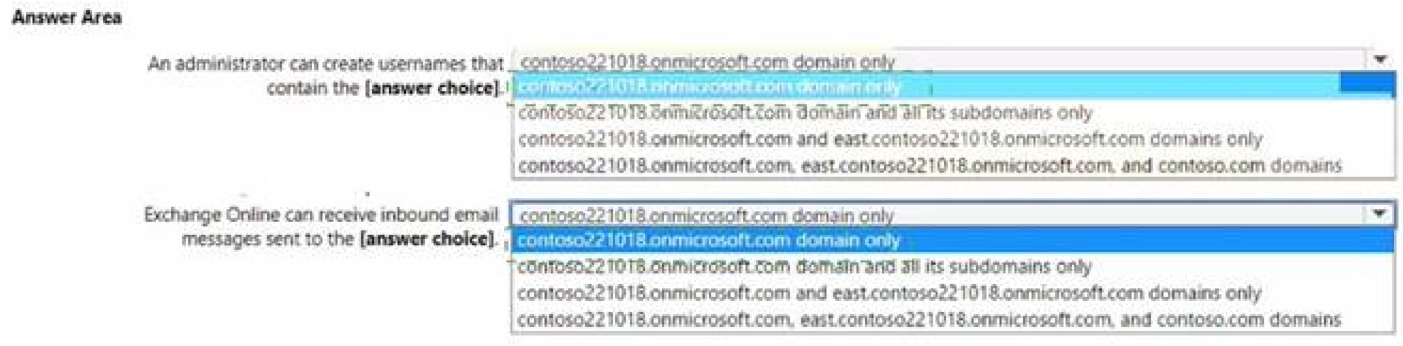
An administrator can create usernames that contain the **[answer choice]**.
- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain and all its subdomains only
- contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

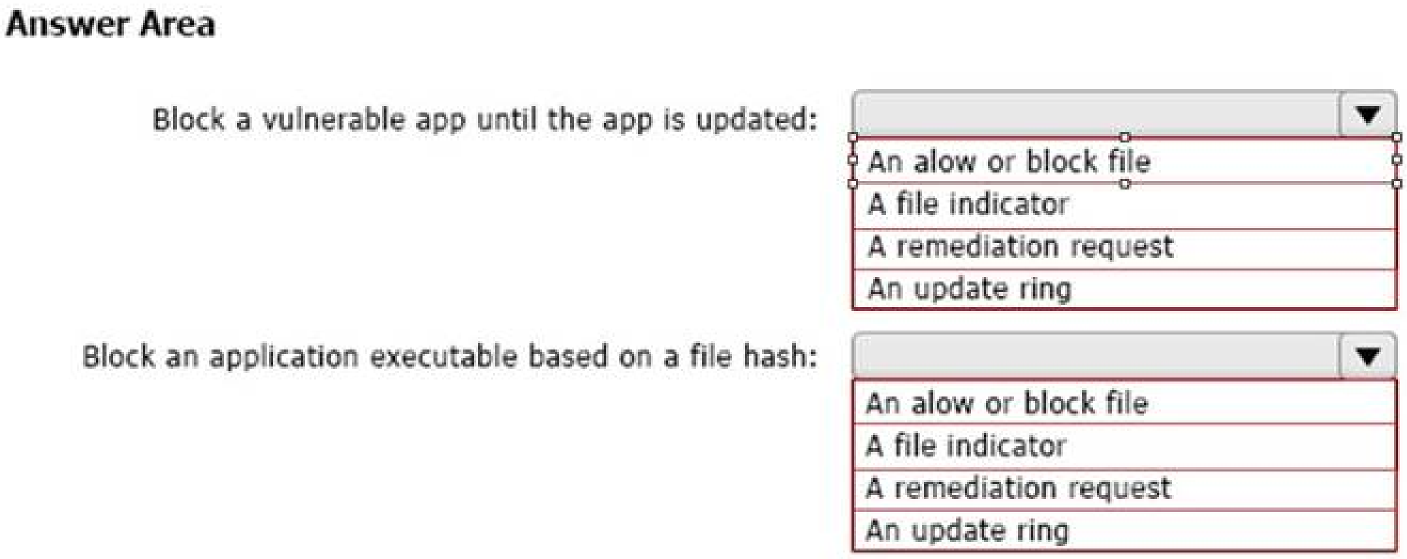
An administrator can create usernames that contain the **[answer choice]**.

- 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 143
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:

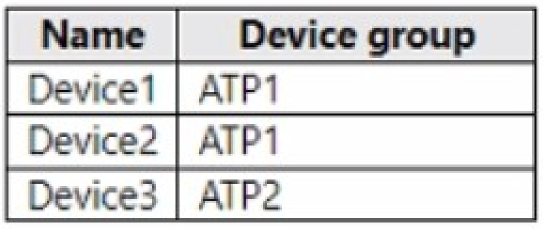
- An alow or block file
- A file indicator
- A remediation request
- An update ring

A. Mastered
B. Not Mastered

Answer: A

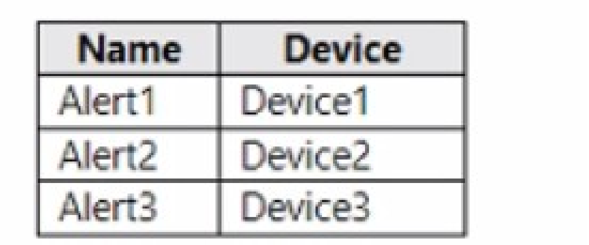
Explanation:
Box 1: A remediation request
Block a vulnerable app until the app is updated.
Block vulnerable applications
How to block vulnerable applications
? Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.
? Select a security recommendation to see a flyout with 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 147
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

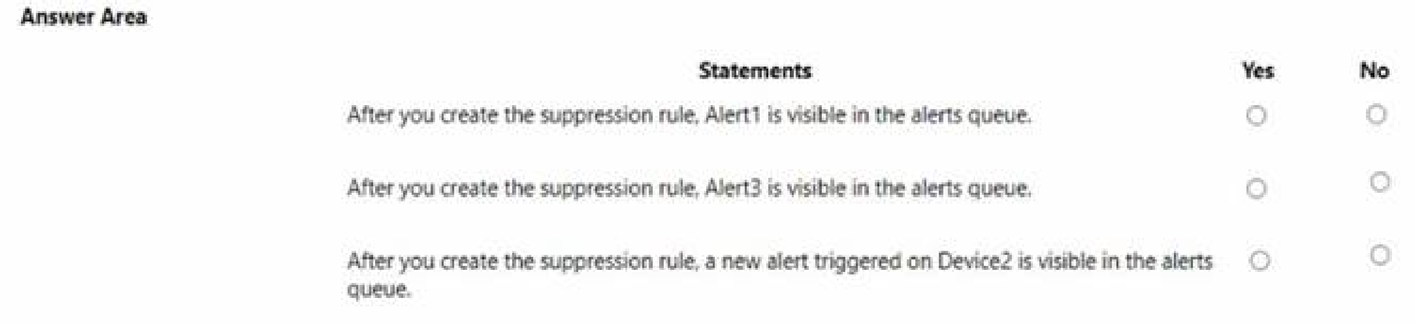
The alerts visible in the Microsoft Defender for Endpoint alerts queue are shown in the following table.



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



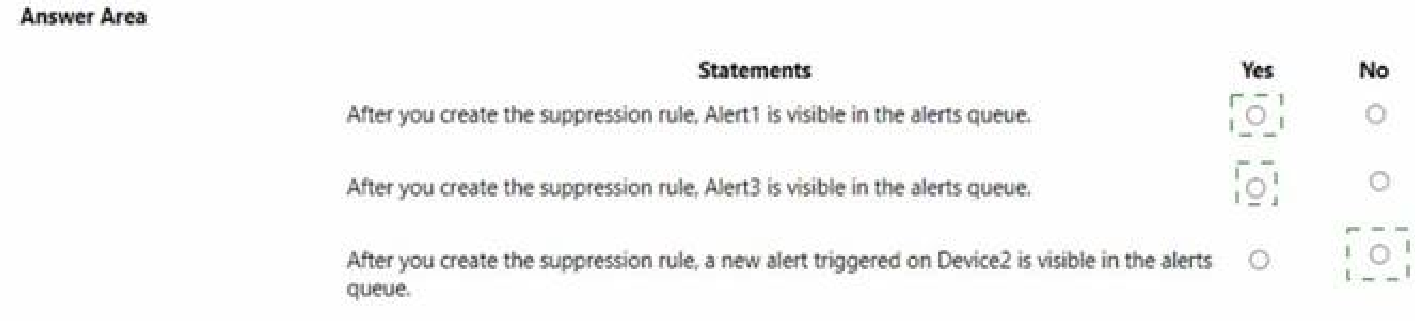
Answer Area

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

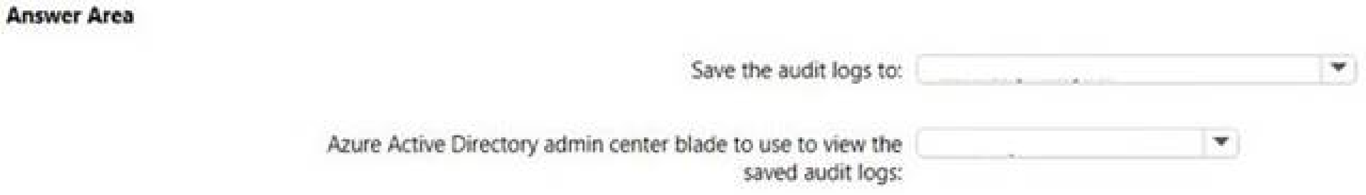
Explanation:



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 152
FILL IN THE BLANK - (Topic 6)
You have a Microsoft 365 tenant.
You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

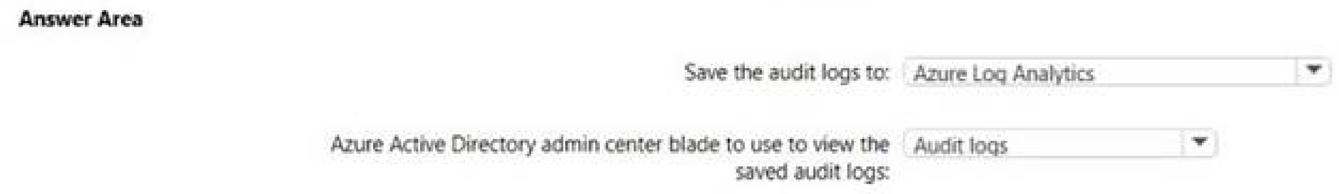
Save the audit logs to: ▾

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



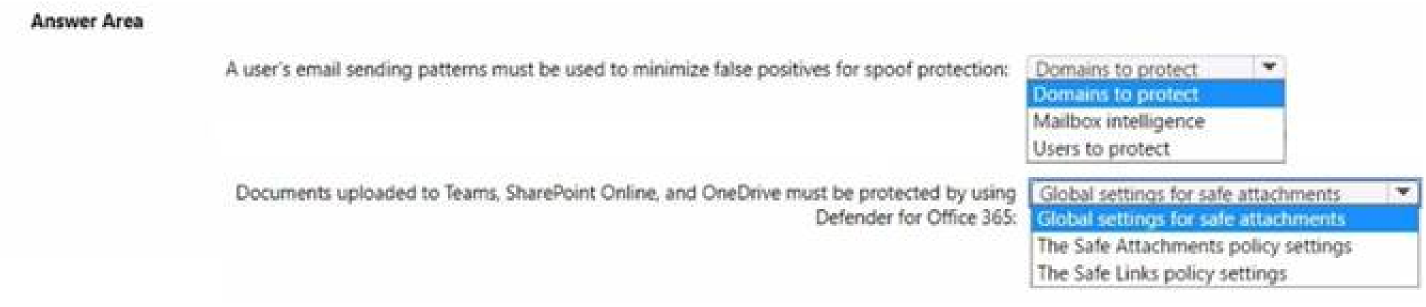
Answer Area

Save the audit logs to: Azure Log Analytics ▾

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

NEW QUESTION 156
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to configure Microsoft Defender for Office 365 to meet the following requirements:
- A user's email sending patterns must be used to minimize false positives for spoof protection.
- Documents uploaded to Microsoft Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365.

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



Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection: Domains to protect

- Domains to protect
- Mailbox intelligence
- Users to protect

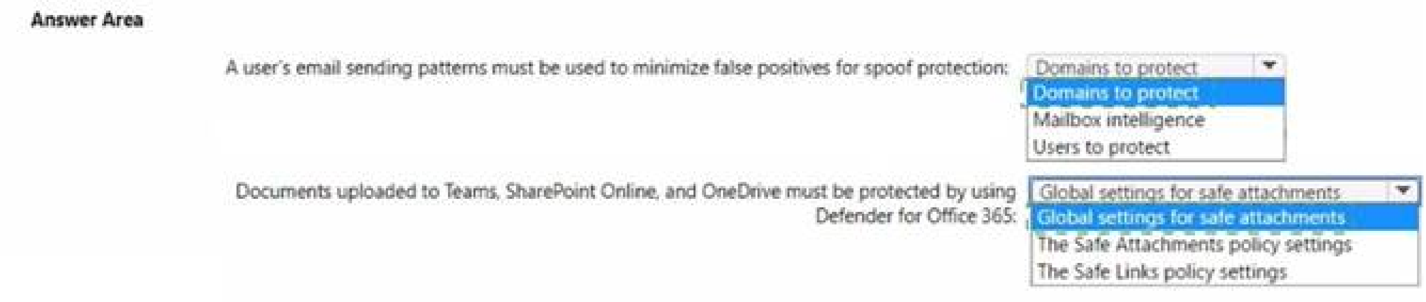
Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365: Global settings for safe attachments

- Global settings for safe attachments
- The Safe Attachments policy settings
- The Safe Links policy settings

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

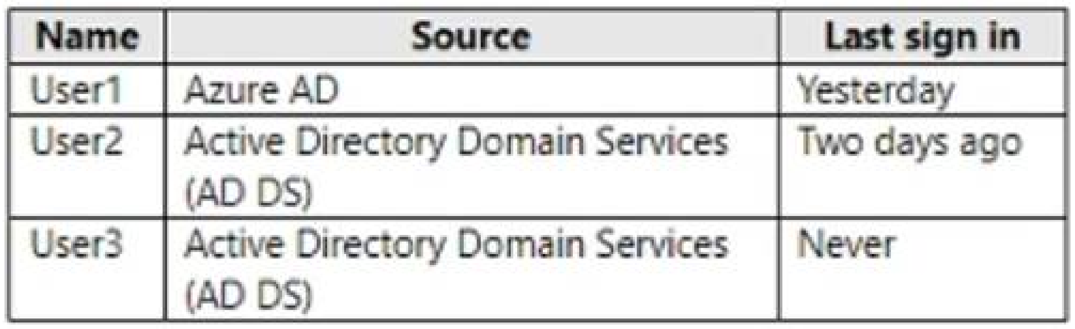
A user's email sending patterns must be used to minimize false positives for spoof protection: Domains to protect

- Domains to protect
- Mailbox intelligence
- Users to protect

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365: Global settings for safe attachments

- Global settings for safe attachments
- The Safe Attachments policy settings
- The Safe Links policy settings

NEW QUESTION 158
- (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

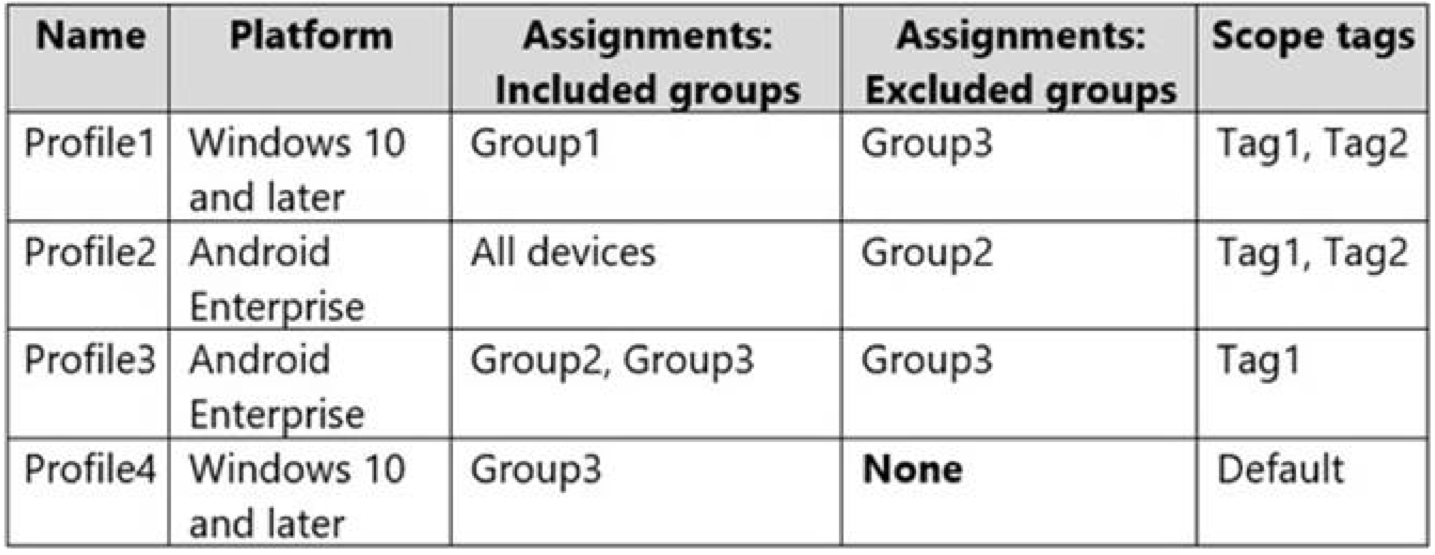
Azure AD Connect has the following settings:
? Password Hash Sync: Enabled
? Pass-through authentication: Enabled
You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.
Which users should you identify?

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

Answer: D

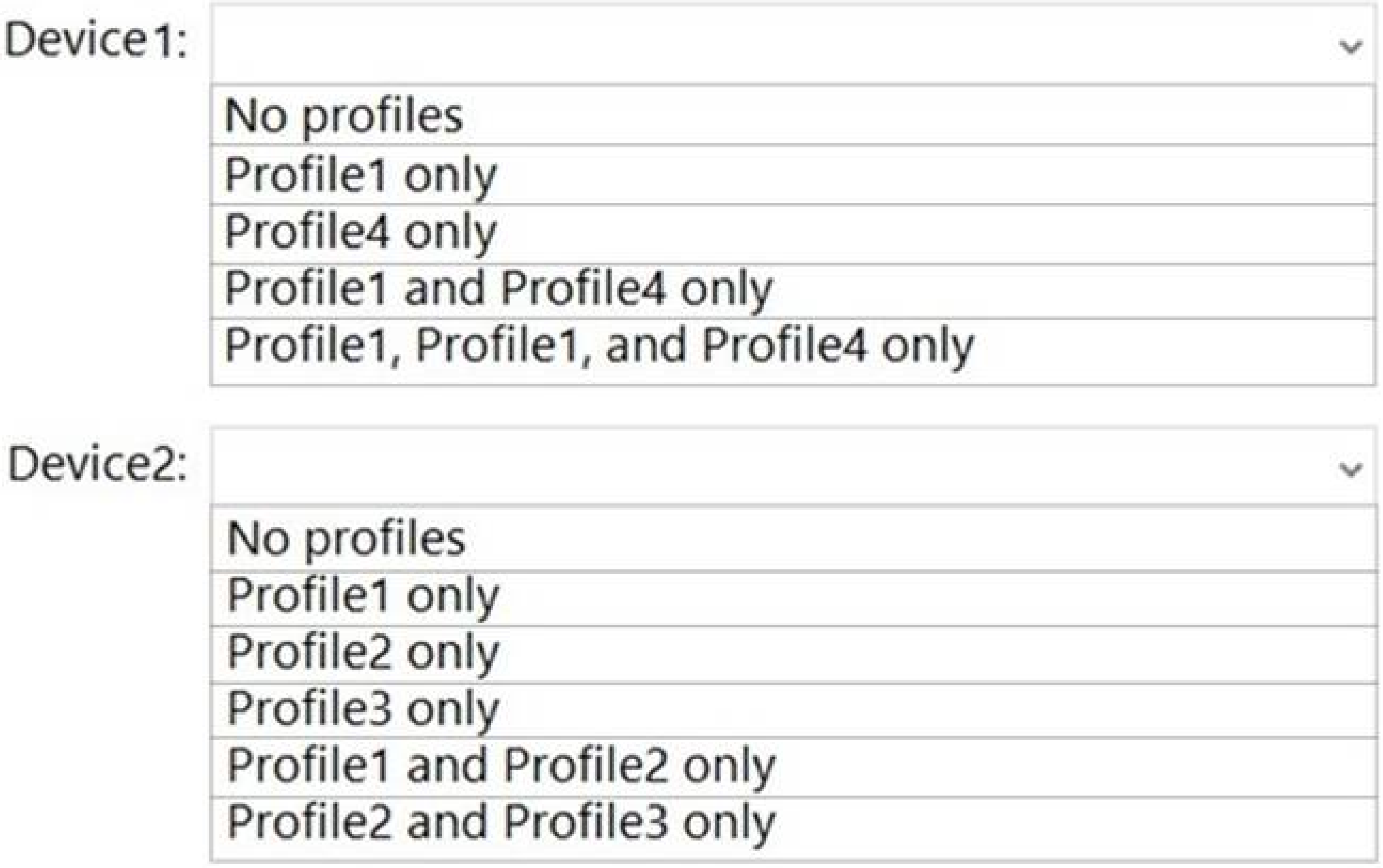
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

NEW QUESTION 162
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.



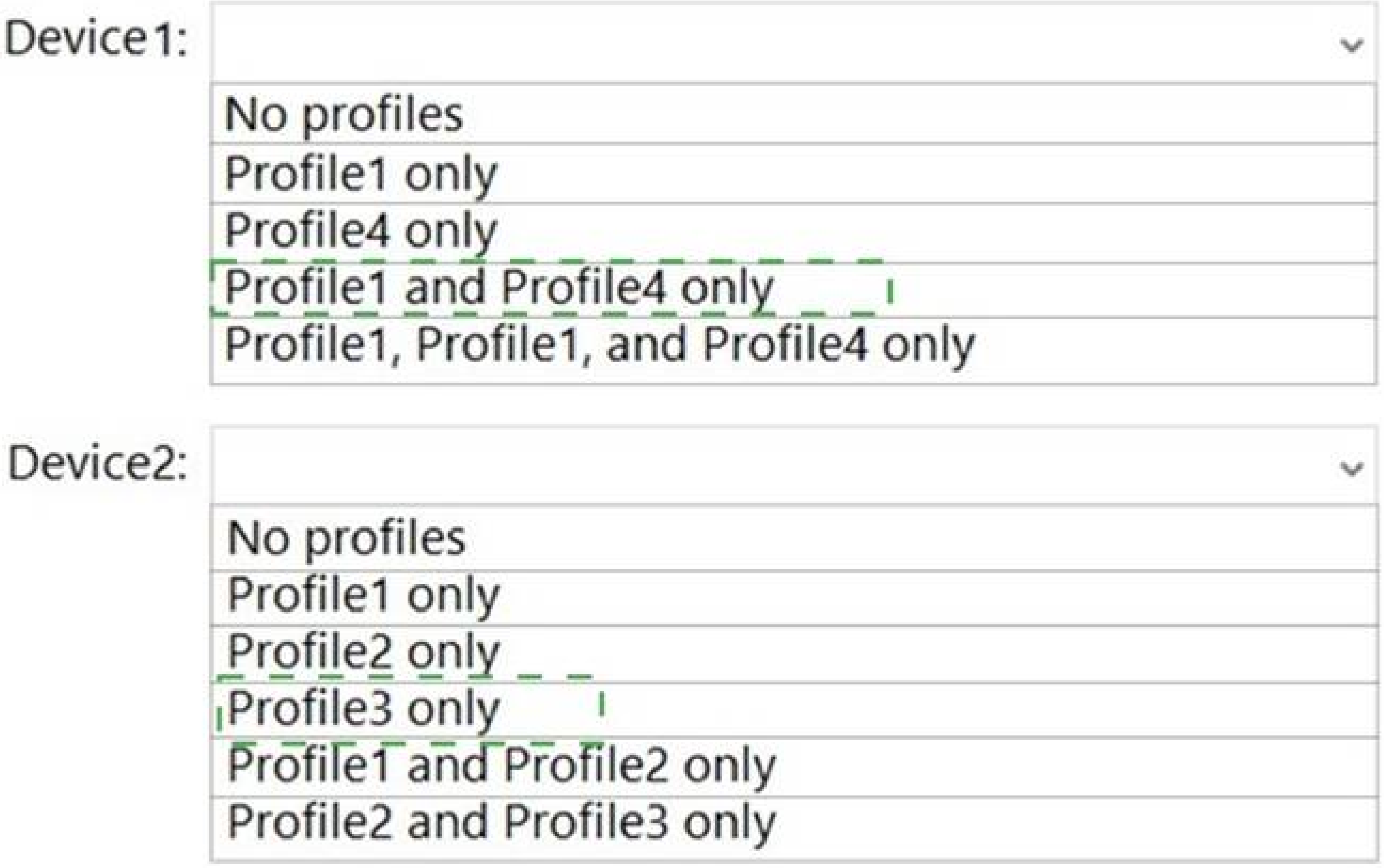
Device1:
- No profiles
- Profile1 only
- Profile4 only
- Profile1 and Profile4 only
- Profile1, Profile1, and Profile4 only

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

A. Mastered
B. Not Mastered

Answer: A

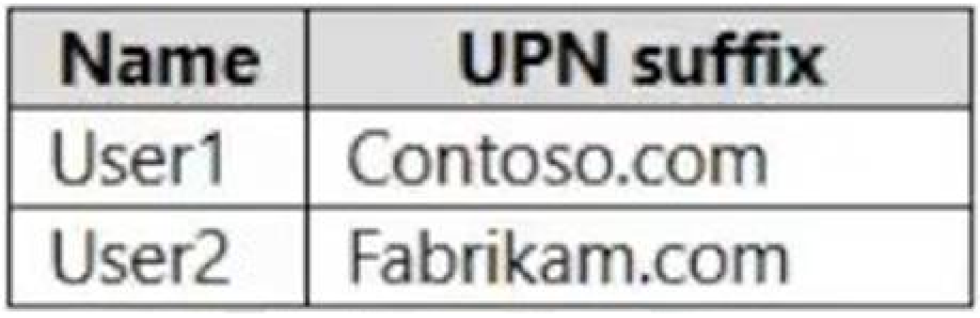
Explanation:



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

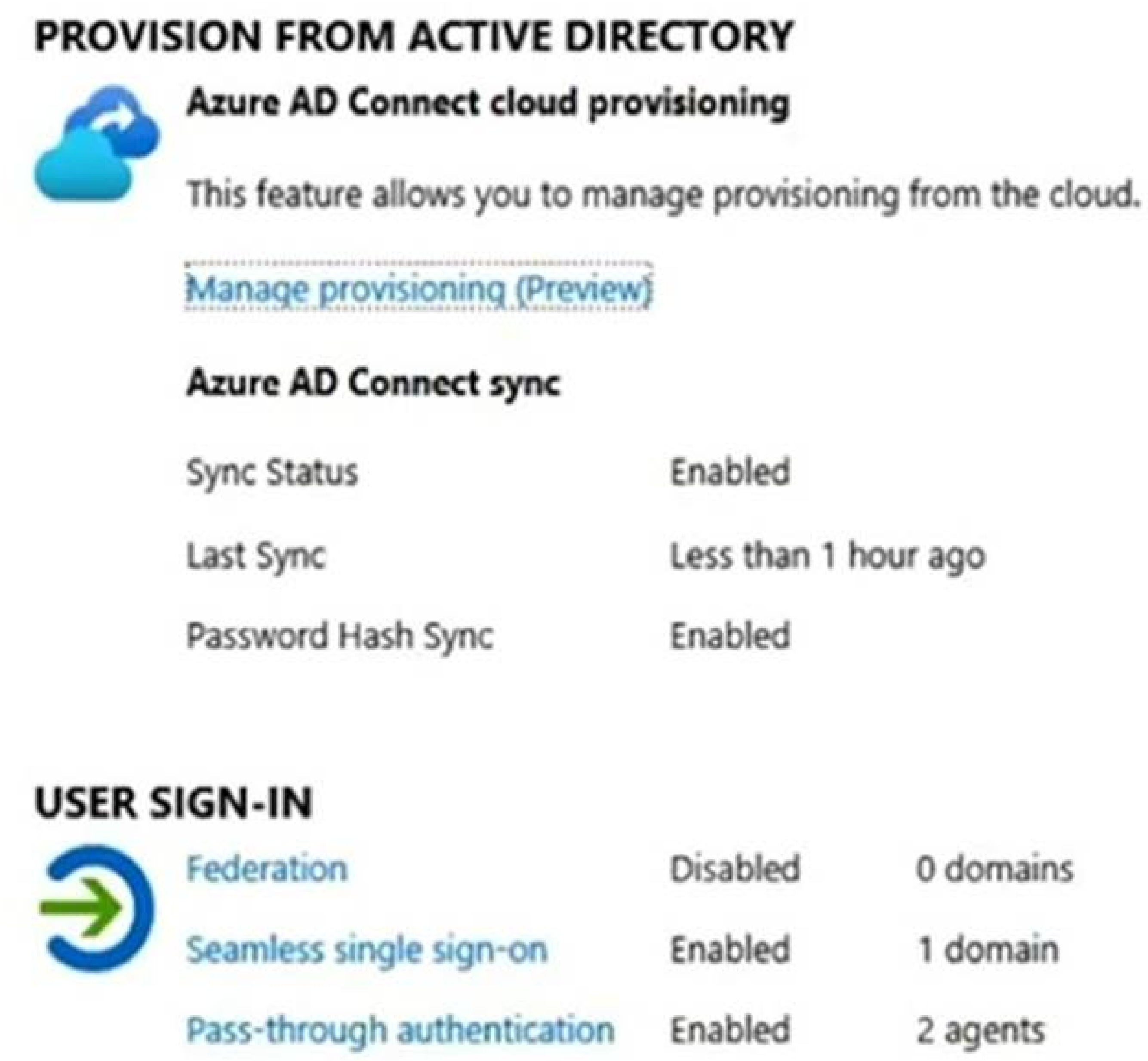
Device2:
- No profiles
- Profile1 only
- Profile2 only
- [✓ Profile3 only]
- Profile1 and Profile2 only
- Profile2 and Profile3 only

NEW QUESTION 165
- (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

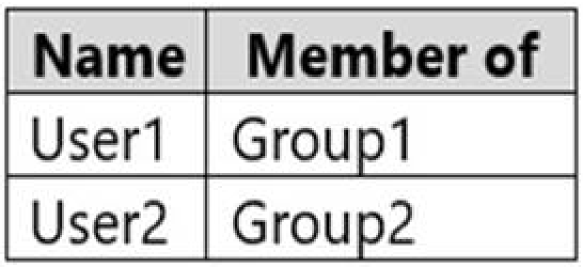
User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com.
Does this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

A. Yes
B. No

Answer: B

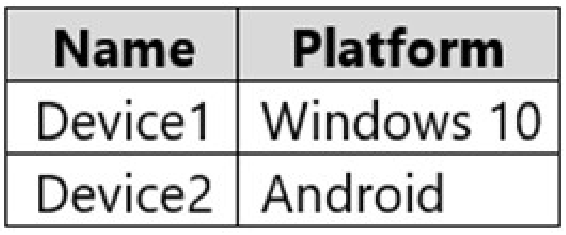
Explanation:
This is not a permissions issue so you do not need to assign the Security Reader role. The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

NEW QUESTION 167
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.



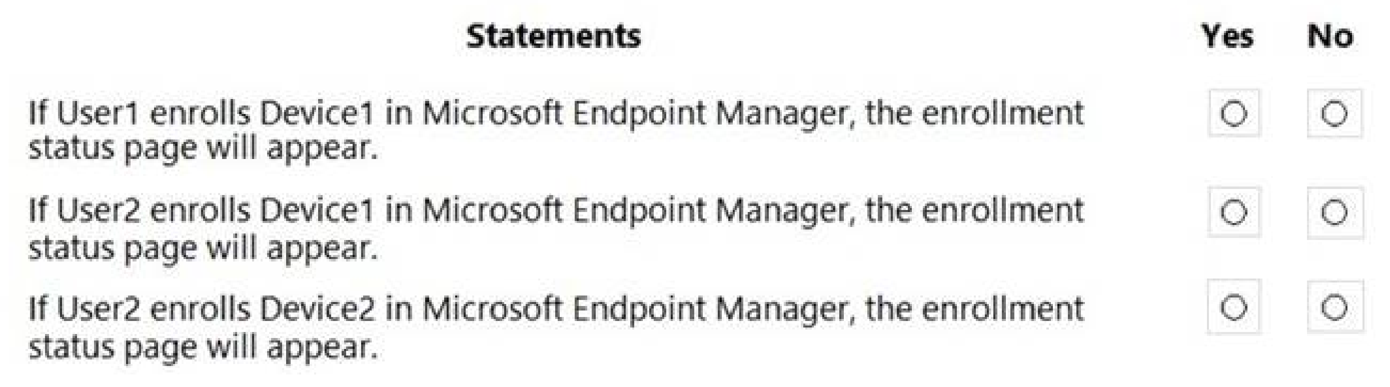
Name	Member of
User1	Group1
User2	Group2

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.

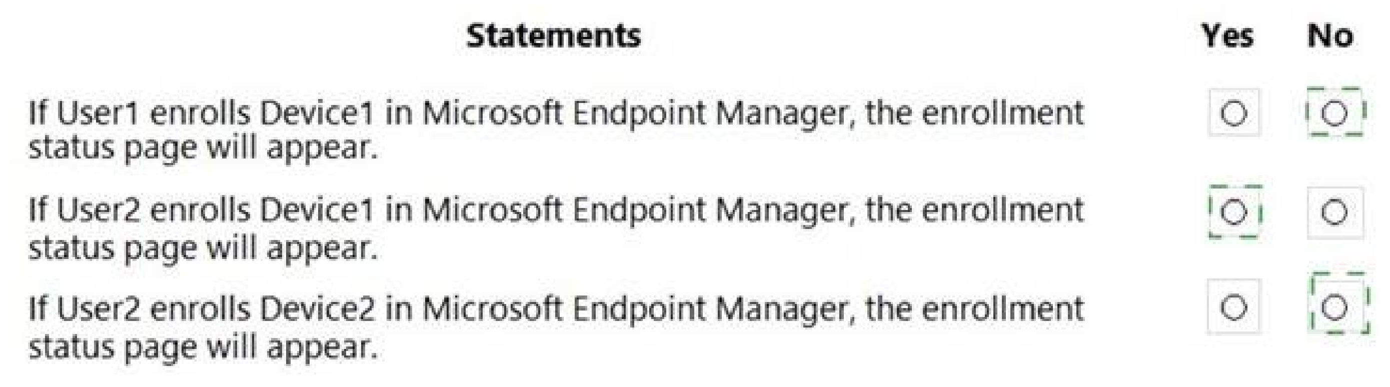


Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page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

A. Mastered
B. Not Mastered

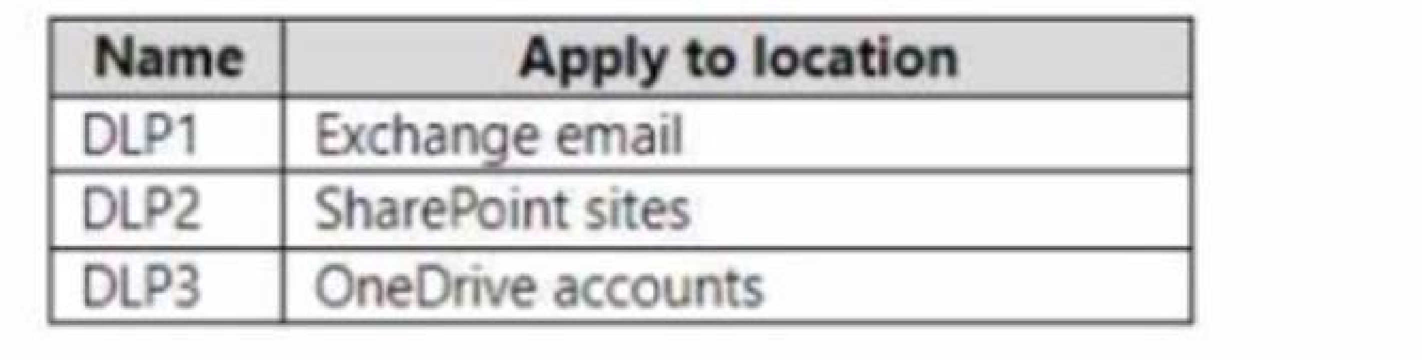
Answer: A

Explanation:



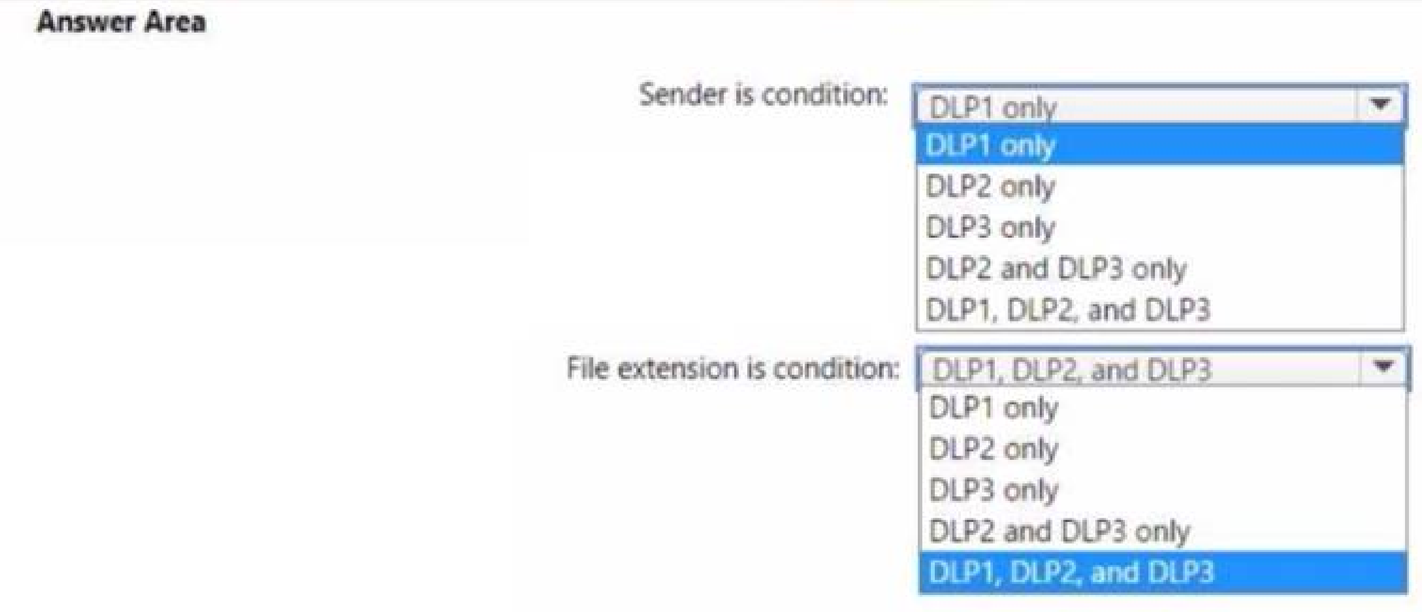
Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	[✓ ○]
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	[✓ ○]	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status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

NEW QUESTION 170
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to create the data loss prevention (DLP) policies shown in the following table.



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

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



Answer Area

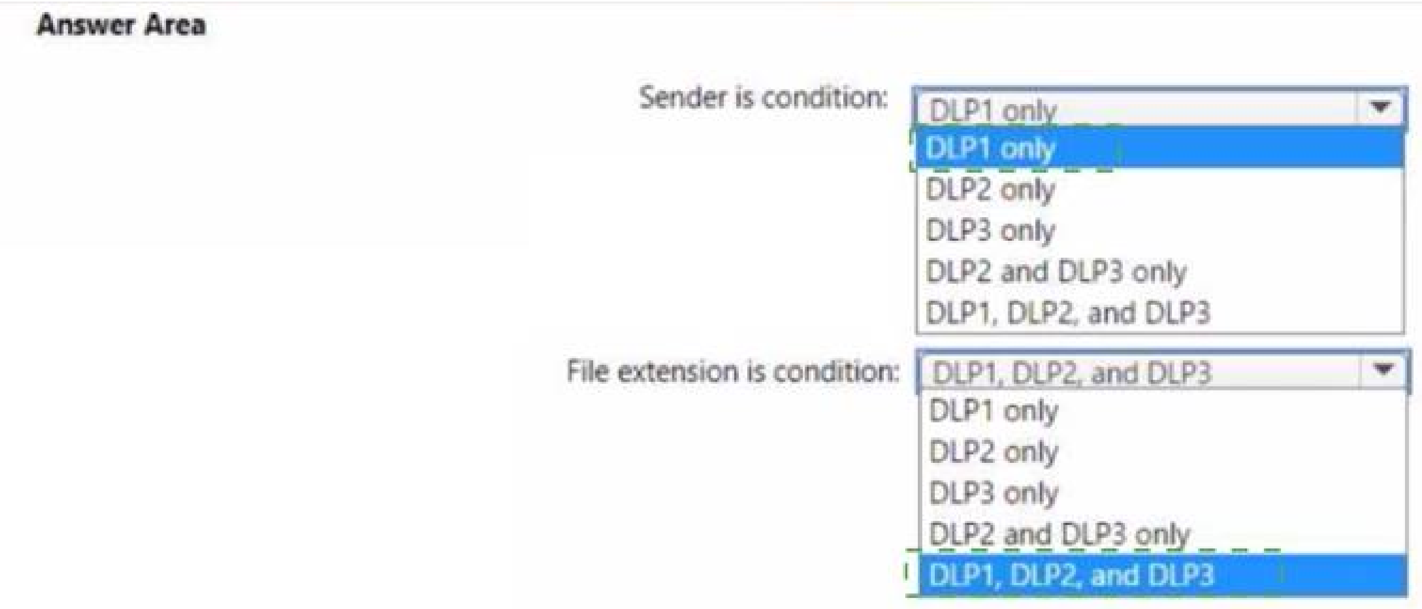
Sender is condition: DLP1 only

File extension is condition: DLP1, DLP2, and DLP3

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Sender is condition: DLP1 only

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

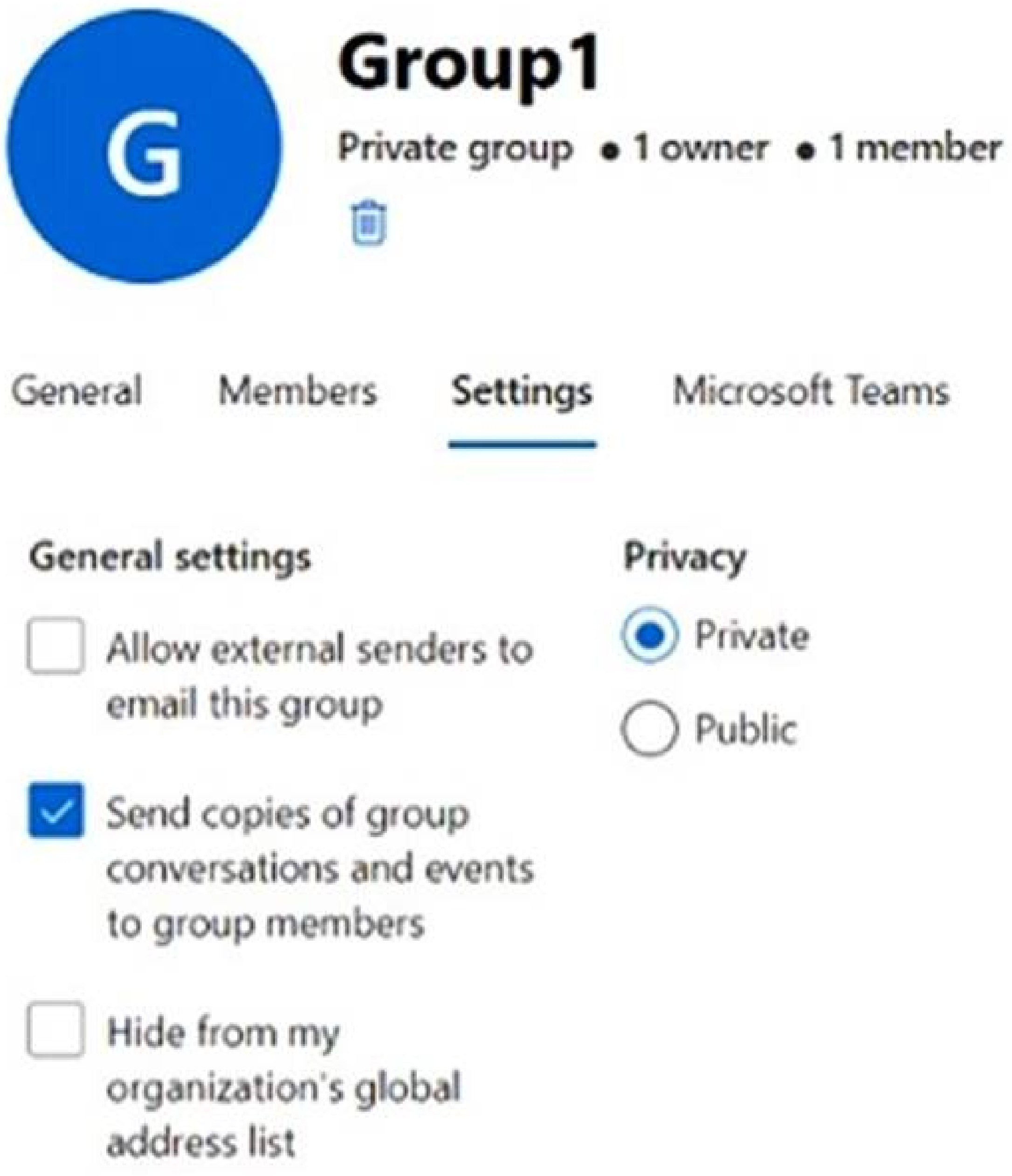
File extension is condition: DLP1, DLP2, and DLP3

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

NEW QUESTION 175

HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



Group1

Private group • 1 owner • 1 member

General settings

□ Allow external senders to email this group

☑ Send copies of group conversations and events to group members

□ Hide from my organization's global address list

Privacy

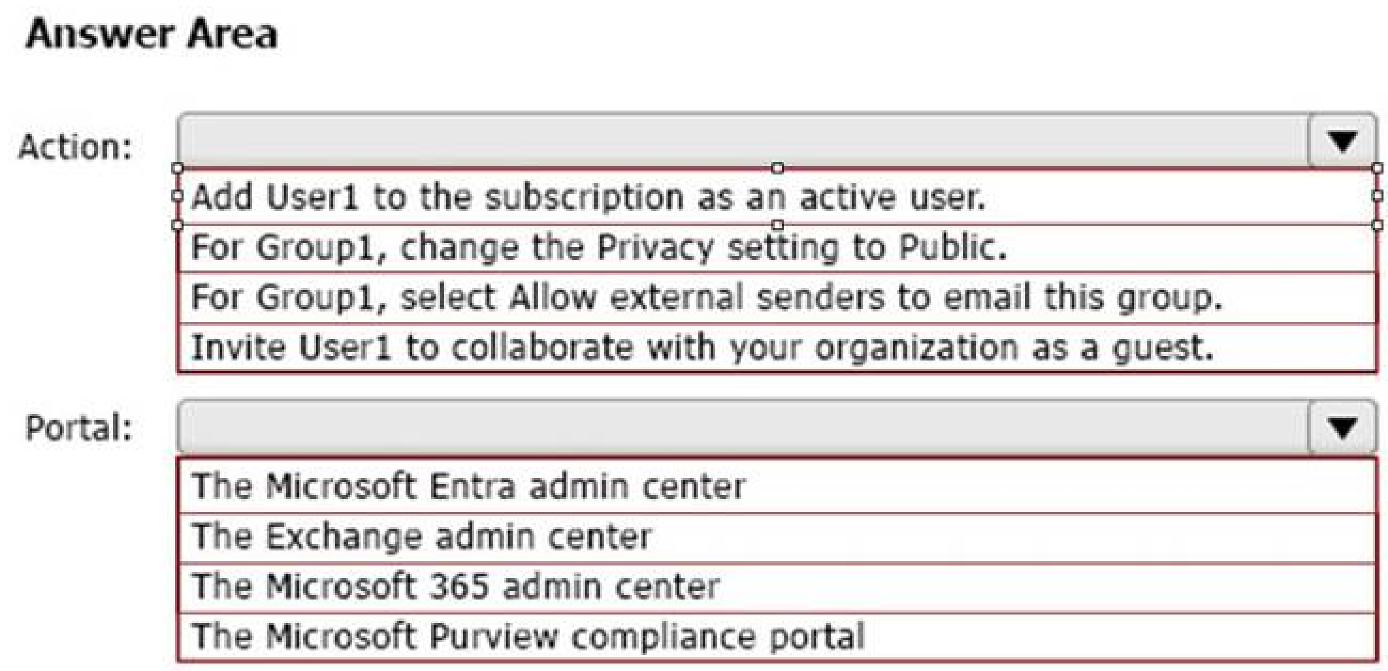
● Private

○ Public

An external user named User1 has an email address of user1@outlook.com. You need to add User1 to Group1.

What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

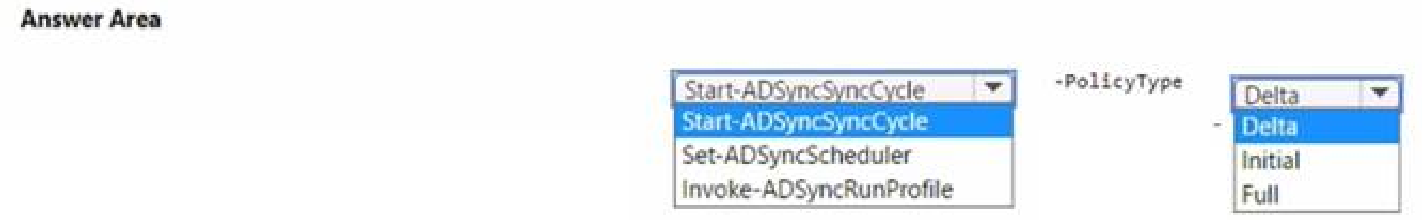
Explanation:
Box 1: Invite User1 to collaborate with your organization as a guest.
To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.
Navigate with your Web browser to https://admin.microsoft.com. On the left pane, click on “Users”, then click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

NEW QUESTION 176
- (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 180
HOTSPOT - (Topic 6)
Your network contains an Active Directory domain and an Azure AD tenant.
You implement directory synchronization for all 10.000 users in the organization. You automate the creation of 100 new user accounts.
You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.
Which command should you run? To answer, select the appropriate options in the answer area.



Answer Area

Start-ADSyncSyncCycle -PolicyType Delta

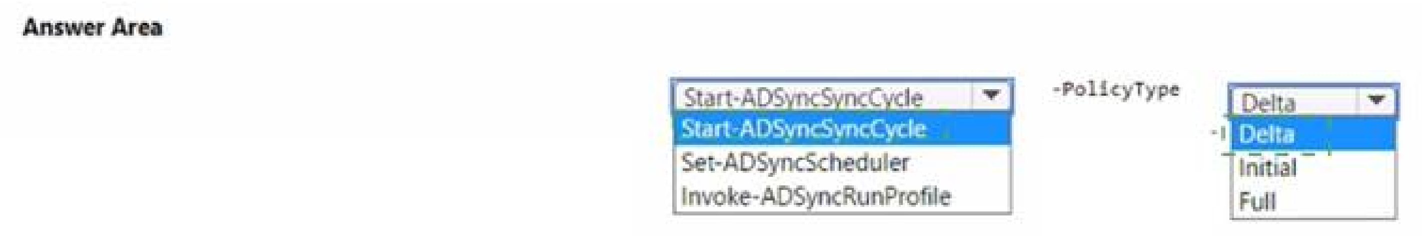
- Start-ADSyncSyncCycle
- Set-ADSyncScheduler
- Invoke-ADSyncRunProfile

- Delta
- Initial
- Full

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Start-ADSyncSyncCycle ▾
- Start-ADSyncSyncCycle
- Set-ADSyncScheduler
- Invoke-ADSyncRunProfile

-PolicyType

Delta ▾
- Delta
- Initial
- Full

NEW QUESTION 185

- (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 186

- (Topic 6)

You have a Microsoft 365 E5 tenant that contains a user named User1.

You plan to implement insider risk management.

You need to ensure that User1 can perform the following tasks:

? Review alerts.
? Manage cases.
? Create notice templates.
? Review user emails by using Content explorer.

The solution must use the principle of least privilege. To which role group should you add User1?

A. Insider Risk Management
B. Insider Risk Management Analysts
C. Insider Risk Management Investigators
D. Insider Risk Management Admin

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide

NEW QUESTION 187

- (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:

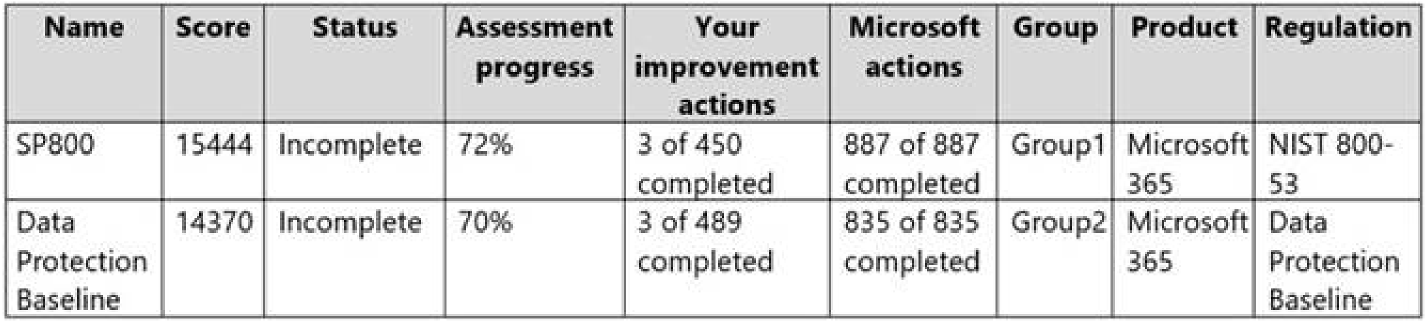
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION 191

HOTSPOT - (Topic 6)

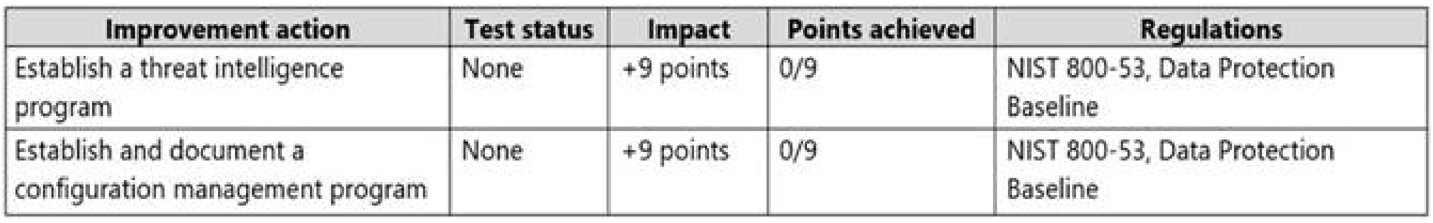
You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).

The tenant has two Compliance Manager assessments as shown in the following table.



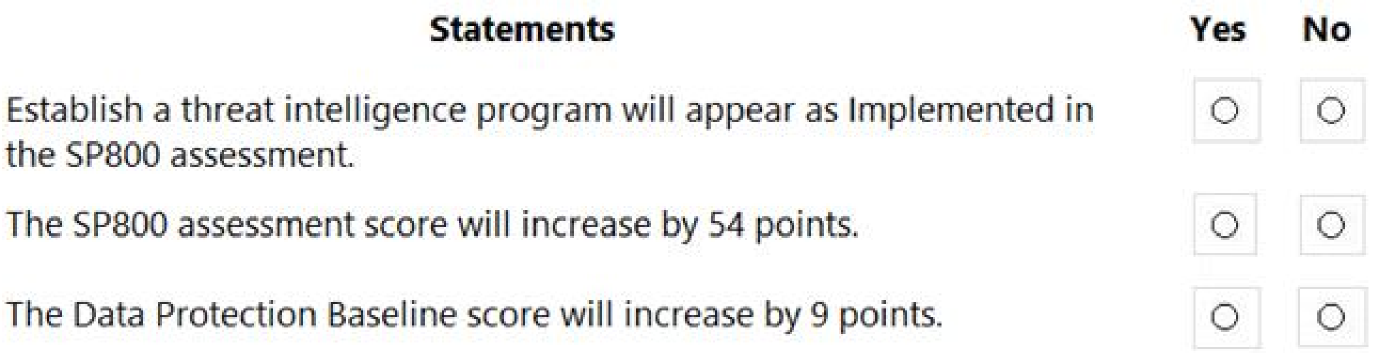
Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft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

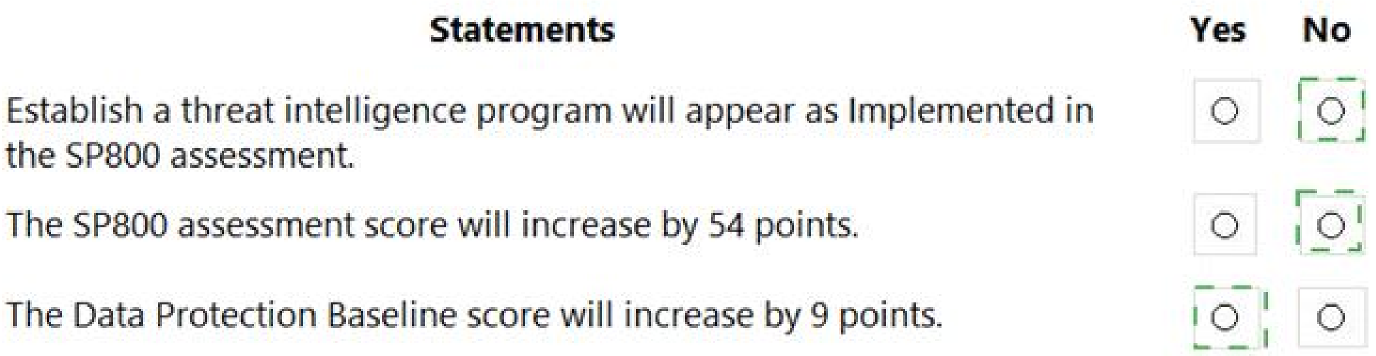


Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

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 194
- (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 195
- (Topic 6)
Your company has a Microsoft 365 E5 subscription.
Users in the research department work with sensitive data.
You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents.
Users in other departments must not be restricted.
What should you do?

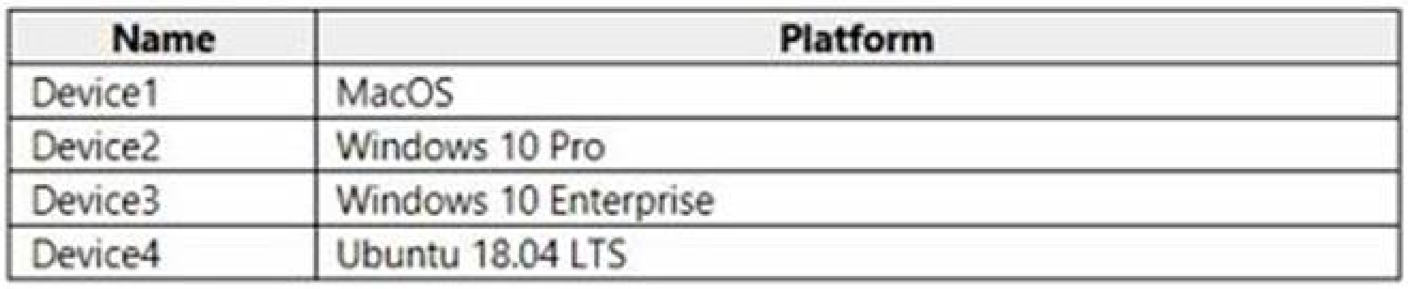
A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
B. Modify the safe links policy Global settings.
C. Create a data loss prevention (DLP) policy that has a Content contains condition.
D. Create a new safe links policy.

Answer: D

Explanation:
Use the Microsoft 365 Defender portal to create Safe Links policies
In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & Collaboration > Policies & Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use https://security.microsoft.com/safelinksv2.
* 1. On the Safe Links page, select Create to start the new Safe Links policy wizard.
* 2. On the Name your policy page, configure the following settings: Name: Enter a unique, descriptive name for the policy.
Description: Enter an optional description for the policy.
* 3. When you're finished on the Name your policy page, select Next.
* 4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions):

Users: The specified mailboxes, mail users, or mail contacts.
*-> Groups:
Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren't supported).
The specified Microsoft 365 Groups.
Domains: All recipients in the specified accepted domains in your organization. Etc.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links- policies-configure

NEW QUESTION 197
- (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

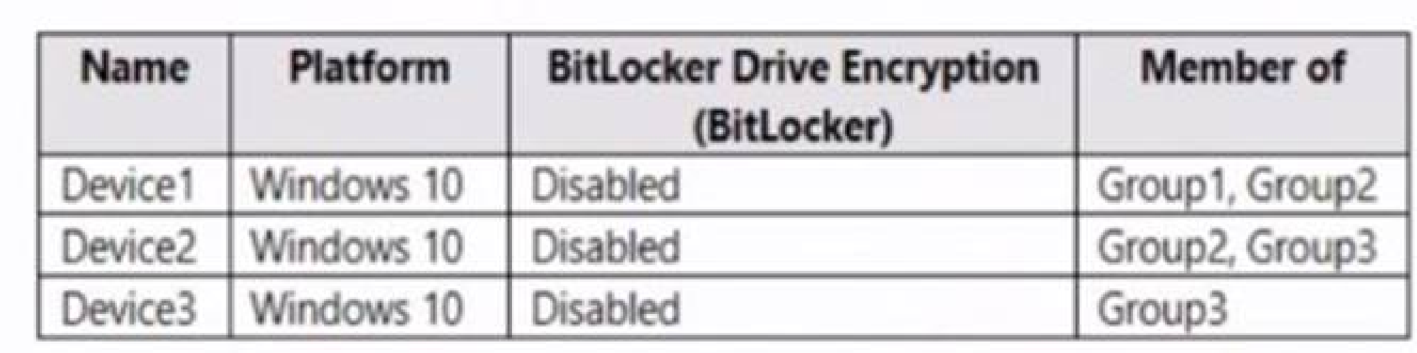
You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?

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

Answer: C

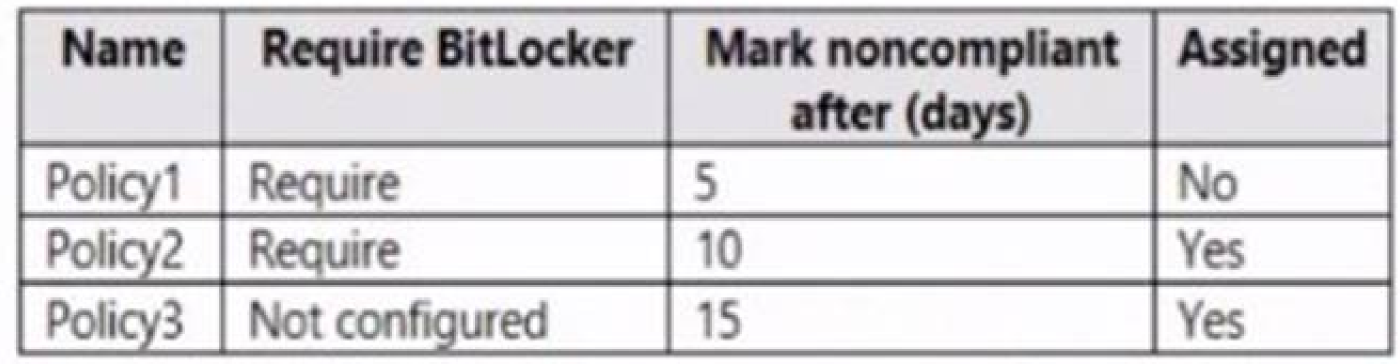
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements

NEW QUESTION 198
HOTSPOT - (Topic 6)
You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.



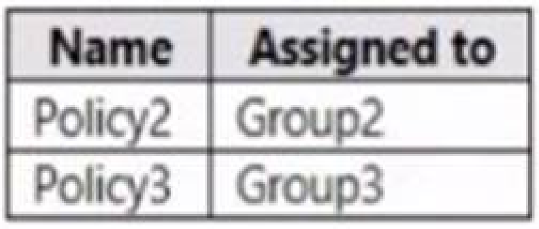
Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

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



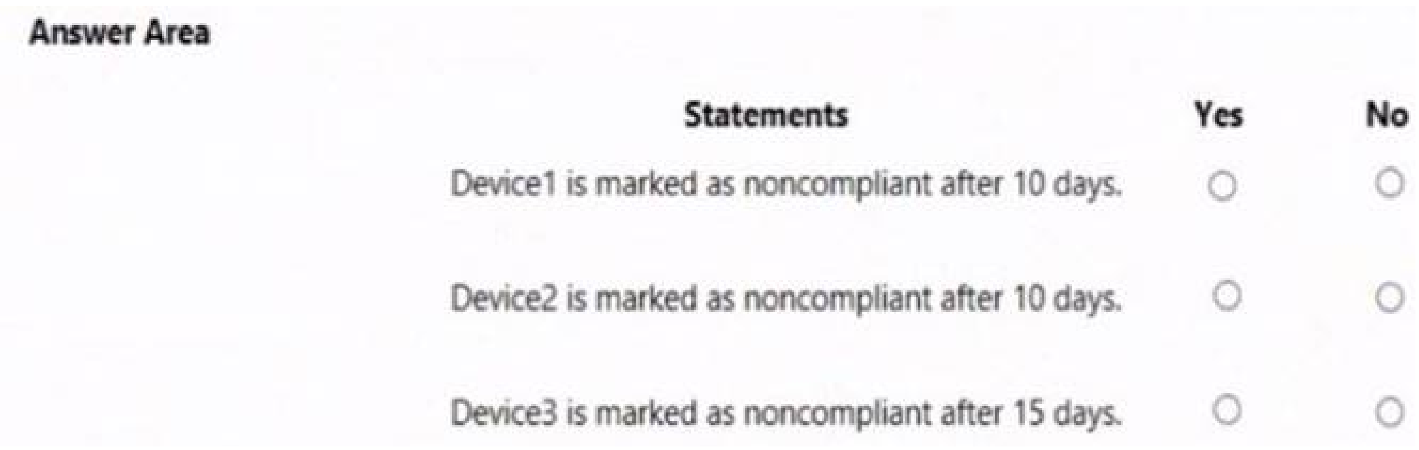
Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Not configured	15	Yes

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



Name	Assigned to
Policy2	Group2
Policy3	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.



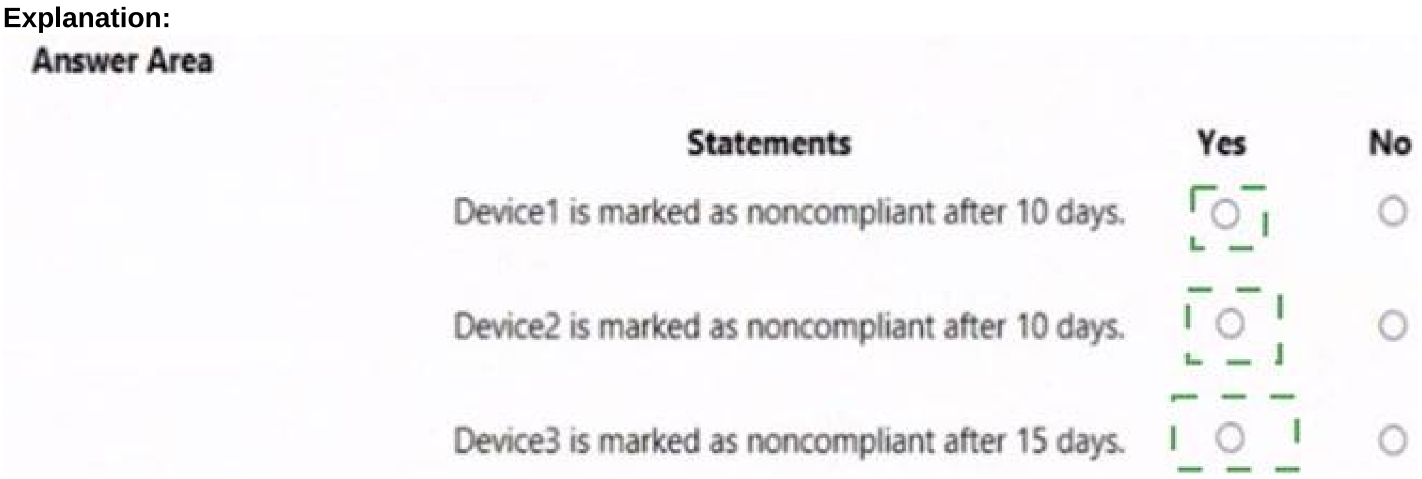
Answer Area

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

A. Mastered
B. Not Mastered

Answer: A

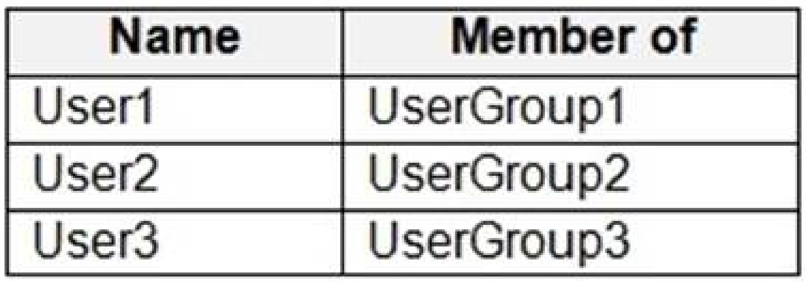
Explanation:



Answer Area

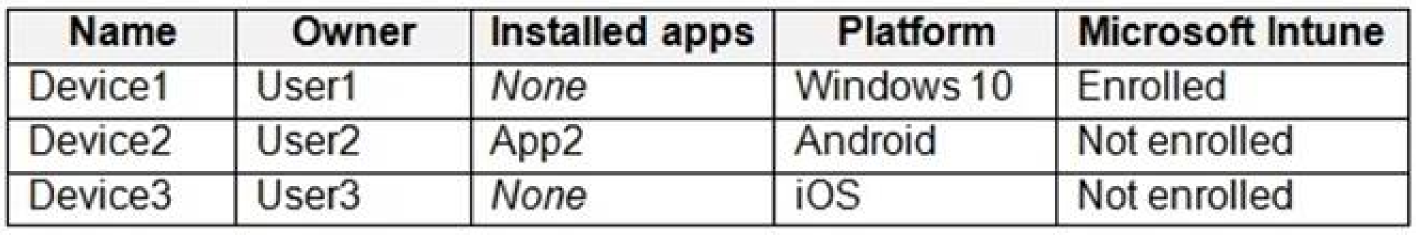
Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	[✓ ○]	○
Device2 is marked as noncompliant after 10 days.	[✓ ○]	○
Device3 is marked as noncompliant after 15 days.	[✓ ○]	○

NEW QUESTION 202
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.



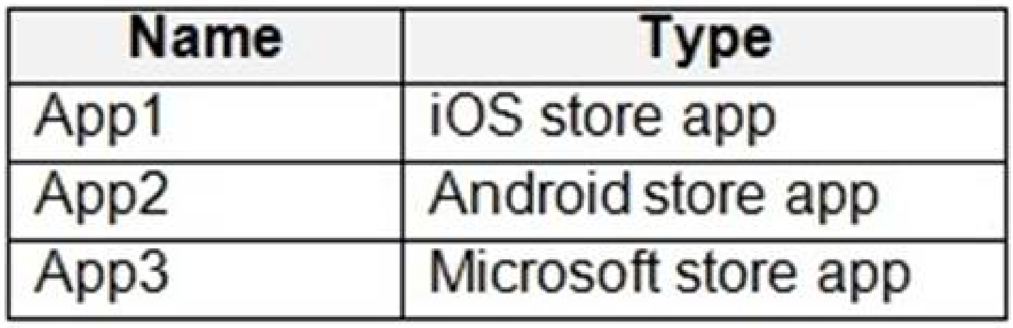
Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.



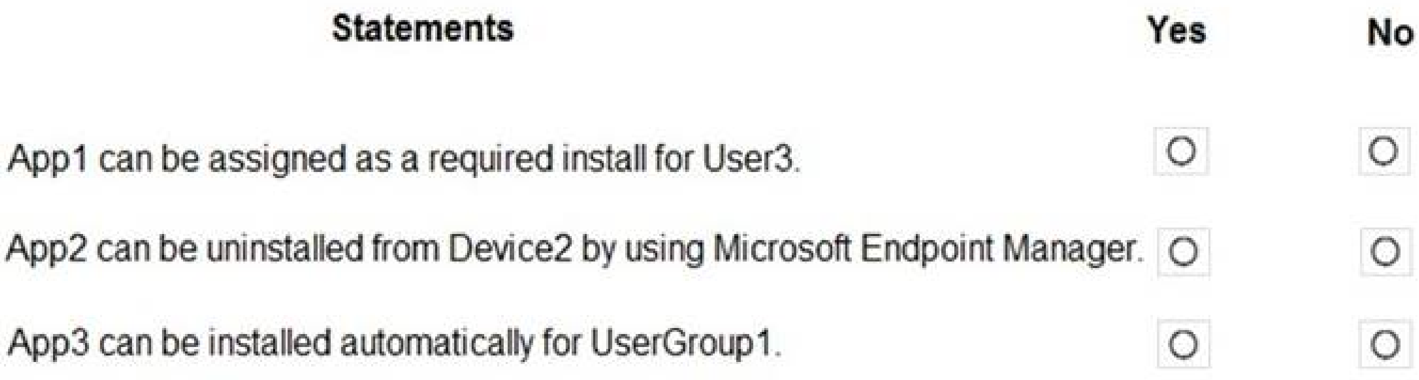
Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	*None*	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	*None*	iOS	Not enrolled

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.

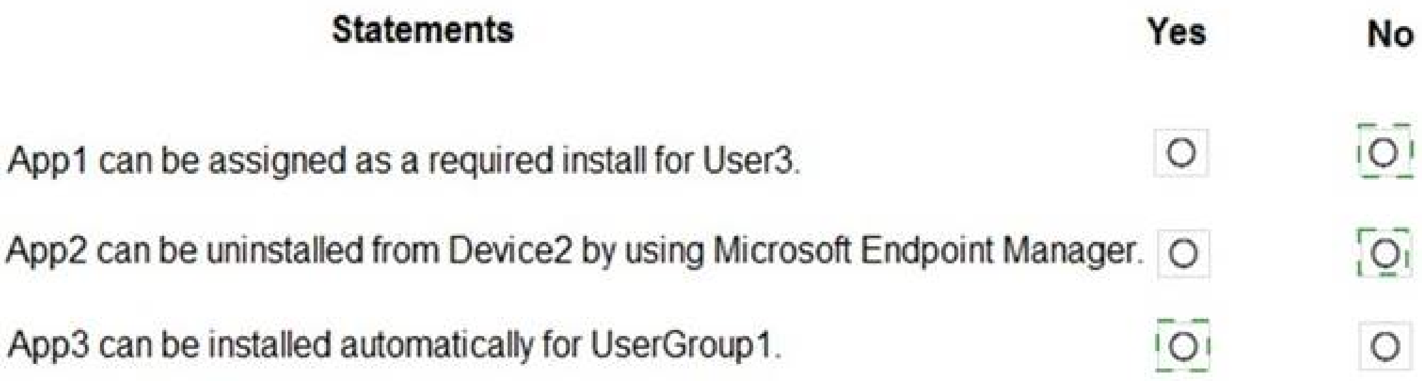


Statements	Yes	No
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

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 206
- (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.

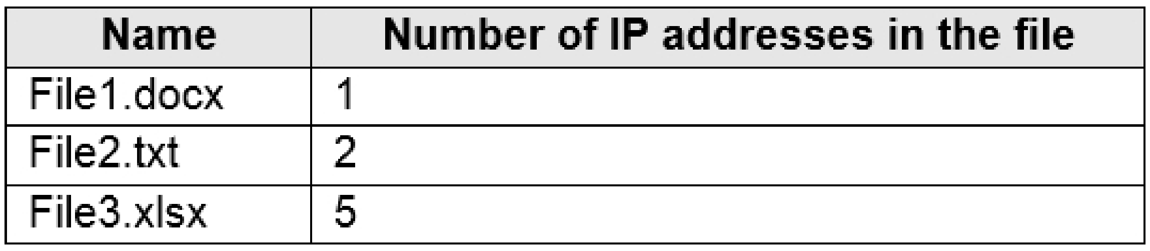
Answer: A

NEW QUESTION 207
- (Topic 6)
You have an Azure AD tenant.
You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD. You purchase a Microsoft 365 E3 subscription.
You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort.
What should you do?

A. From the Microsoft Endpoinf Manager admin center, create a Windows Autopilot deployment profil
B. Assign the profile to all the computer
C. Instruct users to restart their computer and perform a network restart.
D. Enroll the computers in Microsoft Intun
E. Create a configuration profile by using the Edition upgrade and mode switch templat
F. From the Microsoft Endpoint Manager admincenter, assign the profile to all the computers and instruct users to restart their computer.
G. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online sit
H. Instruct users to run the provisioning package from SharePoint Online.
I. From the Azure Active Directory admin center, create a security group that has dynamic device membershi
J. Assign licenses to the group and instruct users to sign in to their computer.

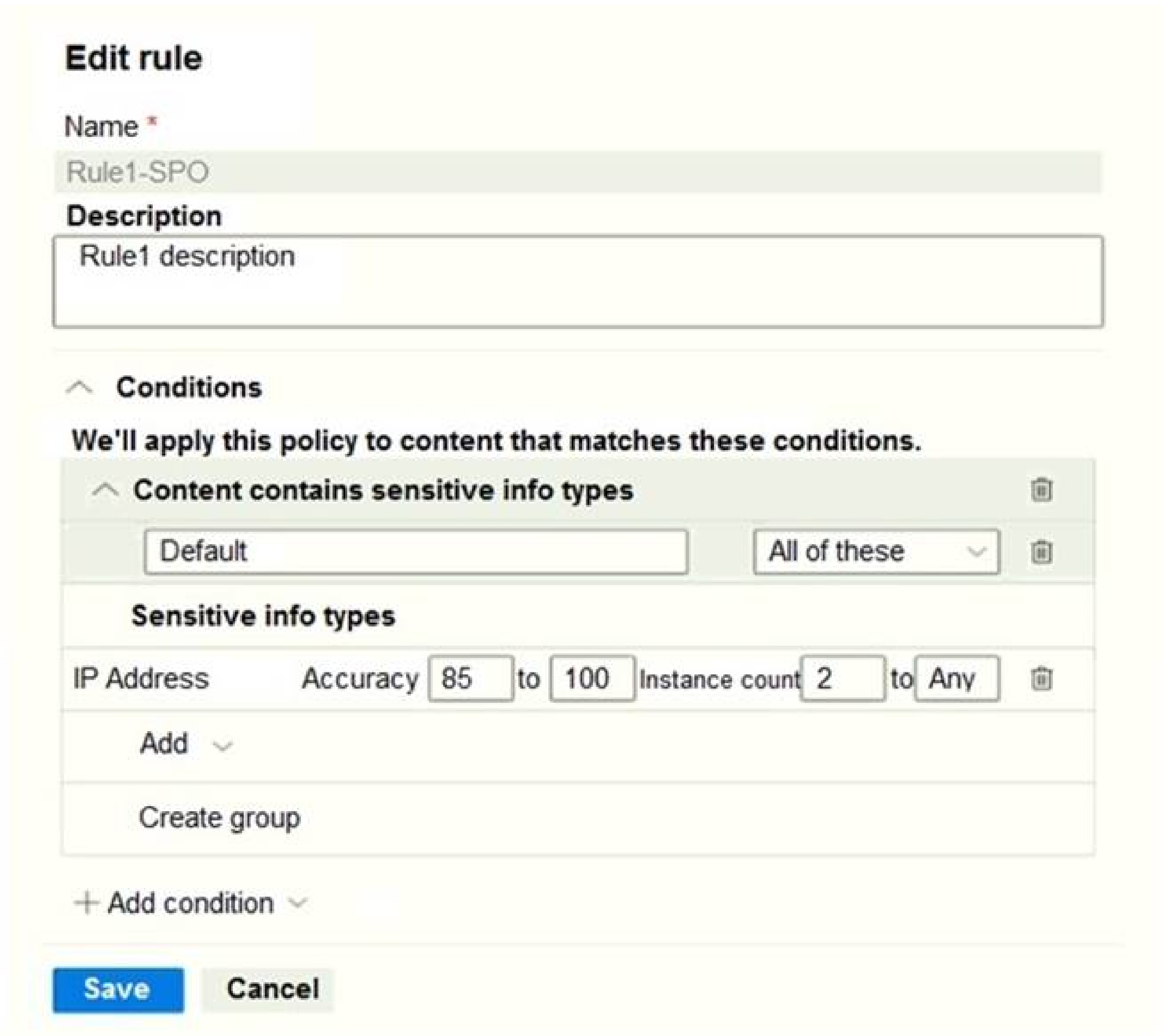
Answer: B

NEW QUESTION 211
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

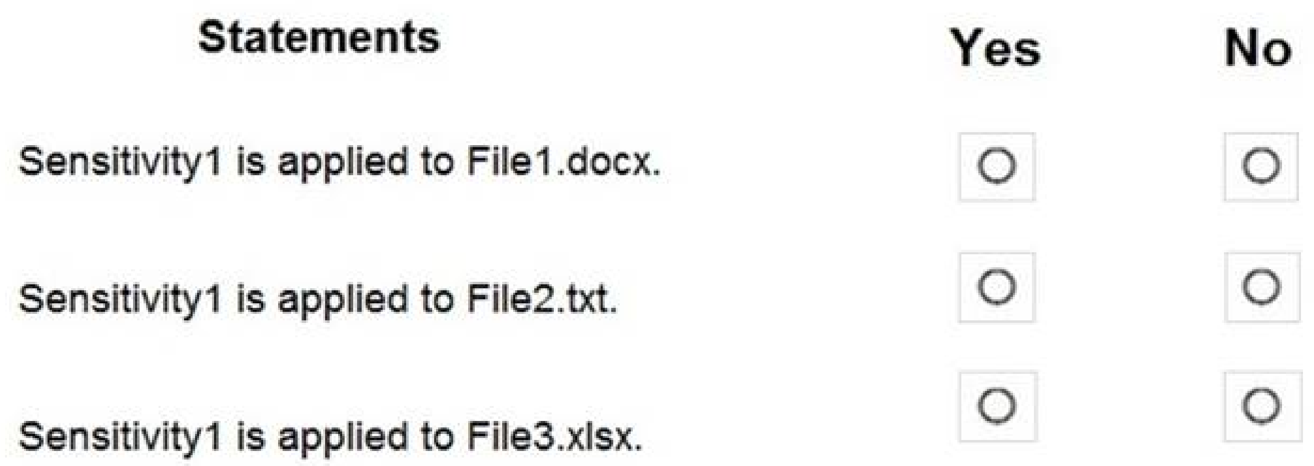
Add

Create group

+ Add condition

Save Cancel

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

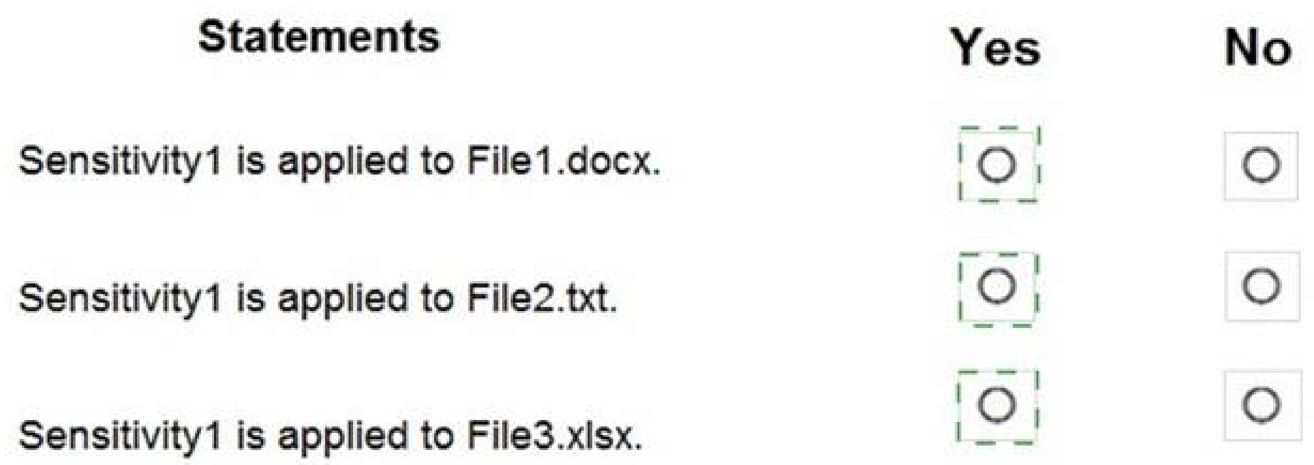


Statements	Yes	No
Sensitivity1 is applied to File1.docx.	○	○
Sensitivity1 is applied to File2.txt.	○	○
Sensitivity1 is applied to File3.xlsx.	○	○

A. Mastered
B. Not Mastered

Answer: A

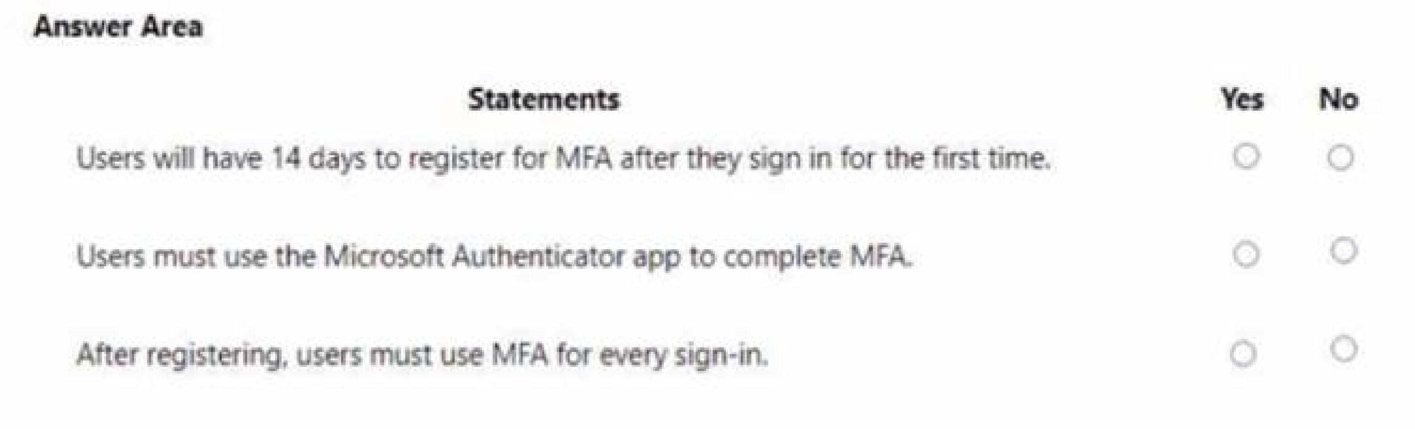
Explanation:



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

NEW QUESTION 214
HOTSPOT - (Topic 5)
You are evaluating the use of multi-factor authentication (MFA).
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



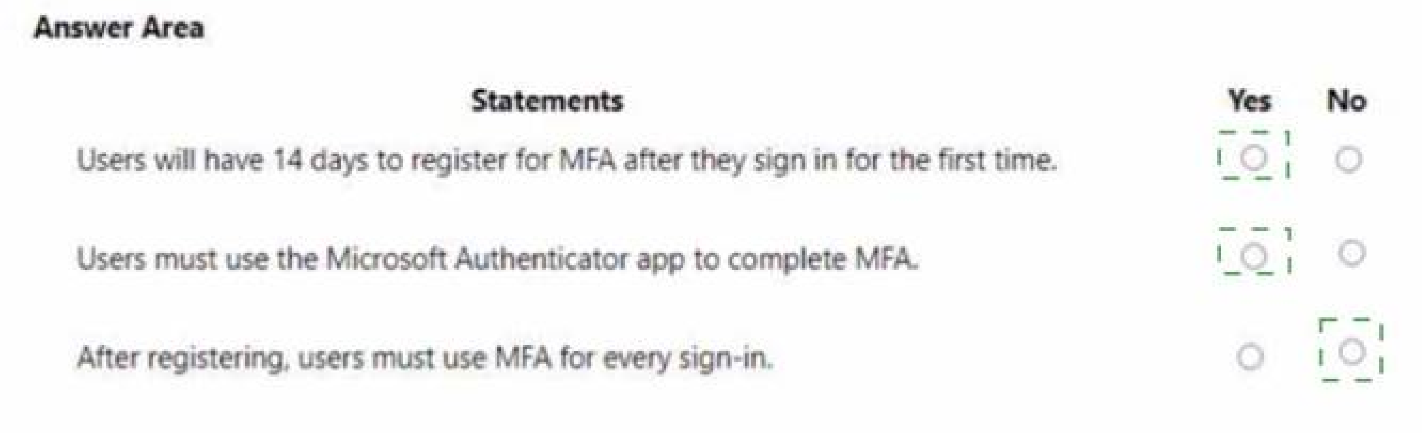
Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	○	○
Users must use the Microsoft Authenticator app to complete MFA.	○	○
After registering, users must use MFA for every sign-in.	○	○

A. Mastered
B. Not Mastered

Answer: A

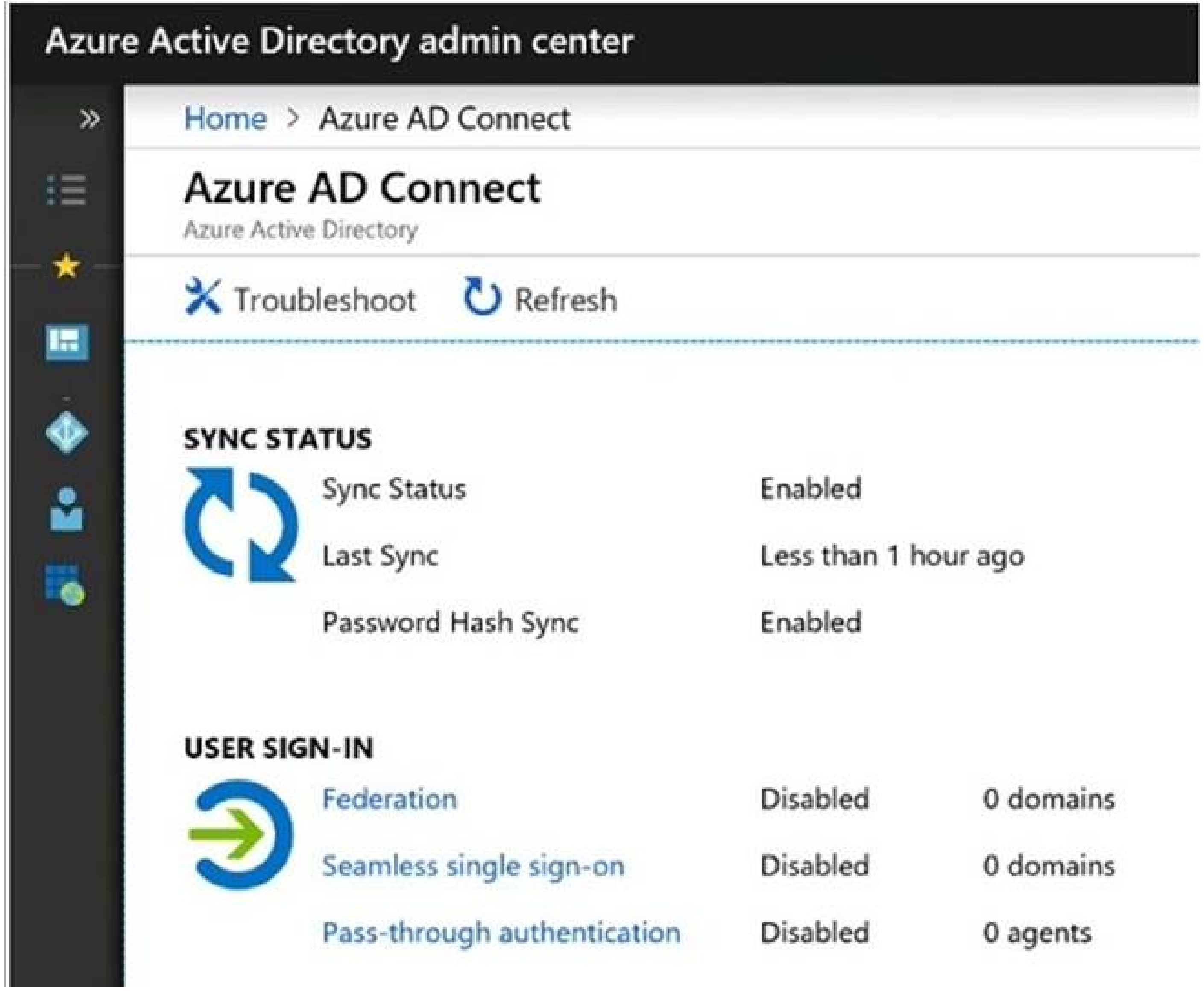
Explanation:



Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	[✓ ○]	○
Users must use the Microsoft Authenticator app to complete MFA.	[✓ ○]	○
After registering, users must use MFA for every sign-in.	○	[✓ ○]

NEW QUESTION 215
HOTSPOT - (Topic 4)
HOTSPOT
You create the Microsoft 365 tenant.
You implement Azure AD Connect as shown in the following exhibit.



Azure Active Directory admin center

Home > Azure AD Connect

Azure AD Connect
Azure Active Directory

Troubleshoot Refresh

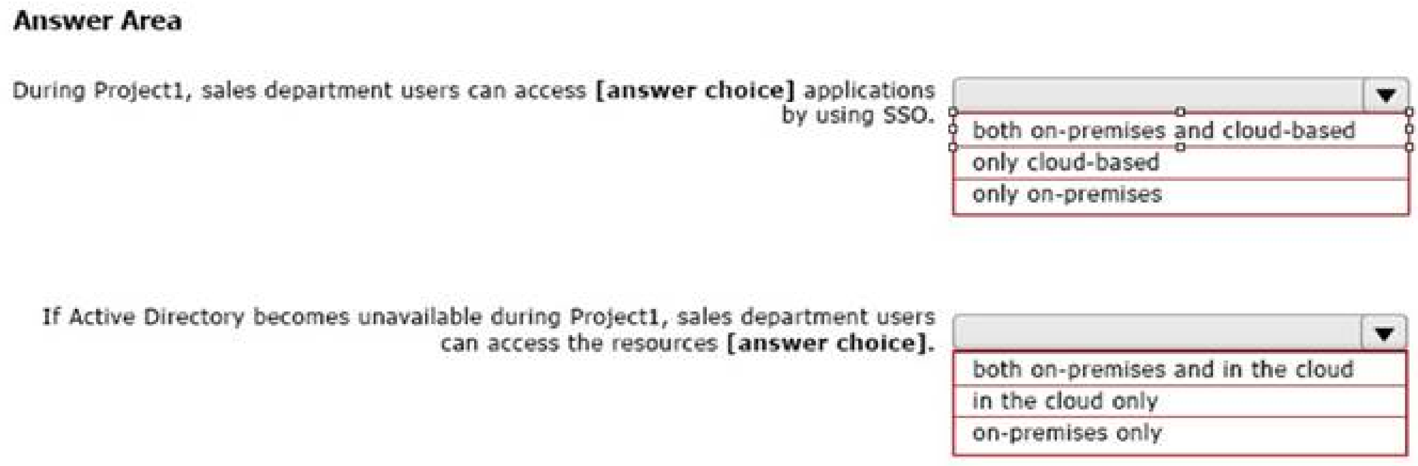
SYNC STATUS

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	Disabled	0 domains
Pass-through authentication	Disabled	0 agents

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

During Project1, sales department users can access [answer choice] applications by using SSO.

- both on-premises and cloud-based
- only cloud-based
- only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources [answer choice].

- both on-premises and in the cloud
- in the cloud only
- on-premises only

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: only on-premises
In the exhibit, seamless single sign-on (SSO) is disabled. Therefore, as SSO is disabled in the cloud, the Sales department users can access only on-premises applications by using SSO.
In the exhibit, directory synchronization is enabled and active. This means that the on- premises Active Directory user accounts are synchronized to Azure Active Directory user accounts. If the on-premises Active Directory becomes unavailable, the users can access resources in the cloud by authenticating to Azure Active Directory. They will not be able to access resources on-premises if the on-premises Active Directory becomes unavailable as they will not be able to authenticate to the on-premises Active Directory.
Box 2: in the cloud only

NEW QUESTION 218
- (Topic 4)
You are evaluating the required processes for Project1.
You need to recommend which DNS record must be created while adding a domain name for the project.
Which DNS record should you recommend?

A. host (A)
B. host information
C. text (TXT)
D. alias (CNAME)

Answer: D

Explanation:
When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
Text (TXT)
Mail exchanger (MX)
incorrect answer options you may see on the exam include the following: alias (CNAME)
Host (A) host (AAA)
Pointer (PTR) Name Server (NS)
host information (HINFO) pointer (PTR)
Reference:
https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns- records-at-any-dns-hosting-provider

NEW QUESTION 221
- (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 222

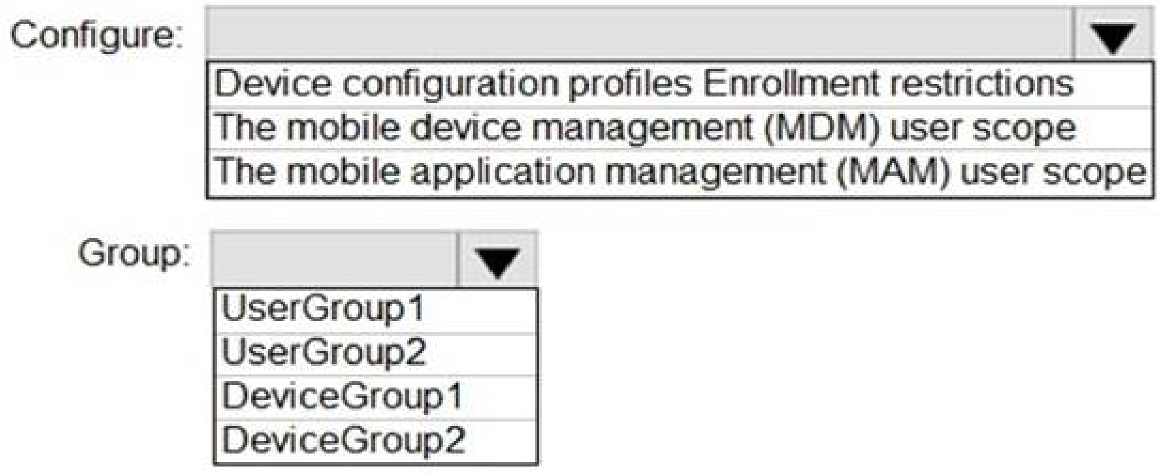
- (Topic 3)
You create the planned DLP policies.
You need to configure notifications to meet the technical requirements. What should you do?

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

Answer: D

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

NEW QUESTION 223
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.

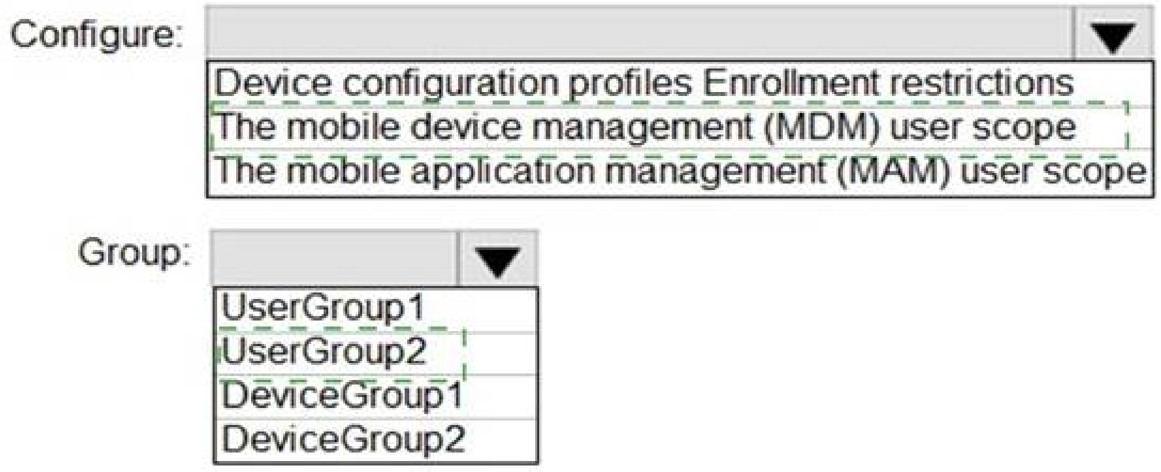

Configure:
- Device configuration profiles Enrollment restrictions
- The mobile device management (MDM) user scope
- The mobile application management (MAM) user scope

Group:
- UserGroup1
- UserGroup2
- DeviceGroup1
- DeviceGroup2

A. Mastered
B. Not Mastered

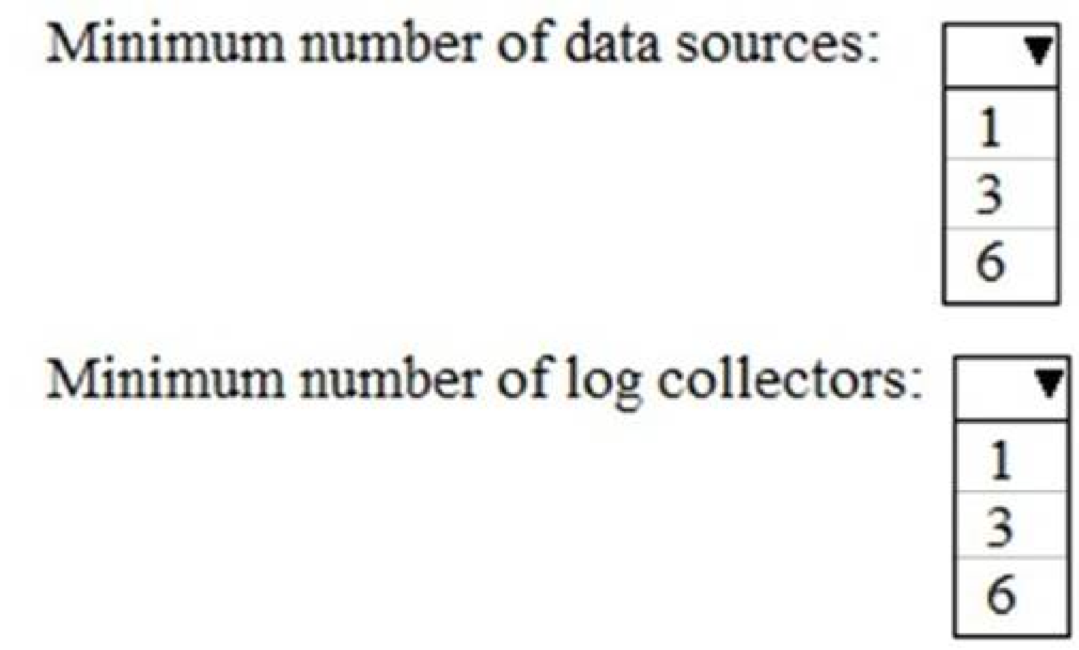
Answer: A

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 225
HOTSPOT - (Topic 2)
You need to meet the technical requirement for log analysis.
What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Minimum number of data sources: ▼
1
3
6

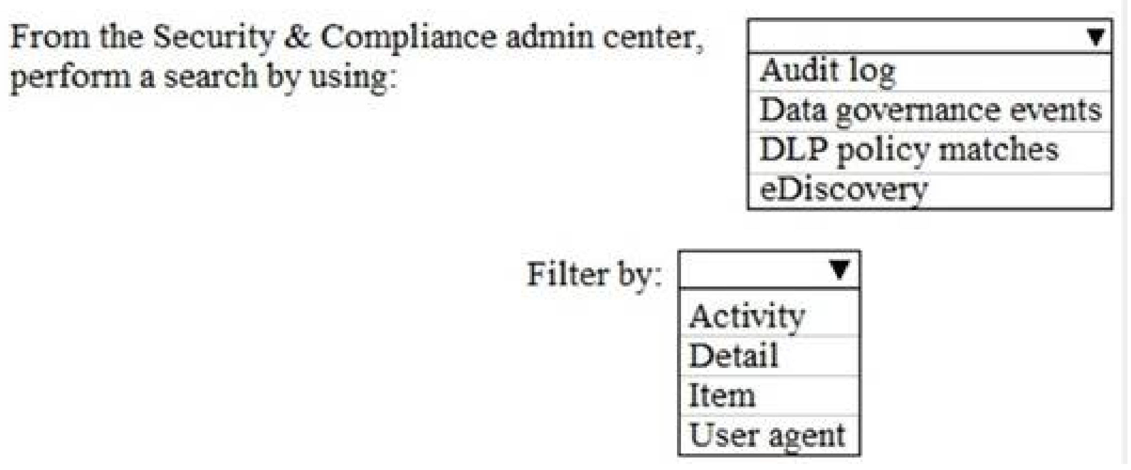
Minimum number of log collectors: ▼
1
3
6

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

NEW QUESTION 228
HOTSPOT - (Topic 2)
You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



From the Security & Compliance admin center, perform a search by using: ▼
Audit log
Data governance events
DLP policy matches
eDiscovery

Filter by: ▼
Activity
Detail
Item
User agent

A. Mastered
B. Not Mastered

Answer: A

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

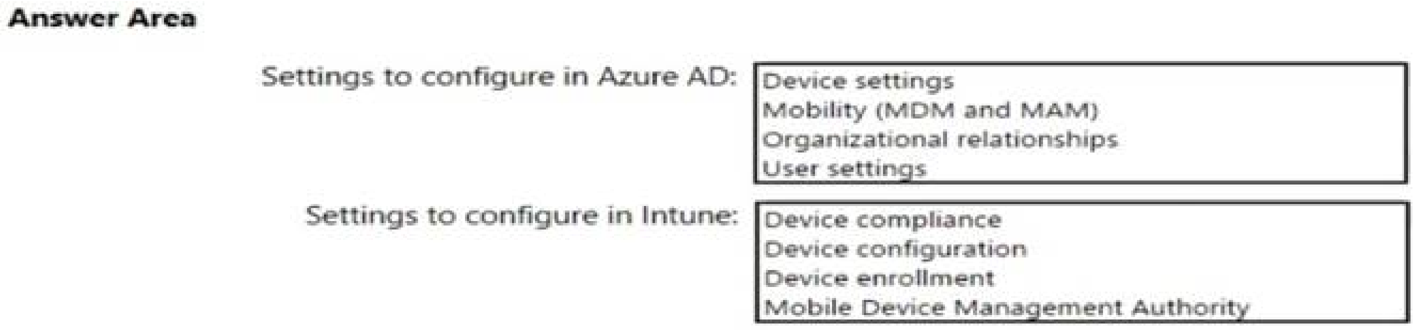
NEW QUESTION 233
- (Topic 1)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You create a device configuration profile from the Device Management admin center.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 236
HOTSPOT - (Topic 1)
You need to meet the technical requirements and planned changes for Intune. What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

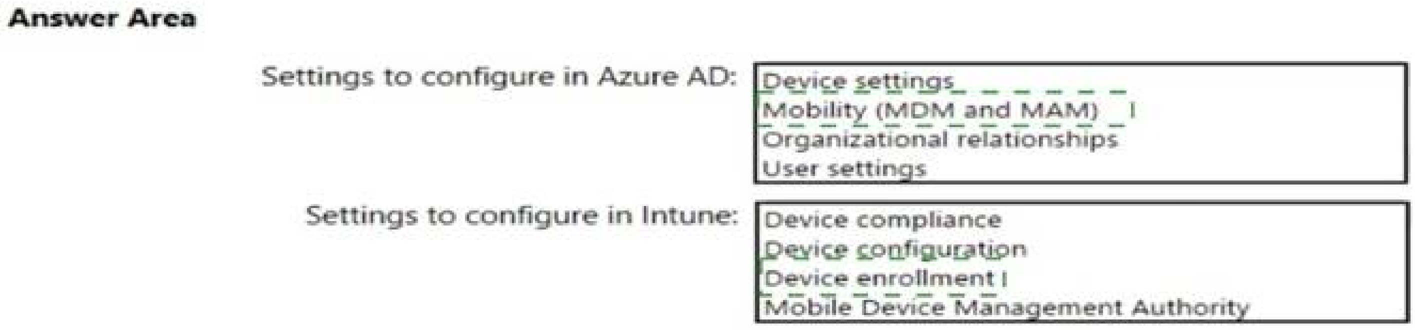
Settings to configure in Azure AD:
Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

A. Mastered
B. Not Mastered

Answer: A

Explanation:

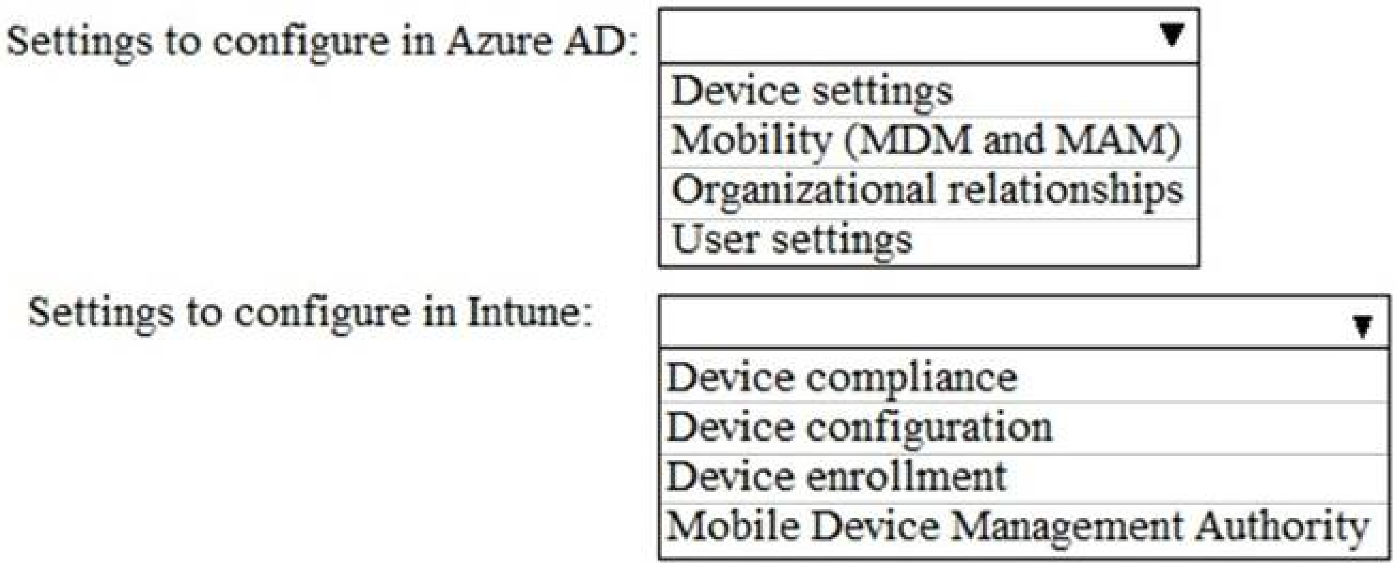


Answer Area

Settings to configure in Azure AD:
Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

NEW QUESTION 237
HOTSPOT - (Topic 1)
You need to meet the Intune requirements for the Windows 10 devices.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Settings to configure in Azure AD:
Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

A. Mastered
B. Not Mastered

Answer: A

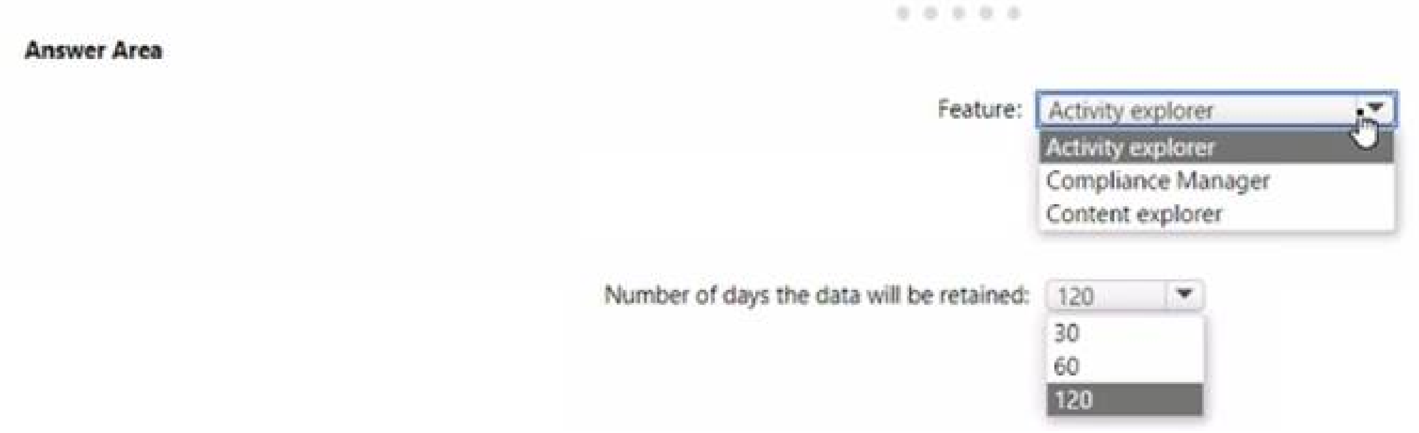
Explanation:
References:
https://docs.microsoft.com/en-us/intune/windows-enroll

NEW QUESTION 242
- (Topic 6)
You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.
During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint.
You need to prevent the user from sharing the credit card information by using email and SharePoint.
What should you configure?

A. the status of the DLP policy
B. the user overrides of the DLP policy rule
C. the locations of the DLP policy
D. the conditions of the DLP policy rule

Answer: D

NEW QUESTION 246
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that.
You need to identify whenever a sensitivity label is applied, changed, or removed within the subscription.
Which feature should you use, and how many days will the data be retained? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point.



Answer Area

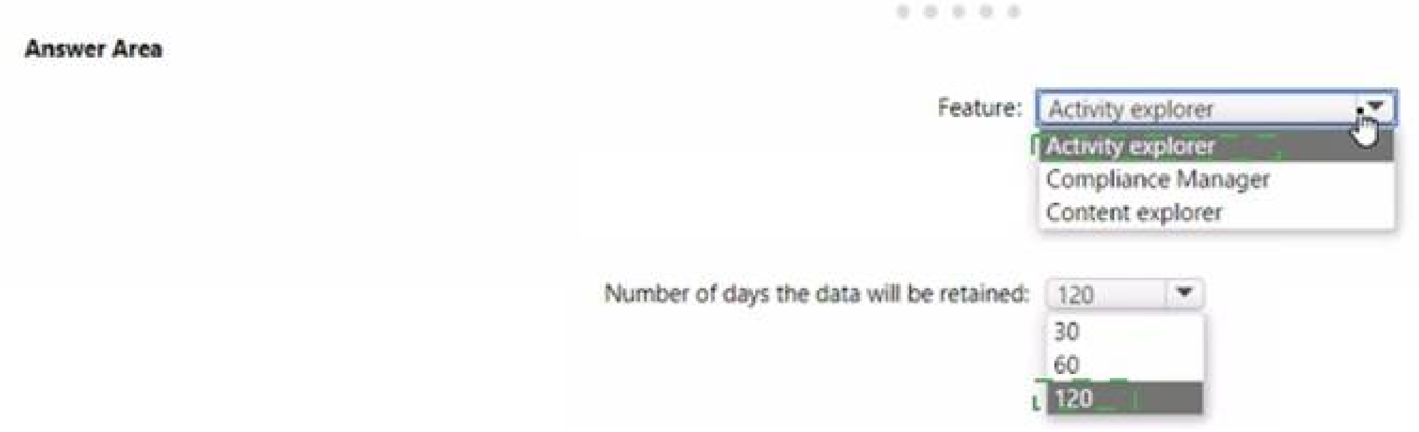
Feature: Activity explorer

Number of days the data will be retained: 120

A. Mastered
B. Not Mastered

Answer: A

Explanation:

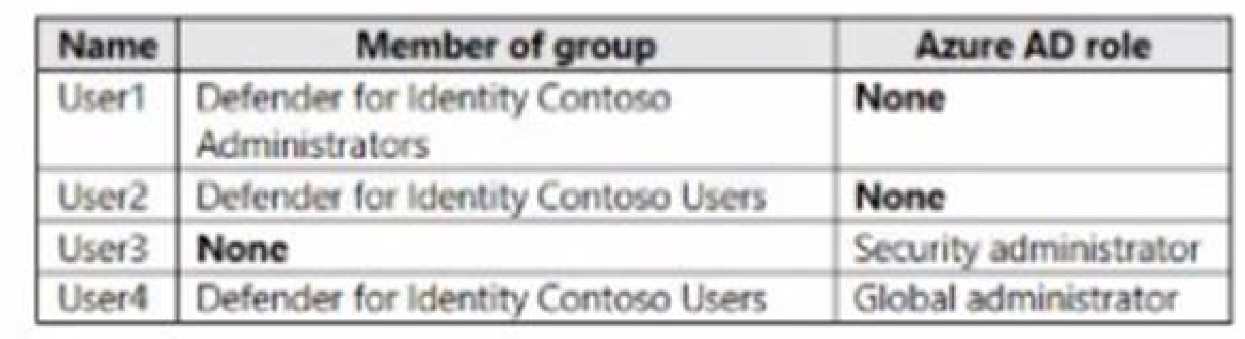


Answer Area

Feature: Activity explorer

Number of days the data will be retained: 120

NEW QUESTION 247
- (Topic 6)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.
The tenant contains the users shown in the following table.



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

You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User4 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 248
- (Topic 6)
You have a Microsoft 365 subscription that contains a user named User1. User1 requires admin access to perform the following tasks:
Manage Microsoft Exchange Online settings. Create Microsoft 365 groups.
You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.
What should you use?

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

Answer: D

Explanation:
Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources Assign time-bound access to resources using start and end dates Require approval to activate privileged roles
Enforce multi-factor authentication to activate any role Use justification to understand why users activate
Get notifications when privileged roles are activated Conduct access reviews to ensure users still need roles Download audit history for internal or external audit
Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity- management/pim-configure

NEW QUESTION 250
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365 and contains a user named User1.
User1 emails a product catalog in the PDF format to 300 vendors. Only 200 vendors receive the email message, and User1 is blocked from sending email until the next day.
You need to prevent this issue from reoccurring. What should you configure?

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

Answer: A

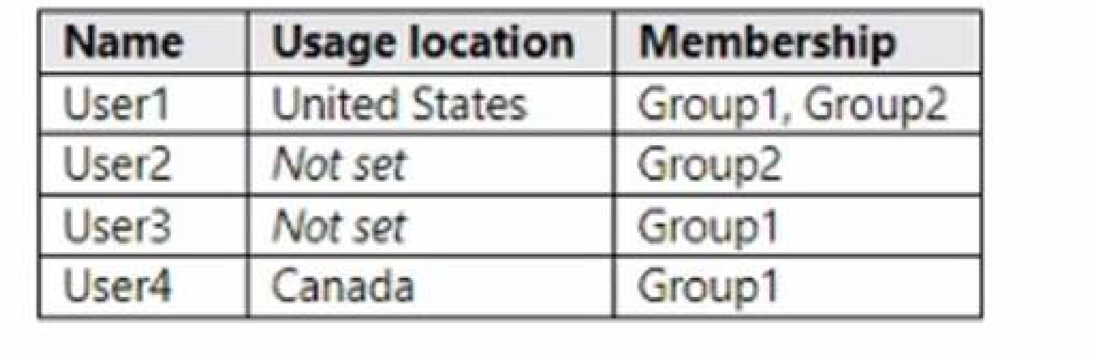
NEW QUESTION 254
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 System, and then you select About to view information about the system.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 259
- (Topic 6)
Your company has an Azure AD tenant named contoso.com that includes the users shown in the following table.



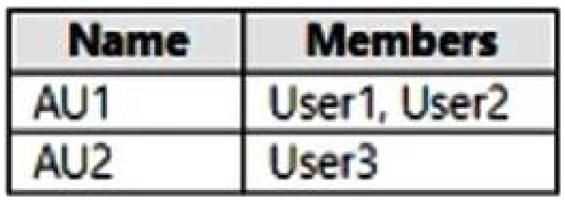
Name	Usage location	Membership
User1	United States	Group1, Group2
User2	*Not set*	Group2
User3	*Not set*	Group1
User4	Canada	Group1

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

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

Answer: C

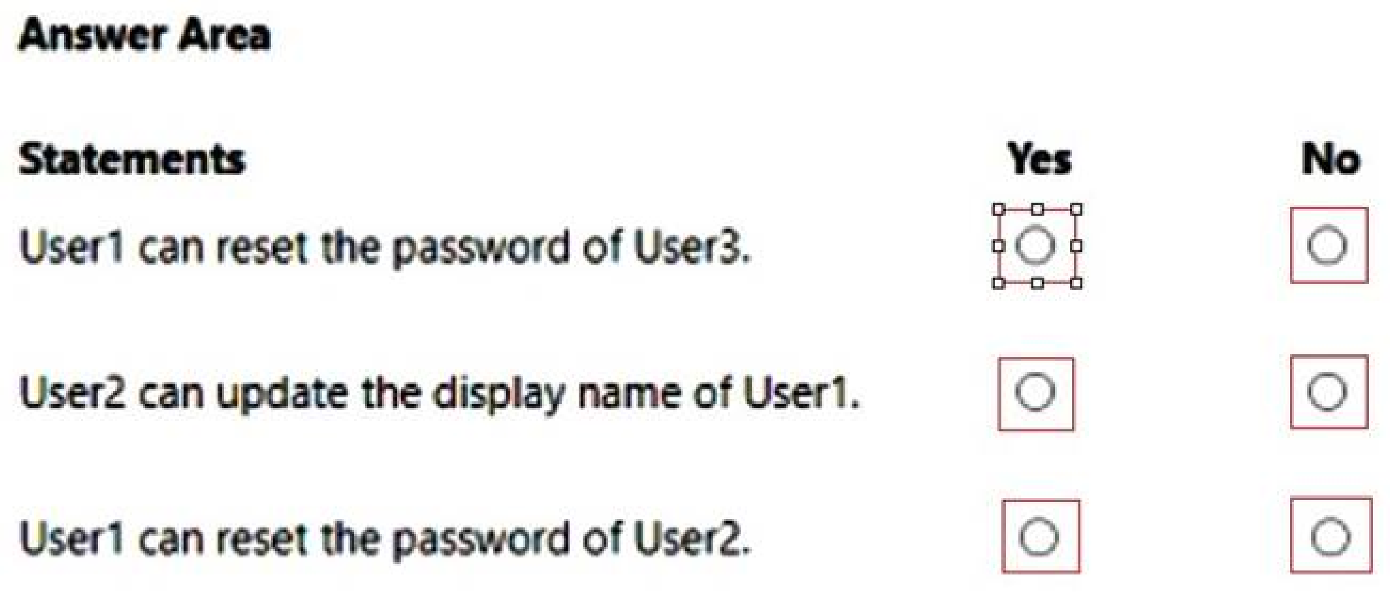
NEW QUESTION 263
HOTSPOT - (Topic 6)
HOTSPOT
You have an Azure AD tenant that contains the administrative units shown in the following table.



Name	Members
AU1	User1, User2
AU2	User3

You have the following users:
? A user named User1 that is assigned the Password Administrator for AU1 and AU2.
? A user named User2 that is assigned the User Administrator for AU1.

? A user named User3 that is assigned the User Administrator for the tenant.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



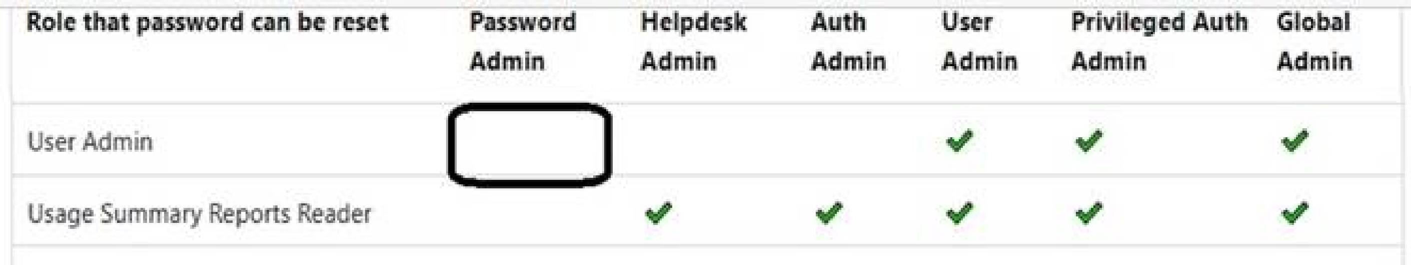
Answer Area

Statements	Yes	No
User1 can reset the password of User3.	○	○
User2 can update the display name of User1.	○	○
User1 can reset the password of User2.	○	○

A. Mastered
B. Not Mastered

Answer: A

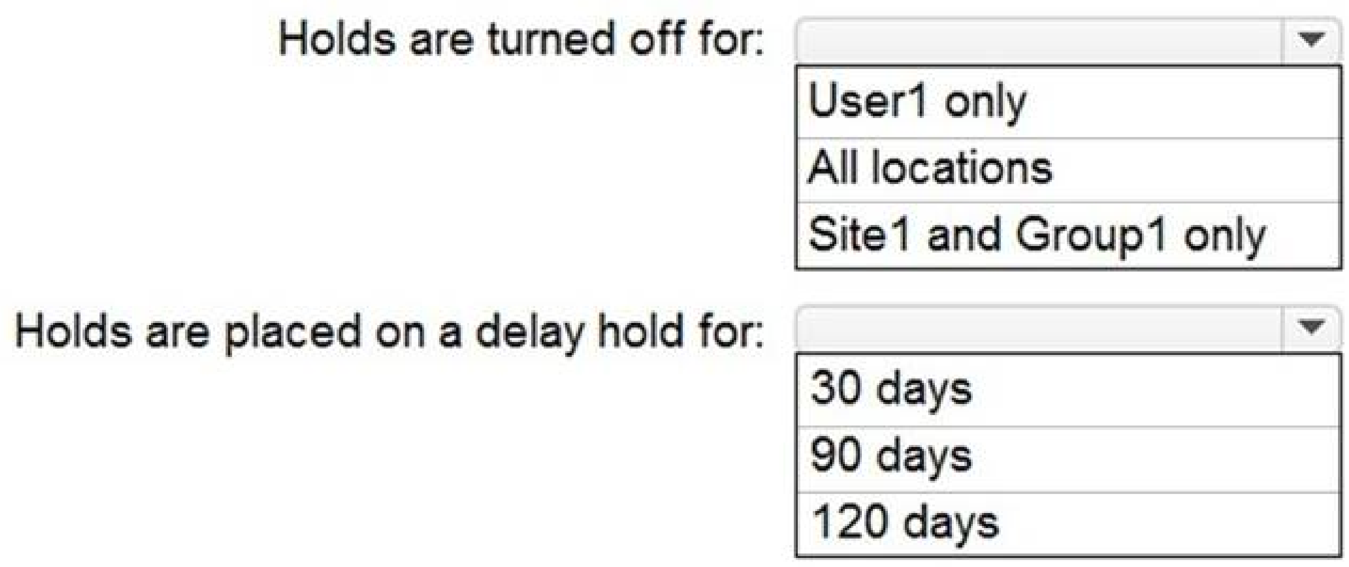
Explanation:
Box 1: No
User1 is assigned the Password Administrator for AU1 and AU2. User3 is in AU2. User3 is User Adminstrator.
Password administrators cannot reset User Administrators passwords.
Note: Password Administrator
Users with this role have limited ability to manage passwords. This role does not grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user's password depends on the role the user is assigned.



Role that password can be reset	Password Admin	Helpdesk Admin	Auth Admin	User Admin	Privileged Auth Admin	Global Admin
User Admin				✓	✓	✓
Usage Summary Reports Reader		✓	✓	✓	✓	✓

Box 2: Yes
Box 3: No
User1 is assigned the Password Administrator for AU1 and AU2. User2 is in AU1. User2 is User Adminstrator.
Password administrators cannot reset User Administrators passwords.
Note: User Administrator
Can manage all aspects of users and groups, including resetting passwords for limited admins.

NEW QUESTION 265
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:
? Name: Case1
? Included content: Group1, User1, Site1
? Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders
The investigation for Case1 completes, and you close the case.
What occurs after you close Case1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



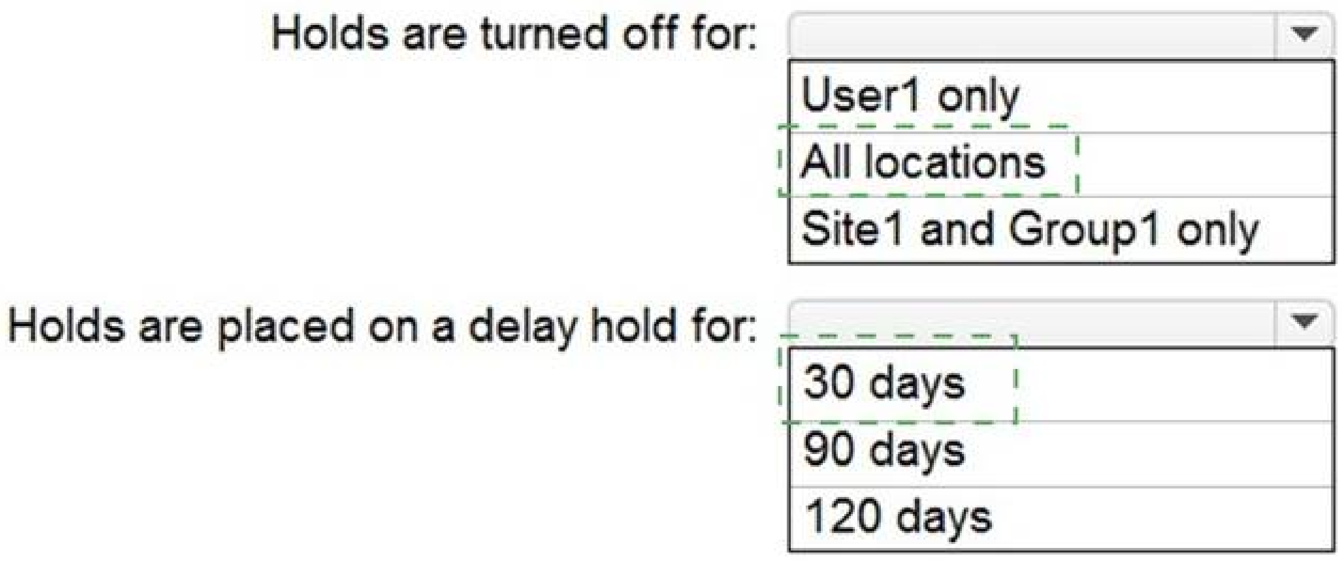
Holds are turned off for:
- User1 only
- All locations
- Site1 and Group1 only

Holds are placed on a delay hold for:
- 30 days
- 90 days
- 120 days

A. Mastered
B. Not Mastered

Answer: A

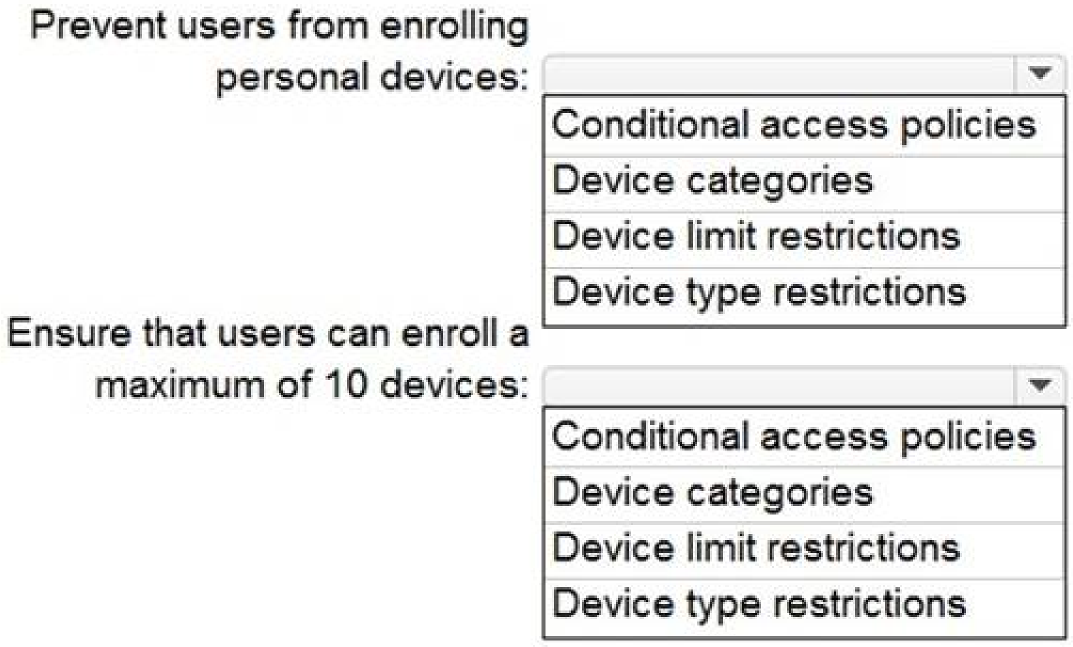
Explanation:



Holds are turned off for:
- User1 only
- [✓ All locations]
- Site1 and Group1 only

Holds are placed on a delay hold for:
- [✓ 30 days]
- 90 days
- 120 days

NEW QUESTION 268
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that uses Microsoft Intune. You need to configure Intune to meet the following requirements:
? Prevent users from enrolling personal devices.
? Ensure that users can enroll a maximum of 10 devices.
What should you use for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



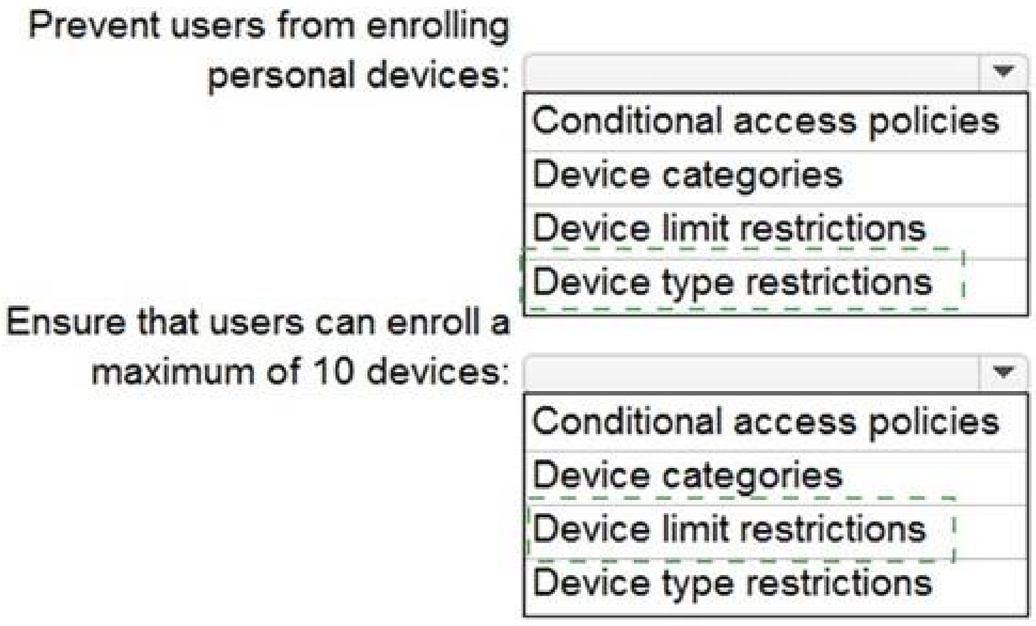
Prevent users from enrolling personal devices:
- Conditional access policies
- Device categories
- Device limit restrictions
- Device type restrictions

Ensure that users can enroll a maximum of 10 devices:
- Conditional access policies
- Device categories
- Device limit restrictions
- Device type restrictions

A. Mastered
B. Not Mastered

Answer: A

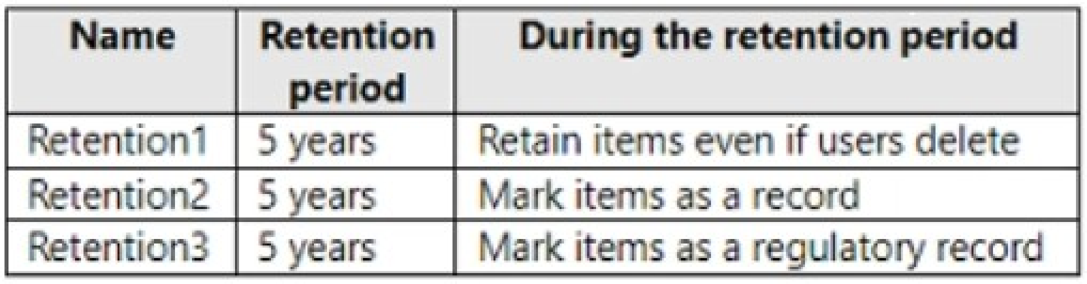
Explanation:



Prevent users from enrolling personal devices:
- Conditional access policies
- Device categories
- Device limit restrictions
- [✓ Device type restrictions]

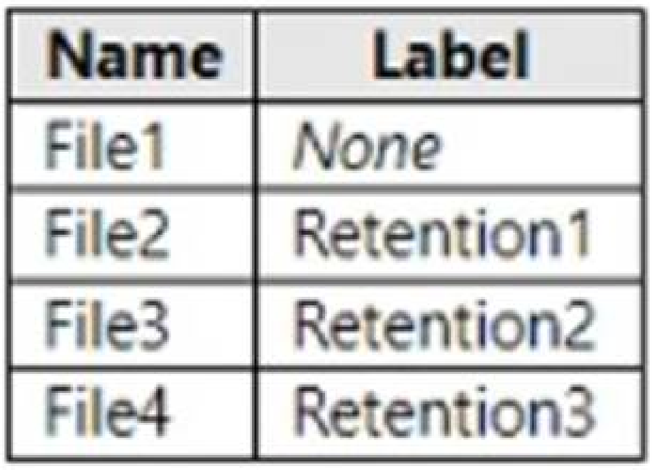
Ensure that users can enroll a maximum of 10 devices:
- Conditional access policies
- Device categories
- [✓ Device limit restrictions]
- Device type restrictions

NEW QUESTION 272
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.



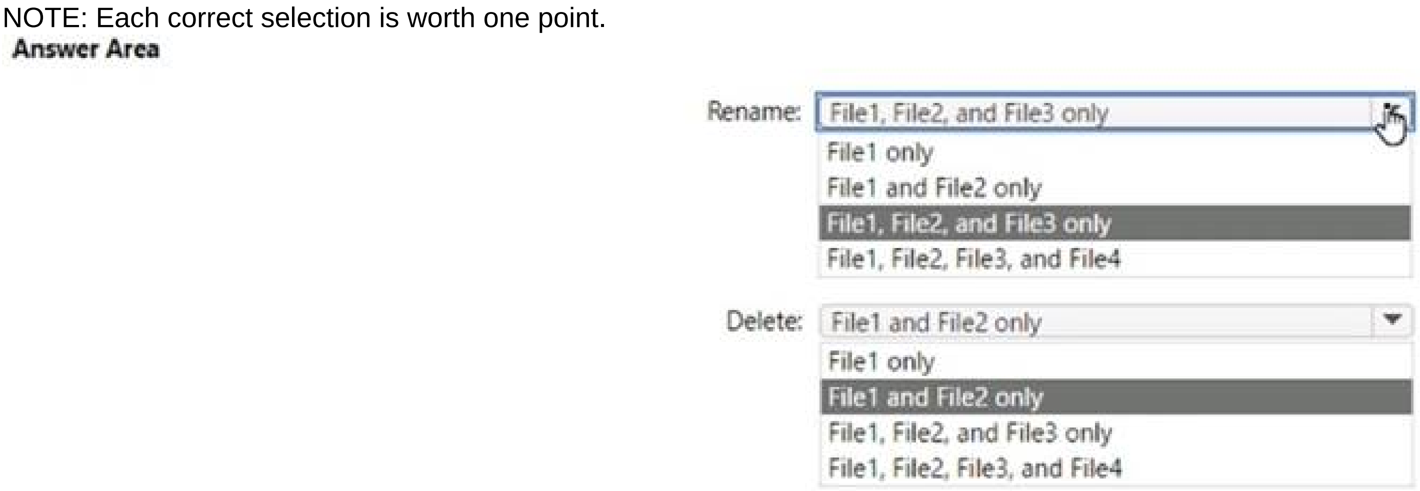
Name	Retention period	During the retention period
Retention1	5 years	Retain items even if users delete
Retention2	5 years	Mark items as a record
Retention3	5 years	Mark items as a regulatory record

Site1 contains the files shown in the following table.



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

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



Answer Area

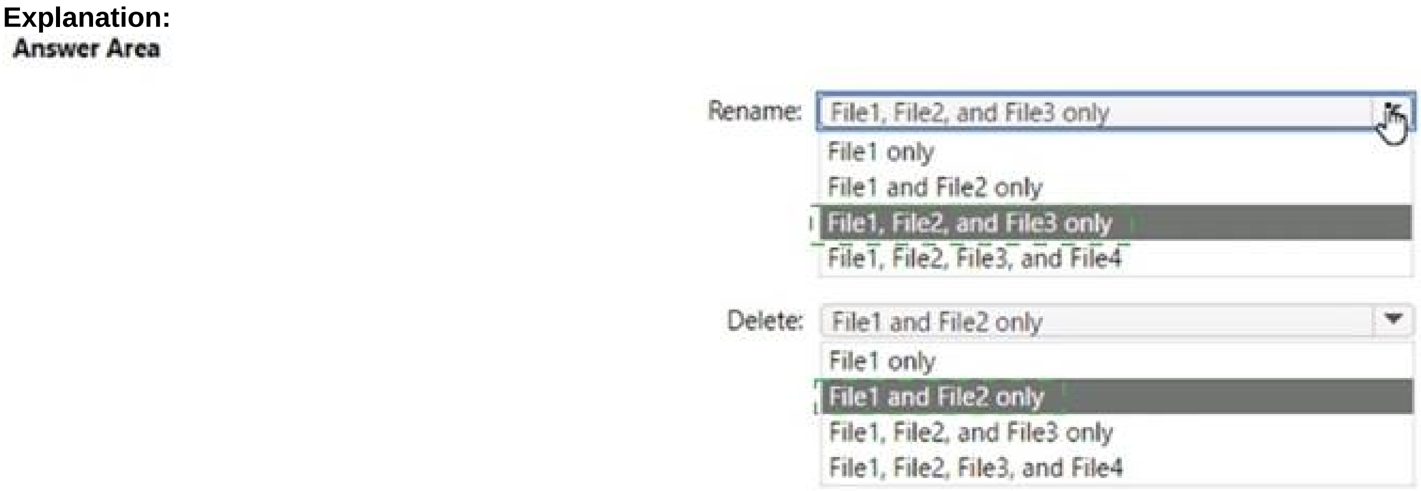
Rename: File1, File2, and File3 only
- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

Delete: File1 and File2 only
- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

A. Mastered
B. Not Mastered

Answer: A

Explanation:

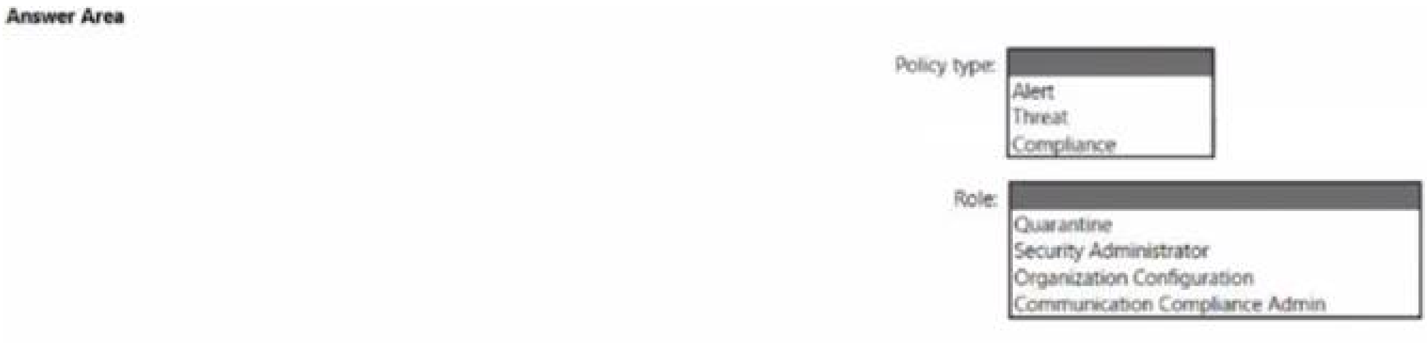


Answer Area

Rename: File1, File2, and File3 only
- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

Delete: File1 and File2 only
- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

NEW QUESTION 273
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant.
You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege.
Which type of policy should you create and which Microsoft 365 compliance center role is required to create the pokey? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

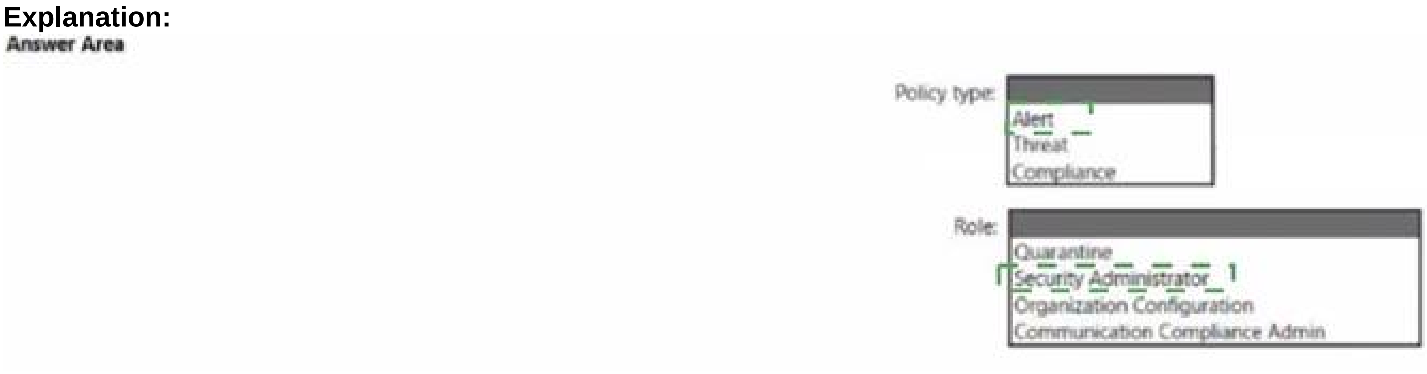
Policy type:
- Alert
- Threat
- Compliance

Role:
- Quarantine
- Security Administrator
- Organization Configuration
- Communication Compliance Admin

A. Mastered
B. Not Mastered

Answer: A

Explanation:

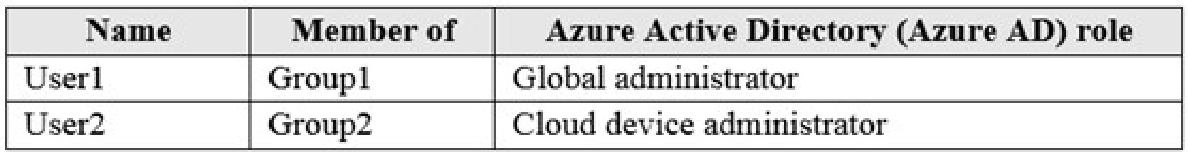


Answer Area

Policy type:
- [✓ Alert]
- Threat
- Compliance

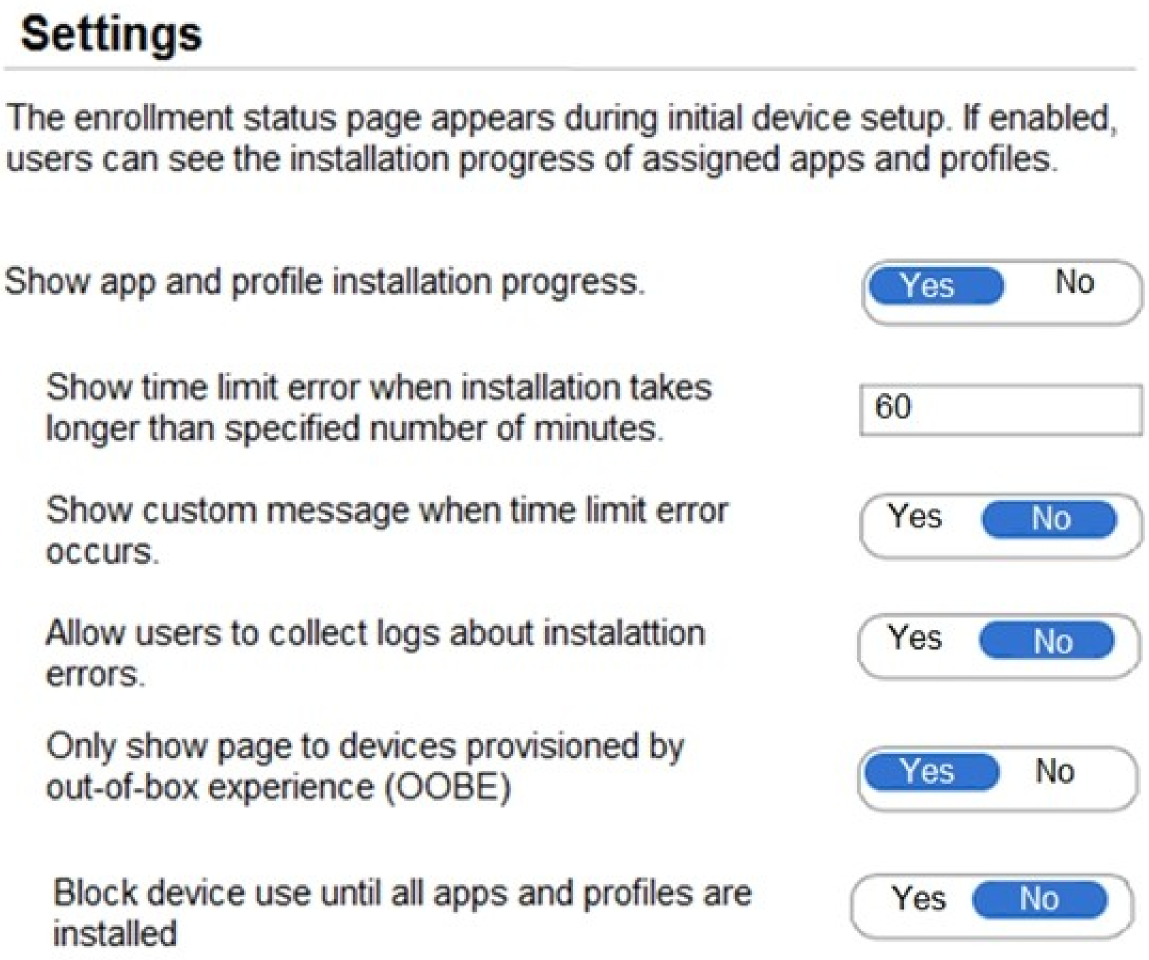
Role:
- Quarantine
- [✓ Security Administrator]
- Organization Configuration
- Communication Compliance Admin

NEW QUESTION 276
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains the users shown in the following table.



Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.



Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress. [✓ Yes] No

Show time limit error when installation takes longer than specified number of minutes. 60

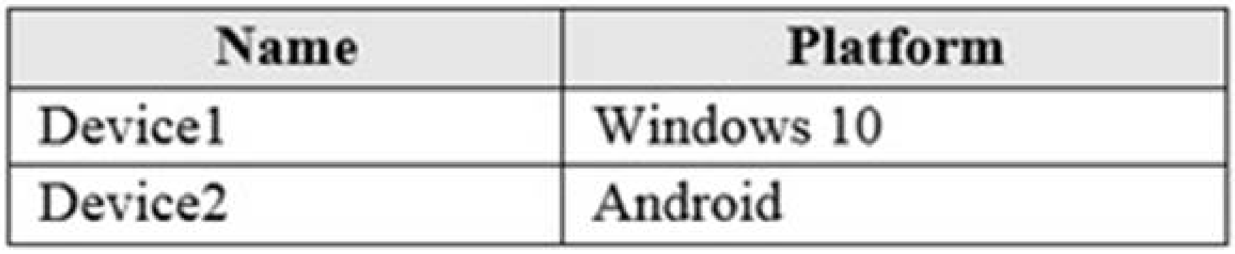
Show custom message when time limit error occurs. Yes [✓ No]

Allow users to collect logs about instalattion errors. Yes [✓ No]

Only show page to devices provisioned by out-of-box experience (OOBE) [✓ Yes] No

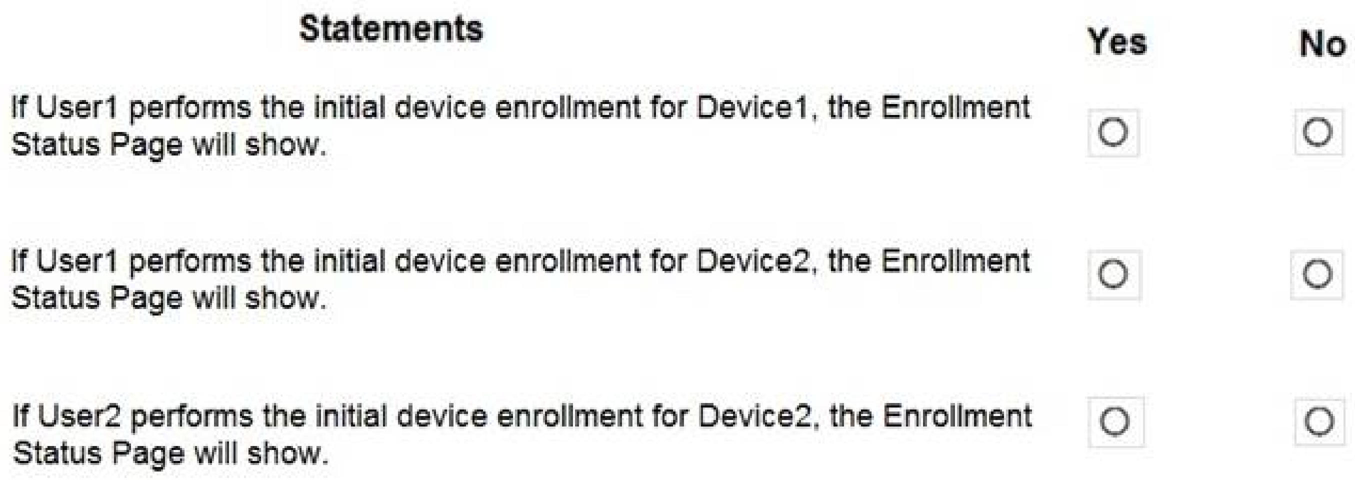
Block device use until all apps and profiles are installed Yes [✓ No]

You assign the policy to Group1.
You purchase the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android

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

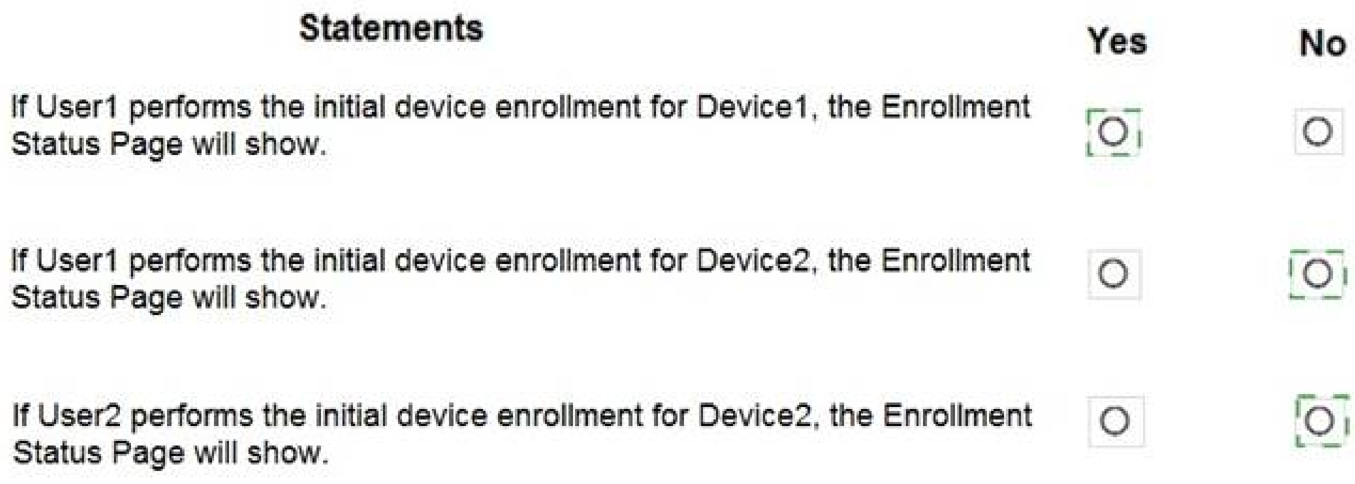


Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	○	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	[✓ ○]	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	[✓ ○]
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	[✓ ○]

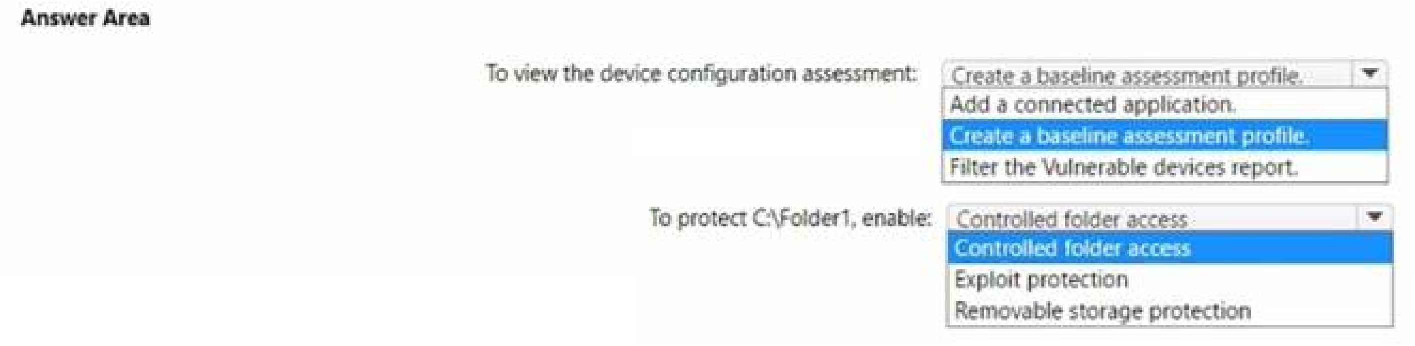
NEW QUESTION 278
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profile?

A. Ubuntu Linux
B. macOS
C. iOS
D. Android

Answer: B

Explanation:
Intune device configuration profiles can be applied to Windows 10 devices and macOS devices
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
? Windows 10
? macOS
Other incorrect answer options you may see on the exam include the following:
? Android Enterprise
? Windows 8.1
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

NEW QUESTION 279
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
All corporate Windows 11 devices are managed by using Microsoft Intune and onboarded to Microsoft Defender for Endpoint.
You need to meet the following requirements:
* View an assessment of the device configurations against the Center for Internet Security (CIS) vl.0.0 benchmark.
• Protect a folder named C:\Folder1 from being accessed by untrusted applications on the devices.
What should you do? To answer, select the appropriate options in the answer area.



Answer Area

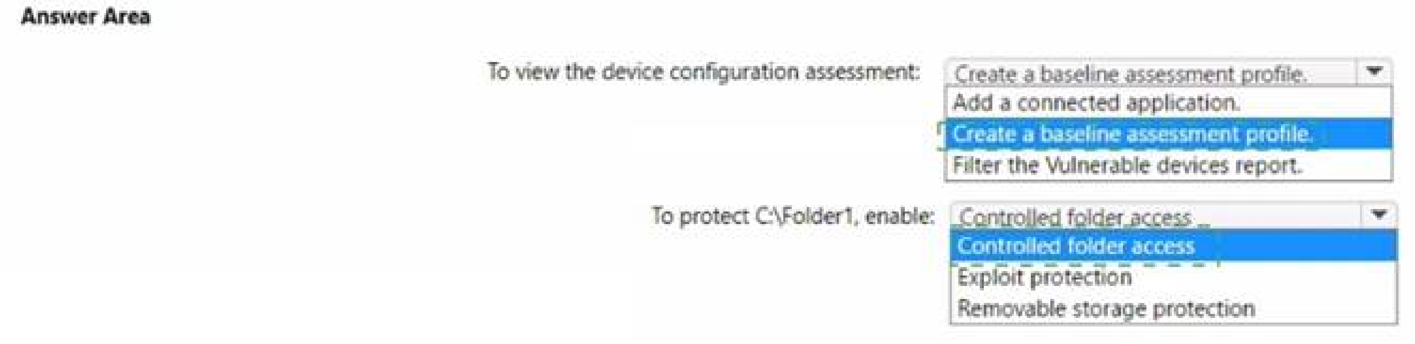
To view the device configuration assessment: Create a baseline assessment profile.
- Add a connected application.
- Create a baseline assessment profile.
- Filter the Vulnerable devices report.

To protect C:\Folder1, enable: Controlled folder access
- Controlled folder access
- Exploit protection
- Removable storage protection

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

To view the device configuration assessment: Create a baseline assessment profile.
- Add a connected application.
- Create a baseline assessment profile.
- Filter the Vulnerable devices report.

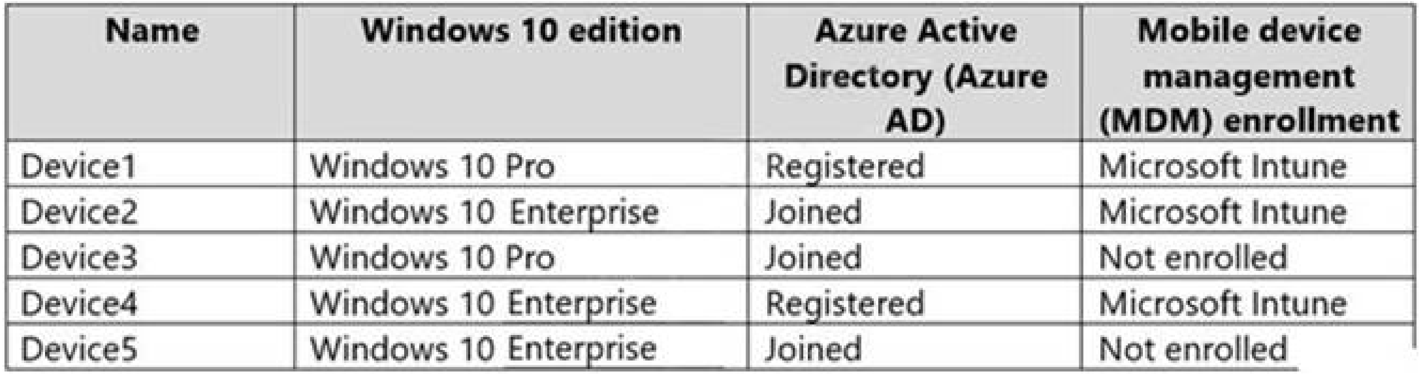
To protect C:\Folder1, enable: Controlled folder access
- Controlled folder access
- Exploit protection
- Removable storage protection

NEW QUESTION 280
- (Topic 6)
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.
Corporate policy states that user passwords must not include the word Contoso. What should you do to implement the corporate policy?

A. From Azure AD Identity Protection, configure a sign-in risk policy.
B. From the Microsoft Entra admin center, create a conditional access policy.
C. From the Microsoft 365 admin center, configure the Password policy settings.
D. From the Microsoft Entra admin center, configure the Password protection settings.

Answer: D

NEW QUESTION 284
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.



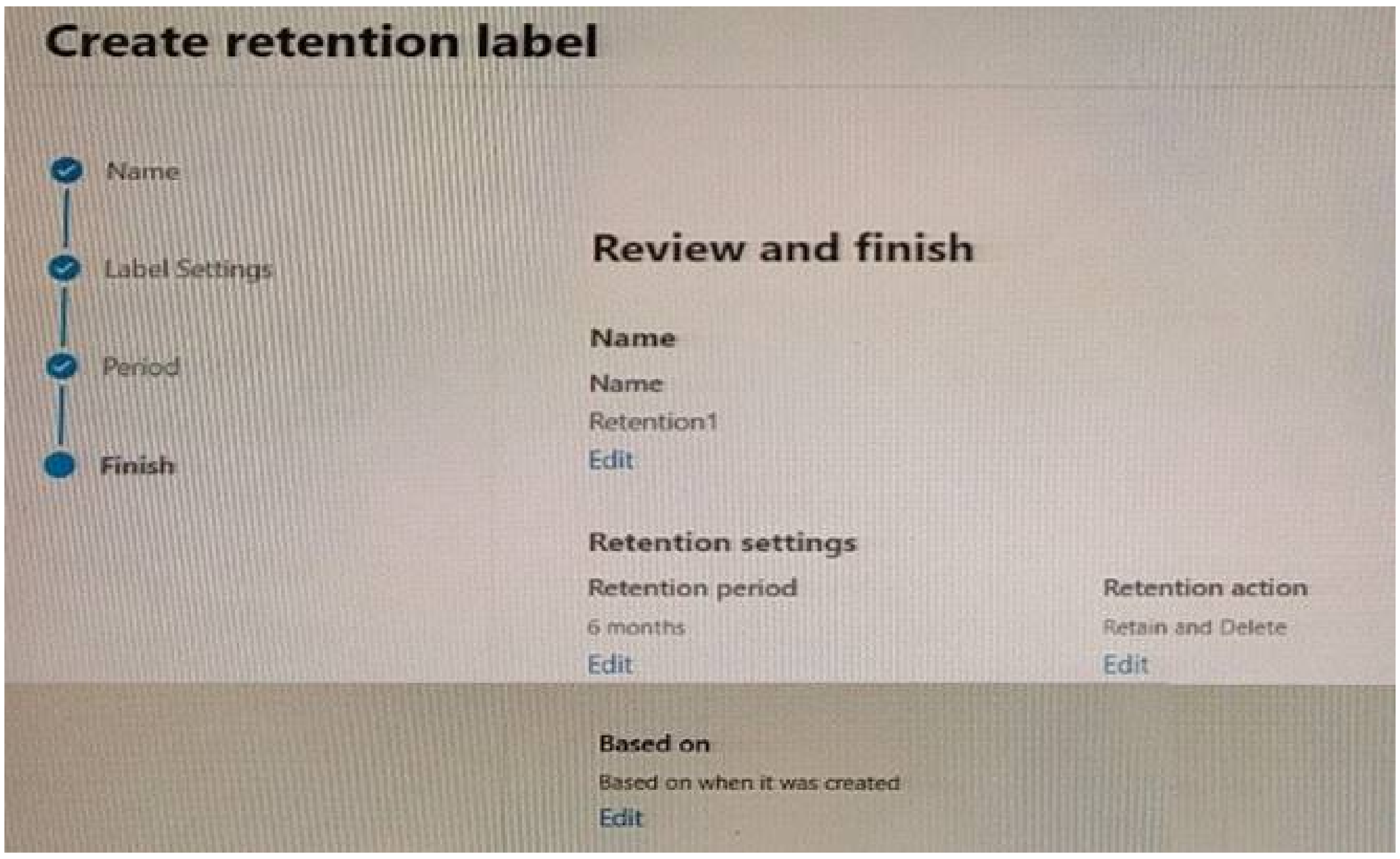
Name	Windows 10 edition	Azure Active Directory (Azure AD)	Mobile device management (MDM) enrollment
Device1	Windows 10 Pro	Registered	Microsoft Intune
Device2	Windows 10 Enterprise	Joined	Microsoft Intune
Device3	Windows 10 Pro	Joined	Not enrolled
Device4	Windows 10 Enterprise	Registered	Microsoft Intune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

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

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

Answer: C

NEW QUESTION 289
- (Topic 6)
You have a Microsoft 365 subscription.
You create a retention label named Retention1 as shown in the following exhibit.



Create retention label

Review and finish

Name

Name
Retention1
Edit

Retention settings

Retention period
6 months
Edit

Retention action
Retain and Delete
Edit

Based on
Based on when it was created
Edit

You apply Retention! to all the Microsoft OneDrive content.
On January 1, 2020, a user stores a file named File1 in OneDrive.
On January 10, 2020, the user modifies File1. On February 1, 2020, the user deletes File1.
When will File1 be removed permanently and unrecoverable from OneDrive?

A. February 1, 2020
B. July 1.2020
C. July 10, 2020
D. August 1, 2020

Answer: B

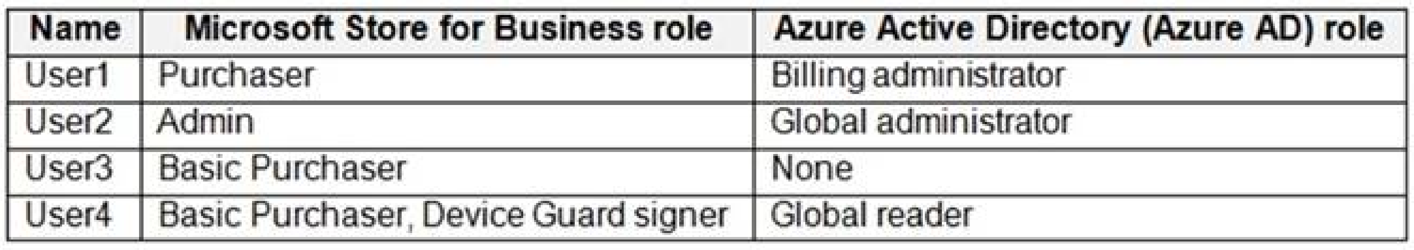
NEW QUESTION 290
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to implement records management and enable users to designate documents as regulatory records.
You need to ensure that the option to mark content as a regulatory record is visible when you create retention labels.
What should you do first?

A. Configure custom detection rules.
B. Create an Exact Data Match (EDM) schema.
C. Run the Sec-RegulacoryComplianceUI cmdlet.
D. Run the Sec-LabelPolicy cmdlet.

Answer: C

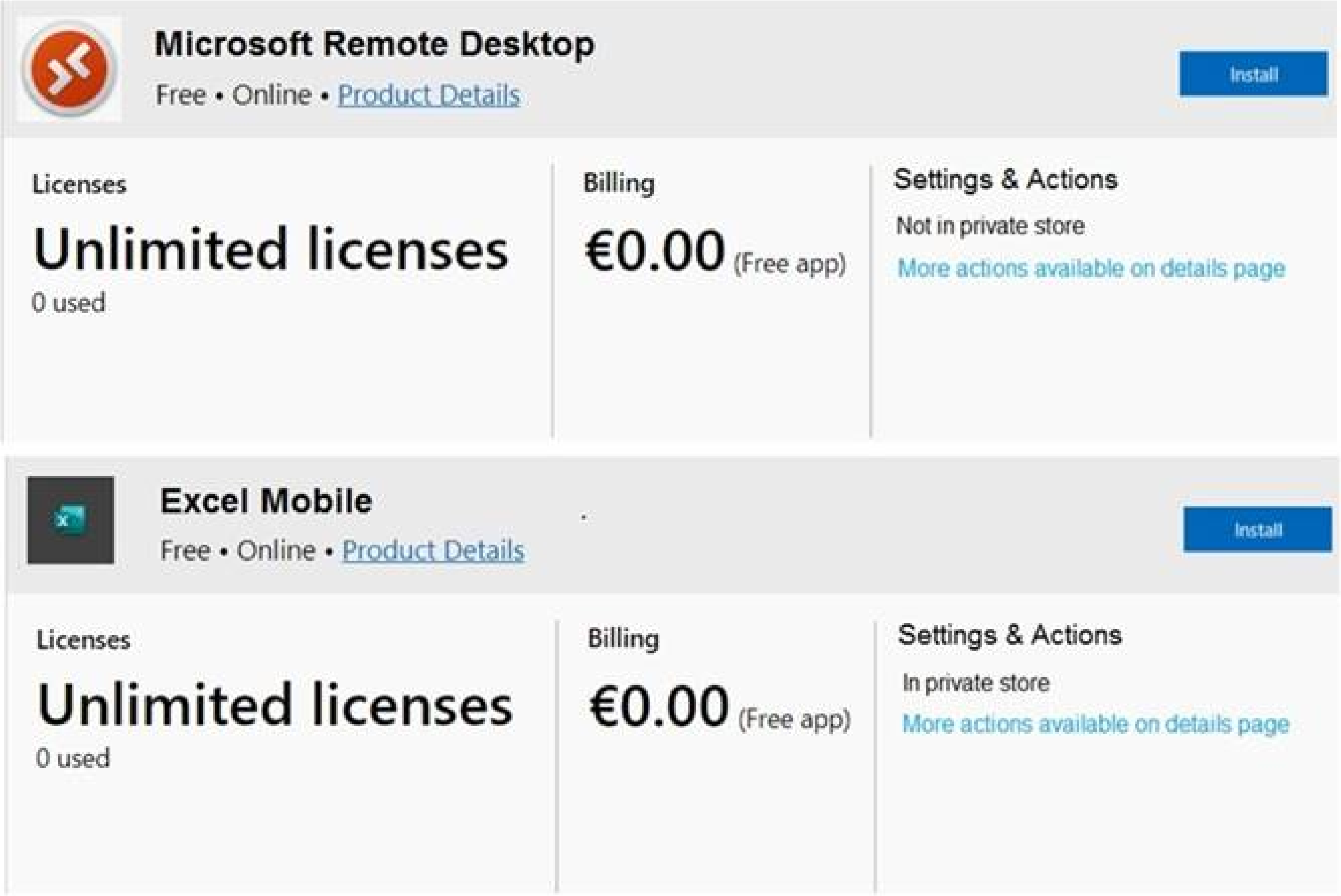
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365- worldwide

NEW QUESTION 292
HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.



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

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



Microsoft Remote Desktop
Free • Online • Product Details

Licenses
Unlimited licenses
0 used

Billing
€0.00 (Free app)

Settings & Actions
Not in private store
More actions available on details page

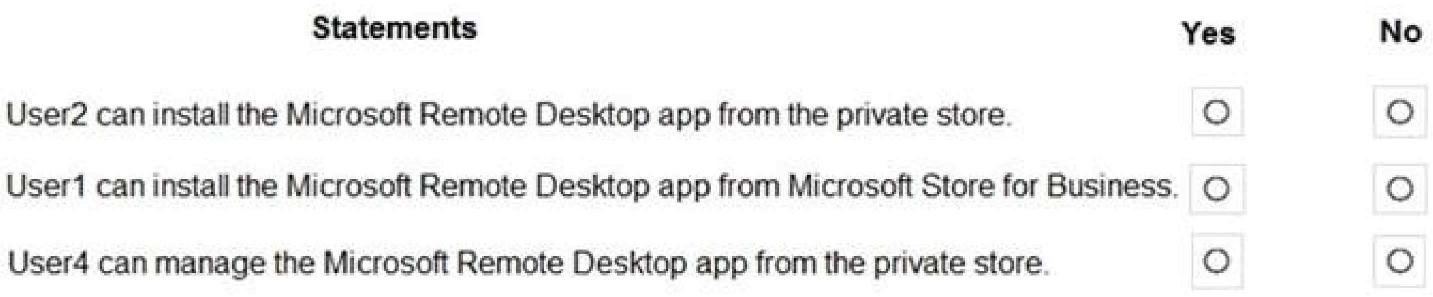
Excel Mobile
Free • Online • Product Details

Licenses
Unlimited licenses
0 used

Billing
€0.00 (Free app)

Settings & Actions
In private store
More actions available on details page

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

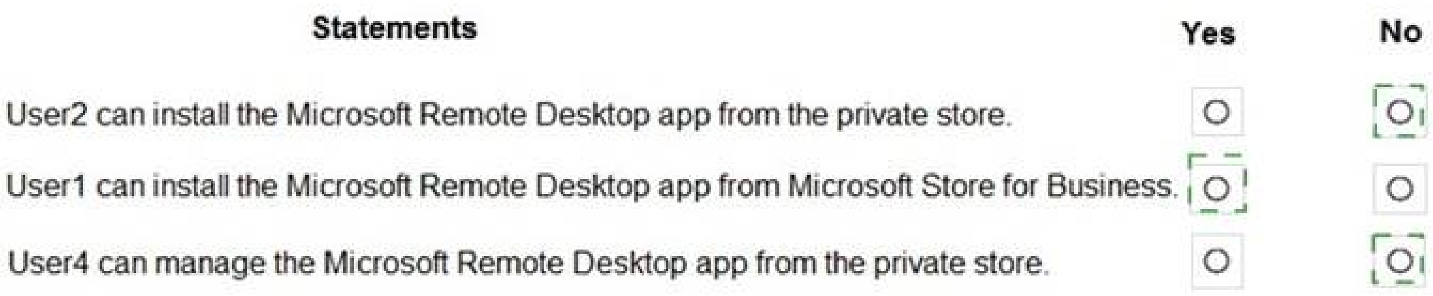


Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	○	○
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	○	○
User4 can manage the Microsoft Remote Desktop app from the private store.	○	○

A. Mastered
B. Not Mastered

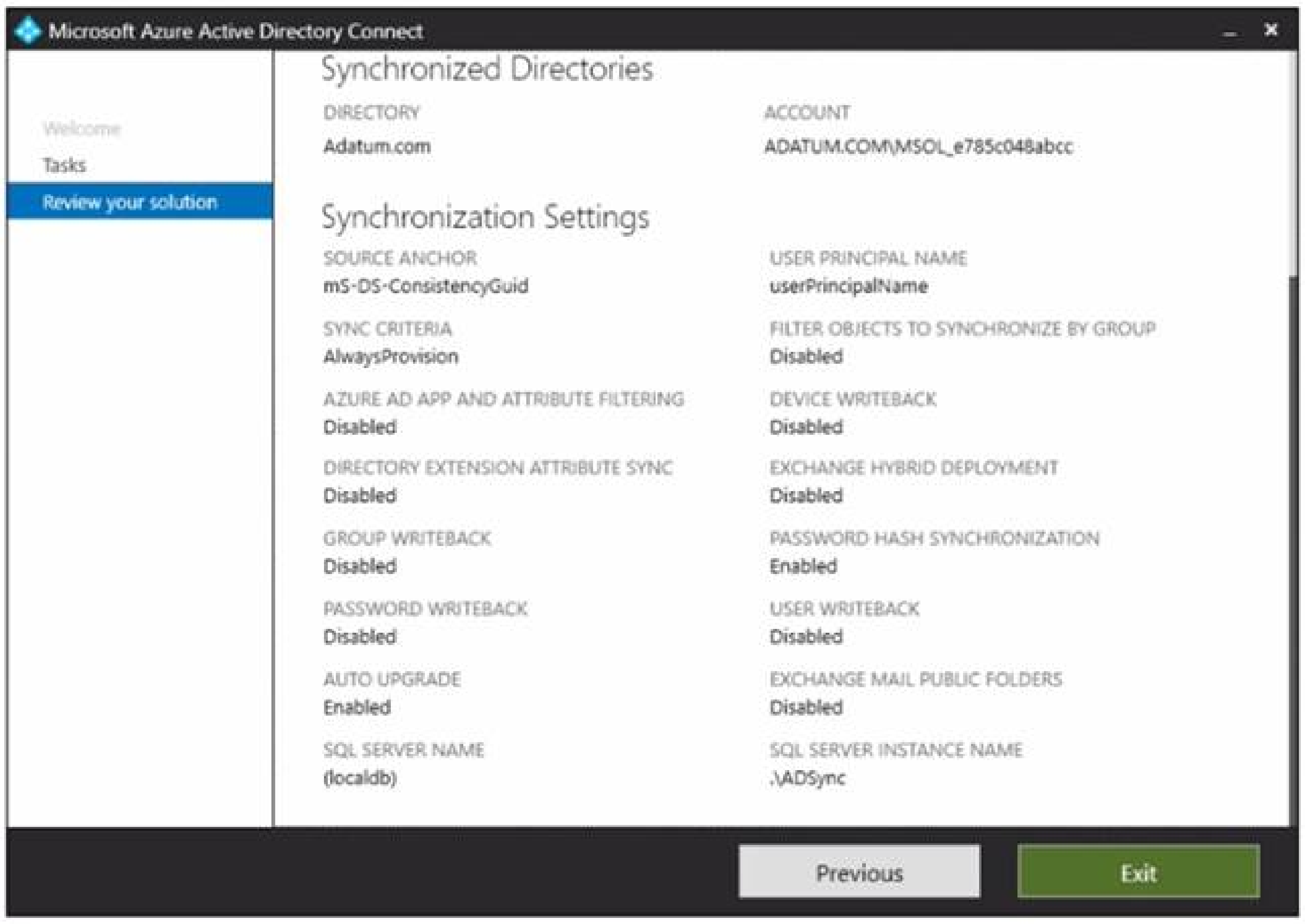
Answer: A

Explanation:



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

NEW QUESTION 295
HOTSPOT - (Topic 6)
Your company has a hybrid deployment of Microsoft 365. An on-premises user named User1 is synced to Azure AD.
Azure AD Connect is configured as shown in the following exhibit



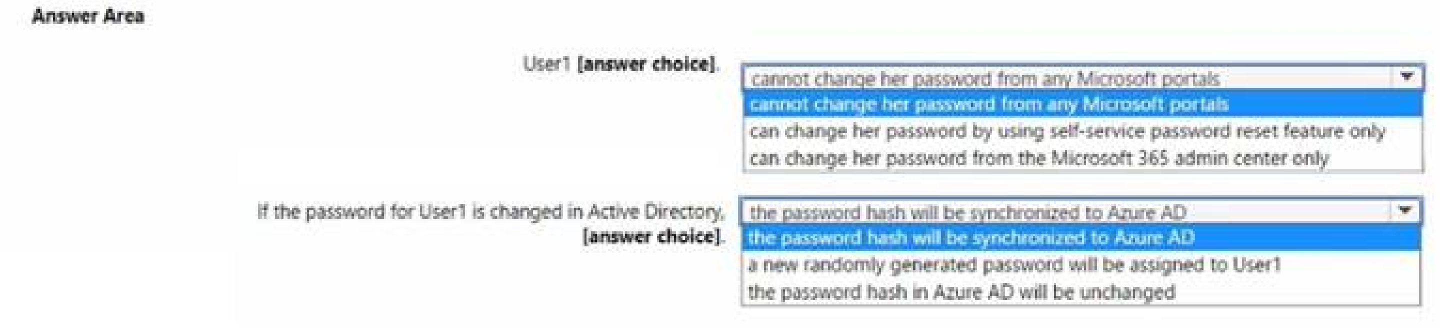
Synchronized Directories

DIRECTORY	ACCOUNT
Adatum.com	ADATUM.COM\MSOL_e785c048abcc

Synchronization Settings

SOURCE ANCHOR mS-DS-ConsistencyGuid	USER PRINCIPAL NAME userPrincipalName
SYNC CRITERIA AlwaysProvision	FILTER OBJECTS TO SYNCHRONIZE BY GROUP Disabled
AZURE AD APP AND ATTRIBUTE FILTERING Disabled	DEVICE WRITEBACK Disabled
DIRECTORY EXTENSION ATTRIBUTE SYNC Disabled	EXCHANGE HYBRID DEPLOYMENT Disabled
GROUP WRITEBACK Disabled	PASSWORD HASH SYNCHRONIZATION Enabled
PASSWORD WRITEBACK Disabled	USER WRITEBACK Disabled
AUTO UPGRADE Enabled	EXCHANGE MAIL PUBLIC FOLDERS Disabled
SQL SERVER NAME (localdb)	SQL SERVER INSTANCE NAME .\ADSync

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

User1 **[answer choice]**.

- cannot change her password from any Microsoft portals
- cannot change her password from any Microsoft portals
- can change her password by using self-service password reset feature only
- can change her password from the Microsoft 365 admin center only

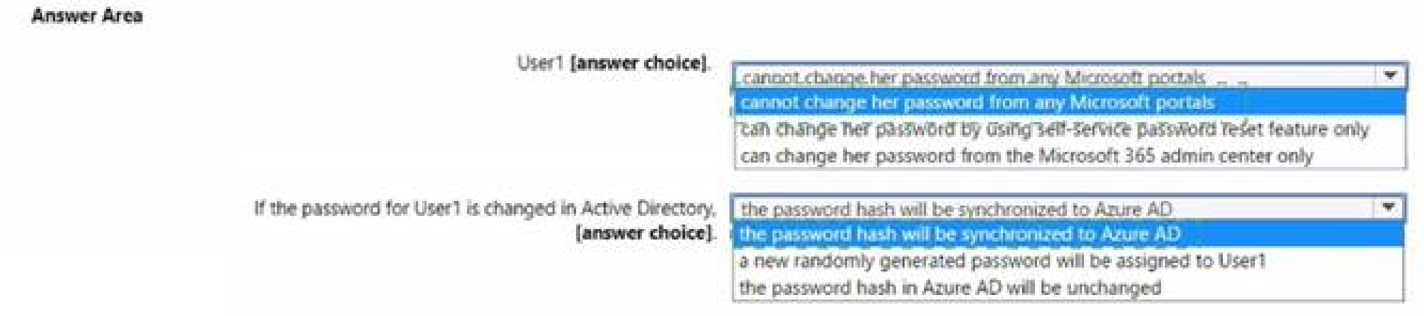
If the password for User1 is changed in Active Directory, **[answer choice]**.

- the password hash will be synchronized to Azure AD
- the password hash will be synchronized to Azure AD
- a new randomly generated password will be assigned to User1
- the password hash in Azure AD will be unchanged

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

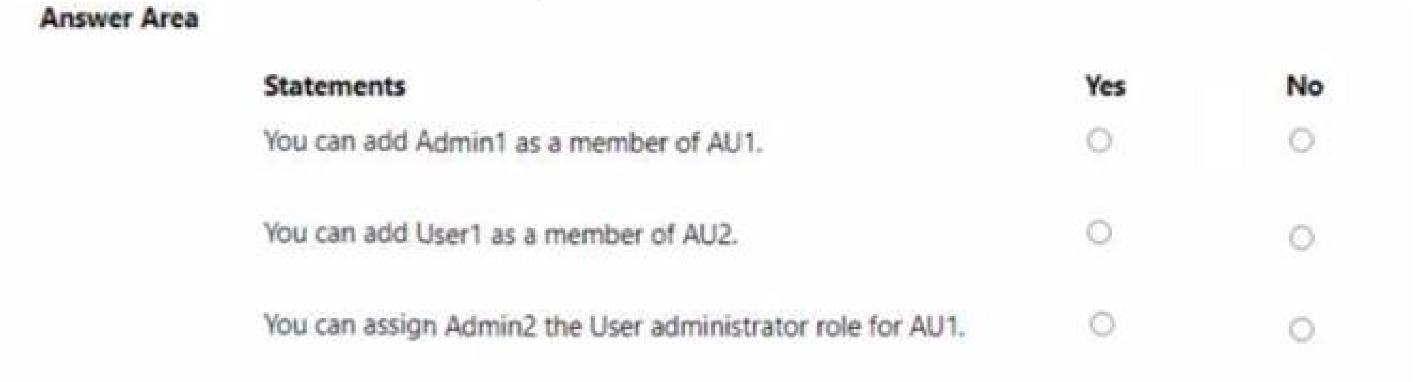
User1 **[answer choice]**.

- cannot change her password from any Microsoft portals
- cannot change her password from any Microsoft portals
- can change her password by using self-service password reset feature only
- can change her password from the Microsoft 365 admin center only

If the password for User1 is changed in Active Directory, **[answer choice]**.

- the password hash will be synchronized to Azure AD
- the password hash will be synchronized to Azure AD
- a new randomly generated password will be assigned to User1
- the password hash in Azure AD will be unchanged

NEW QUESTION 296
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You have an Azure AD tenant named contoso.com that contains the following users:
• Admin1
• Admin2
• User1
Contoso.com contains an administrative unit named AIM that has no role assignments. User1 is a member of AU1. You create an administrative unit named AU2 that does NOT have any members or role assignments. For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



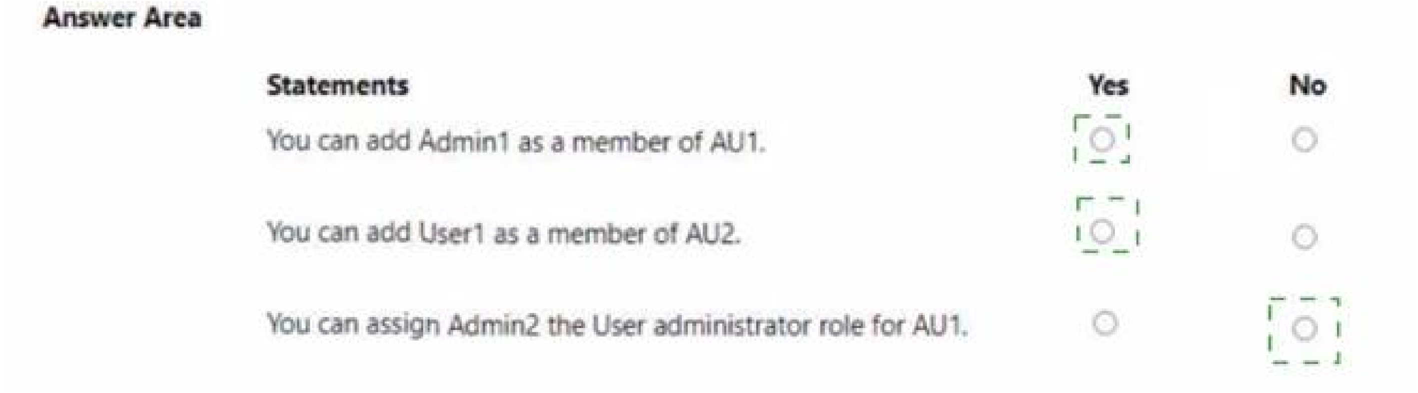
Answer Area

Statements	Yes	No
You can add Admin1 as a member of AU1.	○	○
You can add User1 as a member of AU2.	○	○
You can assign Admin2 the User administrator role for AU1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
You can add Admin1 as a member of AU1.	[✓ ○]	○
You can add User1 as a member of AU2.	[✓ ○]	○
You can assign Admin2 the User administrator role for AU1.	○	[✓ ○]

NEW QUESTION 300

......

Relate Links

100% Pass Your MS-102 Exam with Exambible Prep Materials

https://www.exambible.com/MS-102-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/