Microsoft.MS-102-KR.v2025-03-14.q235

□□□□:	MS-102-KR
□□□□:	Microsoft 365 Administrator (MS-102 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	235
□□:	v2025-03-14
# □□ □:	1162
# □□ □□□:	2350
https://www.krdump.com/Microsoft.MS-102-KR.v2025-03-14.q235.html	

NEW QUESTION: 1

Site1□□□ SharePoint □□□□ □□□ Microsoft 365 E5 □□□ □□□□. Site1□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Number of IP addresses in the file
File1	2
File2	5

□□ □□□ □□□□ □□ □□□□.

Name	Role
User1	Site owners for Site1
User2	Site members for Site1
Admin1	SharePoint admins

□□ DLP □□□□ □□□ □□ □□(DLP) □□□ □□□ Site1□ □□□ □□□□□. DLP □□ □ □□ □□□ □□□ □□ □□□□□.

Edit rule

Conditions

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

Content contains

Default

Any of these

Sensitive info types

IP Address | High confidence | Instance count 3 to Any

Add

Create group

Add condition

Exceptions

Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

Restrict access or encrypt the content in Microsoft 365 locations

Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.

By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

- Block everyone.
- Block only people outside your organization.
- Block only people who were given access to the content through the "Anyone with the link" option.

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□□ □□□ 1□□□□.

Answer:

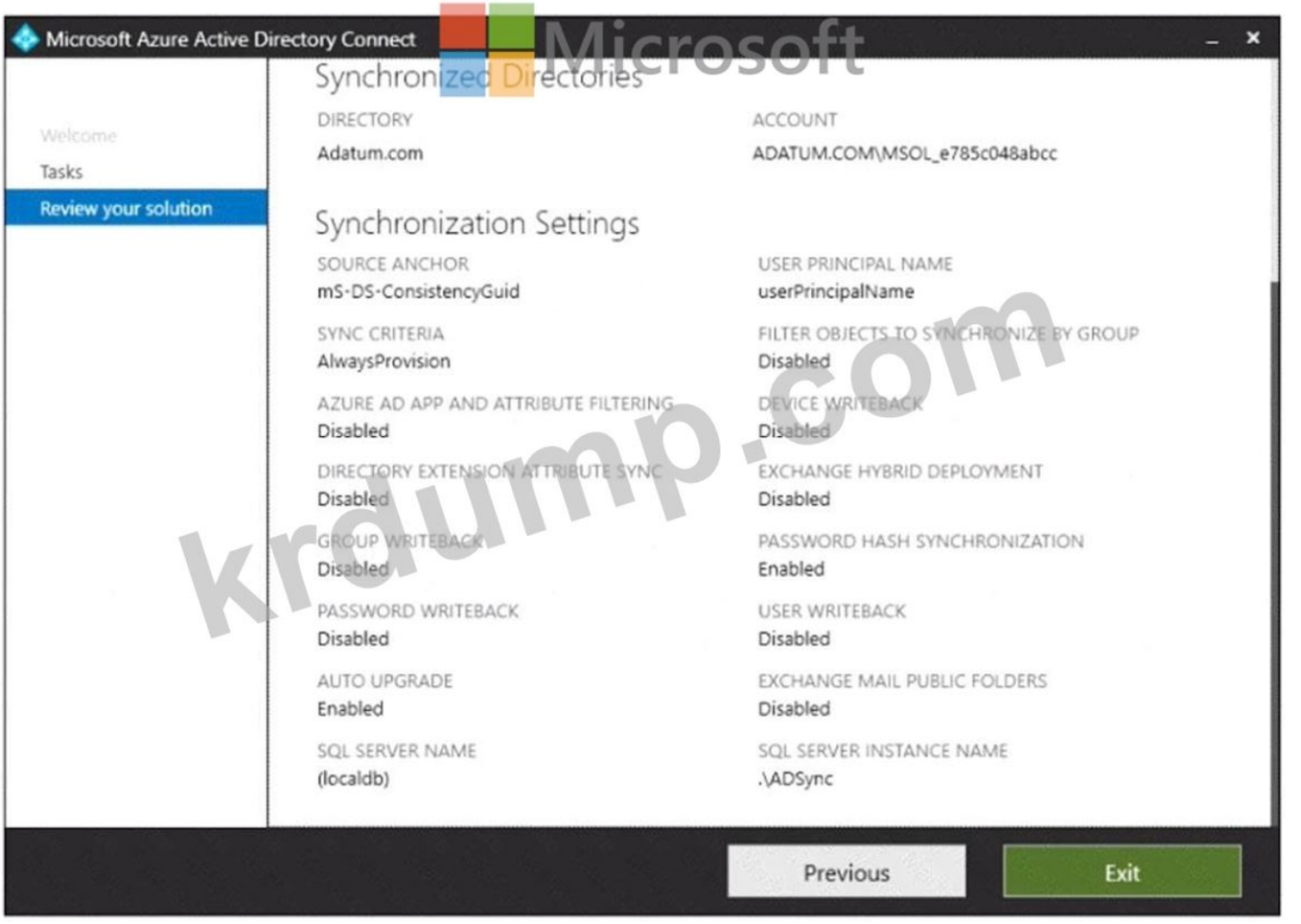
Explanation:
User1 can open File2: NoUser2 can open File1: YesAdmin1 can open File2: Yes User1 can open File2: NoThe DLP policy specifies that if a file contains 3 or more IP addresses, access to that content should be restricted. File2 contains 5 IP addresses, which exceeds the threshold set by the DLP policy. Therefore, User1, who is a site owner, will not be able to access File2 because it matches the conditions set in the DLP rule to block access.
User2 can open File1: YesFile1 contains only 2 IP addresses, which is below the threshold of 3 set by the DLP policy. Since the DLP policy does not apply to files with fewer than 3 IP addresses, User2, who is a site member, can access File1 without any restrictions.
Admin1 can open File2: YesAdmin1 is part of the SharePoint admins group, which typically has elevated privileges. Despite the DLP rule, SharePoint admins are generally not restricted by the same DLP rules that apply to regular users. Therefore, Admin1 can access File2.

NEW QUESTION: 2
Microsoft 365 E5 □□□□ □□□□.
□□□□□ Microsoft Office 365 □□ □□□ □□□□ □□□ □□□□□ □□□ □□□□ □□ □.
□□□ □□□□□ □□□ □□□□ □□□?
A. □□□□ □ □□□ Microsoft Defender
B. Microsoft Apps □□ □□
C. Microsoft Purview □□ □□ □□
D. Microsoft 365 □□ □□

Answer: A (LEAVE A REPLY)

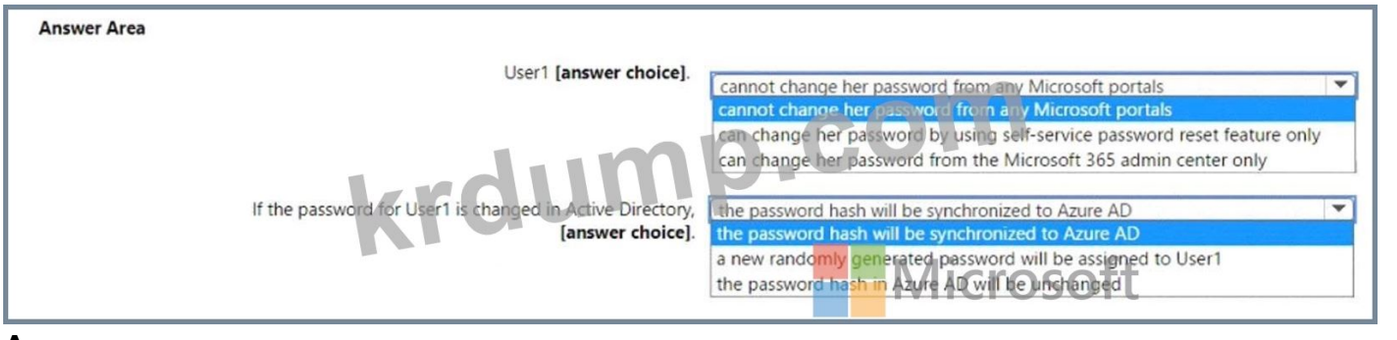
NEW QUESTION: 3
Microsoft 365 E5 □□□ □□□□.
□□□□ User1□□□ □□□ □□□□ □□□□.
□□□□ User1□ □□□□ □□□□□ □□ □□□ □□□□□.
* □□□ IP □□□□ Microsoft Exchange Online□ □□□□□□.
* □□□□ □□□□ Microsoft SharePoint Online□ □□□□□□.
* □□□□ □□□ □□□□ □□ □□□□ □□□ □□□ □□, □□ □□□□ □□□□
SharePoint Online□ □□□□□□. Azure AD Identity Protection□ User1□ □□ □□ □□□ □ □□ □□□ □□□□□?
A. □□ IP □□ □ □□□ □□
B. □□□□ □□ □□□ □□ □ □□□ □□□
C. □□ IP □□□
D. □□ IP □□, □□□ □□ □ □□□□ □□ □□□ □□
E. □□ IP □□ □ □□□□ □□ □□□ □□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
□□□ Microsoft 365□ □□□□□□ □□□□□□.
User1□□□ □-□□□□ □□□□ Azure AD□ □□□□□□.
Azure AD Connect□ □□ □□□ □□ □□□□□.

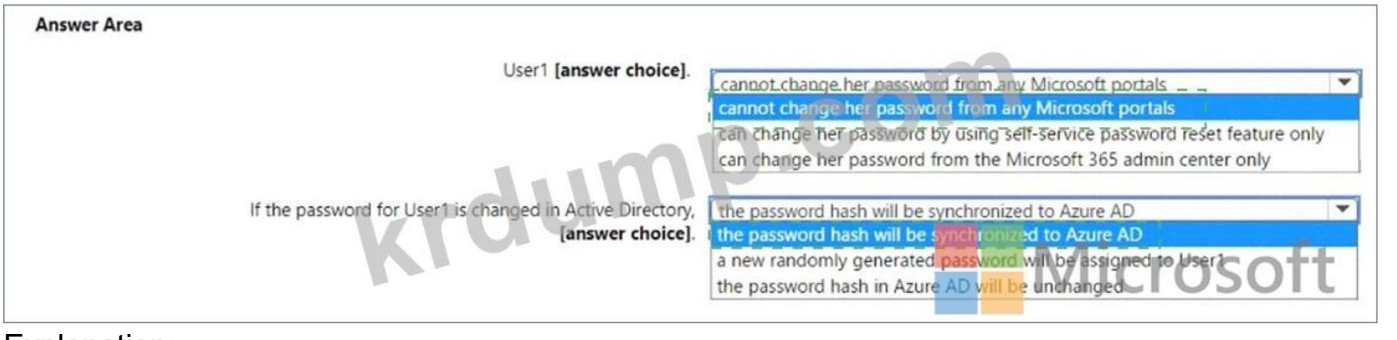


□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Answer Area

NEW QUESTION: 5

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□□ □□□ □ □□ □□ □□□□ □□□ □ □□□, □□ □□□ □□ □□ □ □□□□ □□□□.

□□□□□ Active Directory □□□□ □□□□ □□□□.

Azure AD □□□□ □□□□□.

□□ □□□□ □□□□ Azure AD□ □□□□□□ □□□□□.

□□ □□(OU)□ 10□ □□□ □□□ Azure AD□ □□□□□ □□ □□ □□□□□□. □□ □□ □□□ □□□ □□□□□ □□□□□□□□.

Azure AD Connect Health□ □□□□ □□ □□□ □□ □□□□ □□□□□ □□□□□□ □□ □□□.

10□□ □□□ □□□ Azure AD□ □□□□□□□ □□□□ □□□.

□□ □□: Azure AD Connect□□ □□□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: (SHOW ANSWER)

NEW QUESTION: 6

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.

Microsoft 365 □□□ □□□□.

Microsoft 365 Defender□□ eDiscovery Manager □□ □□□ □□□□ US eDiscovery Managers□□ □□ □□□ □□□□.

□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□□□ □□□ □□□ □□□ □ □□ □ □□ □□□.

□□ □□: Microsoft 365 Defender□□ □□ eDiscovery □□□ □□ □□□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: A (LEAVE A REPLY)

NEW QUESTION: 7

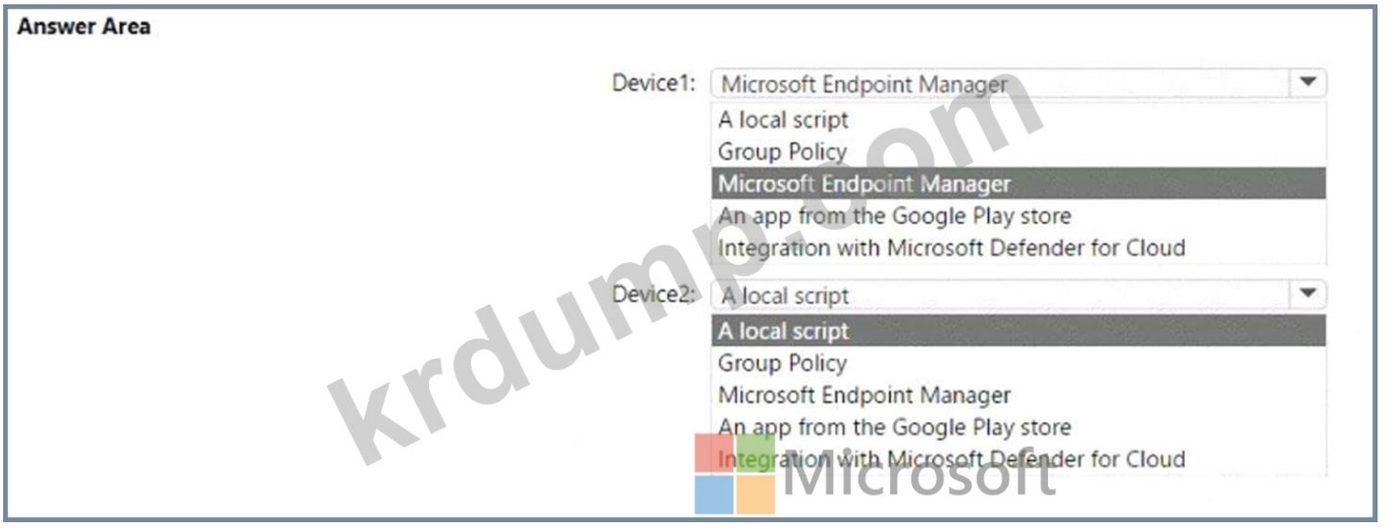
Microsoft Intune□ □□□□ □□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

Device1□ Device2□ Microsoft Defender for Endpoint□ □□□□□ □□□.

□ □□□ □□□□□ □ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□.

□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

NEW QUESTION: 8
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
□□□□□ Active Directory □□□□ □□□□ □□□□.
Azure AD □□□□ □□□□□.
□□ □□□□ □□□□ Azure AD□ □□□□□□ □□□□□.
□□ □□(OU)□ 10□ □□□ □□□ Azure AD□ □□□□□ □□ □□ □□□□□□. □□ □□ □□□ □□□ □□□□□ □□□□□□□□.
Azure AD Connect Health□ □□□□ □□ □□□ □□ □□□□ □□□□□ □□□□□□ □□ □□□.
10□□ □□□ □□□ Azure AD□ □□□□□□□ □□□□ □□□.
□□□: idfix.exe□ □□□□ 10□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
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: 9
□□: □ □□□□ □□□ □□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□ □ □□□ □□□.
□□□ □□ □ □ □□□ □□□□ □□□ □□□ □ □□□□. □□□ □□ □□□ □ □□ □□ □□□ □□□□ □□ □□ □□□□.
□ □□□ □□□ □□ □□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft 365 E5 □□□ □□ Office 365□ Microsoft Defender□ □□□□ □□□□.
□□, □□, □□□□□□ □□□□ □□ □□ □□ □□ □□ □□□□ □□□□ □□ □□□ □□ □□ □□□.
□□□: □□□ □□ □□□ □□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

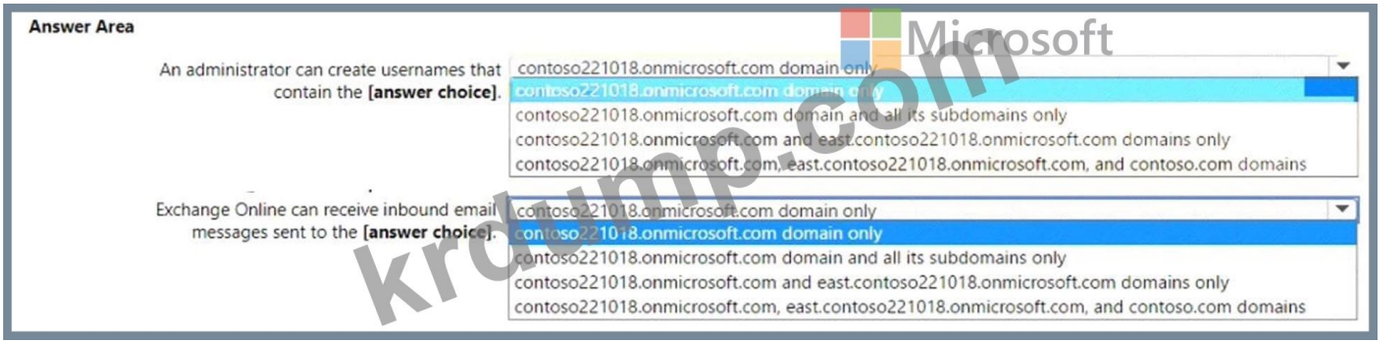
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10

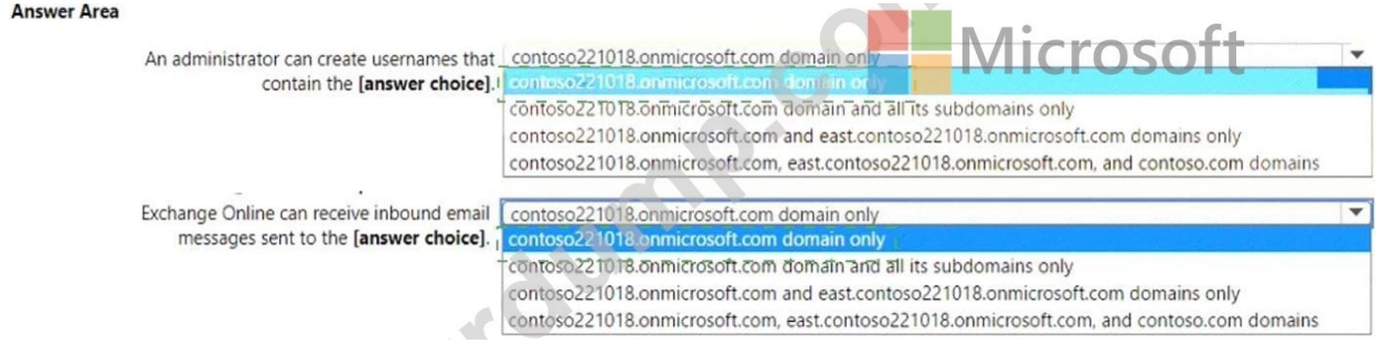
□□□ □□ □□□ □□□ □□□□ □□□□ Microsoft 365 □□□ □□ □□□□.

□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 11

Microsoft 365 E5 □□□□ □□□□.

□□□ □□□□ □□□□□.

□□□□□ □□ Microsoft Word□□ □□□ □□□ □□□ □ □□□ □□□□□. □□□ □□□ Microsoft 365□ Word□□ □□□ □ □□□□.

□□□□ □□ Word□ □□□ □ □□□ □□□□ □□□ □ □□□ □□□□ □□□.

□□□ □□ □□□?

A. Microsoft SharePoint Online □ OneDrive□ □□□ □□ □□□ □□□□ □□□□□□.

B. Azure Information Protection□□ Microsoft 365 Compliance Center□ □□ □□

C. □□□ □□□ □□□□□.

D. □□ □□□ □□ □□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 12

AU1□ AU2□□ □ □□ □□ □□□ □□□ Microsoft 365 □□□ □□□□.

□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Administrative unit	Role	Scope
User1	*None*	User Administrator	AU1
User2	AU1	Global Administrator	*None*
User3	*None*	*None*	Organization

□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Members	Administrative unit
Group1	User3	AU2
Group2	User2 User3	AU1

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 13

Microsoft 36S E5 □□□ □□□□.

□□ □□ □□□ □□ Microsoft Defender for Endpoint□ □□□ □□□□□ □□□□.

Name	Platform
Device1	Windows 11
Computer2	Windows 11
Device3	Android

□□ □□ □□□ □□ □□□ □□□□.

Rank	Name	Matching rule
1	Group1	Name Starts with Dev
2	Group2	OS In Windows 11
Last	Ungrouped devices (default)	*Not applicable*

IP □□ □□□□ □□ □□ □□ □□□□□.

IP address	Action	Scope
131.107.10.50	Block	Group2
20.30.40.50	Block	Group1
2.23.10.15	Block	UnassignedGroup

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□: □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 14

Microsoft 365 E5 □□□ □□□□. □□ □□ □□ □□□□ □□□□ □□□. □□ □□□ □□□ □ □□□?

A. Exchange □□ □□

B. Microsoft Purview □□ □□ □□

C. Intune □□ □□

D. Microsoft Entra □□ □□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 15

Microsoft 365 □□□□ □□□□.

Microsoft Intune□ □□□□ □□ Windows 10 □□□□□ □□ BitLocker □□□ □□□ (BitLocker)□ □□□□ □□□□ □□□□□.

□□□ □□□□ □□□?

A. □□ □□ □□(ASR) □□

B. □ □□ □□

C. □□ □□ □□

D. □□ □□ □□□

Answer: D (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

NEW QUESTION: 16

contoso.com□□□ Azure AD □□□□ □□□ Microsoft 365 □□□ □□□□. □□□□□ □□ □□ □□□ □□□□ □□□□□.

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

Policy1□□□ □□□ □□ □□(DLP) □□□ □□□ □□□□□. Policy1□ □□ □□ □□(PII)□ □□□ □□□ □□ □□□ □□□□□ □□□□ □□□□ □□ □□□□□ □□□□ □□□□.
User!□ □□ □□□□□ PII□ □□□ □□□ □□ □ □□□?

A. □□□2□□

B. User2, User3, User4, User5

C. User2, User3, User4□

D. User2□ User3□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 17

□□□ □□□□ Microsoft E5 □□□□ □□□□.
□□□ ISO/IEC 27001:2013 □□□ □□ □□□ □□□□ □□□.
□□□ □□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□?

A. □□ □□ □□

B. □□ □□□□

C. □□□□□□ □□□

D. □□□ □□ □□(DSR)

Answer: C (LEAVE A REPLY)

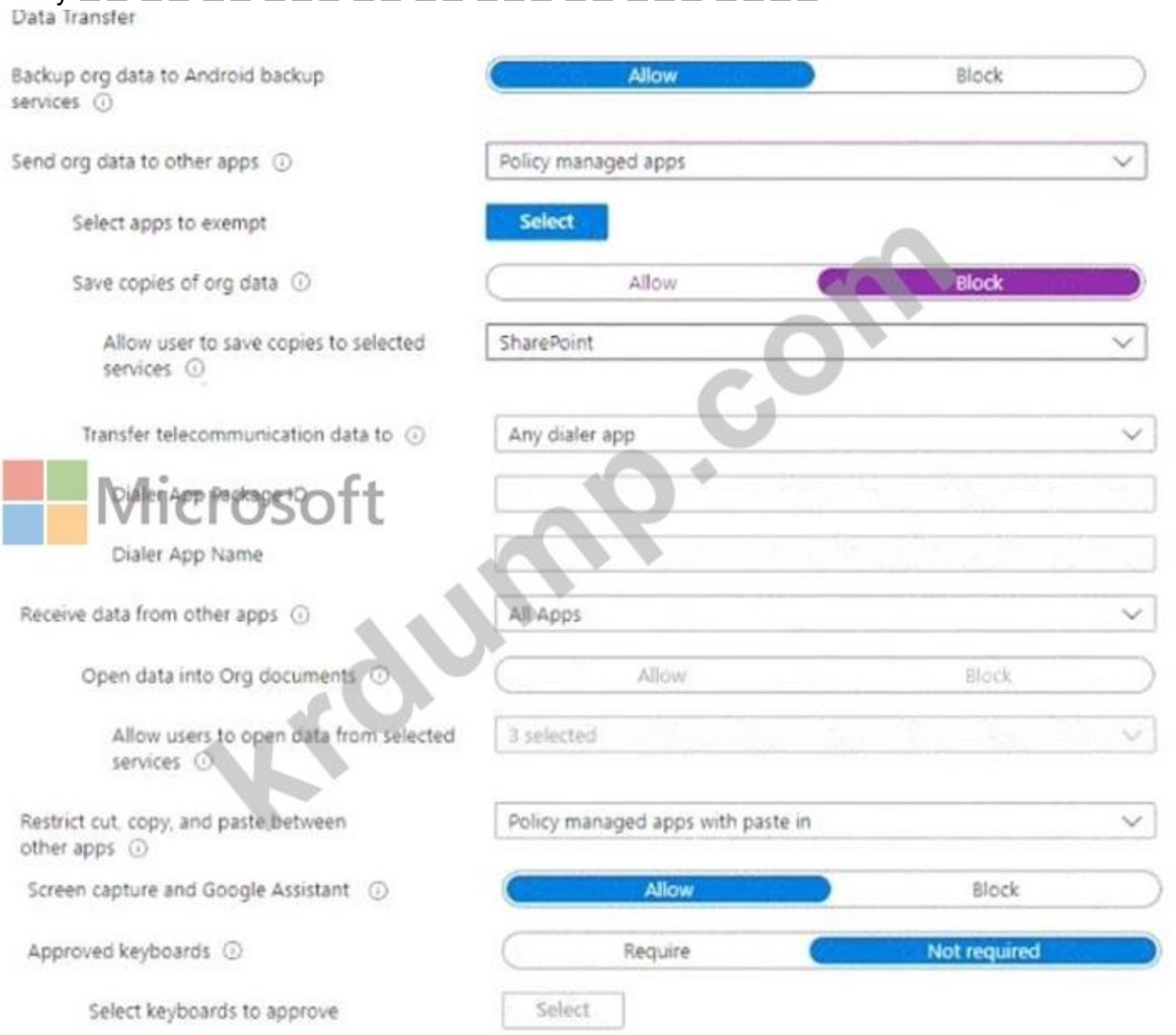
Reference:
https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

NEW QUESTION: 18

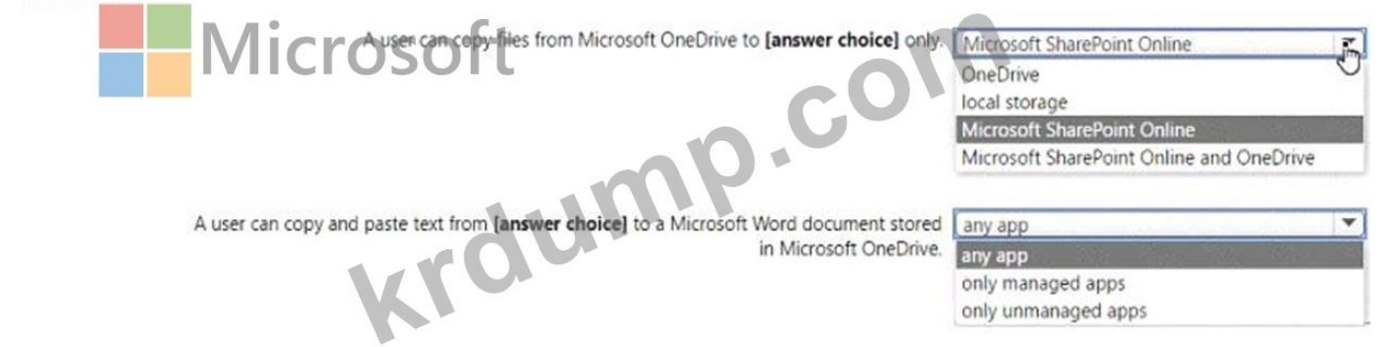
Microsoft Intune□ □□□ Android □□ 200□□ □□□ Microsoft 365 E5 □□□ □□□□.

□□ Microsoft □□ □□□□ □□ □□ □□□□□ □□□□ Policy!□□ □□□ Android □ □□ □□□ □□□□.

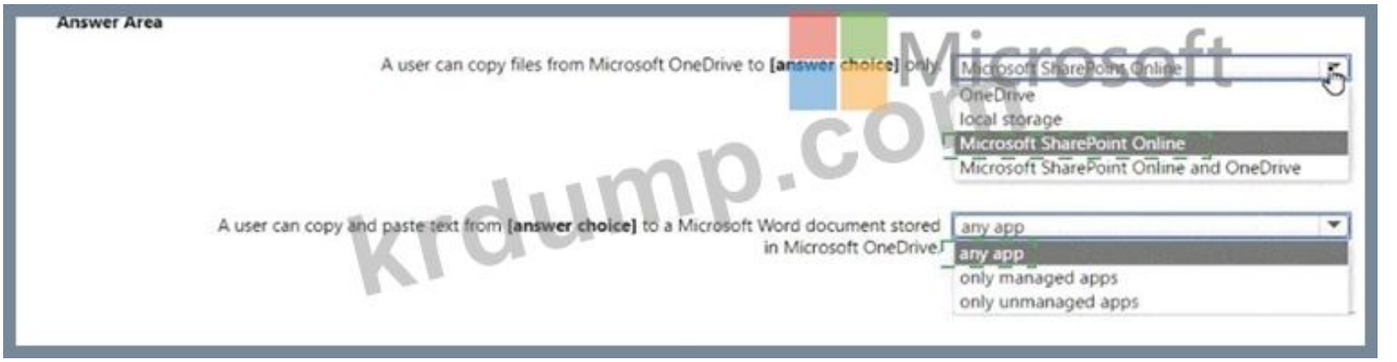
Policy!□□ □□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□.



□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□ □ □□□□ □□□□ □□ □□□□ □□□□□.



Answer:



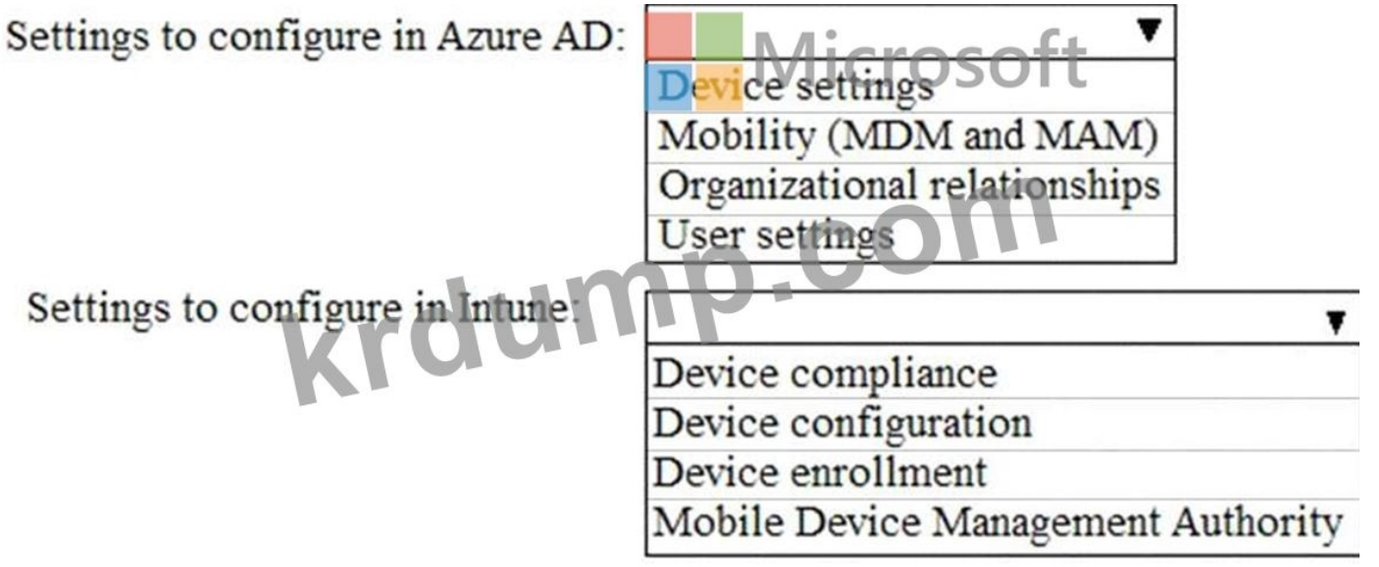
Explanation:

NEW QUESTION: 19

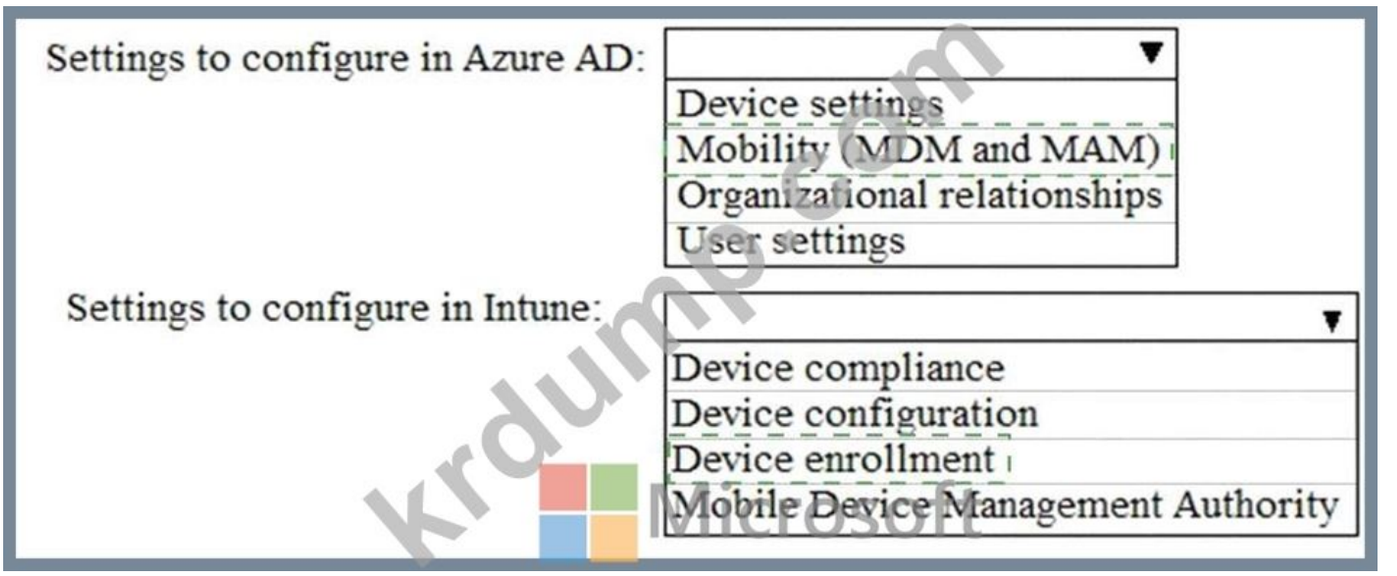
Windows 10 □□□ □□ Intune □□ □□□ □□□□ □□□.

□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

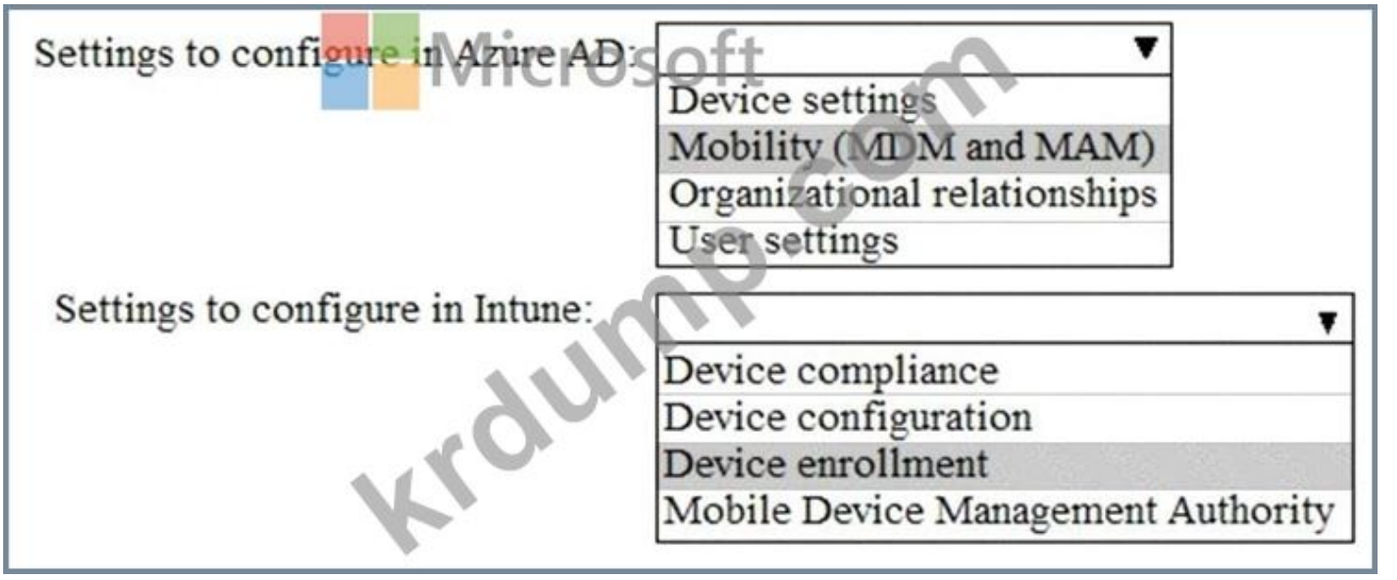
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



References:

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

NEW QUESTION: 20

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 □□□ □□□□.

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

□□ □□□ □□□ □□□ □□ □□□□.

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

□□ □□□ □□ □□□ □□□ □□□ □□□□.

* □□□ □□ □□ ID:

o □□: □□ 1

o □□: □□2

* □□□□ □ □□ □□: □□ □□□□ □□ □□□□□.

* □□ :

o □□: □□ □□

o □□ □□: □□□□

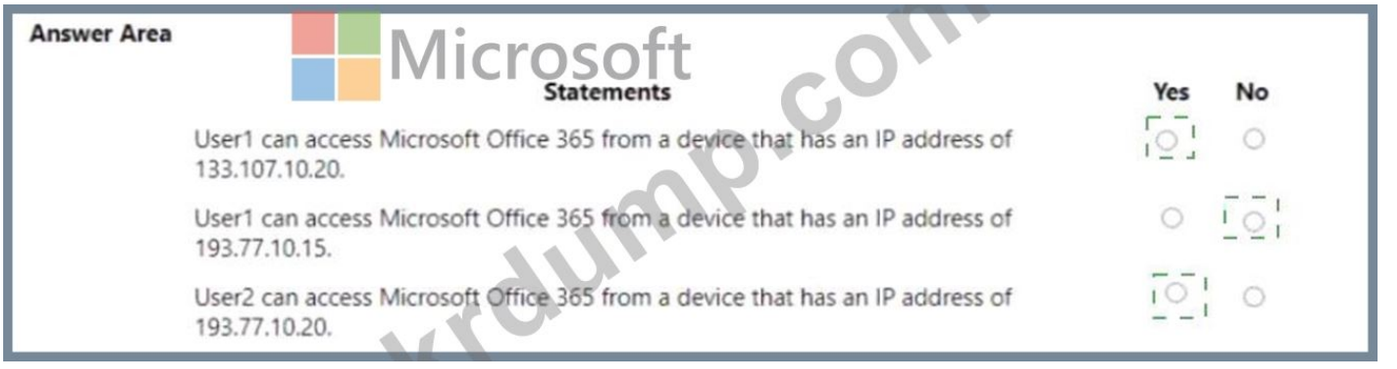
* □□ □□: □□ □□, □□ □□ □□ □□

User1□ □□ □□ □□(MFA) □□ □□□ □□□ □□□□.

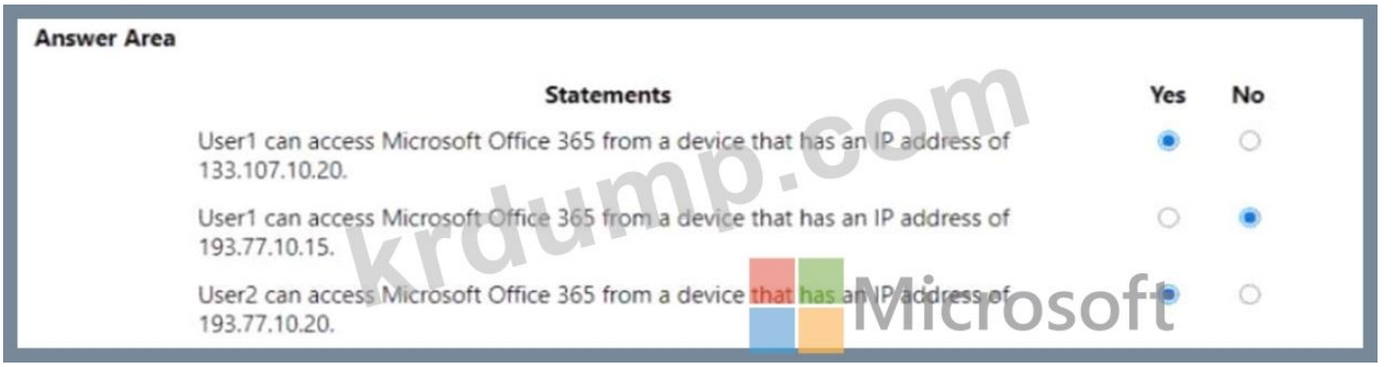
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:



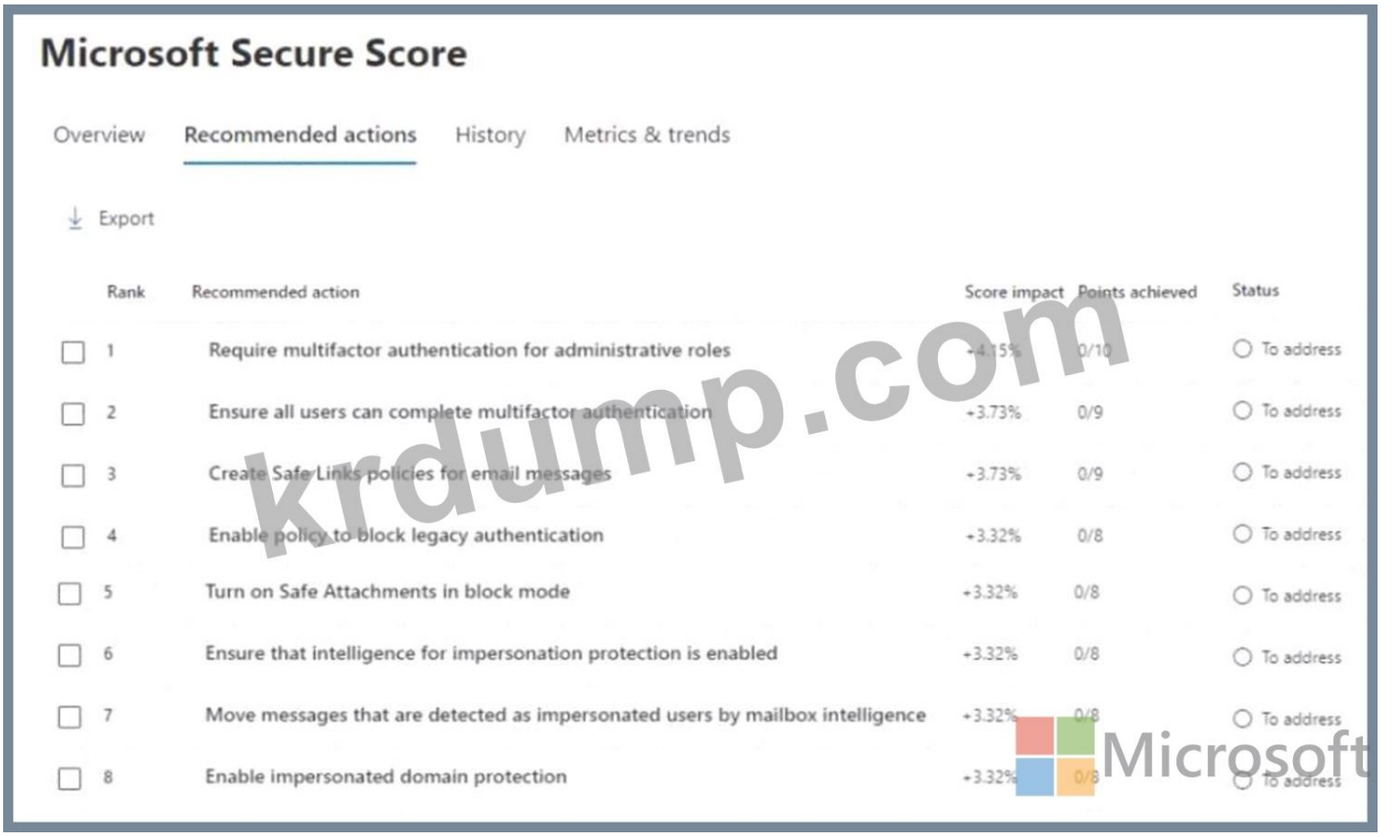
Explanation:



NEW QUESTION: 21

Microsoft 365 E5 □□□ □□□□.

□□□ Microsoft Secure Score□□□ □□ □□ □□□ □□□ □□□□□.



□□□ □□□□ □□ □□□ □□ □□ □□□□ □□□□ □□ □ □□ □□ □□□□ □□□ □ □ □□□□ □□□□□.

□ □□ □□□ Secure Score□ □□ □□□ □□□□?

A. 9□□□ □□□□□.

B. 9□□□ □□

C. 1□□□ □□□□□

D. □□□□ □□□□□

E. 1□□□ □□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 22

□□ □□ □□□ □□ Microsoft Intune□ □□□ 4□□ □□□ □□ Microsoft 365 E5 □□□□ □ □□□.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

Microsoft Endpoint Manager□ □□□□ □□□□□□□ Microsoft 365 □□ □□□ □□□□□.
□□ □□□ □□□□□□□ Microsoft 365 □□ □□□ □ □□□?
A. Device1□
B. Device1□ Device3□
C. Device2□ Device4□
D. Device1, Device2, Device3□
E. Device1, Device2, Device3, Device4
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

NEW QUESTION: 23
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□ □□ Microsoft Purview □□□ □□□ □□□□□.
□□ □□ □□(PII)□ □□□ Microsoft Teams □ SharePoint□ □□□ □□□ □□□□□.
PII□ □□□ □□ □□□ □□ □□□□□.
□□□ □□□□ □□□?
A. □□□ □□ □□(DLP) □□
B. □□ □□
C. □□ □□
D. □□□□ □□ Microsoft Defender □□
Answer: A (LEAVE A REPLY)
Demonstrate data protection
Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities.
With DLP policies, you can automatically protect sensitive information across Microsoft 365.
There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.
In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.
* From the Security & Compliance tab of your browser, click Home.
* Click Data loss prevention > Policy.
* Click + Create a policy.
* In Start with a template or create a custom policy, click Custom > Custom policy > Next.
* In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b. Description: Protect the personally identifiable information of European citizens
* Etc.
Reference:

https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365- dev-test-environment

NEW QUESTION: 24
Microsoft 365 □□□ □□□□.
□□ □□ □□□ □□ □□□□.

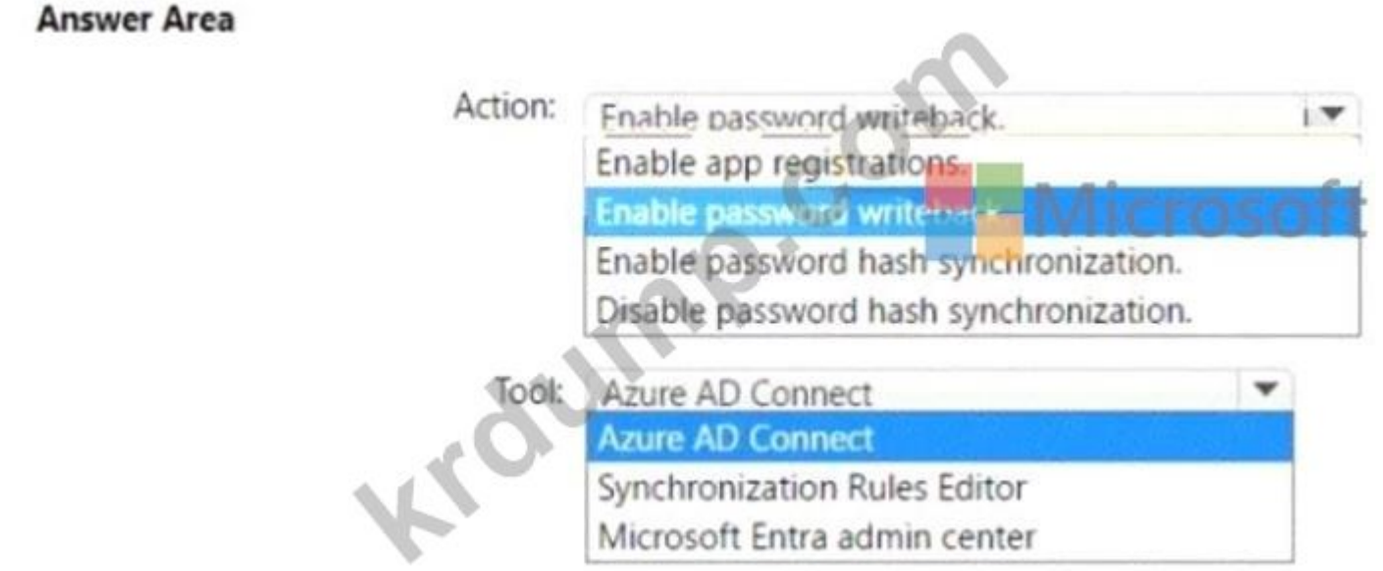
Name	TPM version	Operating system	BIOS/UEFI	BitLocker Drive Encryption (BitLocker)
Device1	TPM 1.2	Windows 10 Pro	BIOS	Enabled
Device2	TPM 2	Windows 10 Home	BIOS	**Not applicable**
Device3	TPM 2	Windows 8.1 Pro	UEFI	Enabled

□□□ Azure Active Directory(Azure AD)□ □□□□□ □□□.
Azure AU □□□ □□□□ □□ □ □□□□□□ □□□ □□ □□□? □□□□□ □□□ □□□ □□ □□□□□ □□□ □□□□. □ □□□ □ □, □□ □, □□ □□ □□□ □ □□□□. □ □ □□ □□ □□□ □□□ □□□ □□□□□ □□□□ □□□□ □ □□ □□□□.
□□□□: □□ □□□ 1□□□□.

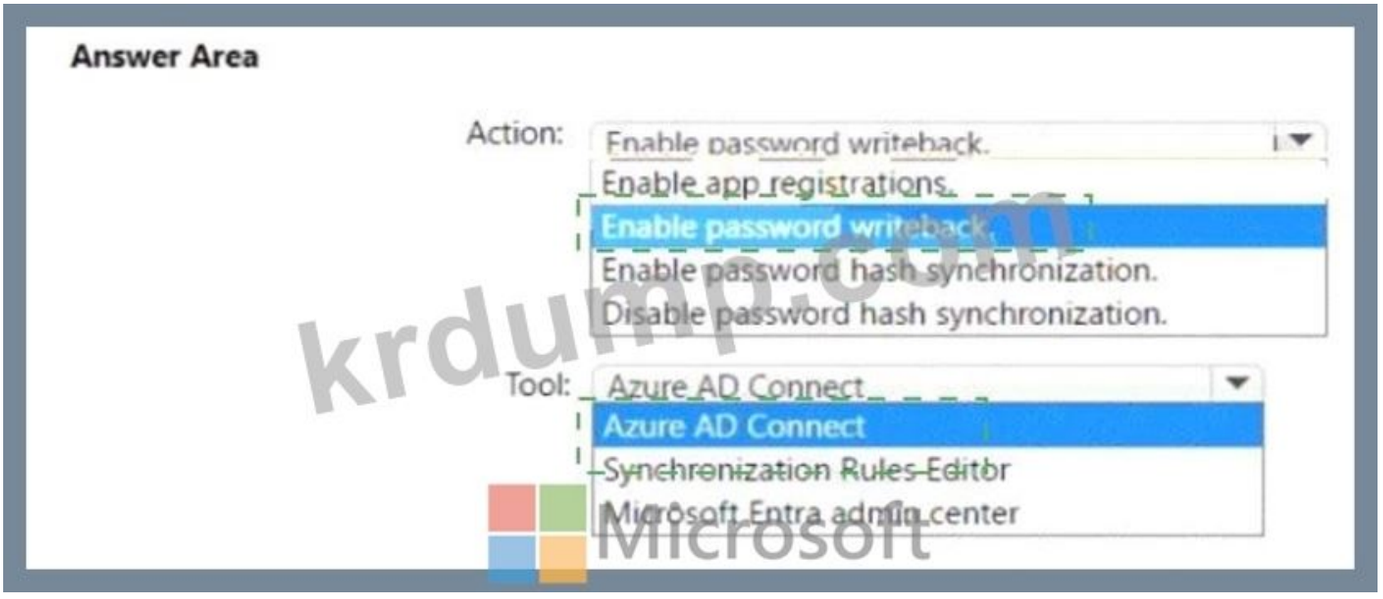
Answer:

Explanation:

NEW QUESTION: 25
Admin4□ SSPR□ □□□ □ □□□ □□□□ □□□.
□□ □□□ □□□□ □□□? □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



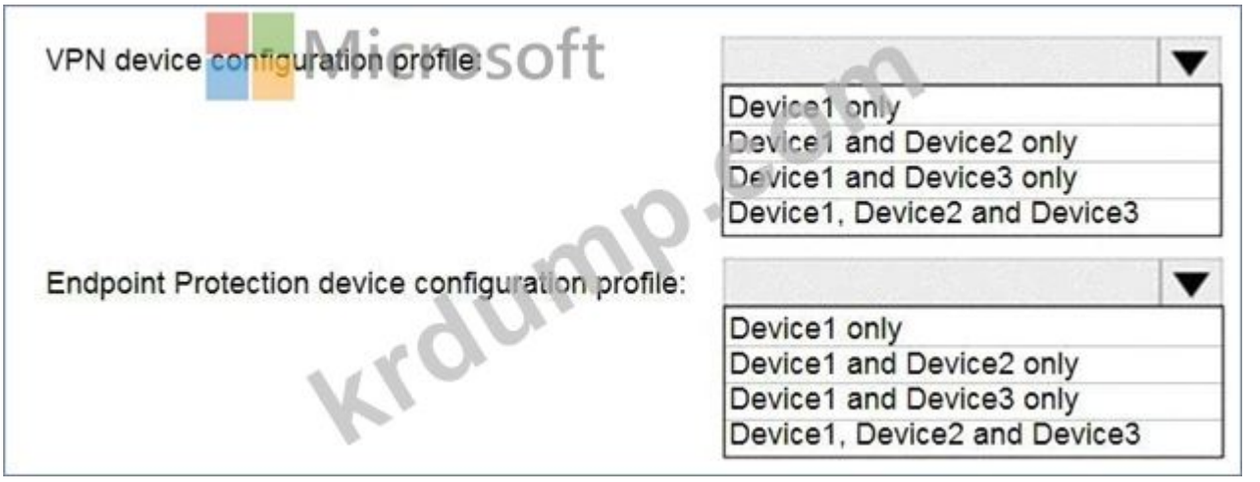
Explanation:

NEW QUESTION: 26

Microsoft Intune□ □□□ □□□□□ □□□□ Microsoft 365 □□□□ □□□□. □□□□□ □ □ □□ □□□ □□ □□□□□.

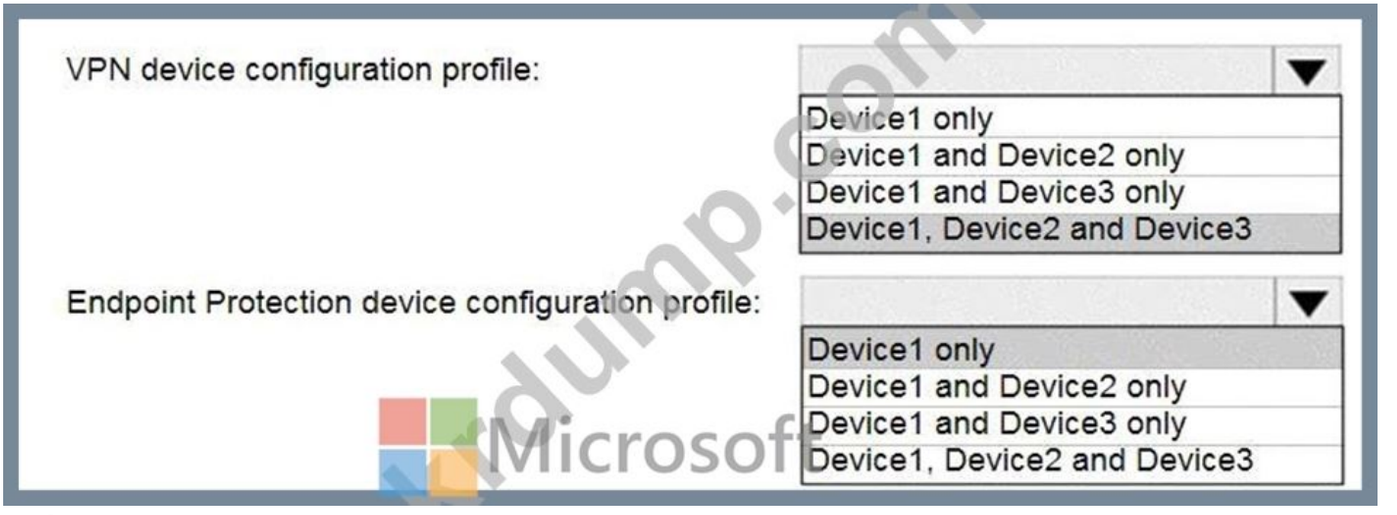
Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

Microsoft Endpoint Manager□□ □□□ □□ □□ □□ □□□ □□□ □□□□□.
* VPN □□ □□ □□□□ □□□□ VPN □□□ □□□□□.
* Endpoint Protection □□ □□ □□□□ □□□□ □□ □□□ □□□□□.
□□□ □□ □□□ □□□□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos

NEW QUESTION: 27
Microsoft Store for Business□ □□□□ □□ User1□□□ □□□□ □□□□ Microsoft 365 □□ □□ □□□□. User1□ Microsoft Store for Business□□ □□ □□□ □□□ □ □□□ □□□□ □□□.
* □□□□□ □□□□□ □□□□□.
* Microsoft Store□□ □□ □□□□□.
* □□ □□□ □□ □□ □□□ □□□ □□□□□.
□□□□ □□ □□□ □□□ □□□□ □□□.
User1□□ □□ Microsoft Store for Business □□□ □□□□ □□□?
A. □□□□□
B. Device Guard □□□
C. □□□
D. □□□
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

NEW QUESTION: 28
Microsoft 365 E5 □□□ □□ Microsoft Defender for Endpoint□ □□□□□. □□□□ Windows 11 □□□ □□□□ □□□□.
□□□ Windows Defender □□ □□□□ □□□□ □□ □□ □□□ □□ □□ □□□ □□□□ □ □□ □□□□ □□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□, □□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □ □□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Explanation:

NEW QUESTION: 29

Microsoft 365 □□□ □□□□.

App1□ App2□□ □ □□ □□□□□□□ Azure AD□ □□□□□.

App1□ □□□□ □□□□□ □□ □□ □□(MFA)□ □□□□ □□□□ □□□. MFA□ App1□ □ □□□□□. □□□ □□ □□□?

A. Microsoft Entra □□ □□□□ □□□ □□□ □□□ □□□□.

B. Microsoft 365 □□ □□□□ □□ □□ □□□ □□□□□.

C. Microsoft Entra □□ □□□ □□□□□□ □□□□□□ □□□□□□ □□□ □□□ □□□□ □.

D. □□ □□ □□□□ □□□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Reference:

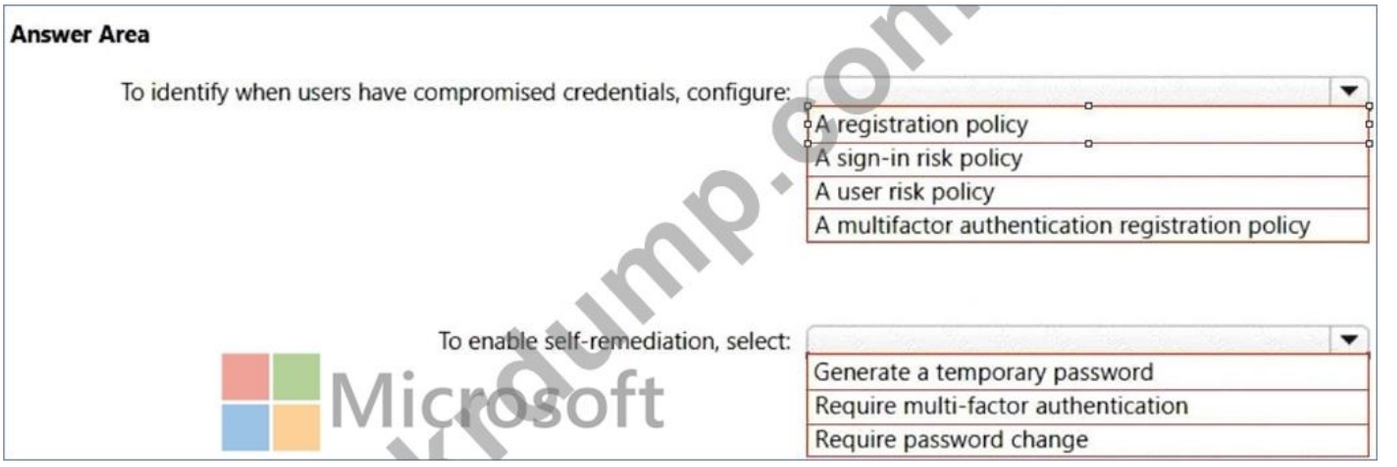
https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor- authentication

NEW QUESTION: 30

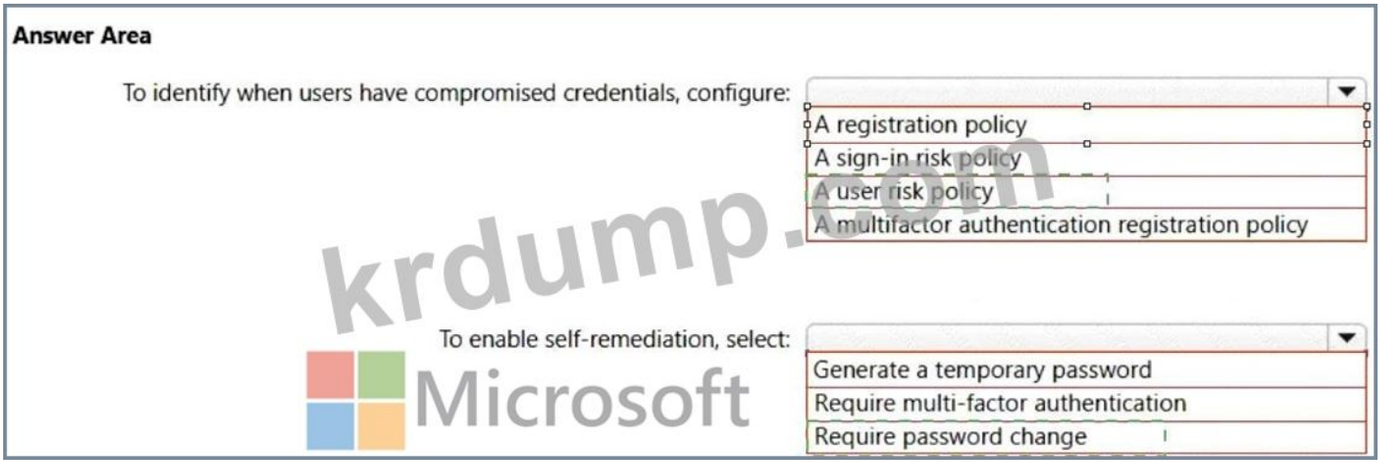
□□□

Microsoft 365 E5 □□□ □□□□.

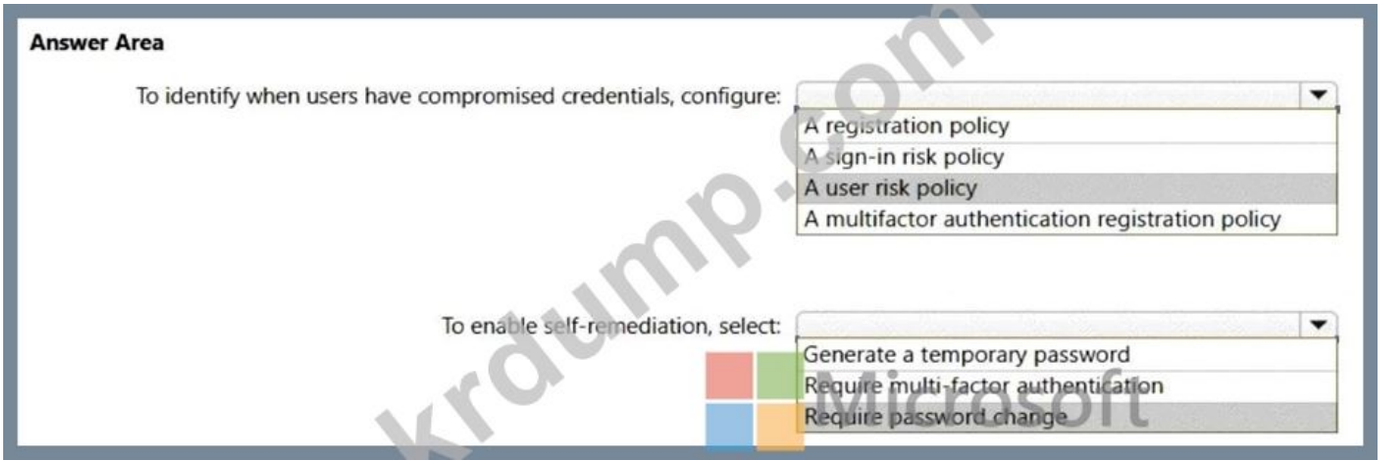
ID □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□□□.
* □□ □□□ □□□ □□□□□ □□□ □□□ □ □□ □□□ □□□□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Box 1: A user risk policy

Identify when a user's credentials are compromised and shared on the dark web.

User risk-based Conditional Access policy

Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their

credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:
Block access
Allow access but require a secure password change.
A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.
Box 2: Require password change
Provide users that have compromised credentials with the ability to self-remediate.
A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators Reference:
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection- policies#user-risk-based-conditional-access-policy

NEW QUESTION: 31
Microsoft 365 □□□ □□□□.
□□ □□□□ Microsoft SharePoint □□□ □□□ □□□□ □□ □□□□□□.
□□ □□□□ □□□□ □□□□ SharePoint □□ □□□ □□□□□.
□□□ SharePoint □□ □□□ □□□□ □□ □□□ □□□ □□□.
□□ □□: □□ $ □□ □□ □□ □□□□ □□ □□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
Microsoft 365 E5 □□□ □□□□.
□□□ □□□ □□□ □□□□□□□ Microsoft Defender for Cloud Apps□ □□□□ □□□. □ □□ □□ □□□?
A. □□□ □□□ □□□□.
B. □□□ □□ □□□ □□□□□□.
C. Microsoft 365□ □ □□□□ □□□□.
D. □□ □□□ □□□□.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 33

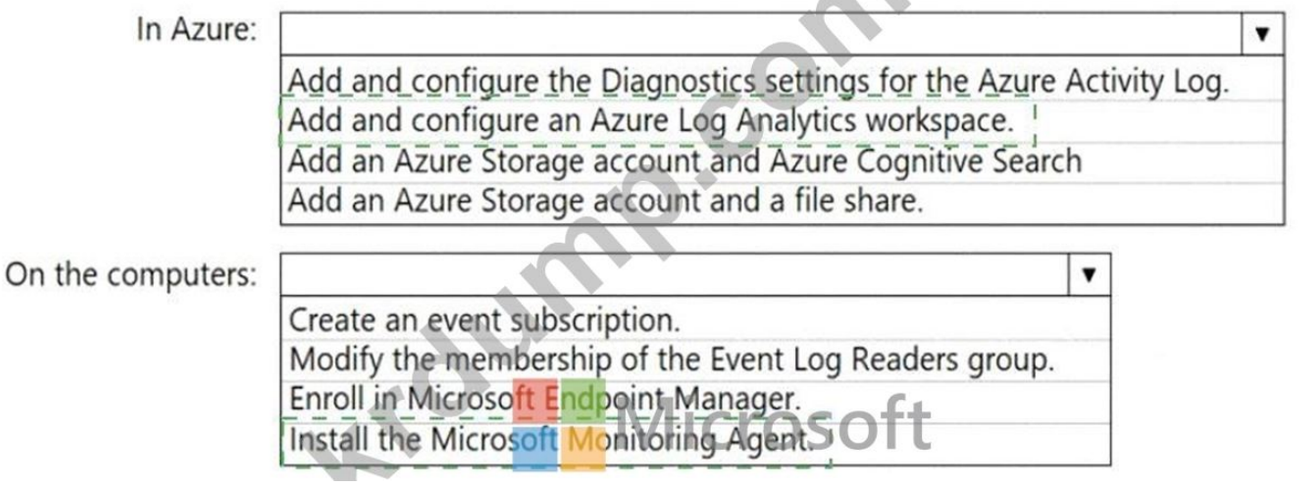
Azure □□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows 10□ □□□ □ 50□□ □□□□ □□□□.

□□□□ □□□ □□ □□□□ □□□□ □□□□□□ □□□.

□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:



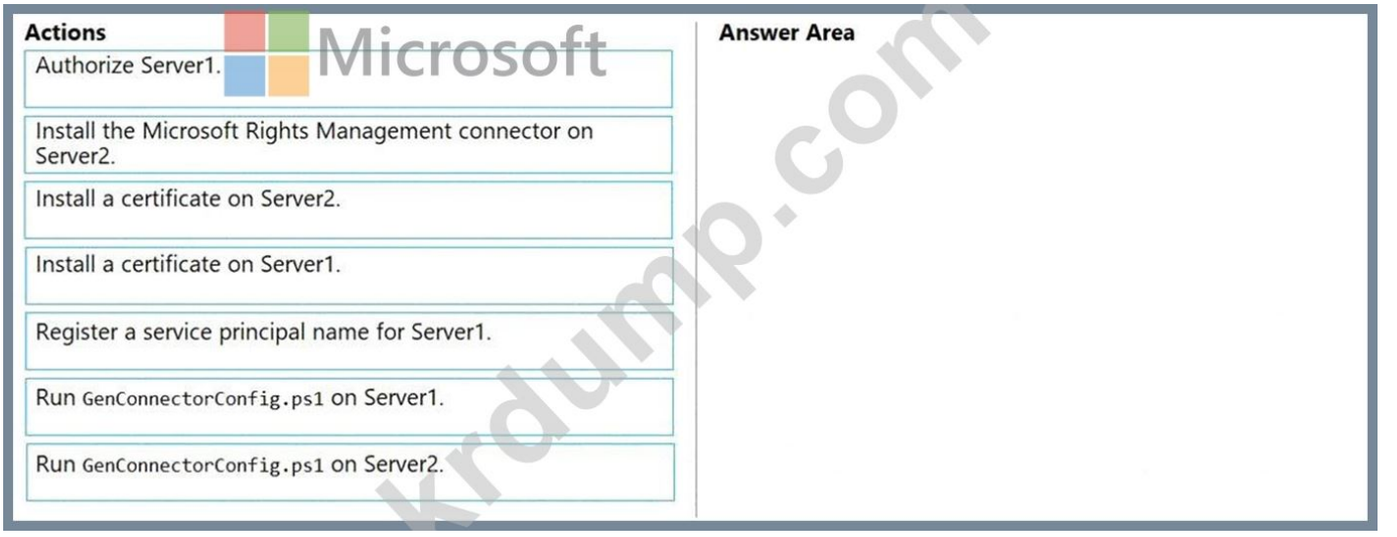
Explanation:

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

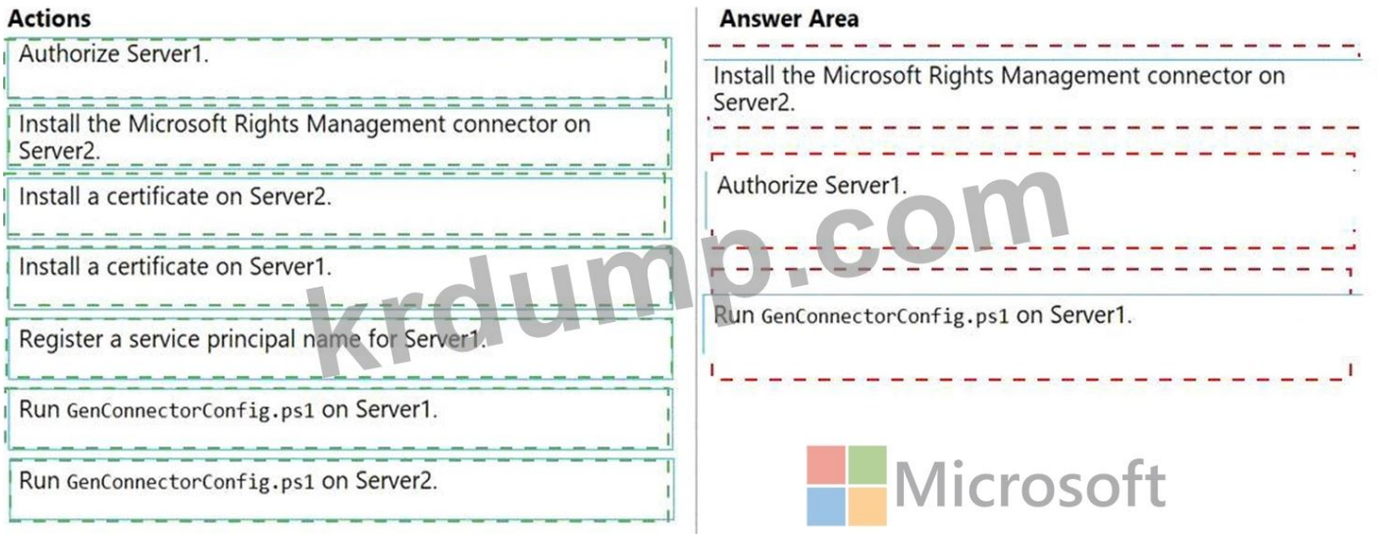
NEW QUESTION: 34
□□□ □ □□
□□□ □□□□□□ Azure Active Directory(Azure AD)□ □□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

Azure Information Protection□ □□□□□.
Server1□ □□ □□□□ Azure Information Protection □□□□ □□□ □ □□□ □□□□ □□ □.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □ □□□ □□□ □□□ □□□ □□□□□.



Answer:



Explanation:

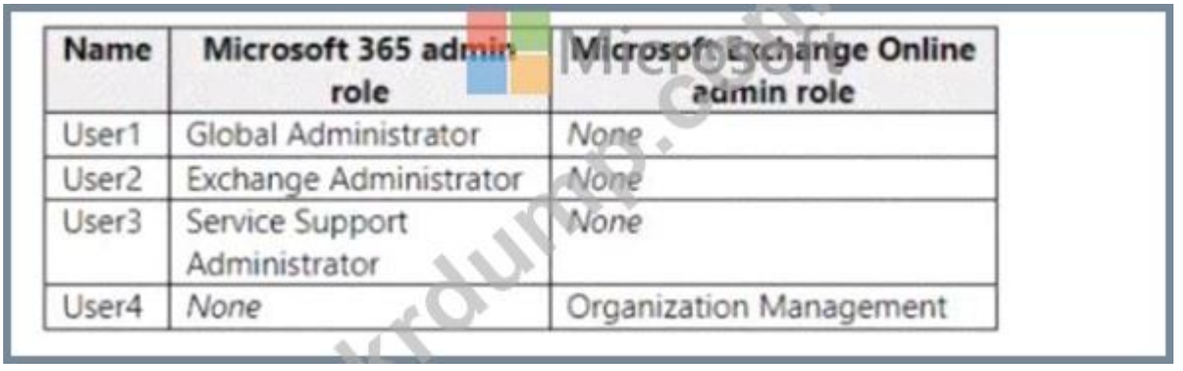
Reference:

https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector

https://docs.microsoft.com/en-us/azure/information-protection/configure-servers-rms-connector

NEW QUESTION: 35

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 □□□ □□□□.



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

DNS □□□□ □□□□ □□□□ □□ Exchange Online□ □□□□□ □□□.

□□□□ □□□ DNS □□□□ □□□□□.

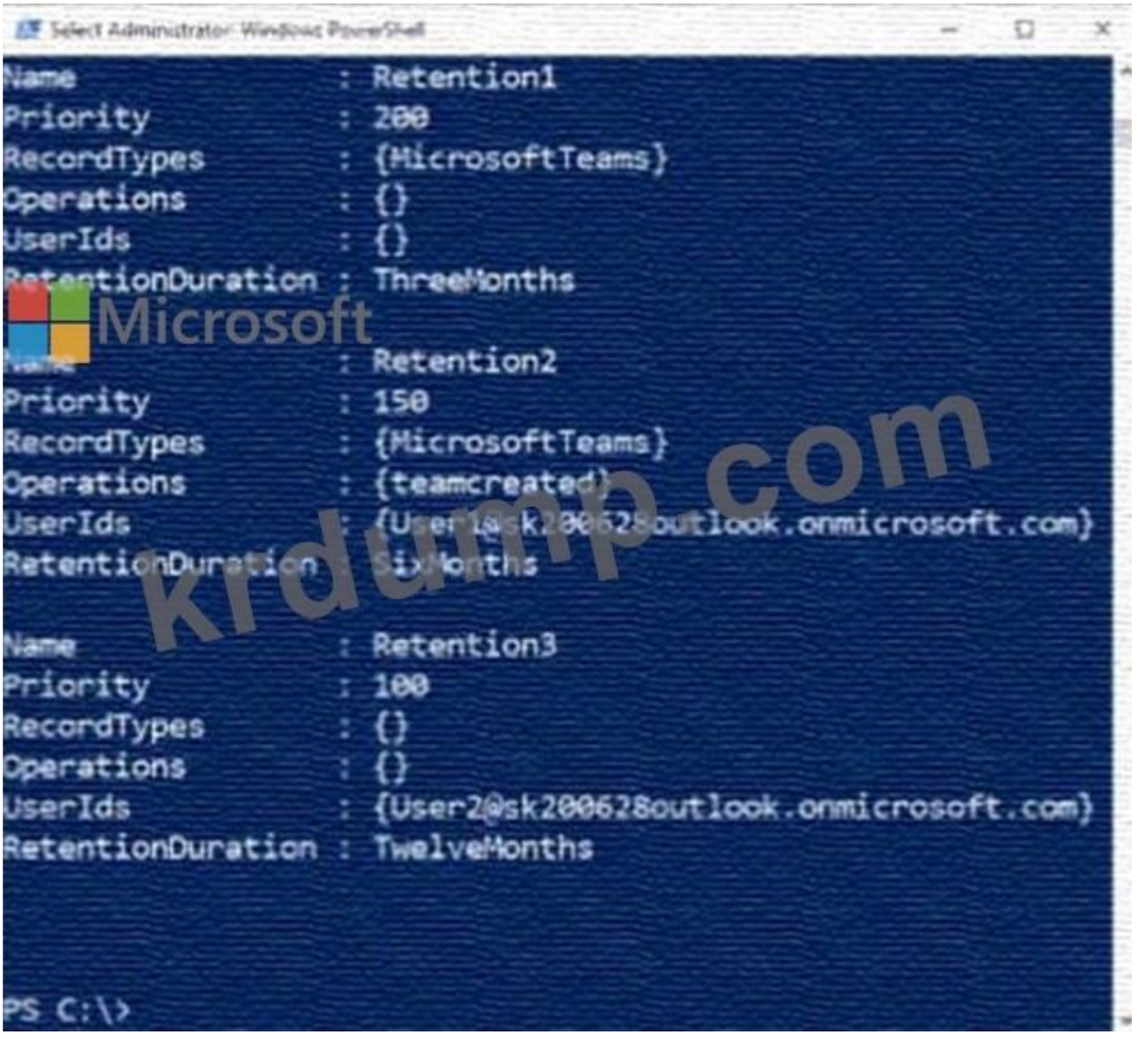
DNS □□□□ □□□ '□□□ □□□□ □□□□□'□□□.

DNS □□□ □□□ □□□ □ □□ □□□□ □□□□ □□□. □□□□ □□ □□□ □□□ □□ □□ □□□.

□□ □□□□ □□□□ □□□?

A. □□□1
B. □□□4
C. □□□3
D. □□□2
Answer: A (LEAVE A REPLY)

NEW QUESTION: 36
□□ □□ □□□ □□□ 3□□ □□ □□ □□□ □□ Microsoft 365 ES □□□ □□□□.



□□□ □□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□ □□□ □ □□□ □□□□□. □□□ □□ 1□□□□.

Answer:

Answer Area

Explanation:

NEW QUESTION: 37

□□□

□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

□□ □□□ □□□□□.

□□ □□□ □□□ □ □□□, □□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Groups that can be restored:

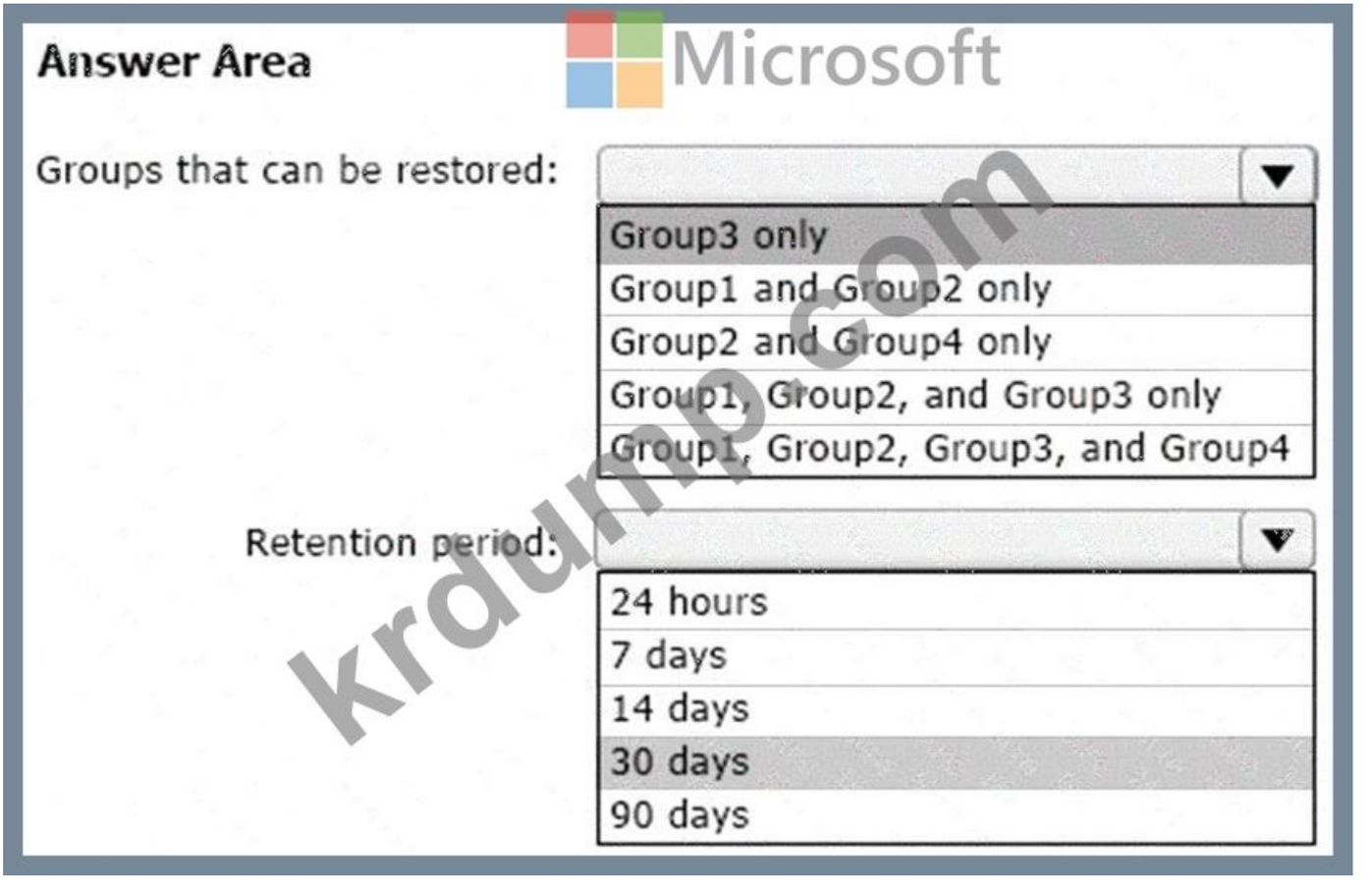
- Group3 only
- Group1 and Group2 only
- Group2 and Group4 only
- Group1, Group2, and Group3 only
- Group1, Group2, Group3, and Group4

Retention period:

- 24 hours
- 7 days
- 14 days
- 30 days
- 90 days

Answer:

Explanation:



Box 1: Group3 only

Box 2: 30 days

If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a "soft- delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/restore-deleted-group

NEW QUESTION: 38
□□ □□ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

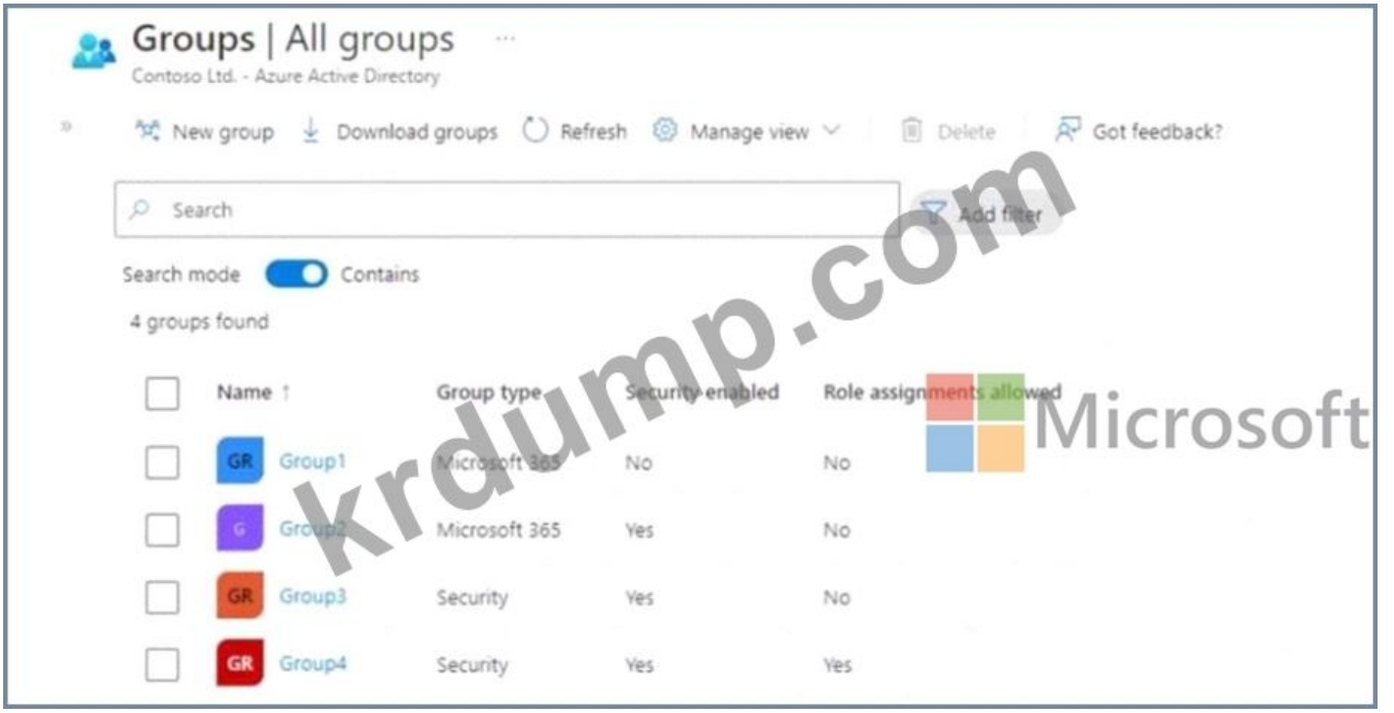
Platform	Count
Windows 10	50
Android	50
Linux	50

Windows 10 □□□□□ □□□ □□□ □ □□□□□ □□□□ □□□ □□ □□□ □□□□ □ □□. □□□□ □□ □□□ □□□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Microsoft 365 □□ □□□□ □□ □□□ □□□ □□ □□□ □□□□.
B. Microsoft 365 Defender □□□□ □□ □□□ □□□□.
C. Microsoft Endpoint Manager □□ □□□□ □□ □□□ □□□□.
D. Azure Active Directory □□ □□□□ □□ □□ □□□ □□□□.
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365- worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?
view=o365-worldwide

NEW QUESTION: 39
□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□: User1
UPN: user1@contoso.com
□□□ □□: user1@marketmg.contoso.com
MFA □□ □□: □□□□□
User1□ user1@marketing.contoso.com □□□ □□□ □□□□ □□□ Outlook□ □□□□□□ □□ □□□□ □□□□ □ □□□□.
User1□ user1@marketing.contoso.com□ □□□□ □□□ Outlook□ □□□□ □ □□□ □□□ □ □□□.
□□□ □□ □□□?
A. User1□ MFA □□ □□□ □□□□□.
B. User1□ □□□□□ □□□□□□.

C. User1□ □□ □□ □□□ □□□ □□□□□.
D. User1□ UPN□ □□□□□.
Answer: D (LEAVE A REPLY)
Microsoft's recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN's to match.
Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user's email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only needs to remember a single name.
Configure the Azure AD multifactor authentication registration policy
Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.
Reference:
https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname

NEW QUESTION: 40
□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.



□□ □□□ Microsoft 365 E5 □□□□□ □□□ □ □□□?
A. □□2□ □□3□
B. □□2, □□3, □□4□
C. □□ 1, □□ 2, □□ 3□
D. □□! □ □□2□
E. □□3□ □□4□
Answer: E (LEAVE A REPLY)

NEW QUESTION: 41

□□ □□ □□□ □□ Microsoft Intune□ □□□ 5□□ □□□ □□ Microsoft 365 E5 □□□□ □ □□□.

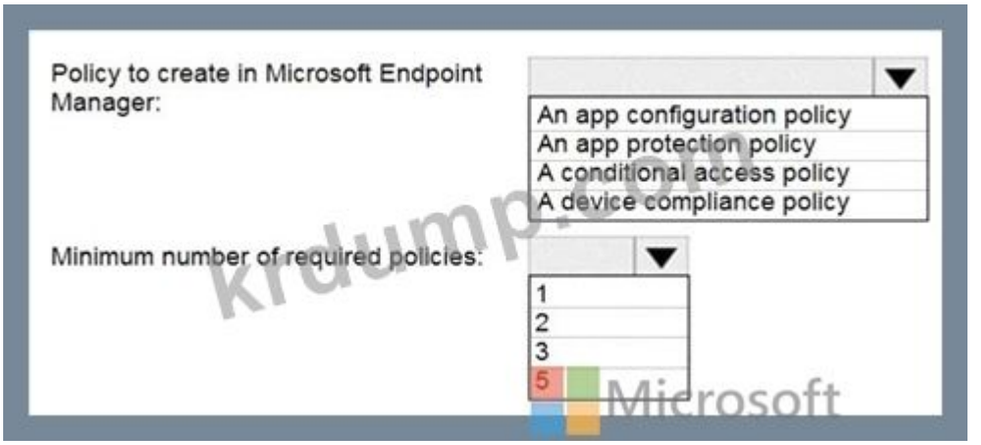
Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

□□ □□□□ App1□□□ □□ □□□□ □□□□.

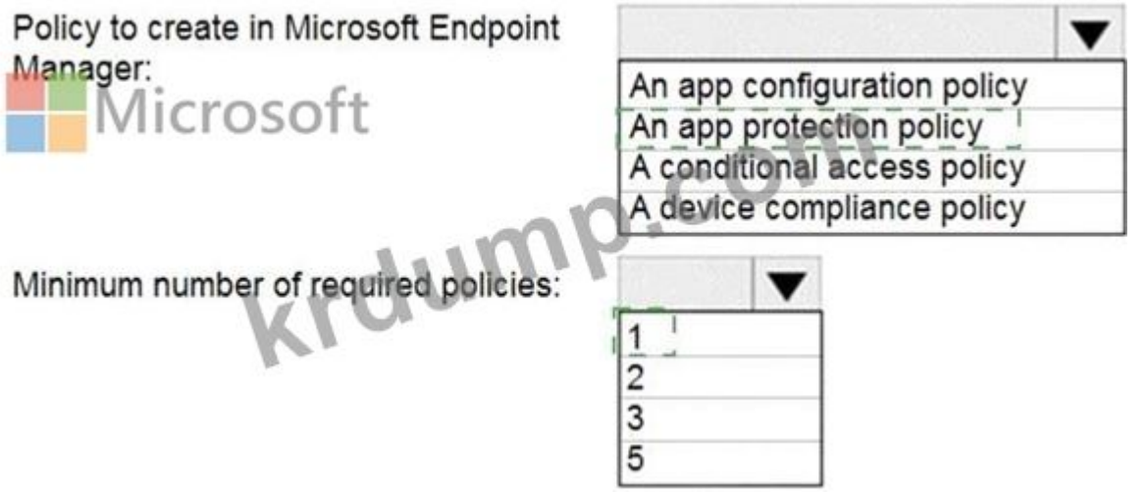
□□□□ App1□□ □□□□ □□□□ □□ □□ □□□□ □□ □□□□ □□□.

Microsoft Endpoint Manager□□ □□ □□□ □□□□ □□, □□□ □□□ □□ □□ □□□□ □? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

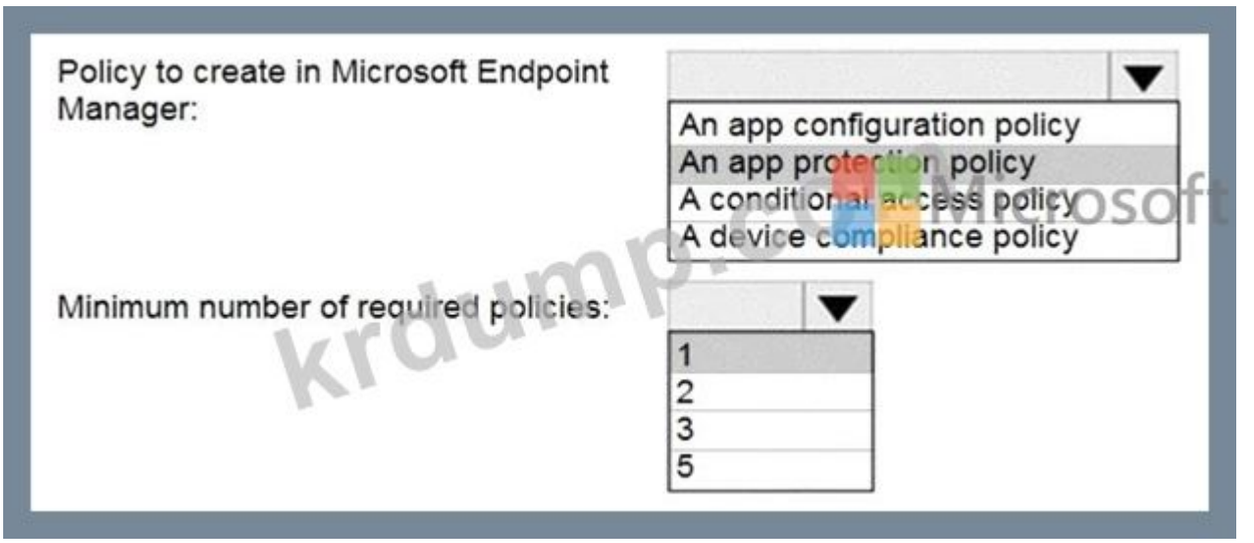
□□□□: □□ □□□ 1□□□□.



Answer:

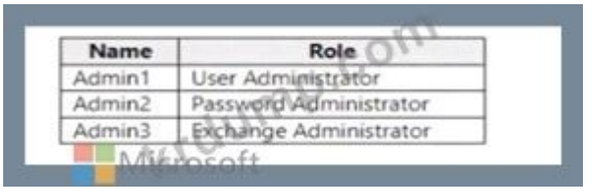


Explanation:



Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

NEW QUESTION: 42
□□ □□ □□□ □□□□ □□□□ Azure AD □□□□ □□□□.



Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Exchange Administrator

□ □□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□ □□□ □□□□ □□□?

A. Microsoft 365 Defender □□1
B. Microsoft Purview □□ □□ □□
C. Microsoft Entra □□ □□
D. Microsoft 365 □□ □□
Answer: B (LEAVE A REPLY)

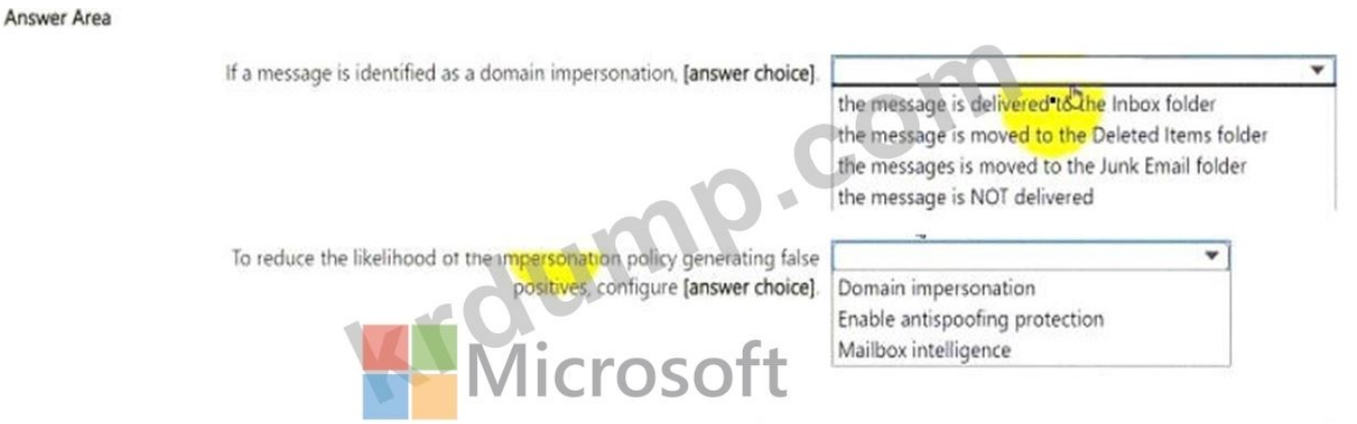
NEW QUESTION: 43
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□(MFA)□ □□□□□ □□□.
□□□□ □□ □□ □□□ □□□□ □□□. □□□□ □□□□□ MFA□ □□□□ □□□□ □
□□ □□□ MFA□ □□□ □□□□□□ □□□ □□□□□ □□ □□□.
□□□ □□□□ □□?

A. FID02 □□ □
B. □□
C. □□□□
D. Microsoft □□□
E. □□□ OTP
Answer: D (LEAVE A REPLY)

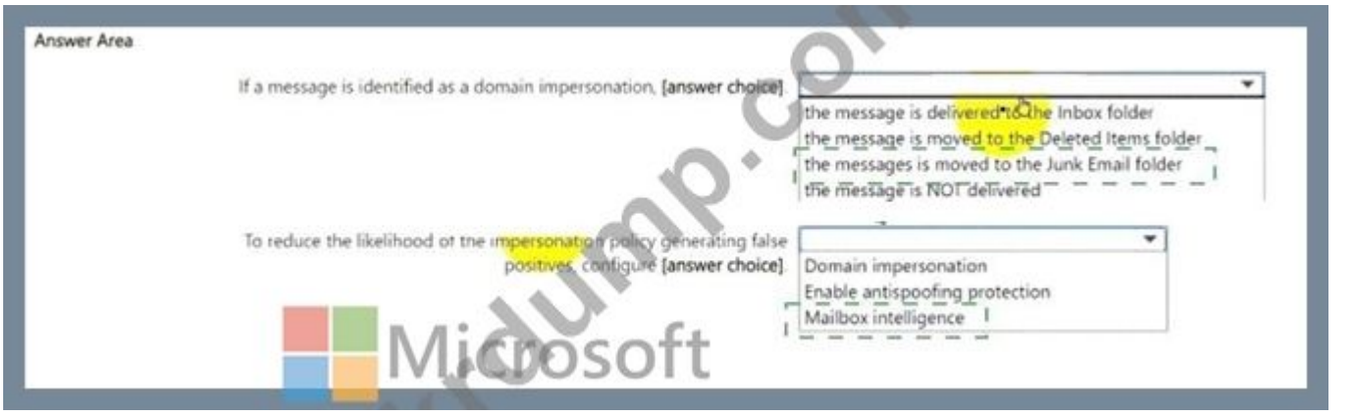
NEW QUESTION: 44
Microsoft 365 □□□□ □□□□.
Microsoft Intune□□ □□ □□ □□□□ □□□ □□□□□.
□□□□ □□□□ □□ □□□□ □□□ □ □□□?
A. □□□ 8.1
B. □□□ □□□
C. □OS
D. □□□□□ □□□□□□
Answer: (SHOW ANSWER)

NEW QUESTION: 45
□□ □□ □□□ □□□ □□ □□ □□□ □□□□□.

□□□□ □□□ □□□ □□□ □ □□□□ □□□□ □□□□ □□□□□ □□□□ □□□ □□ □□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

If a message is identified as a domain impersonation: the message is moved to the Junk Email folderAccording to the anti-phishing policy settings shown in the exhibit, messages identified as domain impersonation should be moved to the Junk Email folder to reduce the risk of phishing attacks.

To reduce the likelihood of the impersonation policy generating false positives, configure: Mailbox intelligenceMailbox intelligence helps in reducing false positives by using machine learning and historical email patterns to make better decisions about which emails are legitimate and which are not.

NEW QUESTION: 46

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

□□ □□□□ Microsoft 365 □□ □□□□ □□ □□□ □□□ □ □□□□?

A. User1□ User2□

B. User2onry

C. □□□□!

D. User1, User2, User3

E. User!☐ User3☐

Answer: D (LEAVE A REPLY)

NEW QUESTION: 47

User1☐☐☐ ☐☐☐☐ ☐☐☐ Microsoft 365 E5 ☐☐☐ ☐☐☐☐. ☐☐ ☐☐☐ ☐☐ Policy!☐☐ ☐ ☐☐☐ ☐☐☐ ☐☐☐☐.

* ☐☐ ☐☐☐, ☐☐ ☐ ☐☐☐☐ ☐☐☐☐☐: User1

* ☐☐ ☐☐☐ ☐☐☐: 3 - ☐ ☐☐☐

User1☐ ☐☐ ☐☐ ☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐.

Name	Phishing confidence level (PCL)
Mail1	Low
Mail2	Medium
Mail3	High
Mail4	Very high

☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐☐☐?

A. Mail3 ☐ Mail4☐ ☐☐

B. Mail1, Mail2, Mail3, Mail4

C. Mail2, Mail3, Mail4☐ ☐☐

D. Mail4☐

Answer: A (LEAVE A REPLY)

NEW QUESTION: 48

Microsoft 365 ☐☐☐ ☐☐☐☐.

Microsoft 365 ☐☐ ☐☐☐☐ ☐☐ ☐☐☐ ☐☐ Microsoft 365 ☐ ☐☐ ☐☐☐☐ ☐☐☐.

□□□□ □□ □□ □□□ □□□□□ □□□□ □□□.

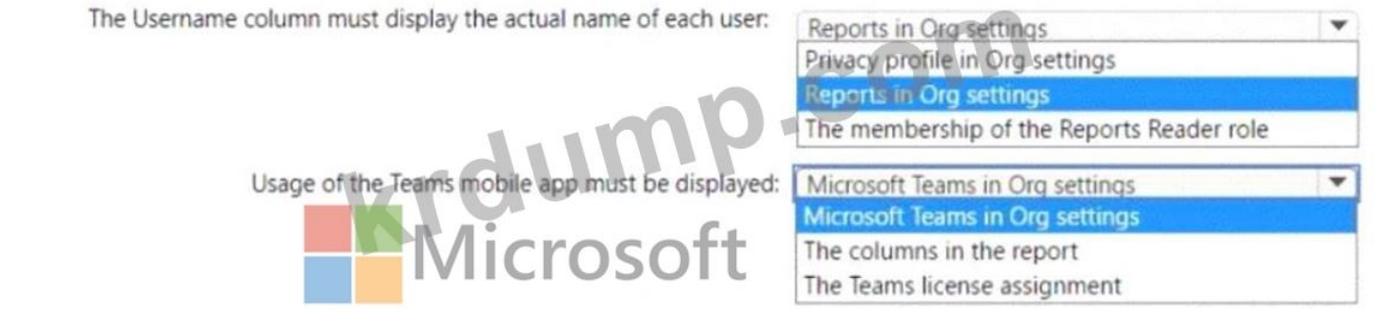
* □□□ □□ □□□ □ □□□□ □□ □□□ □□□□□ □□□.

* Microsoft Teams □□□ □□ □□□□ □□□□□ □□□.

□ □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□□□ □□□ □□□ □□□□□□.

□□: □ □□□ 1□□□□.

Answer Area



Answer:

Explanation:

NEW QUESTION: 49

□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□□ □□□□.

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

Endpoint □□□ □□□□ □□ □□ □□ □□□ □□□ □□□□□.

Endpoint □□□ □□□□ □□ □□□ □□□□□ □ □□□□?

A. Device1□

B. Device1□ Device2□

C. Device1, Device2, Device3□

D. Device1, Device2, Device4□

E. Device1, Device2, Device3, Device4

Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 50

Azure AD □□□□ Microsoft 365 E5 □□□ □□□□. □□□□□ □□ □□ □□□ □□□□ □ □□□□.

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

Endpoint□ Microsoft Defender□ □□□ □□□□□.

Microsoft Defender for Endpoint□□ □□ □□ □□□ □□(RBAC)□ □□ □□□ □□□□□.

Microsoft 365 Defender □□□□ □□ □□□□□ □ □ □□ □□□□ □□□□ □□□.

□□ □□□□ □□□□ □□□?

A. □□□3

B. □□□1

C. □□□4

D. □□□2

Answer: B (LEAVE A REPLY)

NEW QUESTION: 51

Office 365□ Microsoft Defender□ □□□□ Microsoft 365 □□□ □□□□.

□□ □□□ □□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□ □□□.

□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 52

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.

Windows 10□ □□□□ □□□□ □□□□.

□□□ Windows 10 □□□ □□□□ □□□.

□□ □□: □□ □□□ □□□□ □ □□□ □□□□ □□□□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: A (LEAVE A REPLY)

NEW QUESTION: 53

□□□

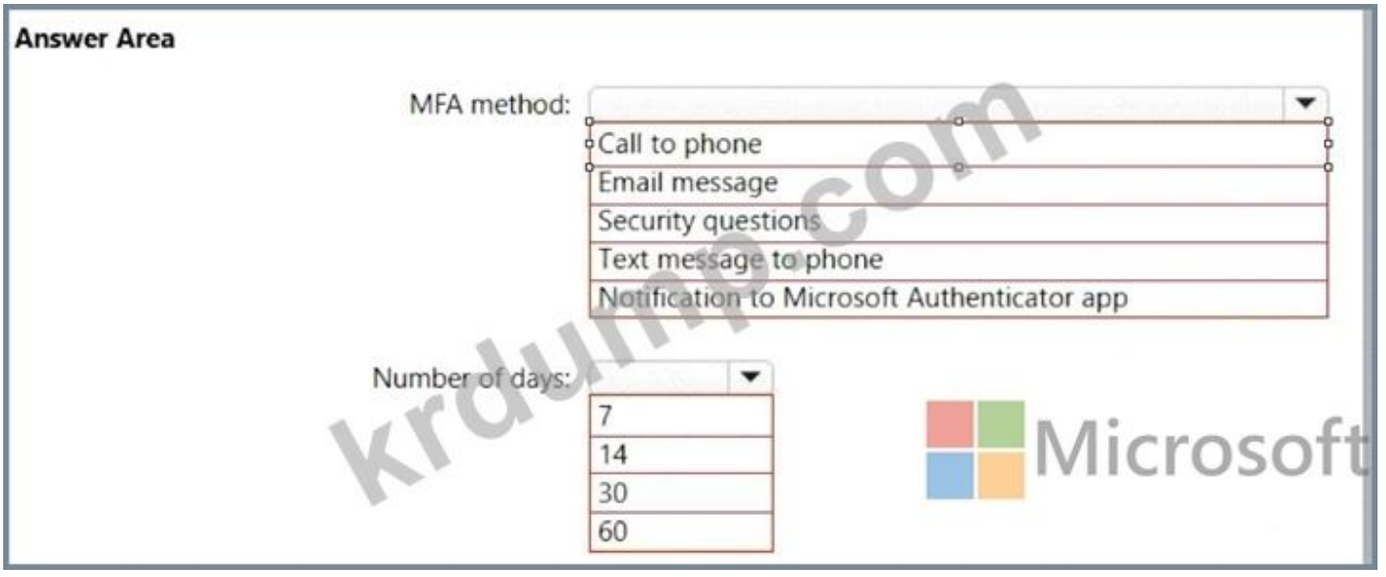
□□□ Microsoft 365 E5 □□□□ □□□□.

□□ □□□ □□□ □□ □□□□□□□.

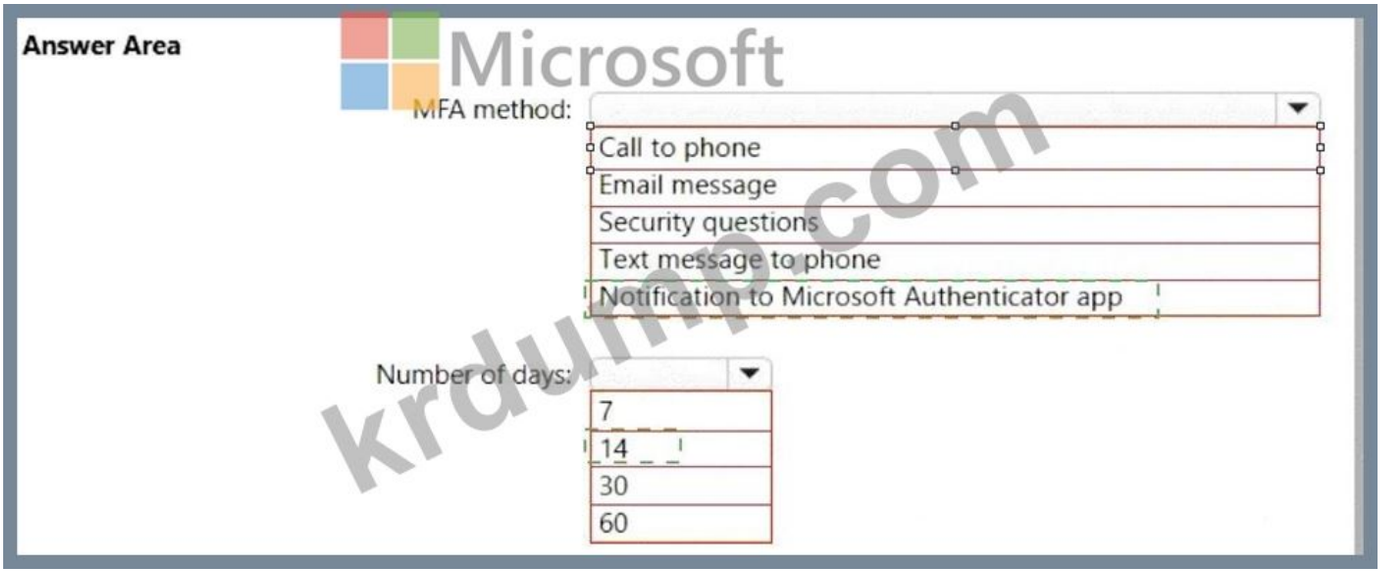
□□□□ □□□□ □□□□ □□□□□□.

□□□□ □□ □□ □□ □□(MFA) □□□ □□□ □ □□□, □□□□ MFA□ □□□□ □□ □ □□ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Answer Area

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.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/solutions/empower-people-to-work-remotely-secure-sign-in

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection- configure-mfa-policy

NEW QUESTION: 54

Office 365□ Microsoft Defender□ □□□□ Microsoft 365 □□□ □□□□.

□□□ □□ □□ □□ □□ □□ □□ □□□ □□□□□.

□□ □□ □□□ □□ □□□ □ □□ □□ □□□ □□□□□? □ □□□ □□□ □□□□ □□ □□□.

□□□□: □□ □□□ 1□□□□.

A. □□□ □□ □□

B. □□ □□

C. □□□ □□

D. □□□ □□

E. □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 55

□□□

Admin1□ Admin2□□ □ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

□□ □□□□□ Microsoft 365 Enterprise E5 □□□□□ □□□□ □□ □□□ □□ □□□□.

□□□ □□□ □□ □□ □□□ □□□□. (□□ □□ □□□□□.)

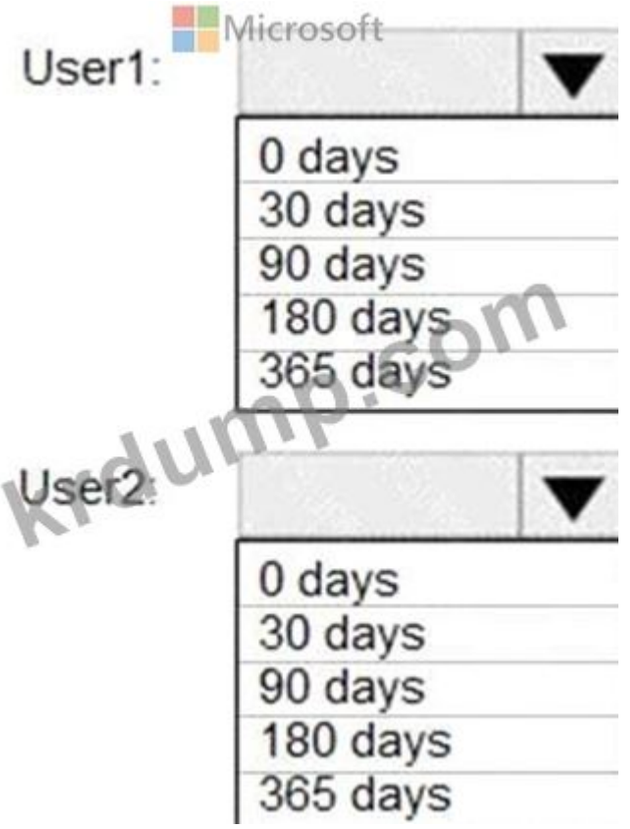
Policy1□ □□□ □□□ □□ □□□ □□□□□.

* Admin1□ User1□□□ □□□□ □□□□□.

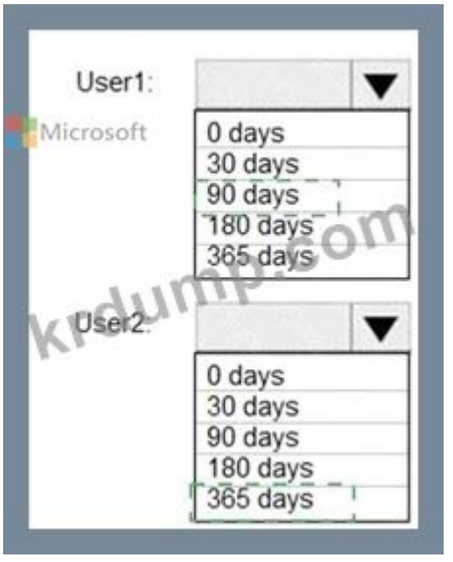
* Admin2□ User2□□ □□□□ □□□□□.

User1□ User2 □□□ □□ □□ □□□□ □□□ □□ □□□□□? □□□□□ □□ □□□□ □ □□ □□□ □□□□□.

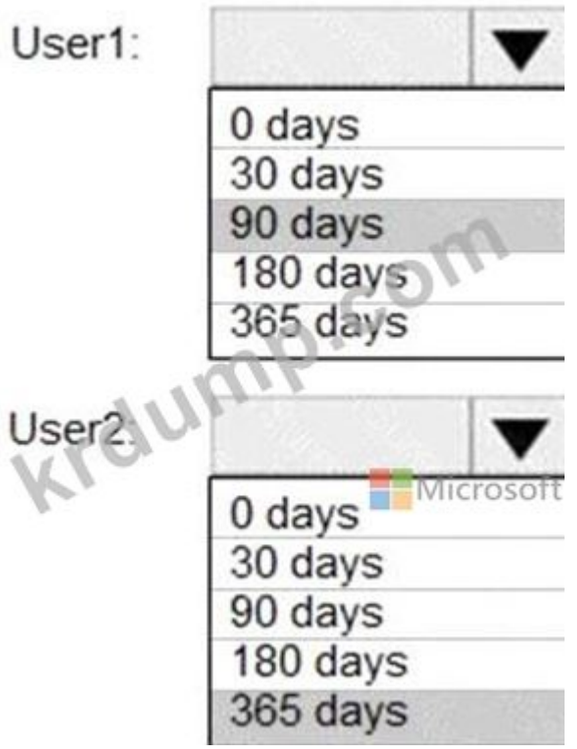
□□□□: □□ □□□ 1□□□□.



Answer:

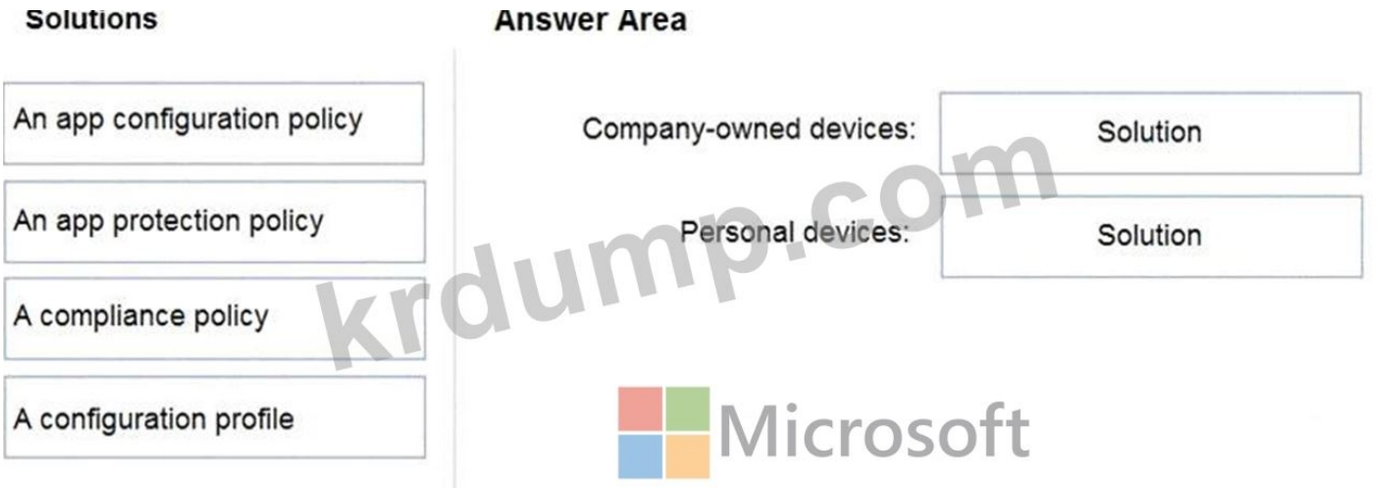


Explanation:

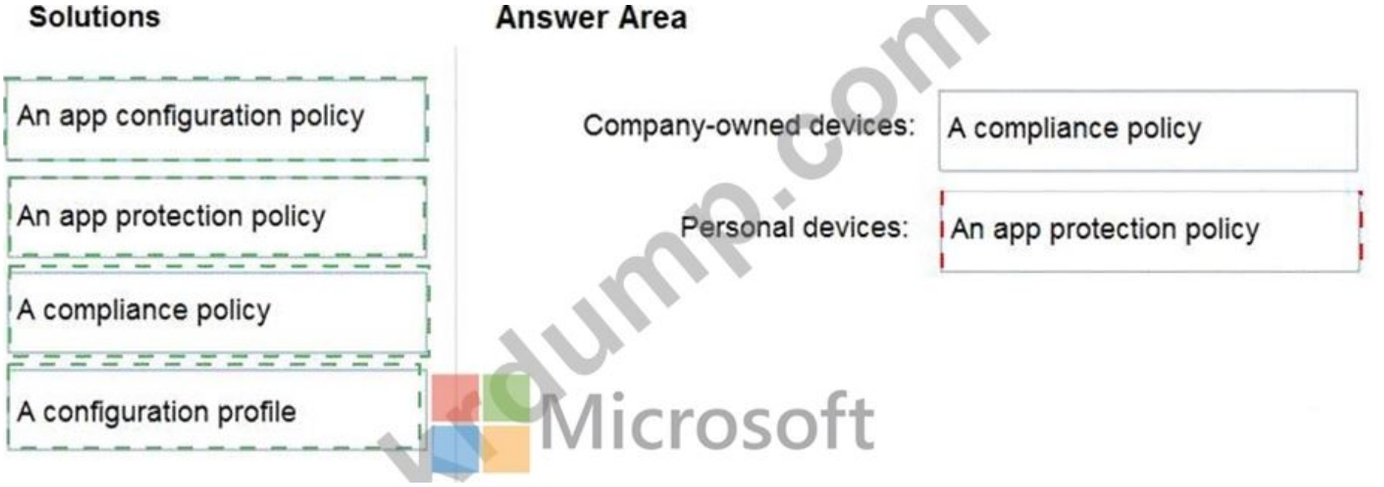


Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365- worldwide

NEW QUESTION: 56
□□□ □□□□ Microsoft 365 E5 □□□□ □□□□.
□□□□ □□ □ □□ □□□ Android □□□ □□ □□□□ □□□□ □□□□ □□□□□□. □ □ □□□ □□ □□□ □□ □□□ □□ □□□□ Microsoft Exchange Online □□□□ □□□□ □ □□□□.
□□□ □□ □□□ □□□□ □□□ □□□□ □□ □□□□ □□□ □ □□ □□□□ □□□□ □□□.
□ □□ □□□ □□ □□□□ □□□ □□□□ □□□? □□□□ □□□ □□ □□□ □□□ □□ □ □□□□□□. □ □□ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□ □ □□ □□□ □□□□□□ □□□□ □□□ □□□□□ □ □□ □□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 57

Azure Active Directory(Azure AD)□□ □□ □□□ □□□ □□□□ □□□ Microsoft 365 □□□ □ □□□□.

□□□□ □□ □□ □□□ □□ □ □□ □□ □□ □□□ □□□ □□□□□.

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

SP800 □□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

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

□□ □□□ □□□□□.

□□□ □□ □□ □□□ □□ □□ □□□□□ □□□□ □□□ □□□ □□□ □□□□□ □□ □□□.

□□ □□□□ □□ □□ □□ □□(MFA)□ □□□□□□.

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

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.	○	○

Answer:

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.	○	○

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.	○	○

Reference:

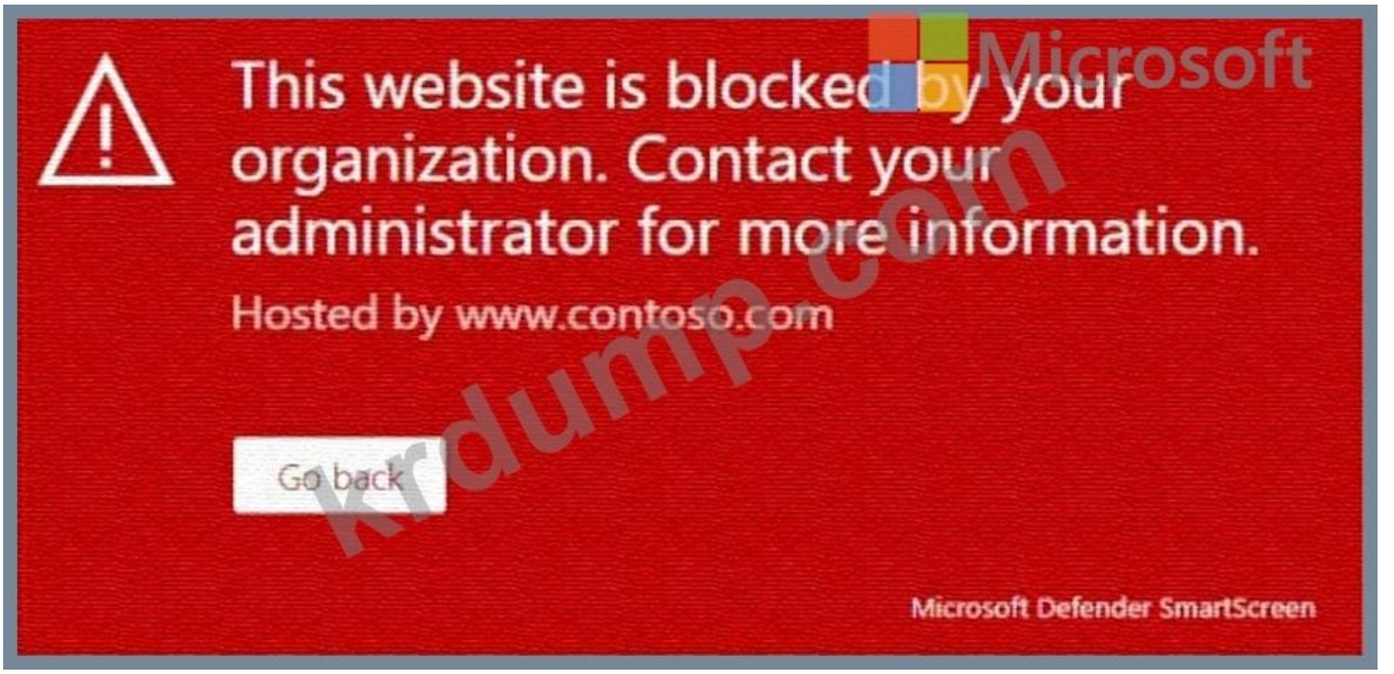
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-assessments?view=o365- worldwide#create-assessments

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365- worldwide#action-types-and-points

NEW QUESTION: 58

Microsoft Defender for Endpoint□ □□□□ Microsoft 365 E5 □□□ □□□□.

□□□□ □□□ □□□ □□□ □□□□□ □□ □□ □□□ □□ □□□□ □□□□□.



□□□ □□ □□□ □□ □□□ □□□□ □□□□□ □□□.

□□ Microsoft Defender for Endpoint □□□ □□□□ □□□?

A. □□ □□

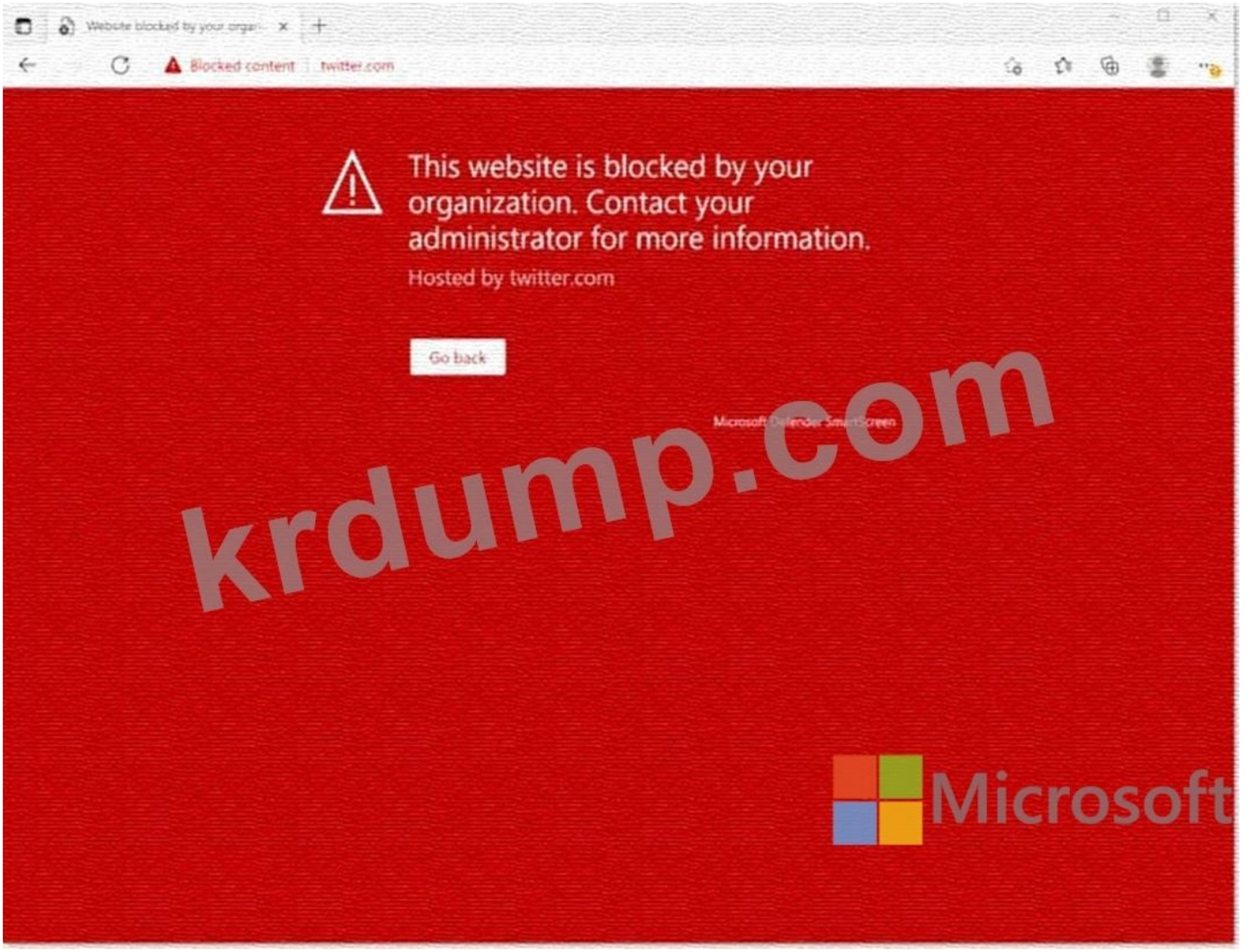
B. □□ □□

C. □□□ □□ □□

D. □□□□

E. □□

Answer: (SHOW ANSWER)



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: 59

Microsoft 365 □□□ □□□□.

□□ □□ □□□ □□□□ □□ □□ □□□□ □□□□ □□□.

□□ □□□ □□□ □□□□ □□□ □□□□ □□□□□.

□□□ □□□□ □□□□ Microsoft SharePoint □□ □□□ □□□□□ □□□ □□□□ □□ □ □□□ □□□□□. □□ □ □□ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□ □□□.

□□□□: □□ □□□ 1□□□□.

A. □□ □□□ □□□

B. □□□ □□ □□

C. □□□ □□ □□

D. □□□ □□ □□

E. □□□ □□ □□(DLP) □□

Answer: A,E (LEAVE A REPLY)

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: 60

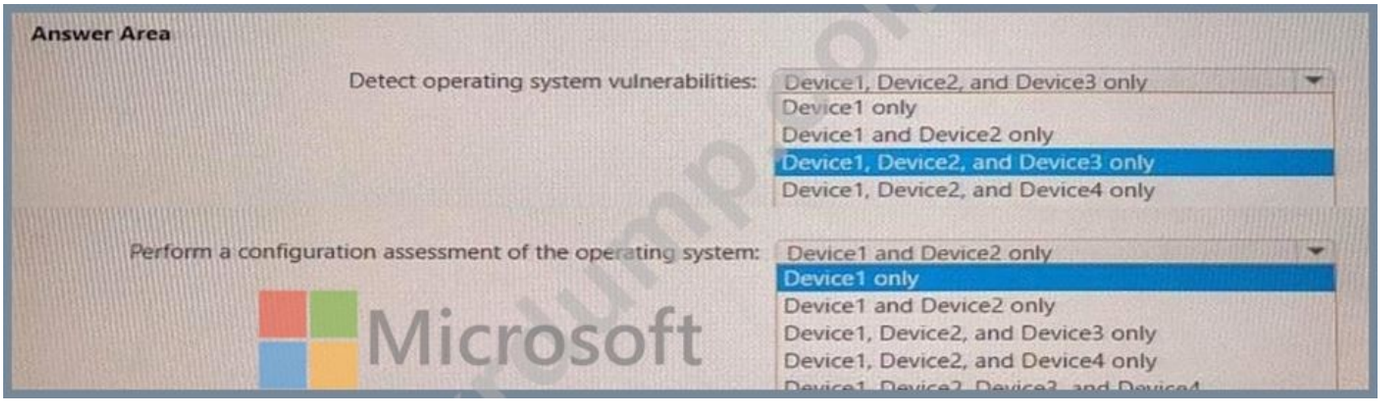
□□ □□ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

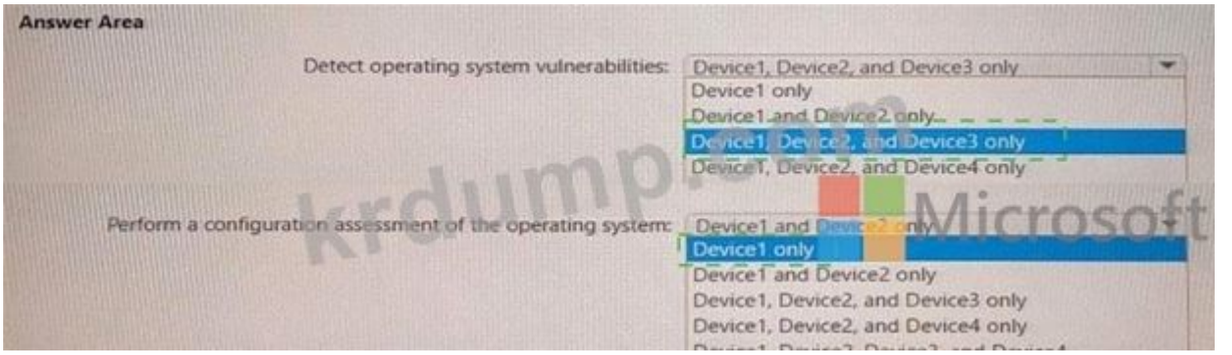
□□ □□□ Endpoint□ Microsoft Defender□ □□□□□□.

□□ □□ □□□ □□□□ □□ Microsoft Defender □□□ □□□ □□□ □□□□□.

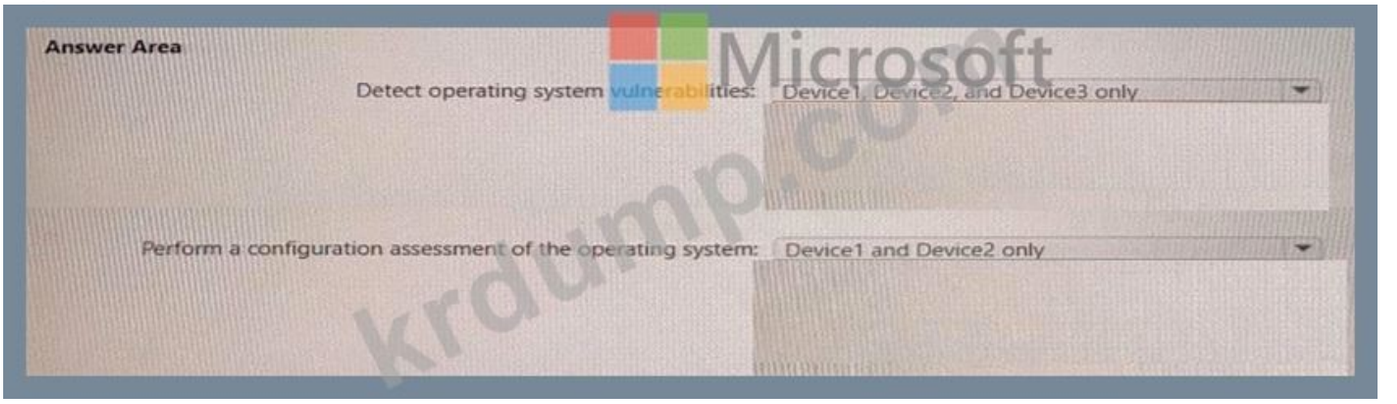
* □□ □□ □□□□ □□□□□.



Answer:



Explanation:



NEW QUESTION: 61

□□ □□ □□ □□

□□□ □□□ Microsoft 365 E5 □□□□ □□□□ .

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

Microsoft Store Business□ □□ □□□□ □□□ □□ □□ □□□□□.

Microsoft Store for Business□□ □□ □□□□ □□□□ □□□ □□ □□□□□.

□□ □□□ □□□ □□□ □ □□□?

A. Device2□

B. Device1, Device2, Device3, Device4, Device5

C. Device2, Device3, Device5□

D. Device2□ Device4□

E. Device1□ Device3□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 62
□□□ 5□ □□□ □□□□ □□ □□□□.
□□ □□□□ Microsoft 365 □□□□ □□□□.
□ □□□□ □□ □□□□ □□□□□.
Microsoft Intune□ □□□ □□□□□.
□□ □□ □□□ □□□□ Intune□ □□□□ □□□□ □□□□ □□□□ □□□.
□□ □□□□ □□□ □□□□ □□ □□□□ □□□ □ □□□ □□□.
□□ □□□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□.
□□□ □□□ □□□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. □□ □□□□
B. □□ □□
C. □□ □□□
D. □□□ □□□ □□
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

NEW QUESTION: 63
User1□□□ □□□□ □□□ Microsoft 365 □□□ □□□□.
User1□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□□□.
Microsoft Exchange Online □□□ □□□□□.
Microsoft 365 □□□ □□□□.
User1□ 8□□ □□□ □□□ □□□ □□□ □□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. zure AD ID □□
B. Microsoft Entra □□□ ID
C. □□□ □□□
D. Azure AD □□ □□ ID □□(PJM)
Answer: D (LEAVE A REPLY)
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: 64
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft 365 E5 □□□ □□□□.
SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.
SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Office 365 Advanced Threat Protection(ATP) □□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Azure Active Directory □□ □□□□ SecAdmin1□□ □□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: B (LEAVE A REPLY)

NEW QUESTION: 65
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft 365 E5 □□□ □□□□.
SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.
SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Microsoft Defender for Office 365 □□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Microsoft 365 □□ □□□□ SecAdmin1□□ SharePoint □□□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

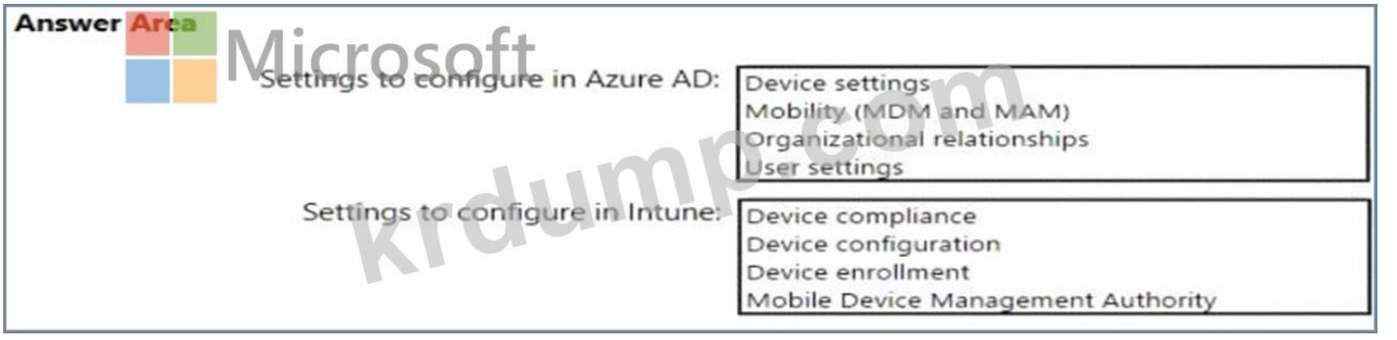
Answer: (SHOW ANSWER)

NEW QUESTION: 66

Intune□ □□ □□□ □□ □□□ □□□ □□ □□□ □□□□ □□□.

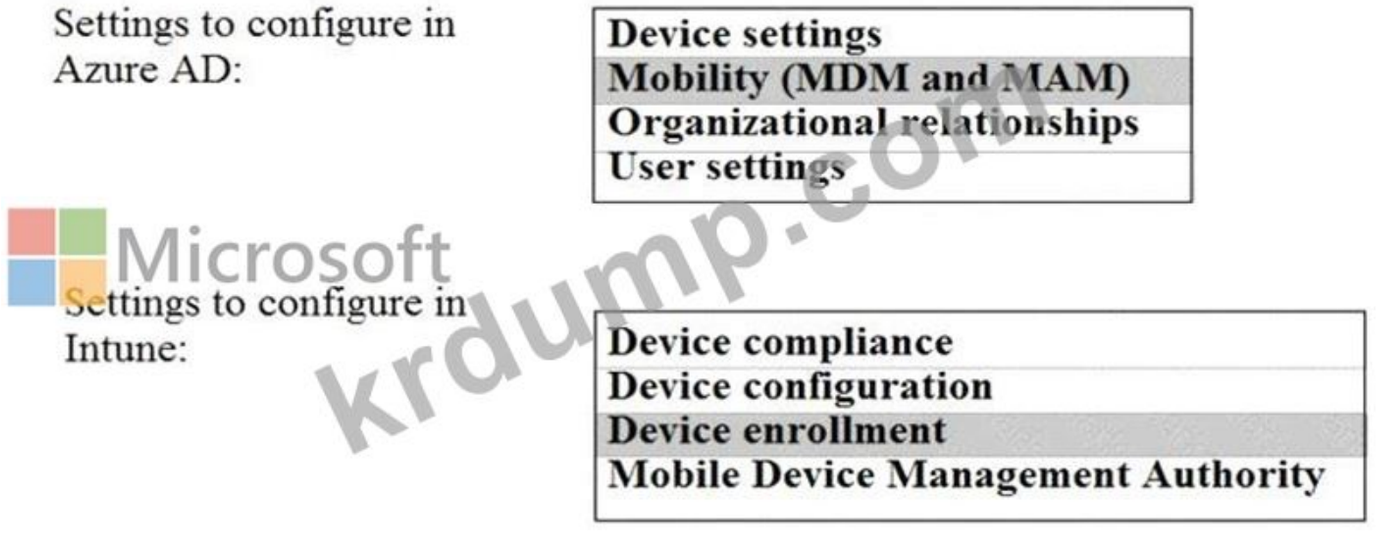
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:



Reference:

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

NEW QUESTION: 67

Office 365□ Microsoft Defender□ □□□□ Microsoft 365 □□□ □□□□.
□□□□ Microsoft Teams, OneDrive □□ SharePoint Online□□ □□ □□□ □□□ □□□□□ □ □□□□ □□ □□□.
□□□ □□ □□□?

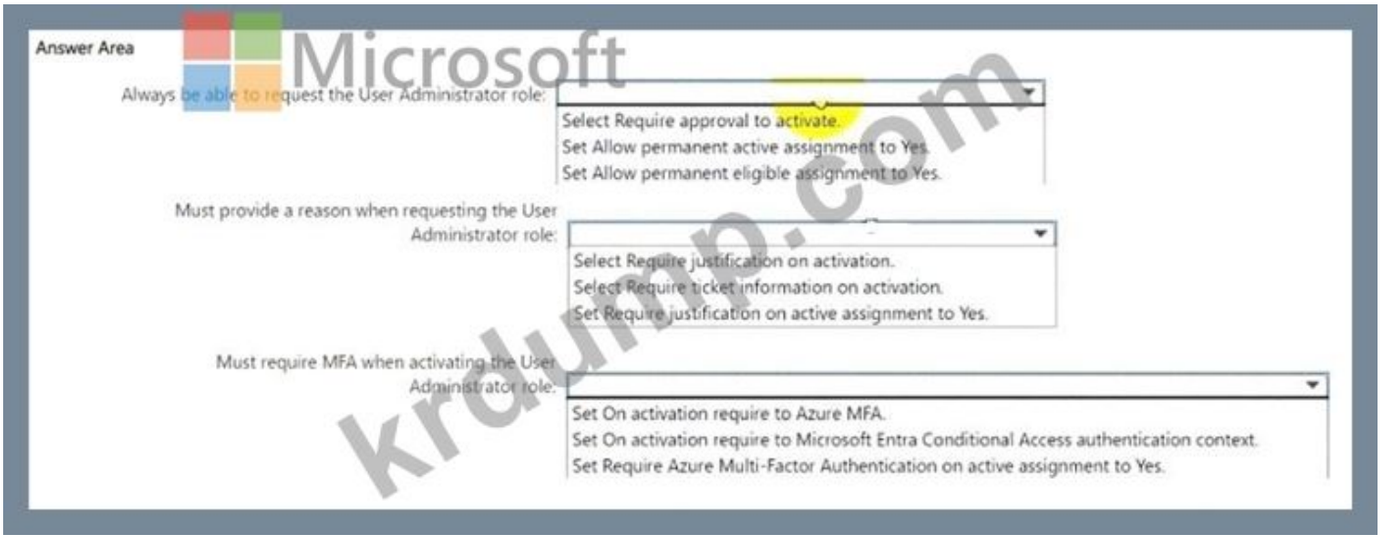
A. □□□ □□□ □□ □□□ □□□□.
B. □□□ □□ □□□ □□□ □□□□□.
C. □□□ □□□□ □□□ □□□□.
D. □□□ □□ □□ □□□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

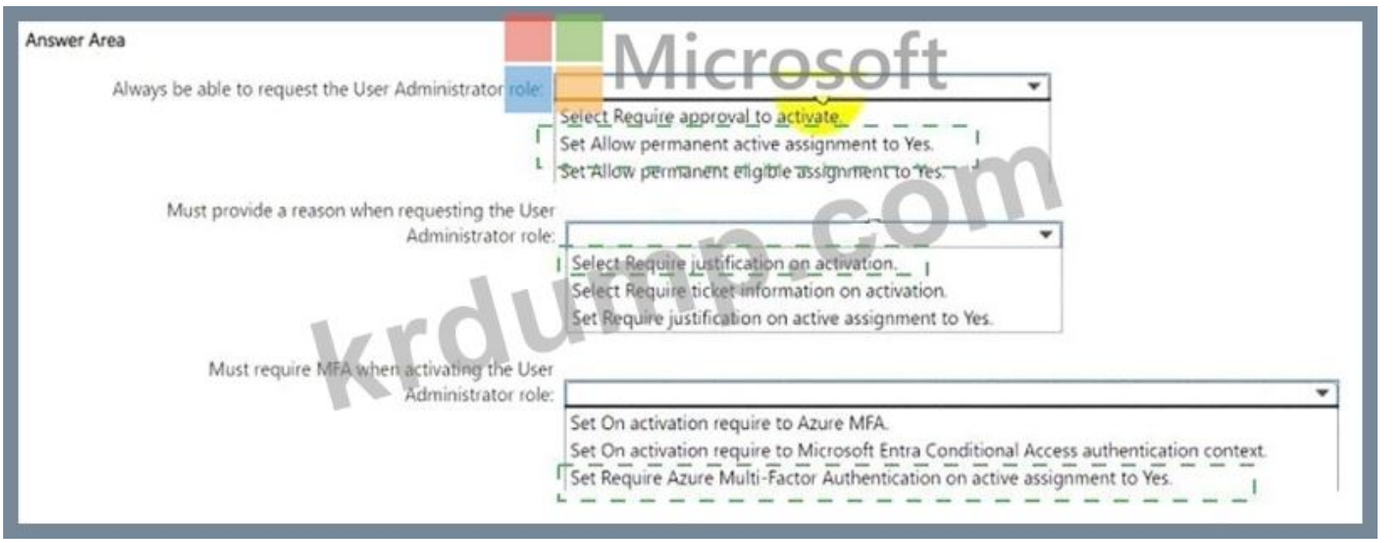
Safe Attachments for SharePoint, OneDrive, and Microsoft Teams
In organizations with Microsoft Defender for Office 365, Safe Attachments for SharePoint, OneDrive, and Microsoft Teams provides an additional layer of protection against malware. After files are asynchronously scanned by the common virus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

NEW QUESTION: 68

Microsoft 365 E5 □□□ □□□□.
Microsoft Entr a□□ □□□ □□□ □□□ □□ Privileged Identity Management(PIM)□ □□□□ □□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.
* □□ □□□ □□□ □□□ □□□ □ □□□□.
* □□□ □□□ □□□ □□□ □ □□□ □□□□ □□□.
* □□□ □□□ □□□ □□□□ □ □□ □□ □□(MFA)□ □□□□ □□□. □□□□ □□ □□ □ □□□□□ □□□.



Answer:



Explanation:

Always be able to request the User Administrator role: Setting "Allow permanent eligible assignment to Yes" ensures that users can always request the User Administrator role when needed.

Must provide a reason when requesting the User Administrator role: Selecting "Require justification on activation" ensures that users must provide a reason each time they activate the User Administrator role, which adds a layer of accountability and tracking.

Must require MFA when activating the User Administrator role: Setting "Require Azure Multi-Factor Authentication on active assignment to Yes" ensures that users must perform MFA to activate the User Administrator role, enhancing security.

NEW QUESTION: 69

□□ □□ □□□ □□□ Microsoft Endpoint Manager□ □□□ □□□ 3□ □□□□.

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

Endpoint Manager□ □□ □□ □□□ □□ □□ □□ □□□□□.

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

□□ □□ □□□ □□□ □□ □□ □□□□ □□□□.

Name	Assigned to
Policy1	Group3
Policy2	Group2

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□□. □□□ □□□ □□□□ □□□□□ □. □□: □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 70

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□ □□ □□□□.

□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows Server 2019□ □□□□ □□□ □□□□□ □□□□. □□□□□ □□□□ □□ □□□ Windows Server 2012 R2□□□.

□ □□□□□ Windows 10□ □□□□ 100□□ □□□□ Windows Server 2012 R2□ □□□□ Server1□□□ □□ □□□ □□□□ □□□□.

Server1□ □□□□ □□□□ □□□□ Windows 10 □□ □□ □□□ □□□ □□□□□.

Server1□ □□ □□ □□ □□(GPMC)□ □□□□□.
Server1□□ □□□□□ Windows □□□□ □□ □□ □□□ □□□□ □□□.
□□ □□: □□□ □□ □□□ Windows Server 2019□ □□□□. Windows 10 □□□□□ □□ □□□ □□□□□ Netlogon □□□ □□ □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

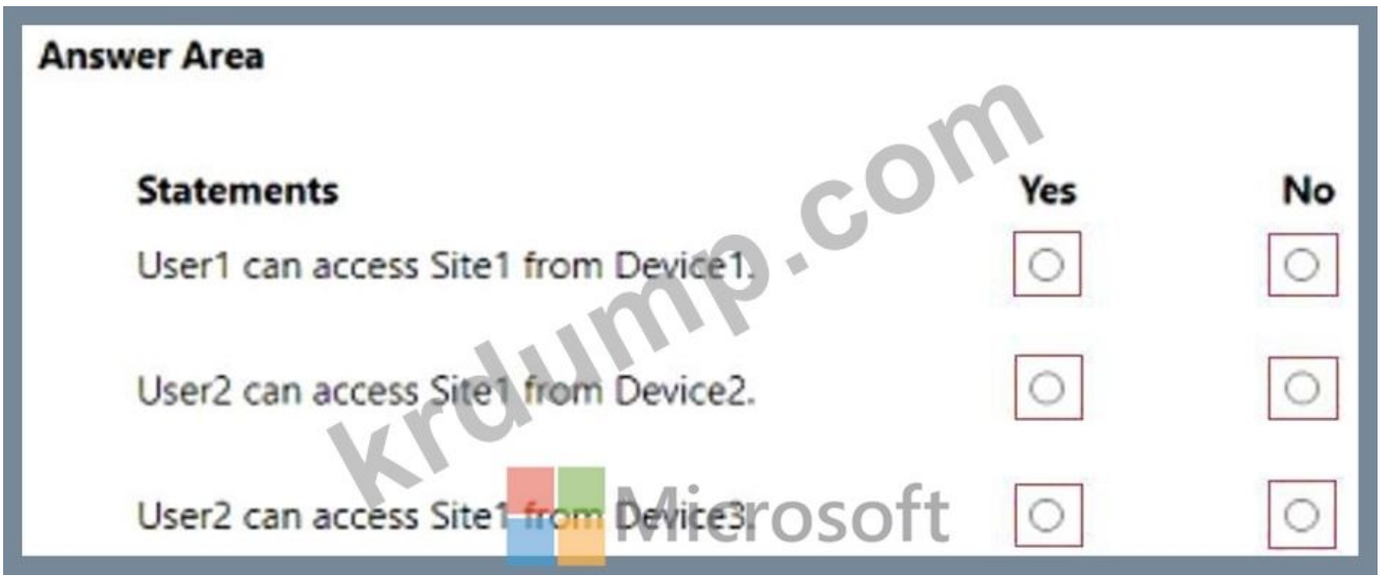
NEW QUESTION: 71
□□□
□□ □□ □□ □□ □□□□ □□□ Site1□□□ Microsoft SharePoint Online □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

□□□ □□ □□ □□ □□□□□.

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

CAPolicy1□□□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□.
1.□□
* □□□ □□ □□ ID: Group1
* □□□□ □ □□ □□: Office 365 SharePoint Online
* □□
- □□ □□□: □□□□ □□□ □□□□ □□□□□.
- □□ □□: device.displayName -startsWith "Device"
2. □□ □□
* □□□□
- □□ : □□ □□
* □□: 0□□ □□□□ □□□□□□□.
3. □□ □□□: □□
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

Box 1: No

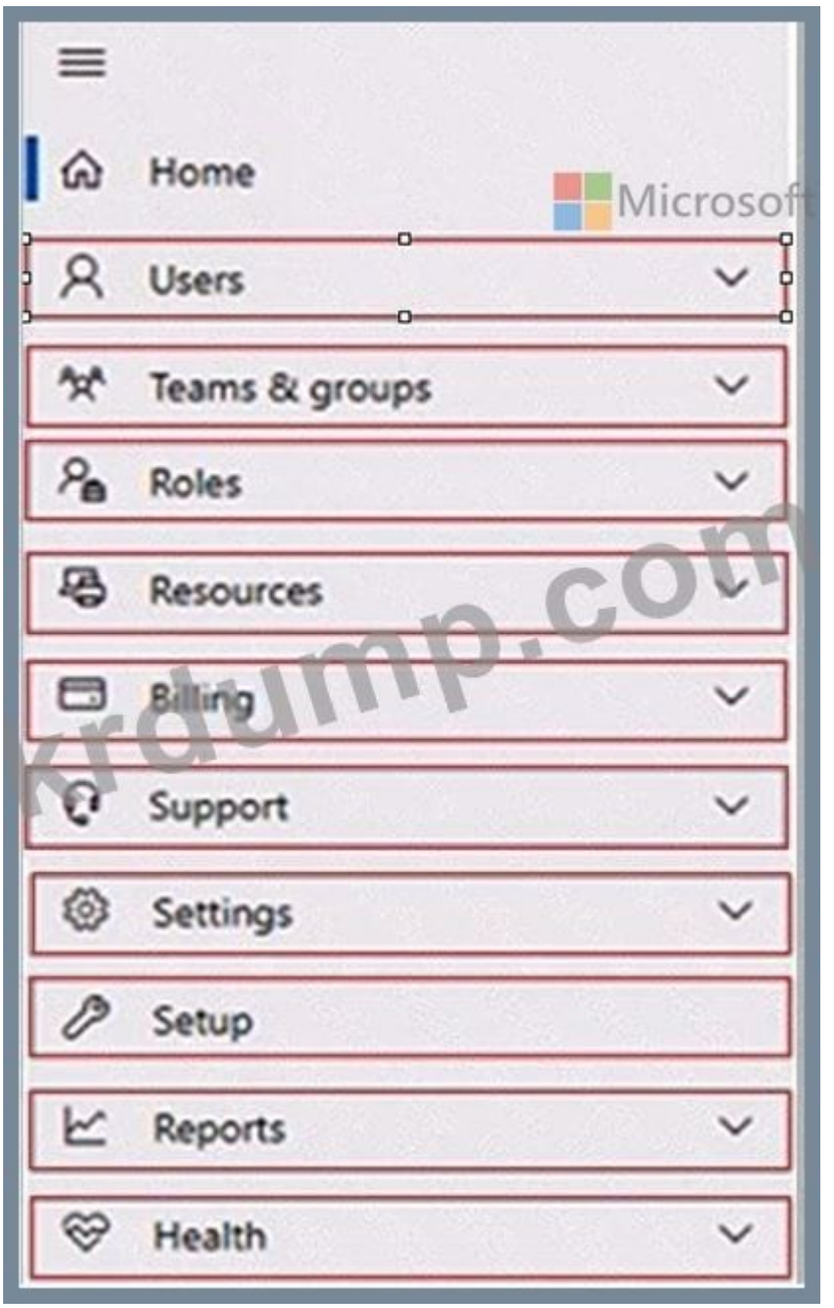
User1 is member of Group1 and has Device1.

Device1 is not Azure AD joined.

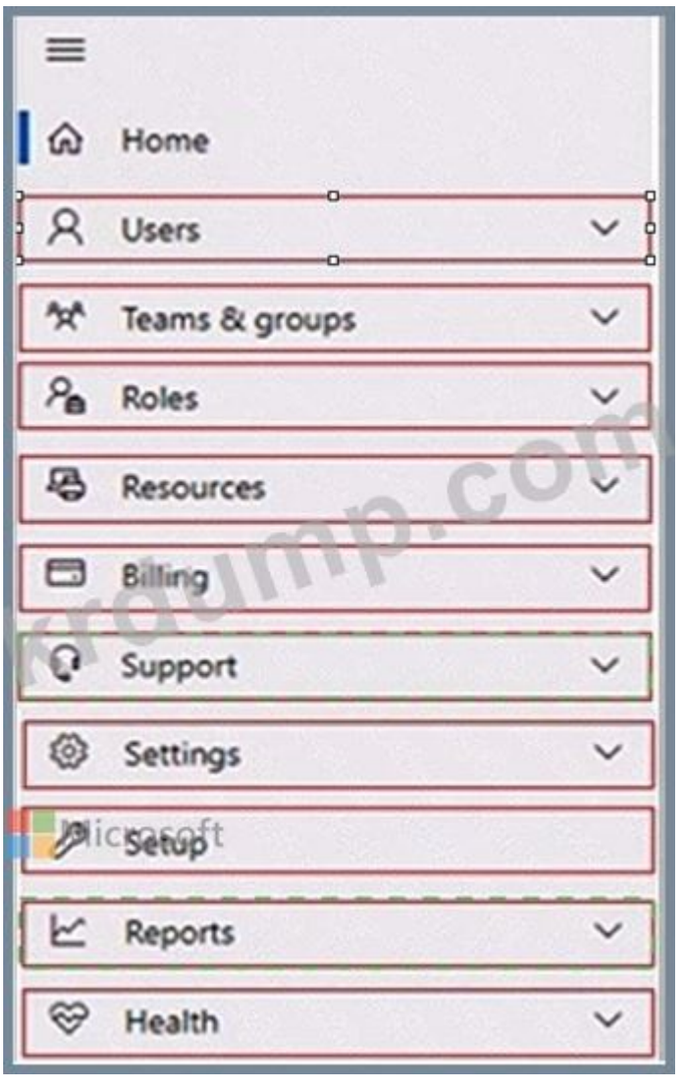
Note: Requiring a hybrid Azure AD joined device is dependent on your devices already being hybrid Azure AD joined.
Box 2: Yes
User2 is member of Group1 and has devices Device2 and Device3.
Device2 is Azure AD joined.
Device2 is excluded from CAPolicy1 (which would block access to Site1).
Box 3: Yes
User2 is member of Group1 and has devices Device2 and Device3.
Device3 is Android and is Azure AD registered.
Device3 is excluded from CAPolicy1 (which would block access to Site1).
Note: On Windows 7, iOS, Android, macOS, and some third-party web browsers, Azure AD identifies the device using a client certificate that is provisioned when the device is registered with Azure AD. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-hybrid-azure-ad-join
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy- compliant-device

NEW QUESTION: 72
Microsoft 365 E5 □□□ □□□□. □□□□□ FID02 □□ □□ □□□□□.
FID02 □□ □□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□□ □□□. □□□ □□ □ □ □□□ □□ □□□ □□□□ □□□?
A. □□ □□ □□
B. □□ □□ □□
C. □□□ □□□□□ □□ □□□□□.
D. □□□ □□□ □□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

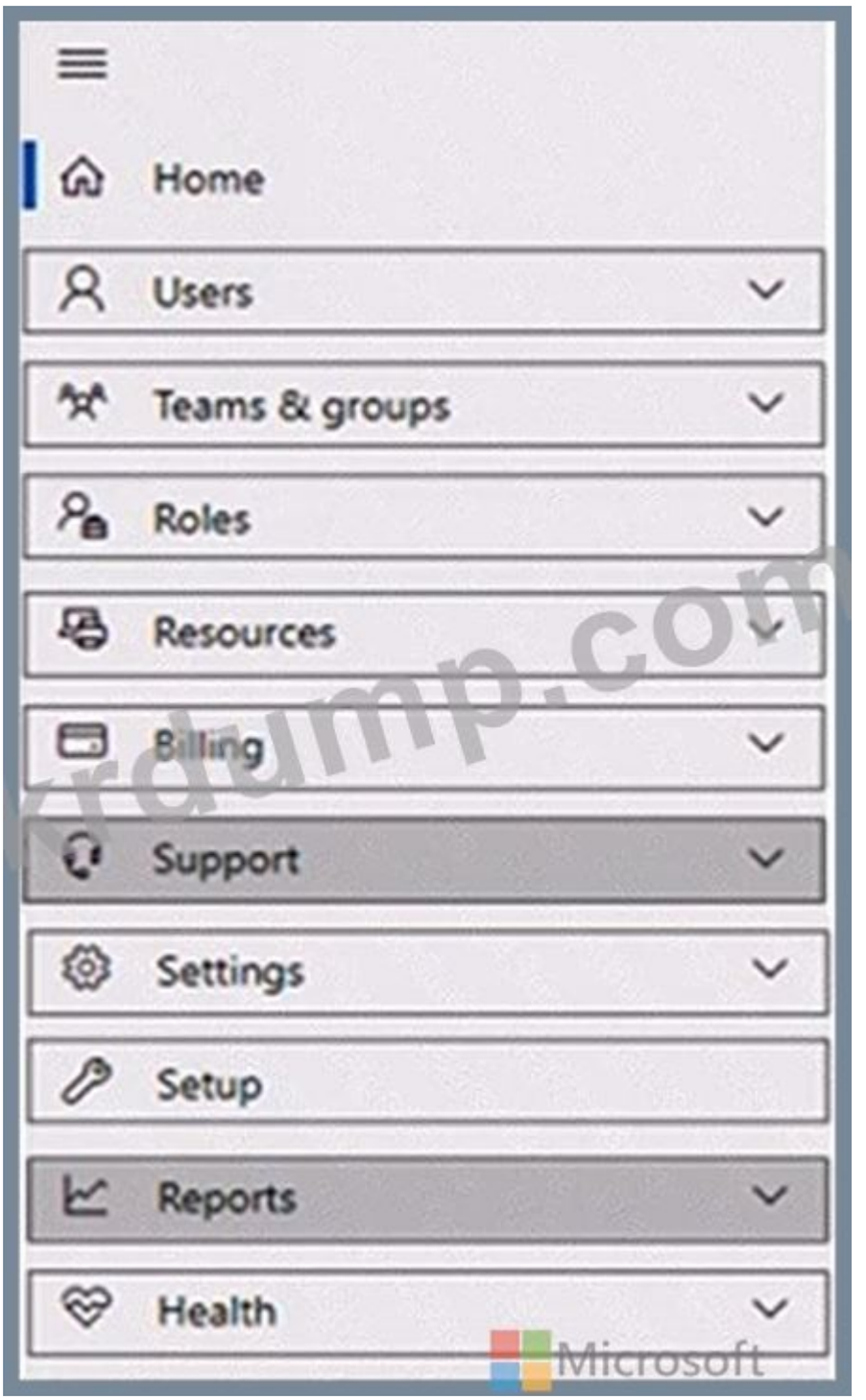
NEW QUESTION: 73
□□□
□□□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□□□ □□□.
□□□ □□ □□□ □□□□□.
Microsoft□ □□□ □□□ □□□ □□□□.
Microsoft 365 □□ □□□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □ □□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.


Home
Users
Teams & groups
Roles
Resources
Billing
Support
Settings
Setup
Reports
Health

Answer:



Explanation:



Box 1: Reports

View the Adoption Score of the company.

How to enable Adoption Score

To enable Adoption Score:

* Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score

* Select enable Adoption Score. It can take up to 24 hours for insights to become available.

Box 2: Support

Create a new service request to Microsoft.

Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request.
If you're in the admin center, select Support > New service request.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score
https://support.microsoft.com/en-us/topic/contact-microsoft-office-support-fd6bb40e-75b7-6f43-d6f9- c13d10850e77

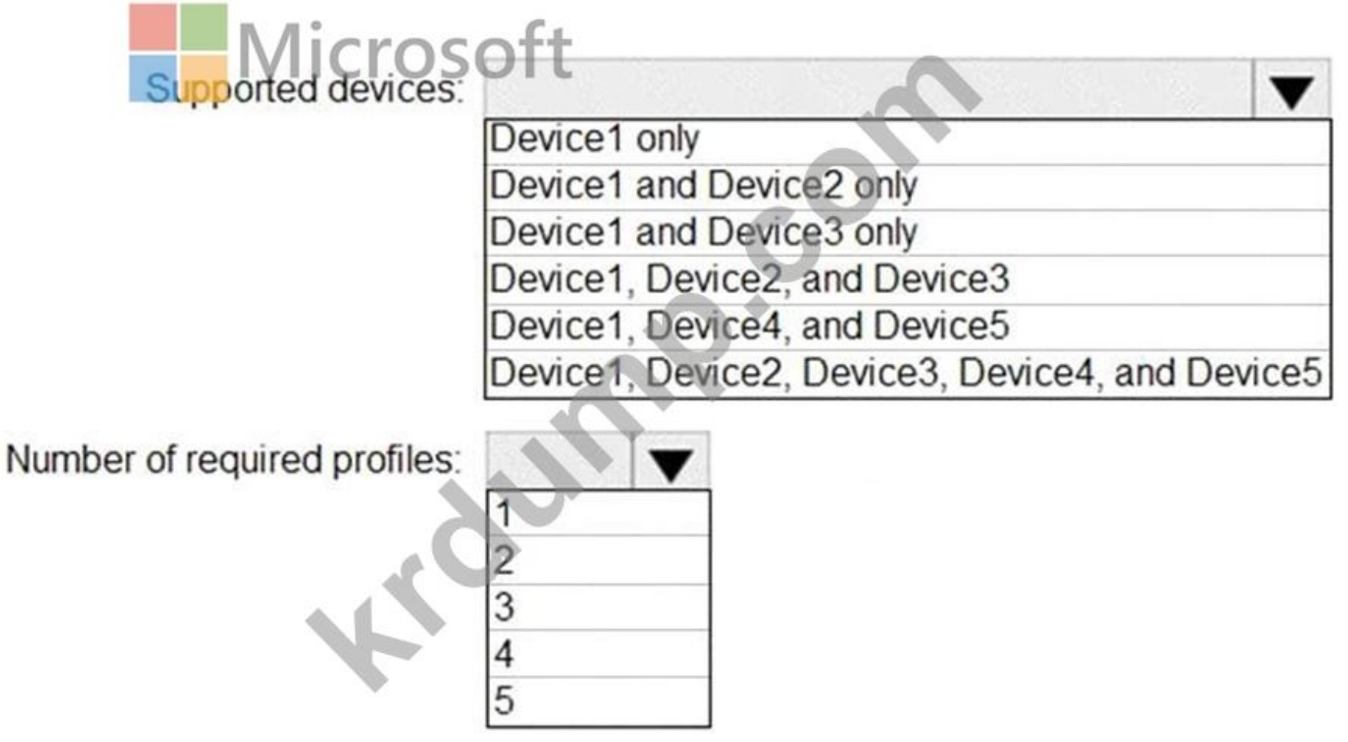
NEW QUESTION: 74
Microsoft 365 IS □□□ □□ □□□□ □□ Microsoft Defender□ □□□□ □□□□.
□□ □□□□ □□ □□□ □□ □□ □□□ □□□.

□□ □□□ □□□ □□ □ □□□?
A. □□ □□
B. □□ □□
C. OAuth □ □□
D. □□ □□
E. □□ □□
Answer: A (LEAVE A REPLY)

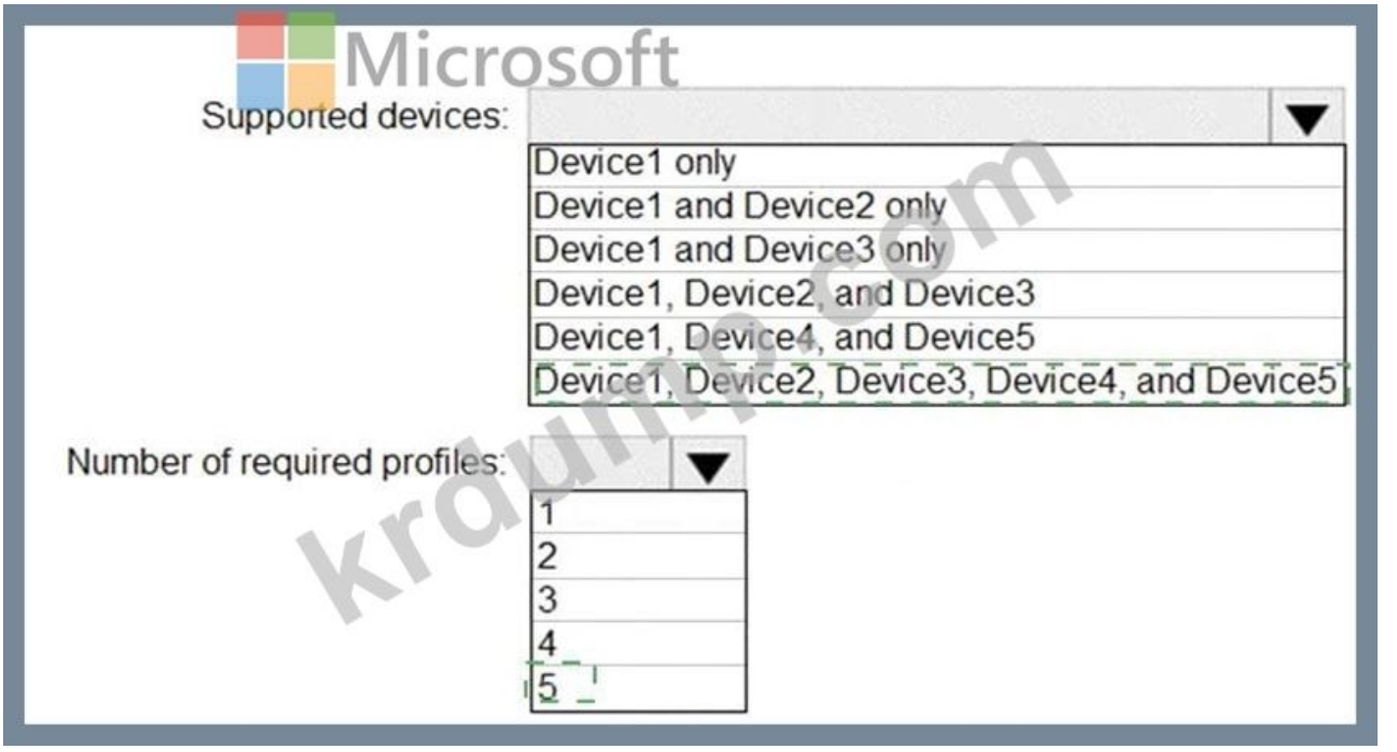
NEW QUESTION: 75
Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□□.
Microsoft Endpoint Manager □□ □□□□ □□□□ □□□□□ □□□ □□ □□□ □□, □□ □□ □□□ □□□□□□. □□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□ □ □ □□□?
A. 10
B. 30
C. 45
D. 90
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
□□□ □□ 3□□ □□ 1□□ □□□ □□□□. □□□ □□□ □□□□□.
□ □□□ Microsoft 365 □□□□ □□□□ □□ □□ □□□ □□□ □□□□□.
□□ □□□□ □□□□□□ □□ □□ □□□ □□□□□ □□ Microsoft 365 □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. Microsoft Intune □□ □□ □□□
B. Microsoft Intune □□ □□ □□
C. Microsoft Entra □□□ □□□
D. Microsoft Entra □□ □□
Answer: C (LEAVE A REPLY)

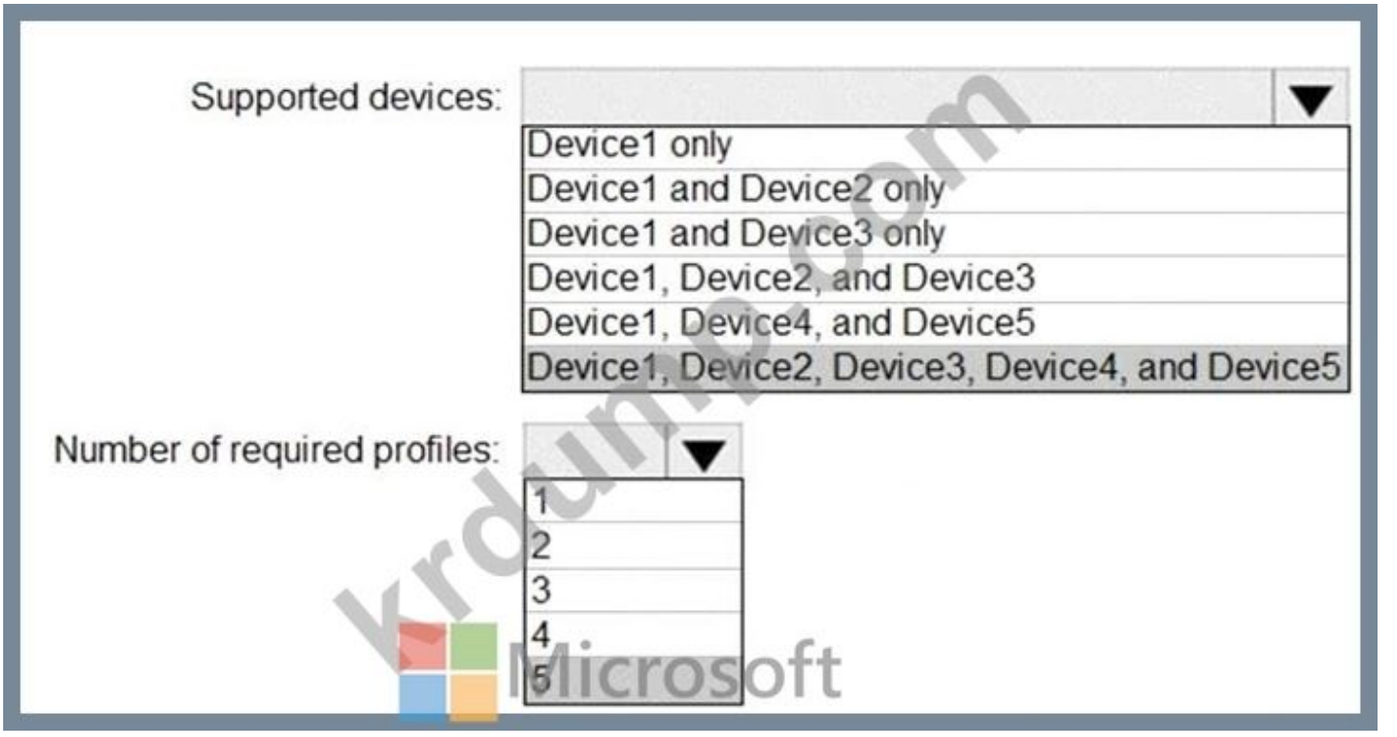
NEW QUESTION: 77
□□□ □□ □□□ □□□□ □□ □□□□□ □□ □□ □□ □□□□ □□□ □□□□□.
□□ □□□ □□□□, □□□ □□□ □□ □□□□ □□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

NEW QUESTION: 78

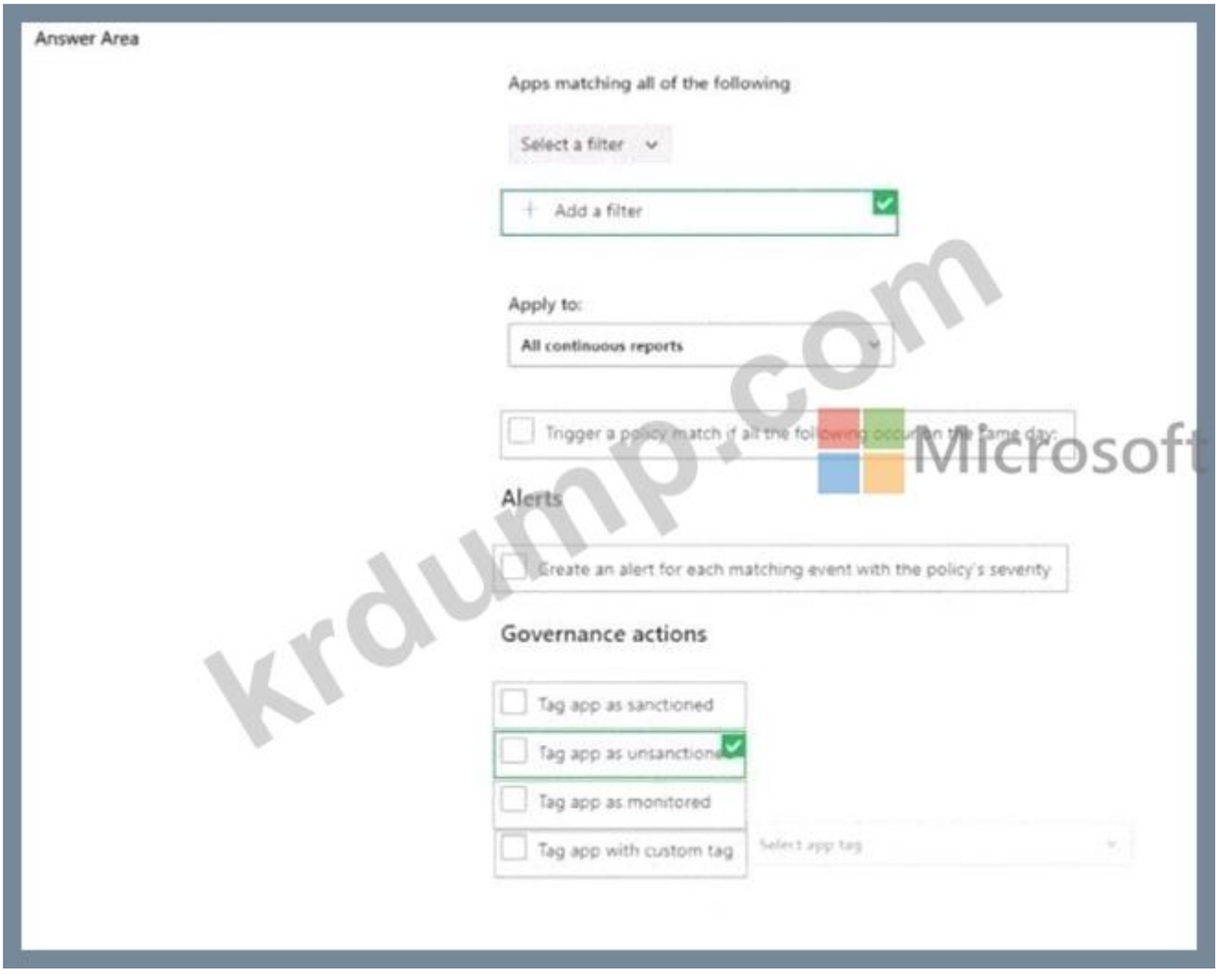
Microsoft 365 □□□ □□□□.

□□□□ □□ Microsoft Defender□ □□□□□□ Microsoft Defender□ □□□□□.

□□ □□□ 4□ □□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□ □□□.

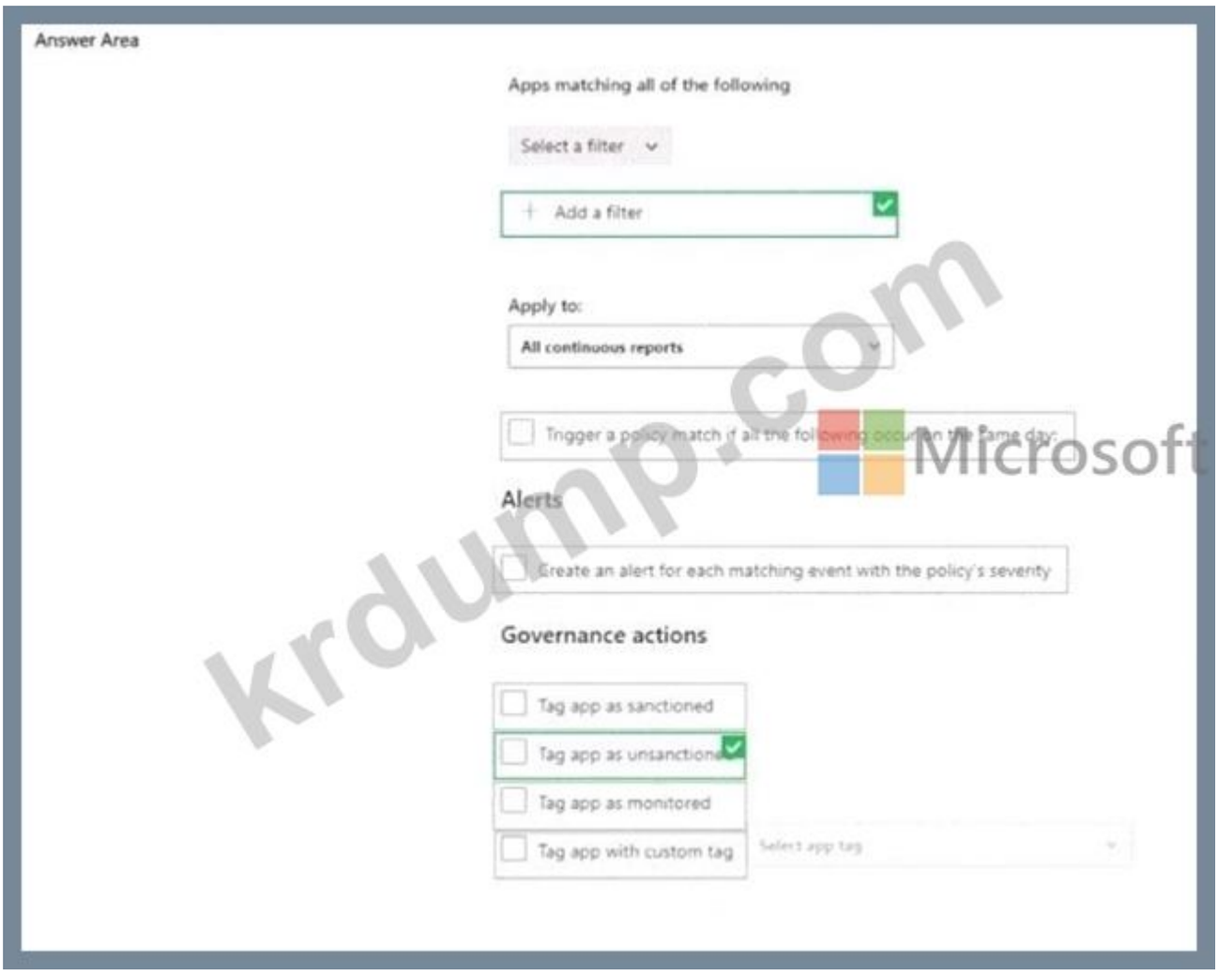
□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:



NEW QUESTION: 79
Microsoft 365 E5 □□□ □□□□.
□□□□ □□□ □□□ □□□□ □□□□ □ App1□□□ □□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□□.
□□□□ □□ □□□□□□ □□□□ □ □□□□ □□□ □□ □□ □□ □□□ □□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□□ □□
B. □□ □□ □□(MFA)
C. □□ □□
D. □□□ □□ □□
Answer: (SHOW ANSWER)

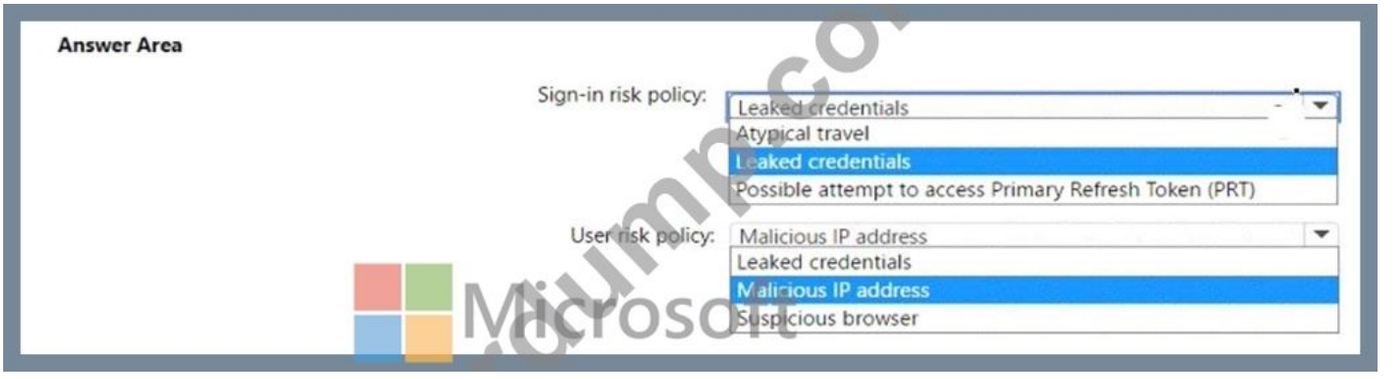
NEW QUESTION: 80
□□□□□ Azure Active Directory(Azure AD) □□□□ Microsoft Endpoint Configuration Manager □□□ □□□□.
□□ □□ □□□ □□ □□□□.

Name	Platform	Configuration
Device1	Windows 10	Hybrid joined to on-premises Active Directory and Azure AD only
Device2	Windows 10	Joined to Azure AD and enrolled in Configuration Manager only
Device3	Windows 10	Enrolled in Microsoft Endpoint Manager and has the Configuration Manager agent installed only

□□ □□□ □□□□ □□□□□.
□□ □□□□□□ □□□□ □□□ □□ □□□ □□□□ □□□ □□□□ □□□.
□□ □□□ □□□□ □□□?

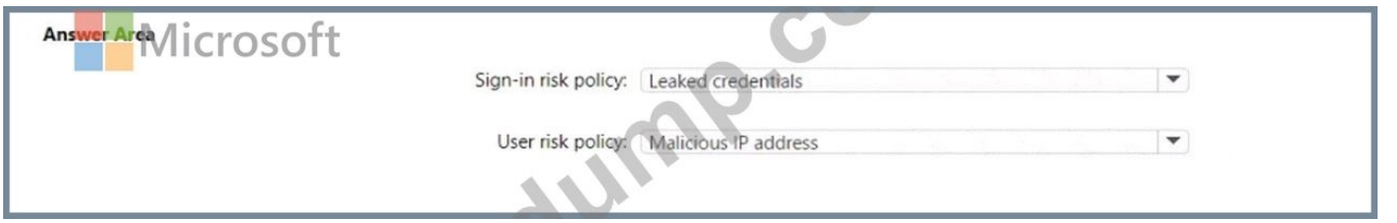
A. Device1, Device2, Device3
B. Device3□
C. Device2□
D. Device2□ Device3□
E. Device1□
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Microsoft 365 E5 □□□ □□□□.
□□□ □□ □□□ □□□ □□ □□□ □□□□ ID □□□ □□□ □□□□□. □ □□□□ □□ □□ □□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:



NEW QUESTION: 82

Microsoft 365 □□□ □□□□.

Enterprise Mobility + Security □□□□ □□ □□ □□□□ □□□ □□, CSV □□□□ □□□ □ □□ □□□□ □□□.

Microsoft 365 □□ □□□□ □□ □□□ □□□□ □□, □□ □□□ □□□□ □□□? □□□□ □ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 83

□□ □□□□ □□□□ □□□ □□□ □□□ □□ □□ □□ □□□ □□□ □ □□□ □□□□ □□□.

□□□ □□□ □□ □□ □□□□ □ □□□□?

A. 1

B. 4

C. 7

D. 31

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 84

Microsoft 365 □□□ □□□□.

□□□□ □ □□□ □□□ □□ ID□ □□□□. □□ ID□ 10□□ □□ □□ 10□□ □□□ □□ □□. □□□ □□ □□ ID□□□: 12-456-7890-abc-de-fghij.

□□ ID□ □□□ □□□□ □□□□ DLP(□□□ □□ □□) □□□ □□ □□□□□.

D18912E1457D5D1DDCBD40AB3BF70D5D

DLP □□□□ □□ ID□ □□□ □ □□□ □□□ □□□ □□□□ □□□?

A. □□□ □□ □□

B. □□□ □□□

C. □□ □□

D. □□ □□

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 85

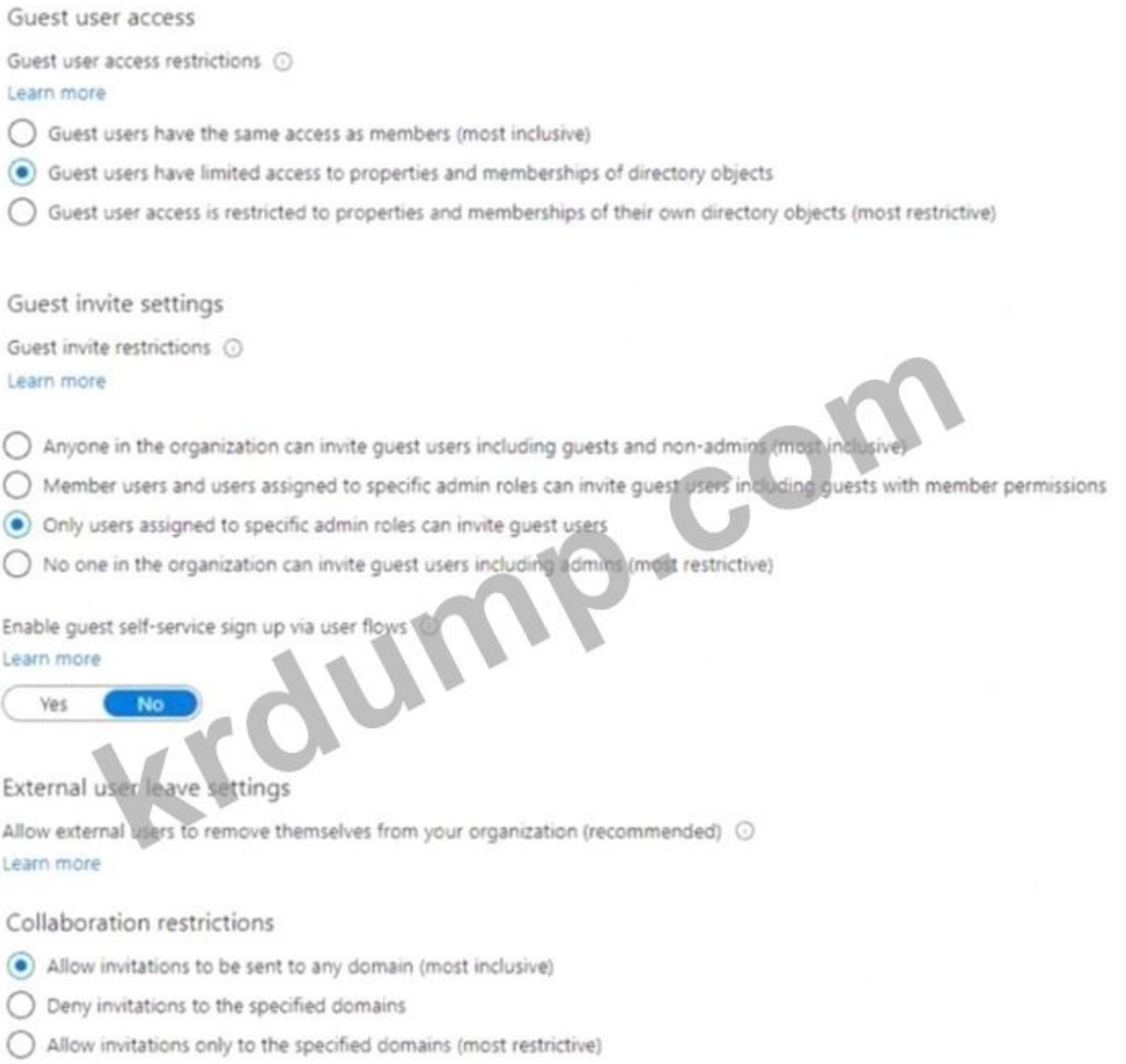
□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Azure AD□□ □□ □□ □□□ □□ □□□ □□ □□□□□.



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

NOTE: Each correct selection is worth one point.

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 86

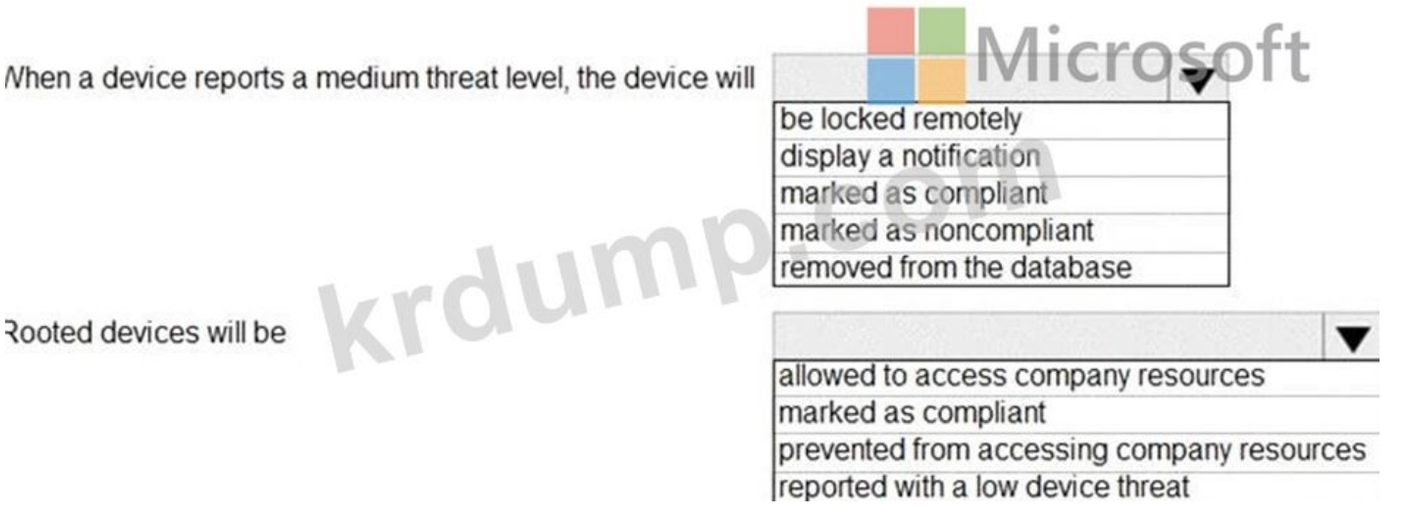
Microsoft 365 E5 □□□□ □□□□.

□□ □□ □□□ □□□ □□ □□ □□□ □□□□□.

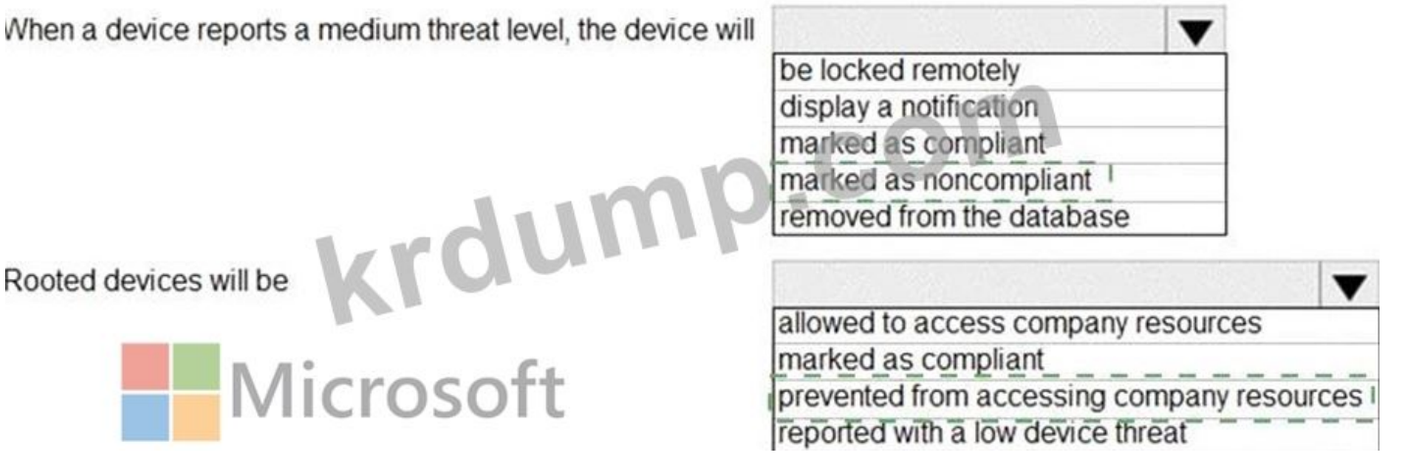

Compliance settings Edit
Microsoft Defender ATP
Require the device to be at or under the machine risk score:
Low
Device Health
Rooted devices
Block
Require the device to be at or under the Device Threat Level
System Security
Require a password to unlock mobile devices
Require
Required password type
Device default
Encryption of data storage on device.
Require
Block apps from unknown sources
Block
Actions for noncompliance Edit
Action
Schedule
Mark device noncompliant
Immediately
Retire the noncompliant device
Immediately

□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.

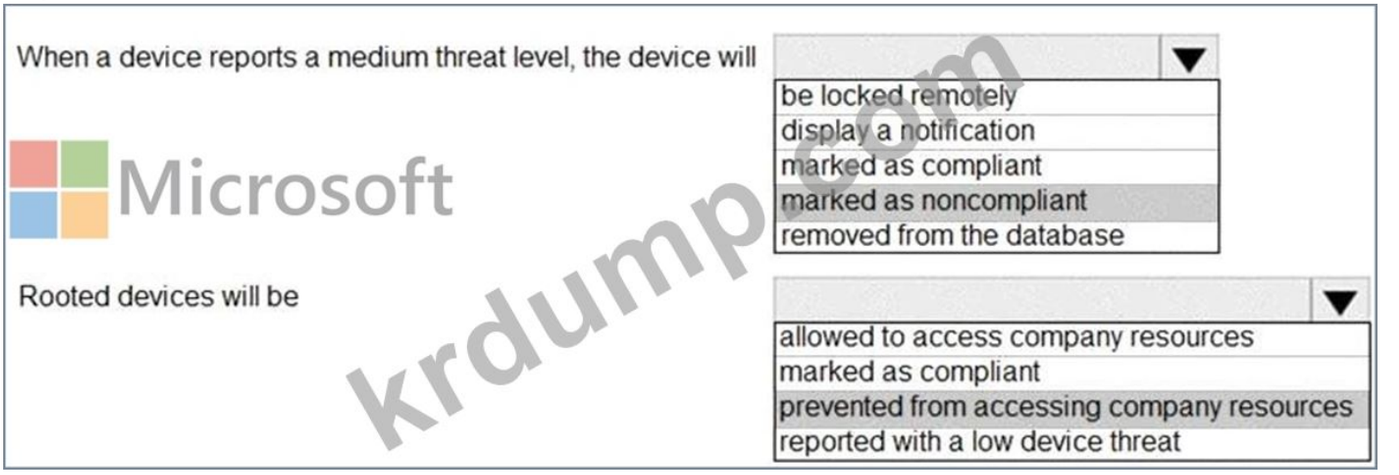
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android

NEW QUESTION: 87

□□□ DLP □□□ □□□□.

□□□ □□ □□□ □□□□□ □□□ □□□□ □□□.

□□□ □□ □□□?

A. Microsoft 365 □□ □□□□ □□ □□□ □□□□□.

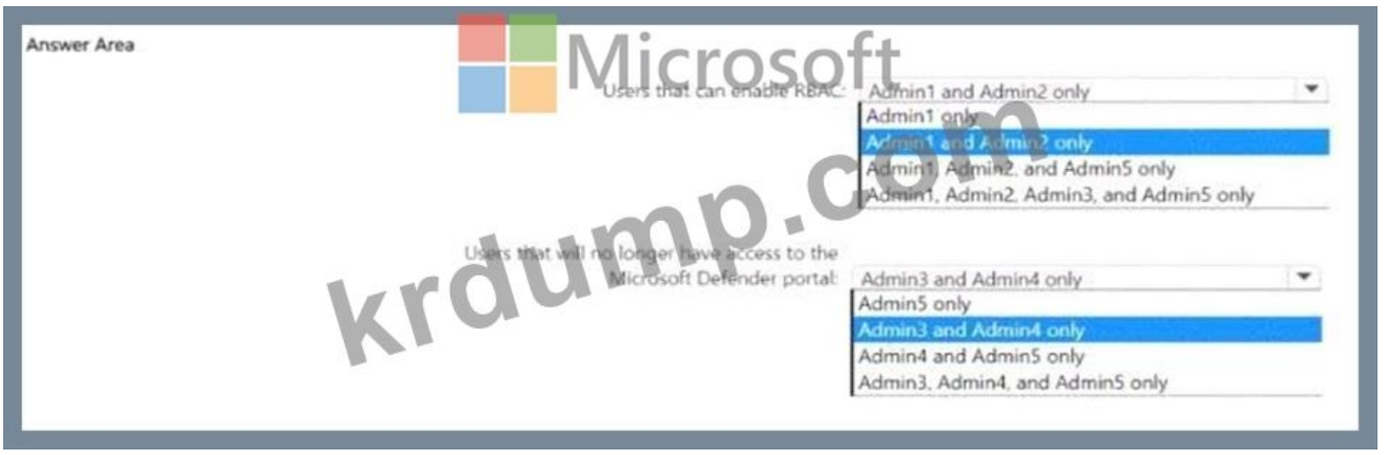
B. Microsoft Endpoint Manager □□ □□□□ □□□ □□ □□□ □□□□□.
C. Microsoft 365 □□ □□□□ □□□ □□□□ □□□□□.
D. Microsoft 365 □□ □□ □□□□ Endpoint DLP □□□ □□□□□.
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide

NEW QUESTION: 88
Microsoft 365 □□□ □□□□.
Adoption Score□ □□□□□ □□□□ □□□ □□ □□ □□ □ □□□□□ □□□□ □□ □ □ □□ □□□□ □□□.
□□□ □□ □□□?
A. □□ □□□□ □□□□□□.
B. □□ □□□ □□□□□.
C. □ □□□□ Microsoft 365 □□□□ □□ □□□□ □□□□□.
D. Endpoint □□□ □□□□□□.
Answer: D (LEAVE A REPLY)

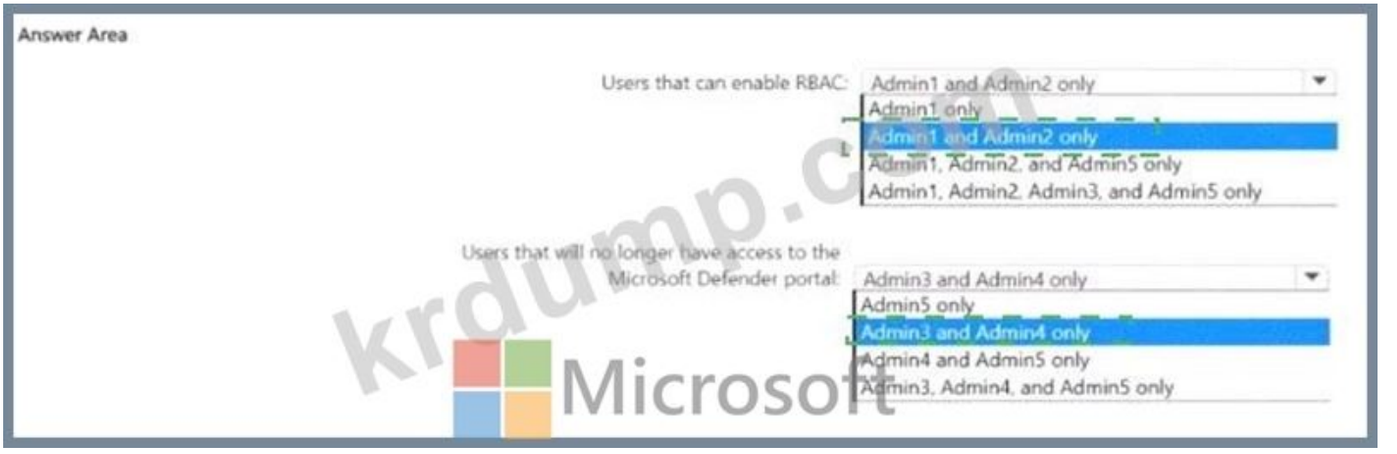
NEW QUESTION: 89
□□ □□ □□□ □□□ □□□ Microsoft 365 ES □□□ □□□□.

Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

Endpoint□ Microsoft Defender□ □□□□ □□□□.
Microsoft Defender □□□ □□ □□□□ □□□□□ □□ □□ □□□ □□(RBAC)□ □□□□ □ □□□.
□□ □□□□ RBAC□ □□□□ □ □□, □□ □□□□ RBAC□ □□□□ □ Microsoft Defender □□□ □ □□ □□□□ □ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □ □□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 90

Microsoft 365 Defender □□□□ □□□ □□□□ □□□□.

□□□ □□□ □□□ □□□□ □□□□□?

A. 30□

B. 60□

C. 3□□

D. 6□□

E. 12□□

Answer: C (LEAVE A REPLY)

Data retention information for Microsoft Defender for Office 365

By default, data across different features is retained for a maximum of 30 days. However, for some of the features, you can specify the retention period based on policy. See the following table for the different retention periods for each feature.

Defender for Office 365 Plan 1

* Alert metadata details (Microsoft Defender for Office alerts)

90 days.

Note: By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the top of the list so you can see it first.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention

NEW QUESTION: 91

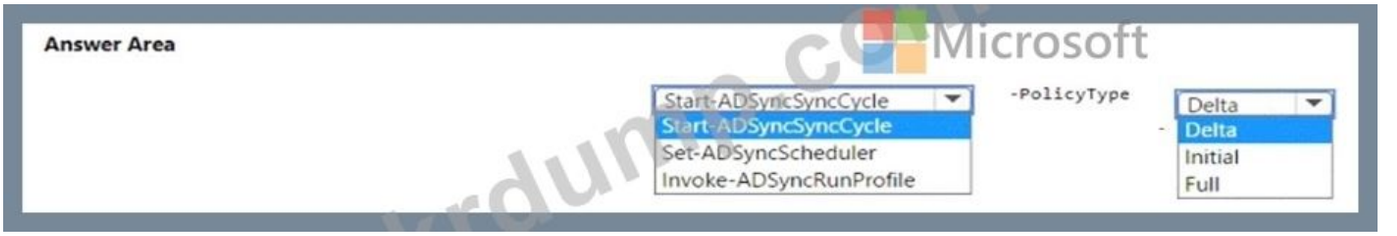
□□□□□□ Active Directory □□□□ Azure AD □□□□ □□□□ □□□□.

□□ □ 10,000□□ □□ □□□□ □□ □□□□ □□□□ □□□□□.

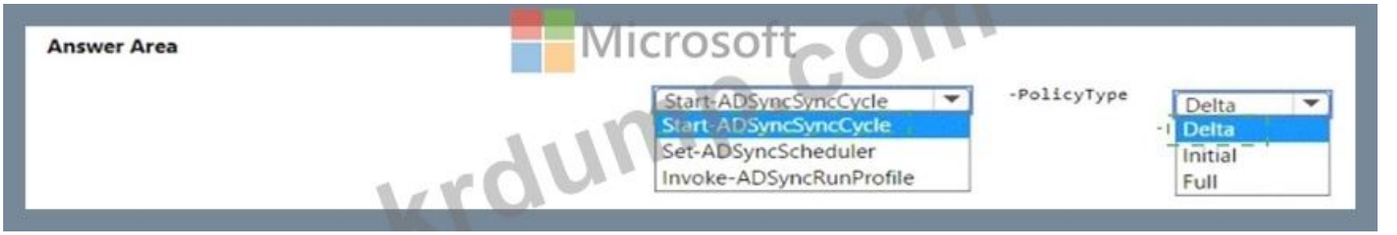
100□□ □□□ □□□ □□□ □□□□ □□□□□.

□□□ □□□ □□□ □□□ □ □□ Azure AD□ □□□□□□ □□□□ □□□.

□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.



Answer:



Explanation:

NEW QUESTION: 92
Microsoft Defender XDR□ □□□□ Microsoft 365 □□□ □□□□.
Microsoft Defender □□□ □□ □□□□ □□□ □□□ ' □□□ □□ □□□ □□ □□ □□'□ □□□□□.
□□□ □□ □□□ □□□□□□ □□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□ □□□ □□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. □□ □□□ □□ □□□ □□□ □□□□□.
B. \program files (X86) \" □□□□ □□□ □□□□ □□□ □□□□ □□□□□.
C. \windows\ □□□□ □□□ □□□□ □□□ □□□□ □□□□□.
D. \users\"\downloads\" □□□□ □□□ □□□□ □□□ □□□□ □□□□□.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 93
Contoso.com□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.
Contoso□ ID □□□□□ □□ Microsoft Defender□ □□□□.
□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□□ □□□□□ Defender□ □□□ □□□□ □□□.
□□□: User1□□ ID □□ □□□ □□ Defender□ □□□□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
Microsoft 365 E5 □□□ □□ Microsoft Defender for Endpoint□ □□□□□. □□□□ □□□ □ □□ □□□ □□□□□.

Name	Platform
Device1	Windows 11
Device2	Android
Device3	Linux

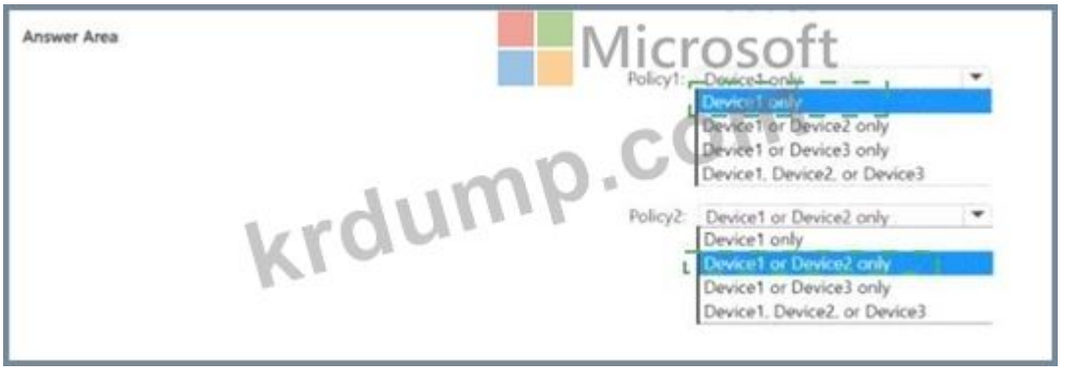
□□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□.

Name	Template
Policy1	Microsoft Defender Antivirus
Policy2	Device Control

□ □□□ □□ □□□ □□□ □ □□□□? □□□□ □□□ □□□ □□□ □□□□□□. a. □ □: □ □□□ 1□□□□.

Answer Area

Answer:



Explanation:

NEW QUESTION: 95

Microsoft 365 □□□ □□□□.

□□ □□□ □□ □□□ □□ □□□□.

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

□ □□ □□ File1.docx□□ □□□ □□□ Site1□□□ Microsoft SharePoint □□□□ □□□□ □.

File1.docx□ 2022□ 1□ 1□□ □□□□□ □□□□□ 2022□ 1□ 31□□ □□□□□□□. □ □ □□ □□ □□□□ □□□□□.

File1.docx□ □□ □□□□ □□□□□?

A. 2023□ 1□ 1□

B. 2024□ 1□ 1□

C. 2023□ 1□ 31□

D. 2024□ 1□ 31□

E. □□ □□

Answer: D (LEAVE A REPLY)

Retention wins over deletion.

Note:

Explanation for the four different principles:

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

2. Etc.

Reference:

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

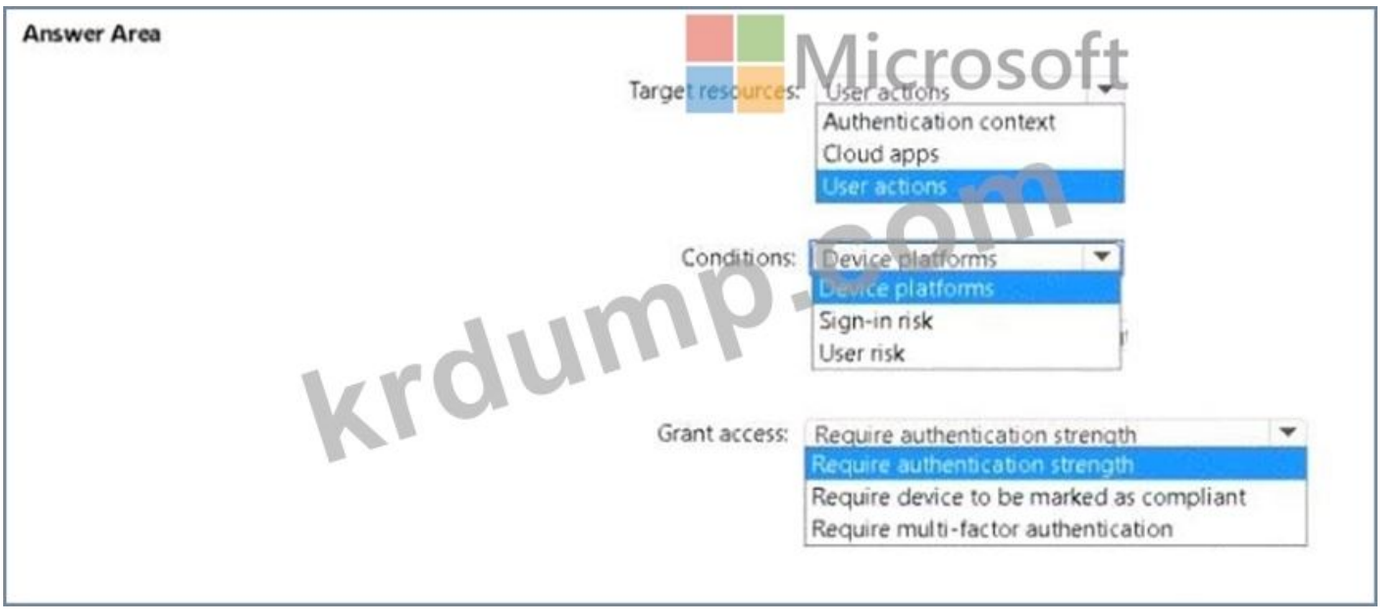
NEW QUESTION: 96

Microsoft 365 E5 □□□ □□□□.

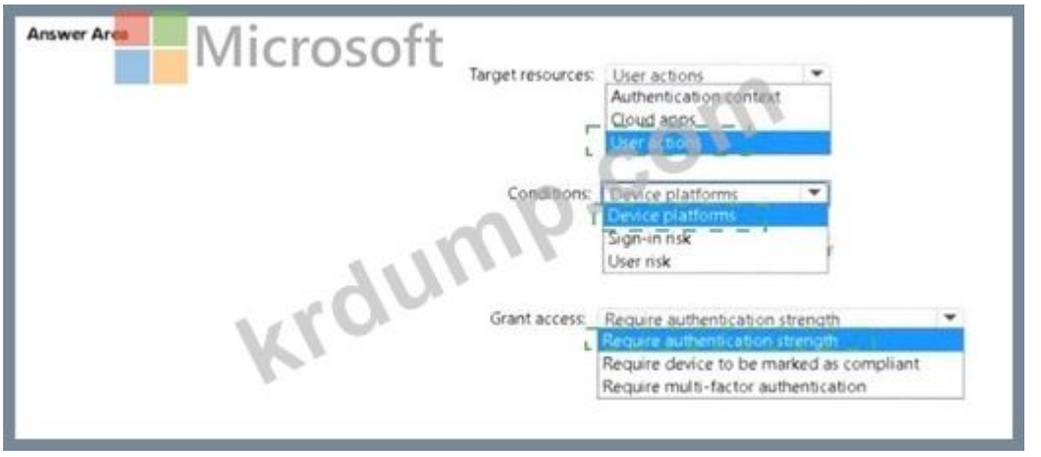
□□□□ Windows □□□ Microsoft Entra ID□ □□□ □□ FID02 □□ □□ □□□□□ □□□ □ □□□ □□□ □□□ □□□□ □□□.

□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□ □□: □□□ □□□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 97

□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.

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

□□ □□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□□ □ □□□□?

A. Mailbox1□ Site1□

B. Mailbox1, Account1, Site1□

C. Account1□ Site1□

D. Mailbox1, Account1, Site1, Channel1

E. Account1, Site1, Channel1□

Answer: (SHOW ANSWER)

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

NEW QUESTION: 98

Microsoft E5 □□□ □□□□.

Microsoft Exchange Online□ □□□□ □□ □□□□□ □ □□ 5□□ □□ Exchange □□□ □ □□ □□□□□ □□ □□□.

□□□ □□□□ □□□?

A. Azure AD □□ □□ ID □□(PIM)

B. □□□ □□□ □□

C. □□□□□□ □□ □□)

D. Azure AD ID □□

E. □□ □□□□ □□ □□

Answer: A (LEAVE A REPLY)

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

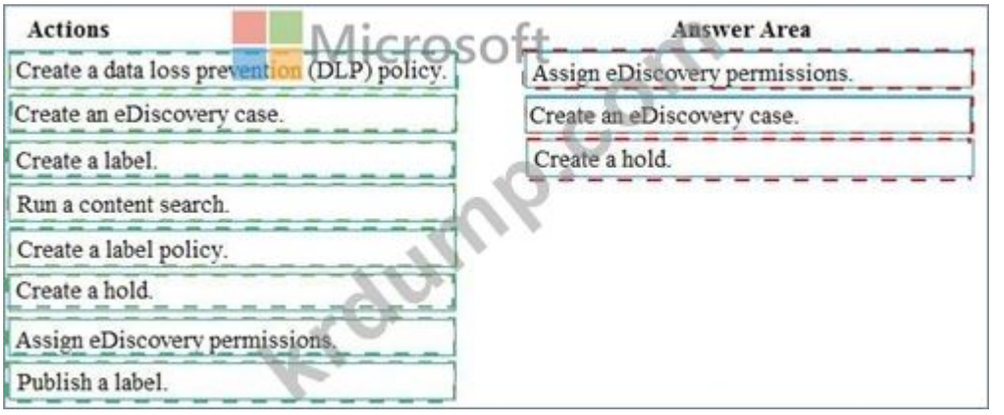
NEW QUESTION: 99

□□□□ □□ □□□ □□□□ □□□.

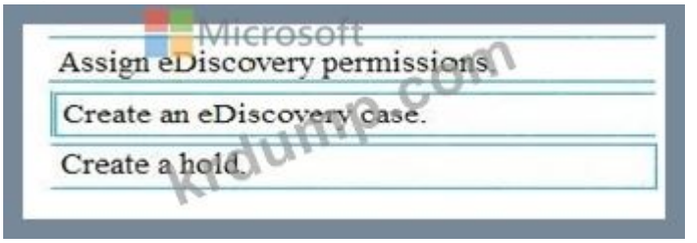
□□ □ □□ □□ □□ □□□□ □□□□ □□□□ □□ □ □□ □□□ □□□□□? □□□□□ □□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□ □□□ □□□□□.

Actions	Answer Area
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Answer:



Explanation:



References:

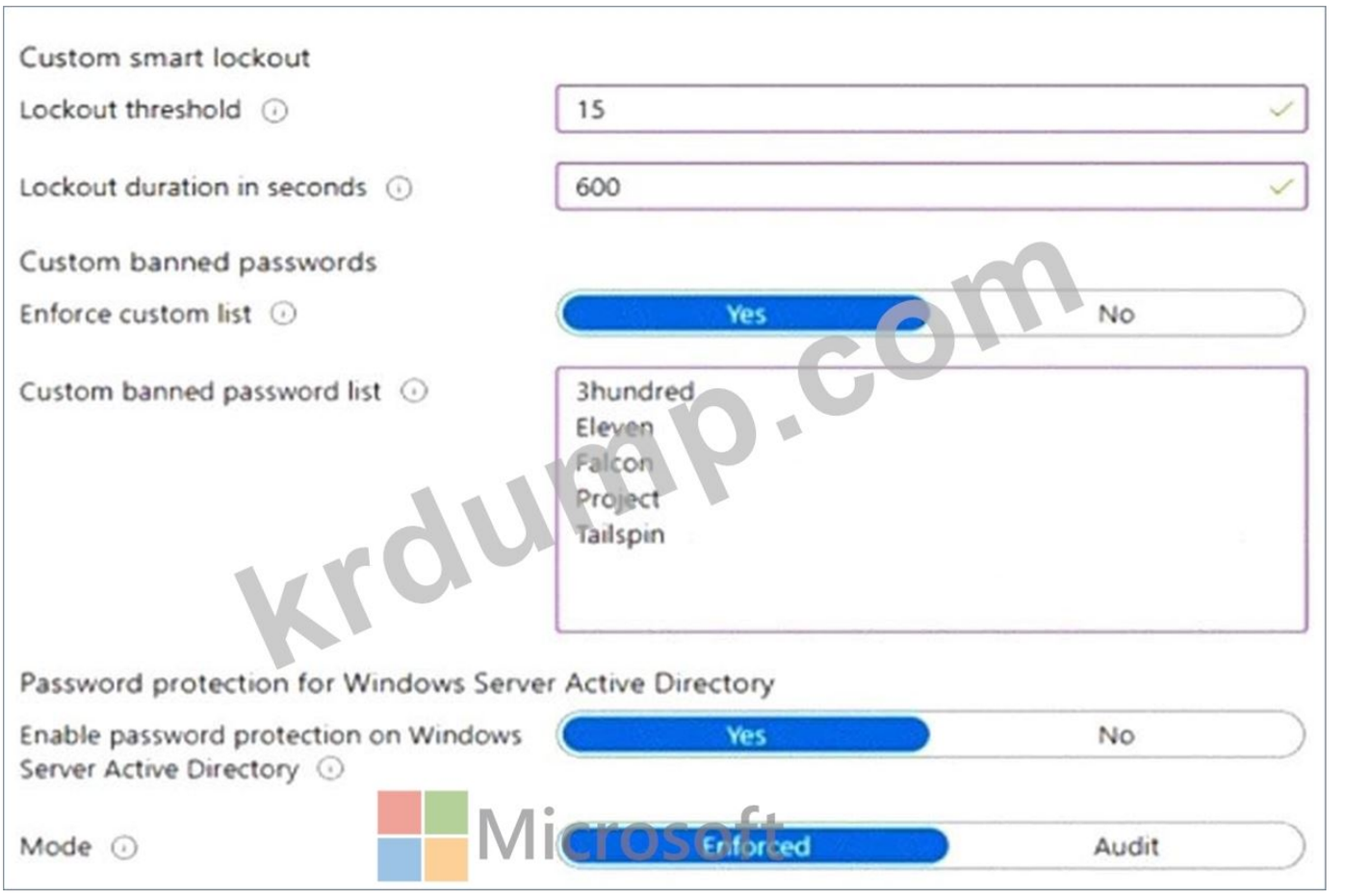
https://www.sherweb.com/blog/ediscovery-office-365/

NEW QUESTION: 100

□□□

User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Azure AD □□ □□□ □□ □□□ □□ □□□□□.



User1□ □□□ □□□□□ □□ □□□□□ □□□□□□□ □□□□□.

* □□

* □□□□22

* T4il$pin45dg4

□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

[Answer choice] will be accepted as a password.

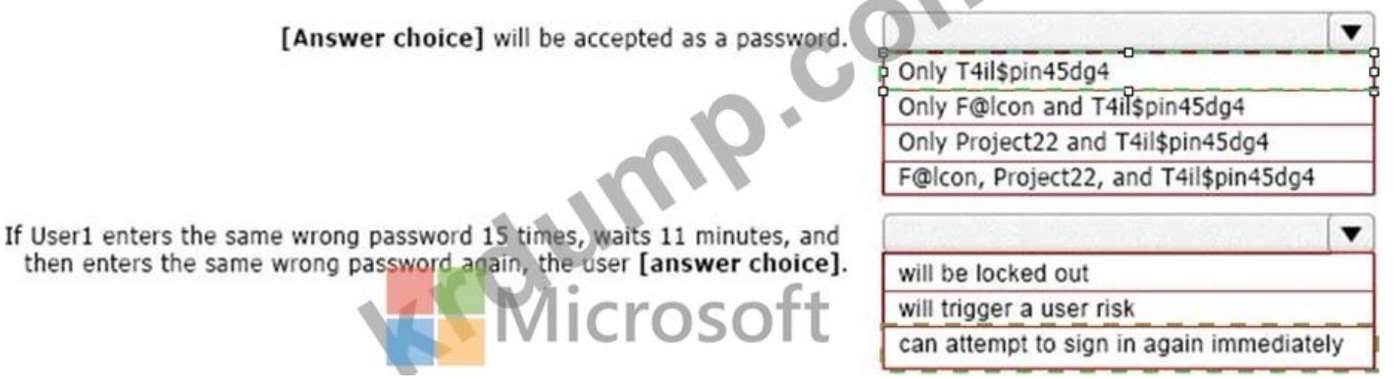
- Only T4il$pin45dg4
- Only F@lcon and T4il$pin45dg4
- Only Project22 and T4il$pin45dg4
- F@lcon, Project22, and T4il$pin45dg4

If User1 enters the same wrong password 15 times, waits 11 minutes, and then enters the same wrong password again, the user **[answer choice]**.

- will be locked out
- will trigger a user risk
- can attempt to sign in again immediately

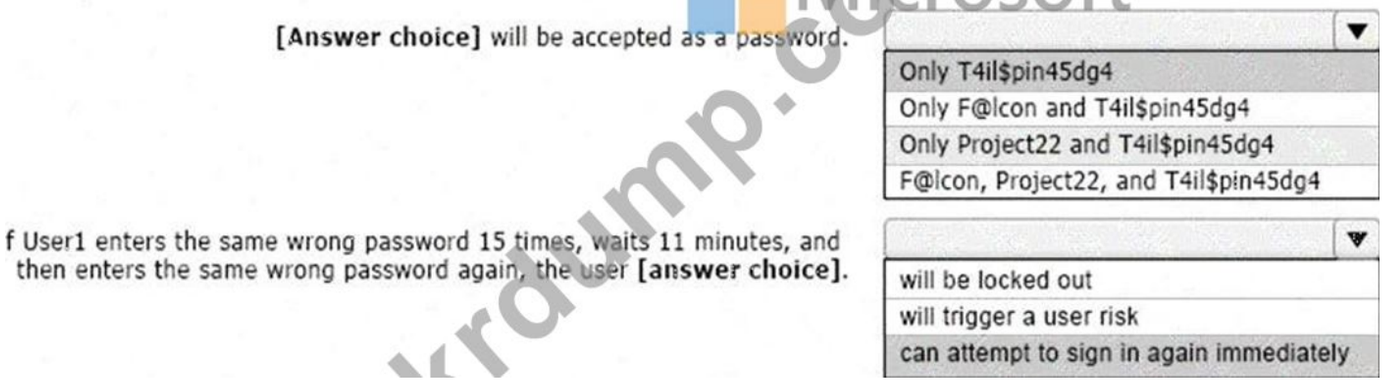
Answer:

Answer Area



Explanation:

Answer Area



Box 1: Only T4il$pin45dg4

Box 2: can attempt to sign in immediately

Note: Manage Azure AD smart lockout values

Based on your organizational requirements, you can customize the Azure AD smart lockout values.

Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users. Customization of the smart lockout settings is not available for Azure China 21Vianet tenants.

To check or modify the smart lockout values for your organization, complete the following steps:

* Sign in to the Entra portal.
* Search for and select Azure Active Directory, then select Security > Authentication methods > Password protection.
* Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.
* The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.
* Set the Lockout duration in seconds, to the length in seconds of each lockout.
* The default is 60 seconds (one minute).

If the first sign-in after a lockout period has expired also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

NEW QUESTION: 101

□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.

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

□□ □□□ □□□□□.

Microsoft Store for Business□□ □□ □□□□ □□□□□.

App1□□□ □□ □□ □□□□ □□□□□.

App1□ □□ □□□ □□□□ □□ □□□□ □□□ □□, Group3□ □□□□□.

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

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.	○	○

Answer:

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.	○	○

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.	○	○

Reference:
https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store-for-business#private-store-availability

NEW QUESTION: 102
□□□□ contoso.com□□□ Azure AD □□□□ □□□□ Microsoft 365 □□□ □□□□. □□ □□□ □□ □□ □□□ □□□□ □□□□□.

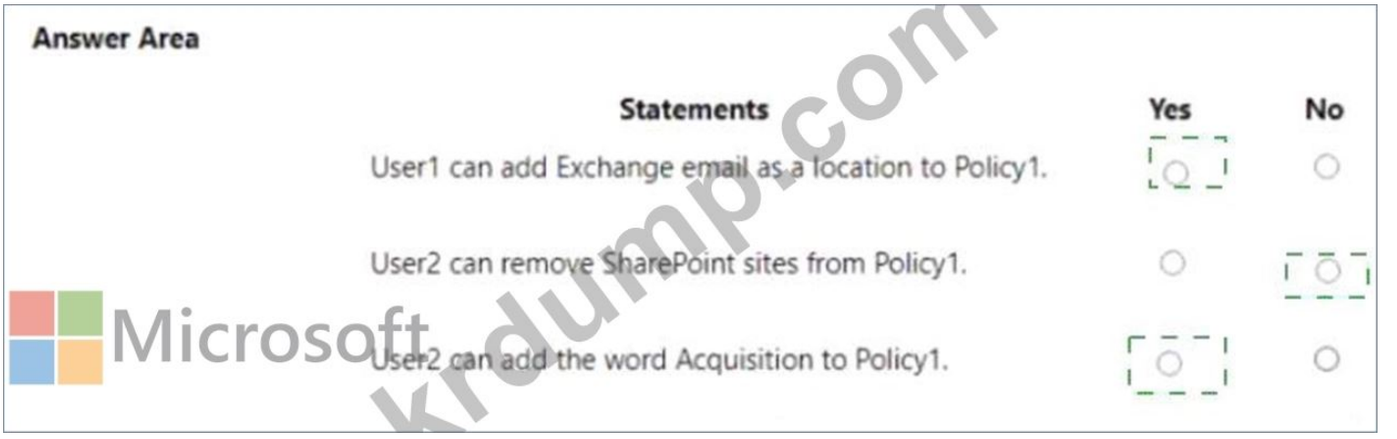
Name	Role	Office 365 role group
User1	*None*	Compliance Data Administrator
User2	Global Administrator	*None*

□□ □□□ □□ □□□ 1□□□ □□ □□□□ □□□□.
* 5□□ □□□ □□
* 5□ □□ □ □□ □□□□ □□□□ □□□□□.
Policy1□□□ □□□ □□□□ Label1□ □□ □□ □□□ □□□ □□□. Policy1□□ □□□ □ □ □□□ □□□□.
* Merger□□ □□□ □□□ □□□□ □□□□□.
* OneDrive □□ □ SharePoint □□□ □□□ □□□□□.
□□ □□□ □□□□□.
Set-RetentionConpliancePolicy Policy1 -RestrictiveRetention Strue -Force □□ □ □□□ □□ □ □□ □□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:



Explanation:

NEW QUESTION: 103

Office 365□ Microsoft Defender□ □□□□ Microsoft 365 □□□ □□□ Mailbox1□□□ □□□ □ □□□□.

Mailbox1□ □□□□ □□□□□ □□ □□□ □□□□ □□□□ □□□ □□□□□.

Defender for Office 365□ Mailbox1□ □□□ □□ □□ □□□□ □□ □□□ □□□ □□□ □□ □ □□ □□□.

□□□ □□ □□□?

A. Mailbox1□ □□ □□□ □□□□□.

B. Mailbox!□ SecOps □□□□□ □□□□□.

C. Mailbox1□ □□ □□ □□□ □□□□□.

D. □□ □□ □□□ □□□□.

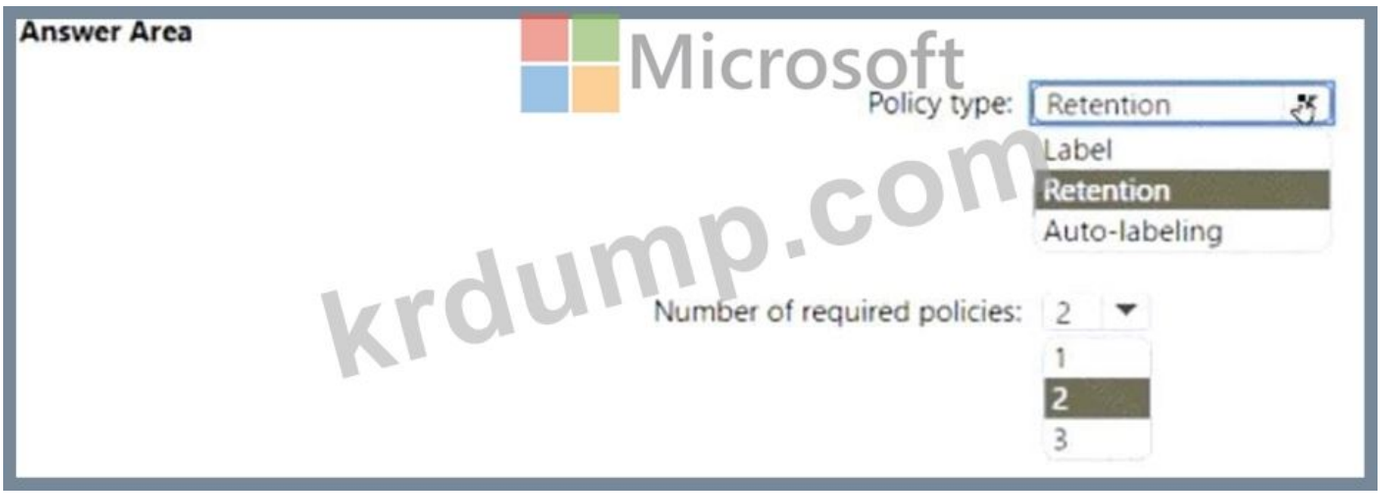
Answer: A (LEAVE A REPLY)

NEW QUESTION: 104

□□□ □□ □□□ □□□□□ □□ □□□□ □□□ □□□□ □□□.

□□ □□□ □□□ □□□□ □□, □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

NEW QUESTION: 105

□□□ □□□□ Microsoft 365 E5 □□□□ □□□□.

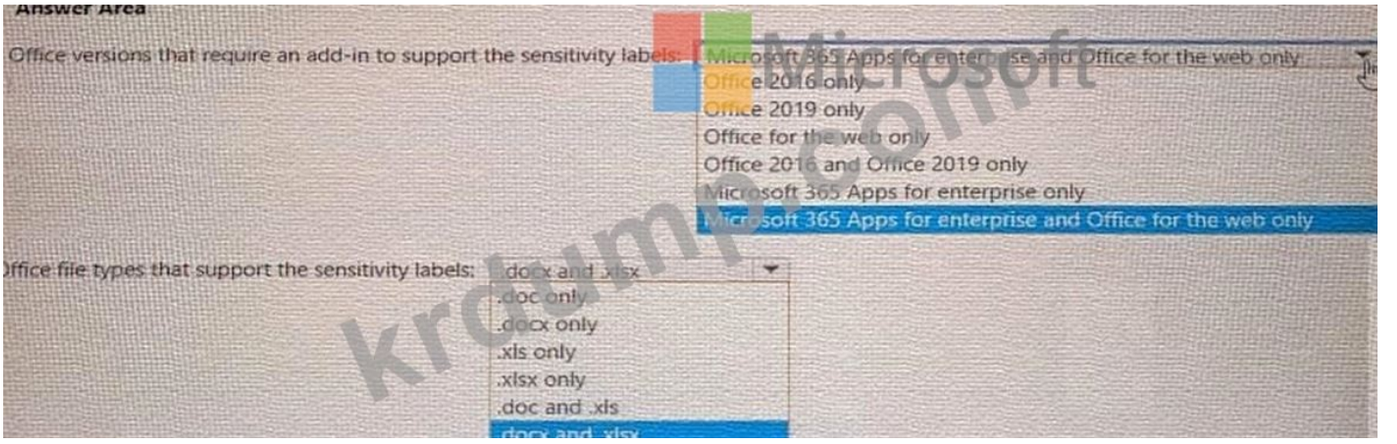
□□ □□□□ □□ □□□ Microsoft Office□ □□□□□.

* □□□ Microsoft 365 □
* □□ Office
* □□□ 2016
* □□□ 2019

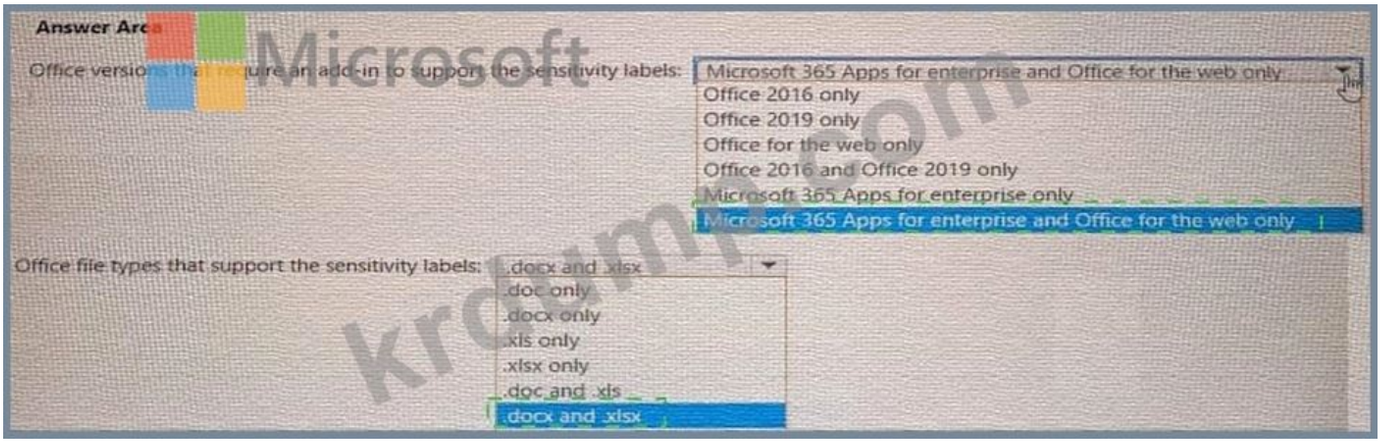
□□ □□□□□ □□□ □□ Office □□ □□□ □□□□□.

* .docx
* .xlsx
* .□□

* □□
□□□ □□□□ □□□ □□□□□. □□□ □□□□ □□□.
* □□□ □□□□ □□□□ □□ □□ □□□ □□□ Office □□□ □□□□□?
* □□□ □□□ □□□□ □□ □□□ □□□□□?
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □ □□□ 1 □□□□.



Answer:



Explanation:

NEW QUESTION: 106
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1, Group2	Enabled
User3	Group2	Disabled

□□ □□□ □□□ □□ □□ □□ □□ □□□ □□□□□.
* □□ :
* □□ : Group1
* □□ : Group2
* □□□ : Microsoft Entra ID □□ □□ □□ □□

* □□ □□: □□□□
□□ □□□ □□□ □□□ □□□ □□□ □□□□.
* □□ : Policy1
* □□ :
* □□ : Group1
* □□; □□1
* □□: □□ □□ □□ □□
* □□□ □□□□□□. □□
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□□ □ □□ 1□□□□.

Answer Area

Answer:

Explanation:
User1 will be required to register for MFA on the next sign-in: YesUser1 is a member of Group1, which is included in the MFA registration policy. Since User1 is not excluded, they will be required to register for MFA on the next sign-in.
User2 will be required to register for MFA on the next sign-in: NoUser2 is a member of both Group1 and Group2. Since Group2 is excluded from the MFA registration policy, User2 will not be required to register for MFA.
User3 will be required to register for MFA on the next sign-in: NoUser3 is a member of Group2, which is excluded from the MFA registration policy. Therefore, User3 will not be required to register for MFA.

NEW QUESTION: 107

□□□

□□□□□ 100□□ □□□□ □□ □□ □□□□□ LDAP □□□□□ □□□□□.

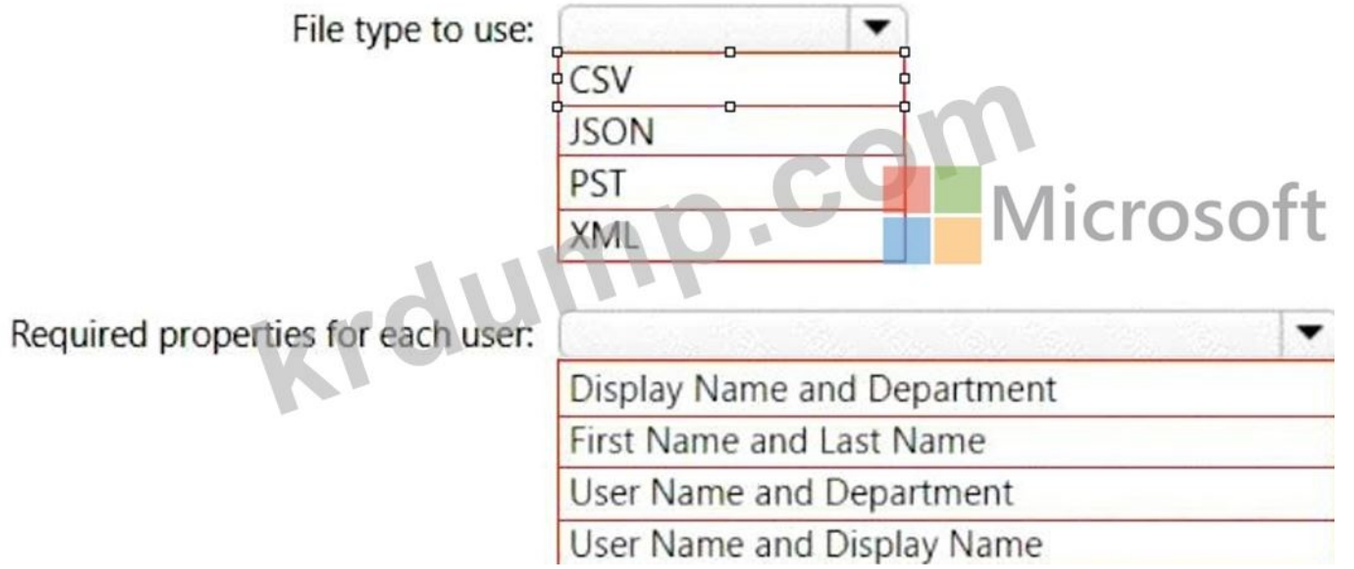
□□□ Microsoft 365 □□□ □□□□□.

Microsoft 365 □□ □□□ □□□□ 100□□ □□□□ Microsoft 365□ □□□□ □□□.

□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □ □□ □□□□□.

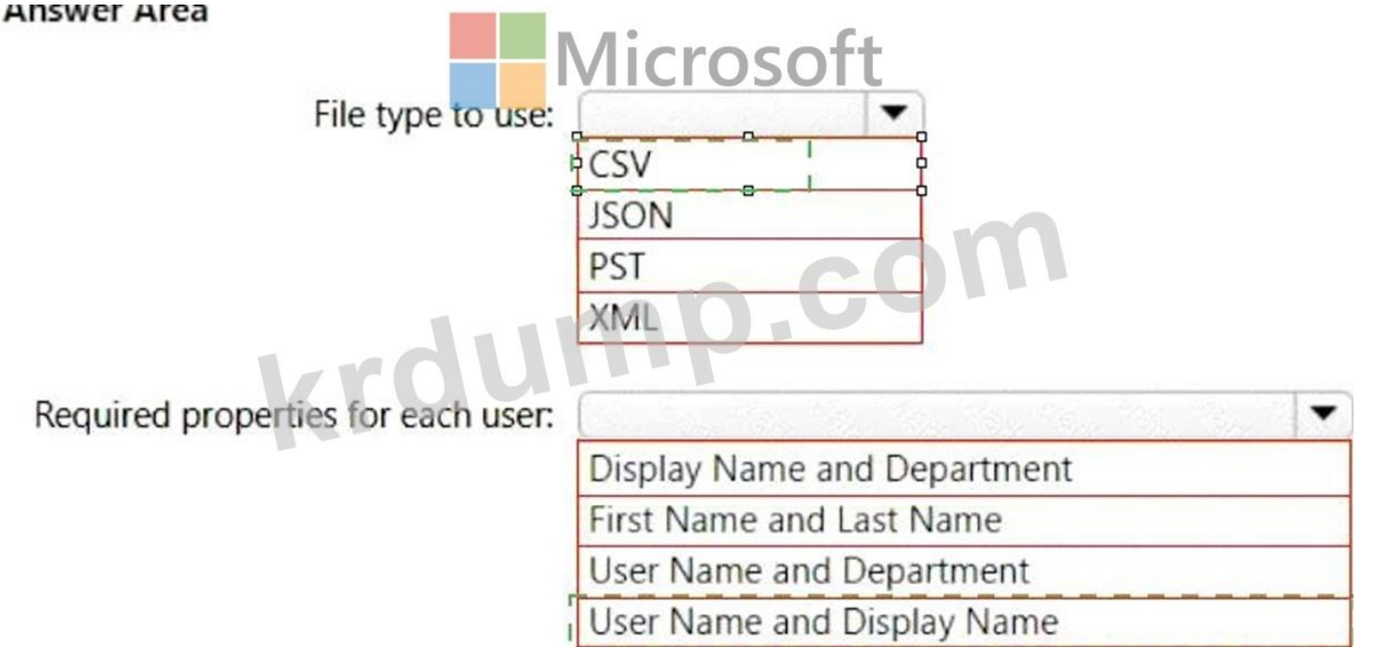
□□□□: □□ □□□ 1□□□□.

Answer Area



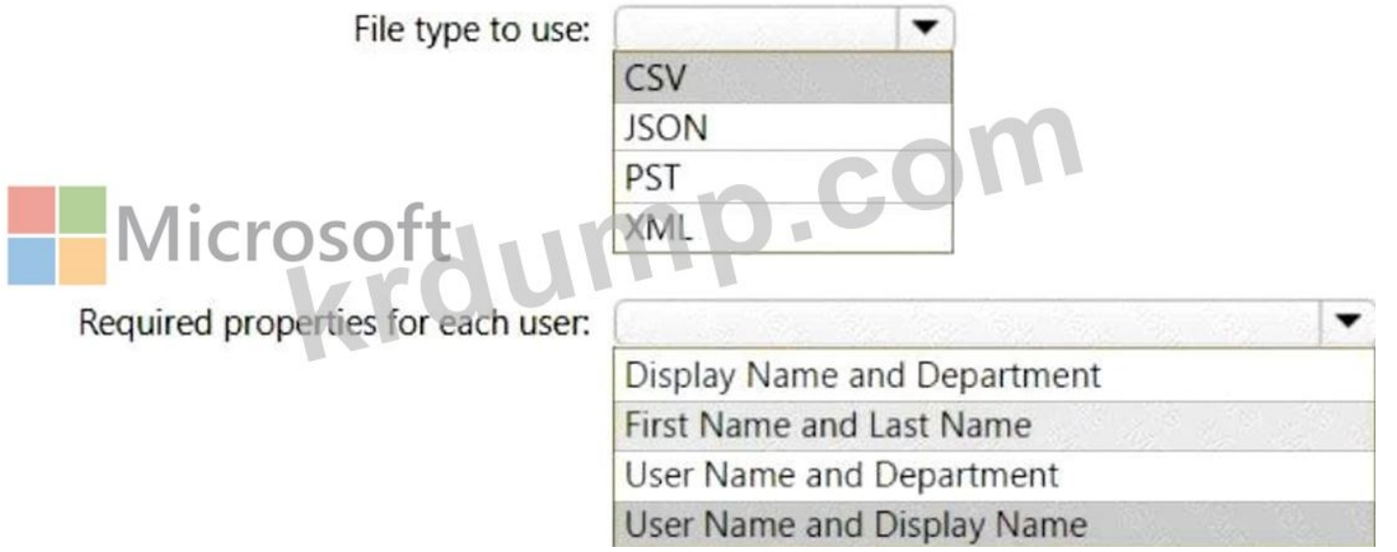
Answer:

Answer Area



Explanation:

Answer Area



Box 1: CSV

Add multiple users in the Microsoft 365 admin center

* Sign in to Microsoft 365 with your work or school account.
* In the admin center, choose Users > Active users.
* Select Add multiple users.
* On the Import multiple users panel, you can optionally download a sample CSV file with or without sample data filled in.
* Etc.

Note: More information about how to add users to Microsoft 365

Not sure what CSV format is?

A CSV file is a file with comma separated values. You can create or edit a file like this with any text editor or spreadsheet program, such as Excel.

Box 2: User Name and Display Name

What if I don't have all the information required for each user? The user name and display name are required, and you cannot add a new user without this information. If you don't have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.

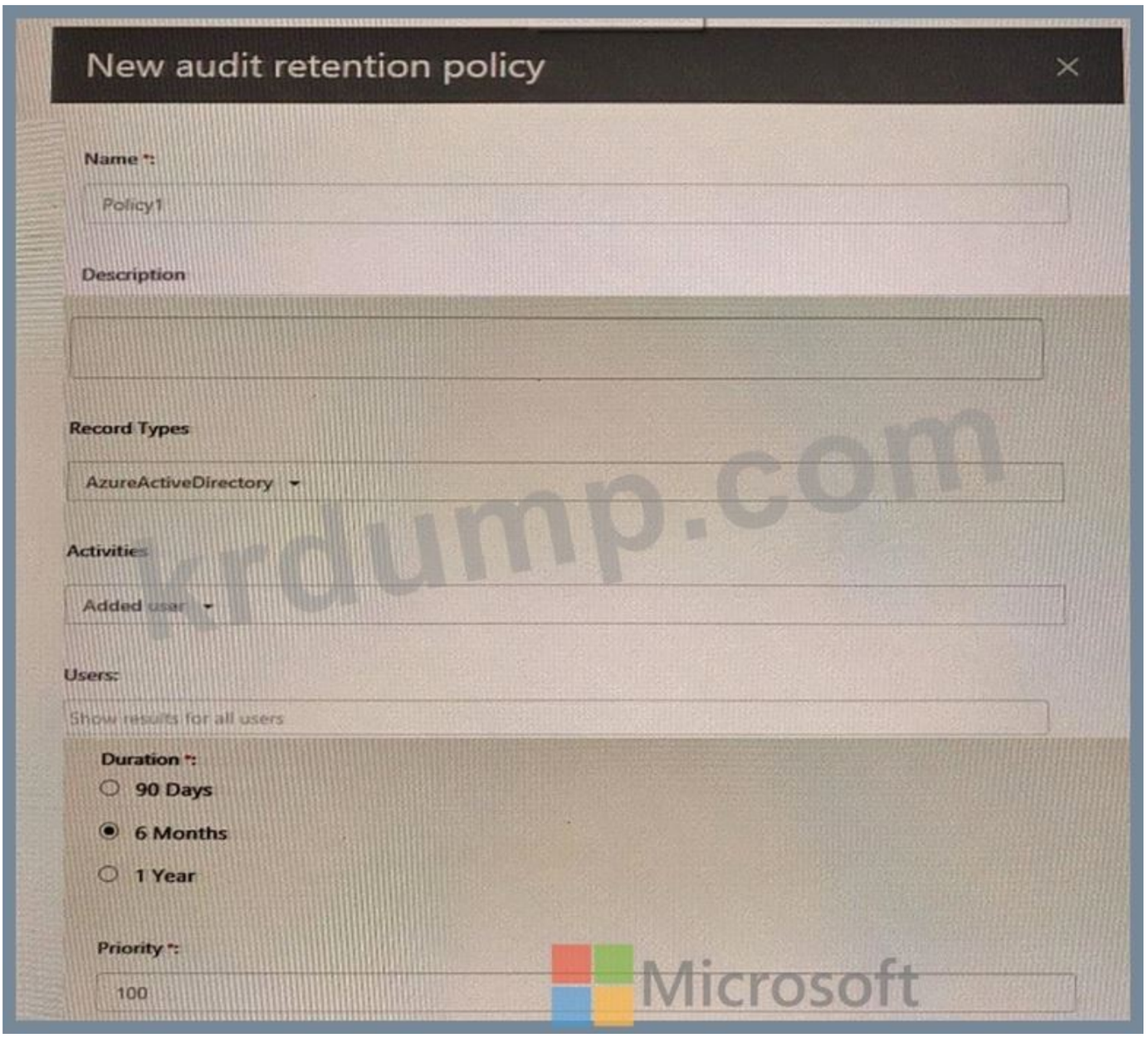
Reference:

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

NEW QUESTION: 108

□□□ □□ Microsoft 365 E5 □□□ □□□□. □□□□ □□ □□ □□□ □□□□ □□□□ □ □□□.

Name	License
Admin1	Microsoft Office 365 E5
Admin2	*None*



User1□□□ □□□ □□□ □□□□ □□ □□□□□.

Admin1 □□ Admin2□ User1□ □□□□ □□□ □□ □□ □□□□ □□□ □□ □□□ □ □□ □□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□ □□□ 1□□ □□□□□.

Answer:

NEW QUESTION: 109

Microsoft 365 E5 □□□ □□□□.

□□ □□□□ □□□□ contoso.com□□□ Azure AD □□□□ □□□□.

* □□□1
* □□□2
* □□□1

Contoso.com□□ □□ □□□ □□ AIM□□□ □□ □□□ □□□□. User1□ AU1□ □□□□ □. □□□ □□ □□□ □□ AU2□□ □□ □□□ □□□□. □□ □ □□□ □□ □□□ □□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

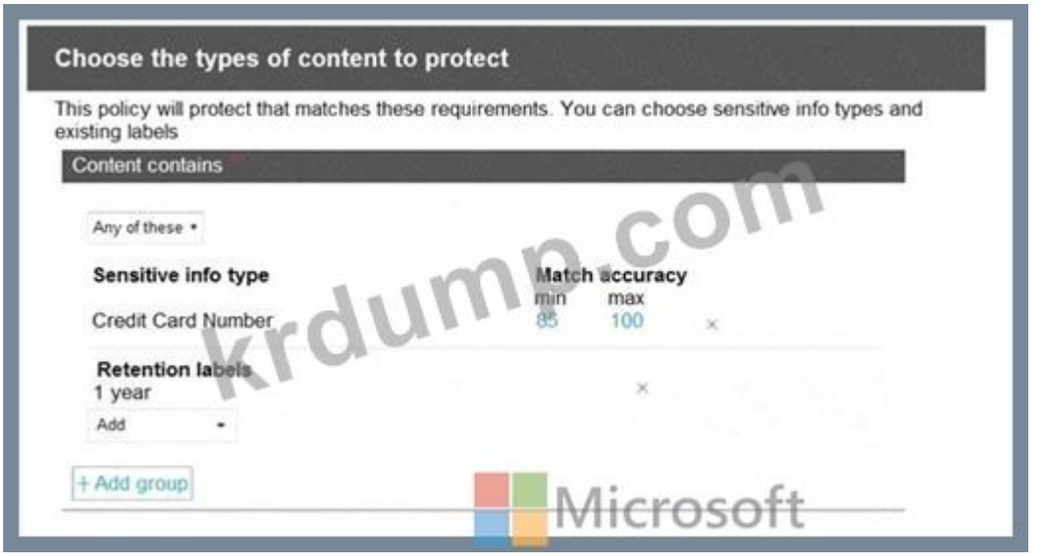
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

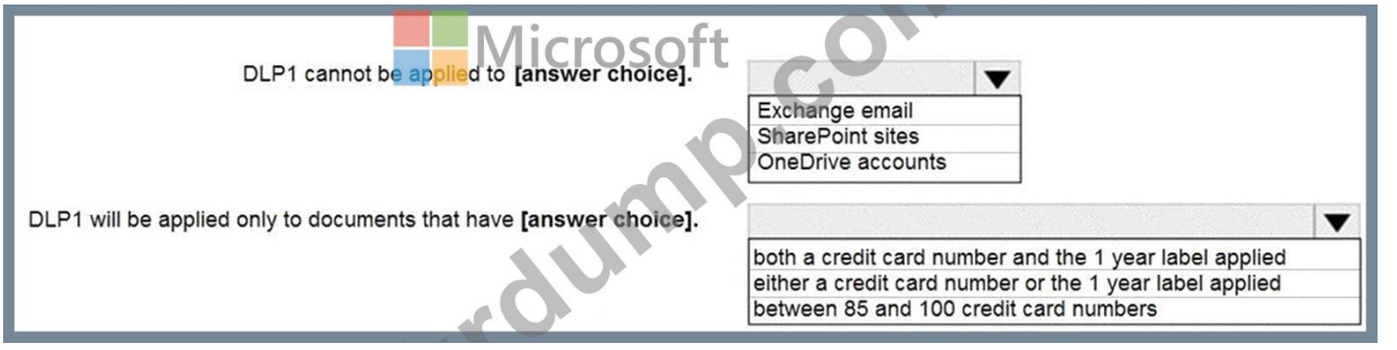
NEW QUESTION: 110

□□ □□□ □□ DLP1□□□ □□□ □□□ □□ □□(DLP) □□□ □□□□□.

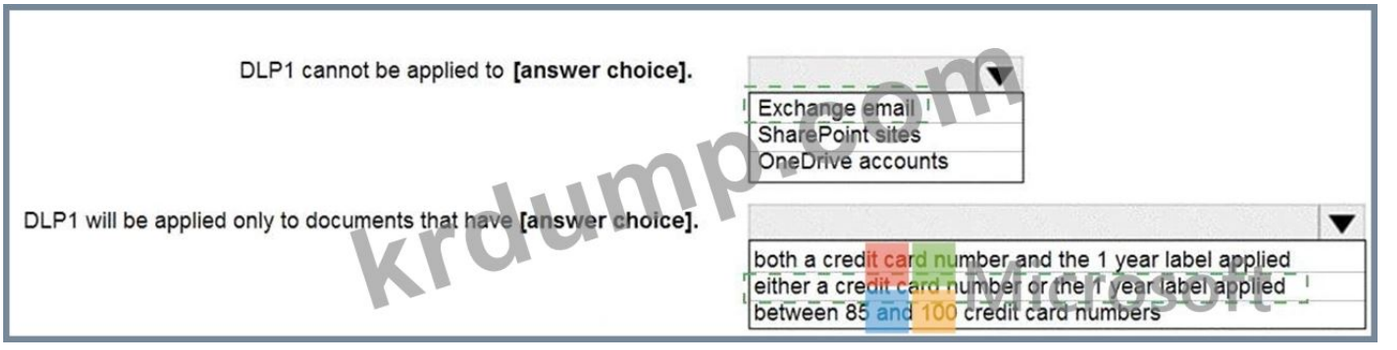


□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.

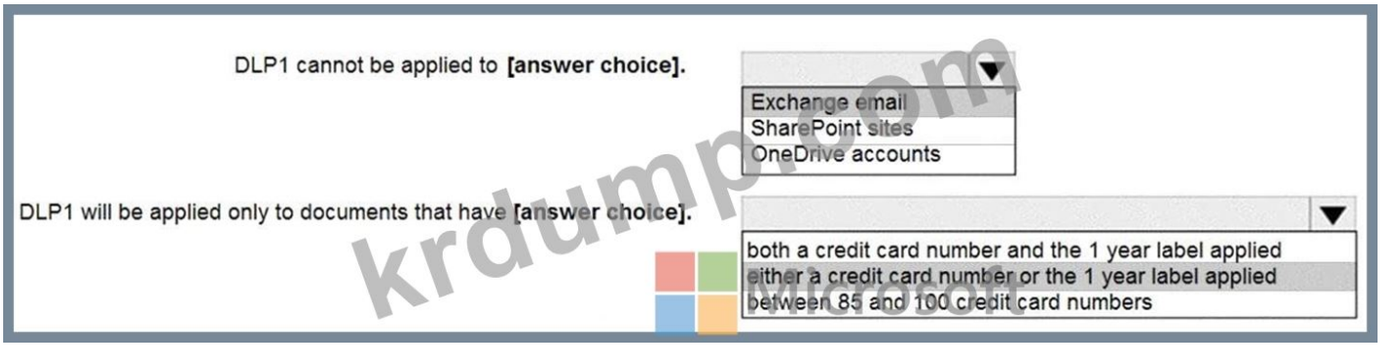
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365- worldwide#using-a-retention-label-as-a-condition-in-a-dlp-policy

NEW QUESTION: 111

□□ □□ □□□ □□ □□□ □□□ Microsoft 365 □□□ □□□□.

Name	Members
AU1	Group1, User2
AU2	Group2, User3, User4

□□□□ □□ □□ □□□ □□□□ □□□□□.

Name	Members
Group1	User1
Group2	User2, User4

□□□□□□ □□ □□ □□□ □□□ □□□□□.

Name	Role	Scope
User1	None	Not applicable
User2	Password Administrator	AU1
User3	License Administrator	Organization
User4	None	Not applicable

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 112

Microsoft 365 E5 □□□ □□□□.

□□ □□ □□□ □□□□ □□ Microsoft 365 □□ □□ □□□ □□□ □□□□□.

□□ □□ □□(PII)□ □□□ Microsoft Teams □ SharePoint Online□ □□□ □□□ □□□□□.

PII□ □□□ □□ □□□ □□ □□□□□.

□□□ □□□□ □□□?

A. □□ □□

B. □□□ □□ □□(DLP) □□

C. □□ □□

D. Microsoft Cloud App Security □□

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 113
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 □□□ □□□□.

Name	Department	Job title
User1	IT engineering	Technician
User2	Engineering	Senior executive
User3	Finance	Manager

AU1□□□ □□□ □□ □□□ □□□ □□ AU1 □□ □□□ □□□ □□□□□.
□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Name	Role
Admin1	AU1\User Administrator
Admin2	Global Administrator

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	○	○
Admin1 can reset the password of User2.	○	○
Admin2 can reset the password of User3.	○	○

Answer:
Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	○	○
Admin1 can reset the password of User2.	○	○
Admin2 can reset the password of User3.	○	○

Explanation:
Admin1 can reset the password of User1: YesAdmin1 has the User Administrator role within AU1. User1 is a member of Group1, which is included in AU1's dynamic membership rule.

Admin1 can reset the password of User2: NoUser2 is a member of both Group1 and Group2. However, User2's job title contains "Executive," which excludes them from AU1's dynamic membership rule.
Therefore, Admin1 cannot reset User2's password.
Admin2 can reset the password of User3: YesAdmin2 has the Global Administrator role, which grants the ability to reset passwords for any user within the organization, including User3.

NEW QUESTION: 114
Microsoft 365 □□□ □□□□.
□□□□ eDiscovery □□□ □□□ □□□□ □□□□ □□□.
□□ □ □□ □□ □□ □□□□ □□□ □□ □□□?
A. eDiscovery □□ □□
B. □□ □□ □□ □□
C. □□ □□ □□
D. □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 115
□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

Label1□□□ □□□ □□□ □□□□ □□□ □□□□□.
□□ □□□ Label1□ □□□ □ □□□?
A. □□1□
B. □□1□ □□2□
C. □□1□ □□4□
D. Group1, Group2, Group3□
E. □□1 □□2, □□3, □□4
Answer: A (LEAVE A REPLY)
In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites

NEW QUESTION: 116
□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
* □□ : User1
* UPN: user1@contoso.com
* □□□ □□: user1@marketmg.contoso.com
* MFA □□ □□: □□□□□
User1□ user1@marketing.contoso.com □□□ □□□ □□□□ □□□ Outlook□ □□□□□□ □□ □□□□ □□□□ □ □□□□.
User1□ user1@marketing.contoso.com□ □□□□ □□□ Outlook□ □□□□ □ □□□ □□□ □ □□□.
□□□ □□ □□□?
A. User1□ □□ □□ □□□ □□□ □□□□□.
B. User1□ UPN□ □□□□□.
C. User1□ MFA □□ □□□ □□□□□.
D. User1□ □□□□□ □□□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 117
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
□□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft Entra □□□□ □□□□□.
□□ □□□□ □□□□ Microsoft Entra □□□□ □□□□□□ □□□□□.
□□ □□(OU)□ 10□ □□□ □□□ Microsoft Entra □□□□ □□□□□ □□ □□ □□□□□ □. □□ □□ □□□ □□□ □□□□□ □□□□□□□□.
Microsoft Entra Connect Health□ □□□ □□ □□ □□□ □□ □□□□ □□□□□ □□□□□ □ □ □ □□□□.
10□□ □□□ □□□ Microsoft Entra □□□□ □□□□□□□ □□□□ □□□.
□□ □□: Microsoft Entra Connect□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: (SHOW ANSWER)

NEW QUESTION: 118
□□ □□ □□□ □□□□ □□□ Azure AD □□□□ □□□□.

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

□□ □□□□ □□ □□ □□□ □□ □□□□ □□□□□□. □□□□ □□□ □□ □□ 1□ □ □□□ □□□□□ □□□□ □□□ □□ □□□□□ □□□□□.
□□□□ □□ □□□ □□ □□□□ □□□□ □□ □ □□□□ □□ □□ □□□ □□□□ □□ □? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

Answer Area

User1: Phone number and email address

User2: Phone number and email address

User3: Security questions only

NEW QUESTION: 119

□□□

□□ □□ □□ □□ □□□ □□□ Microsoft Defender for Endpoint□ □□□□ Microsoft 365 E5 □□□ □□□□.

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

Defender for Endpoint□□ □□ □□ □□□ □□ □□□ □□□□.

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*

□□ □□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□.

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

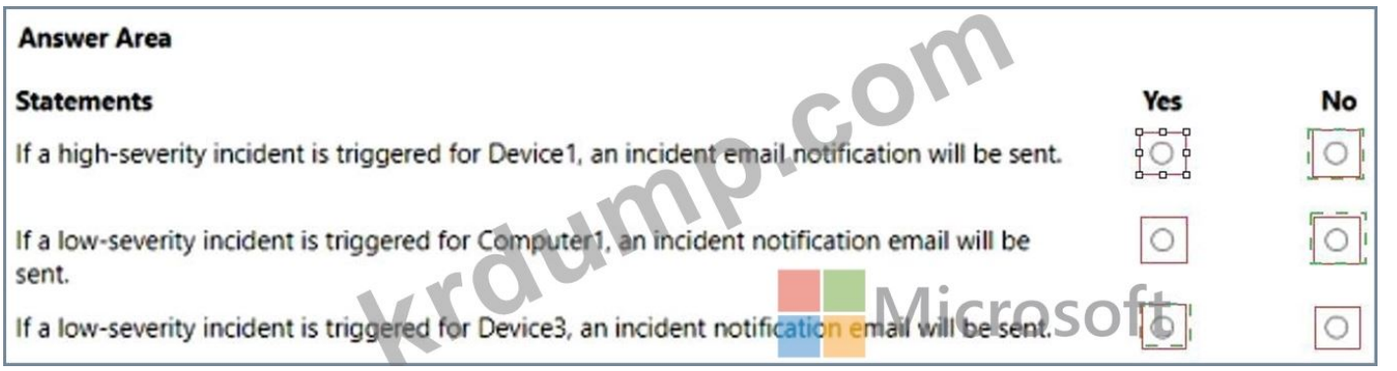
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

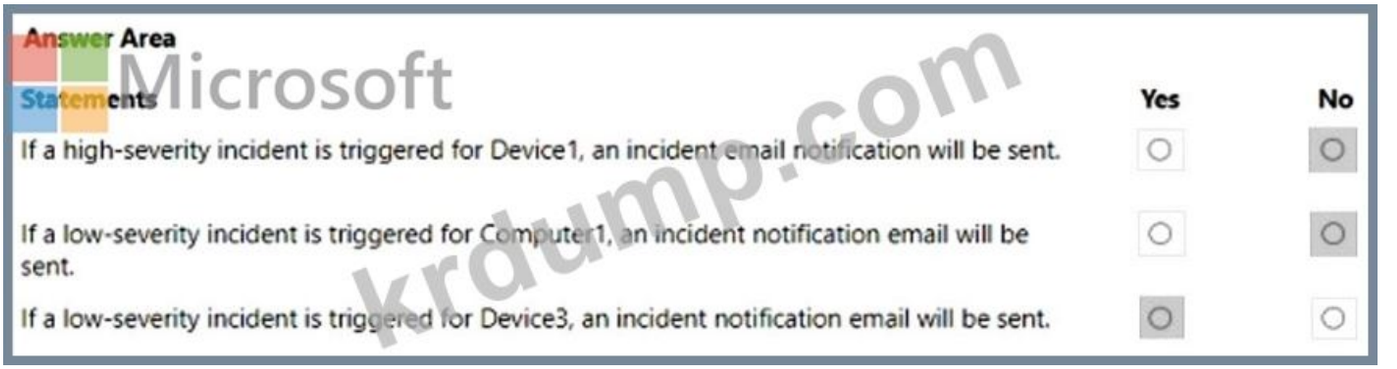
Answer Area

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.	○	○

Answer:



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.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue

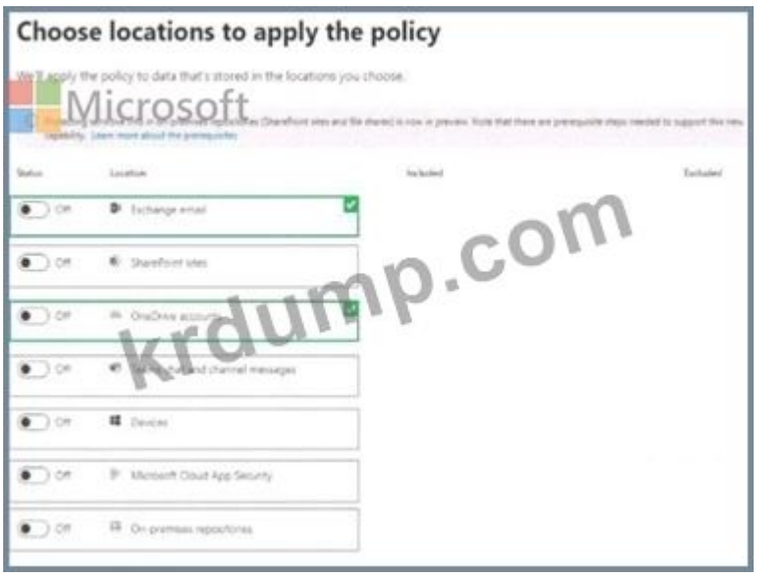
NEW QUESTION: 120

Microsoft 365 E5 □□□□ □□□□.

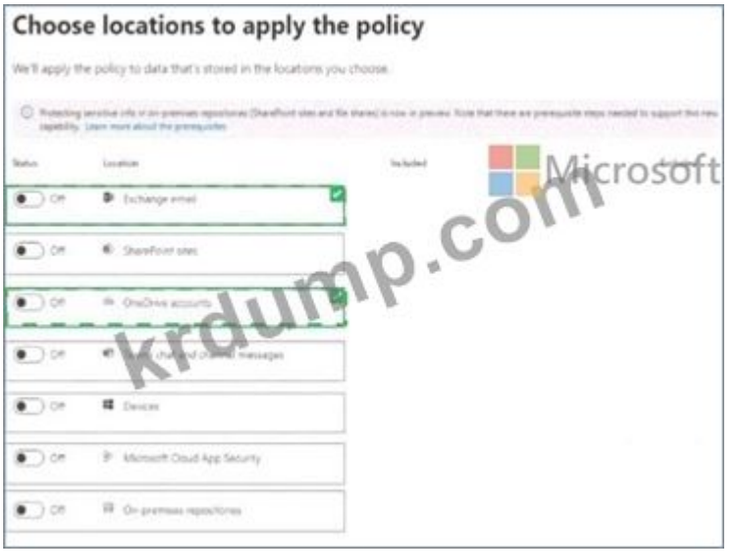
□□□□ Microsoft Teams□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□□□□ □□ □ □□ □□(DLP) □□□ □□□□.

□□□ □□□□ □□ □ □□□ □□□□□? □□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:



NEW QUESTION: 121

Microsoft 365 E5 □□□□ □□□□.

□□□ □□ □□□□ □□□ □□ □□□ □□ □□□□ □□ □□□□□ □□□ □□ □□□ □ □□ □□□.

□□ □ □□ □□□ □□□ □ □□□□? □ □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

A. Microsoft Cloud App Security □□ □□

B. □□□ □□ □□(DLP) □□

C. □□ □□ □□

D. □□□□□□ □□ □□

E. □□□ □□□ □□

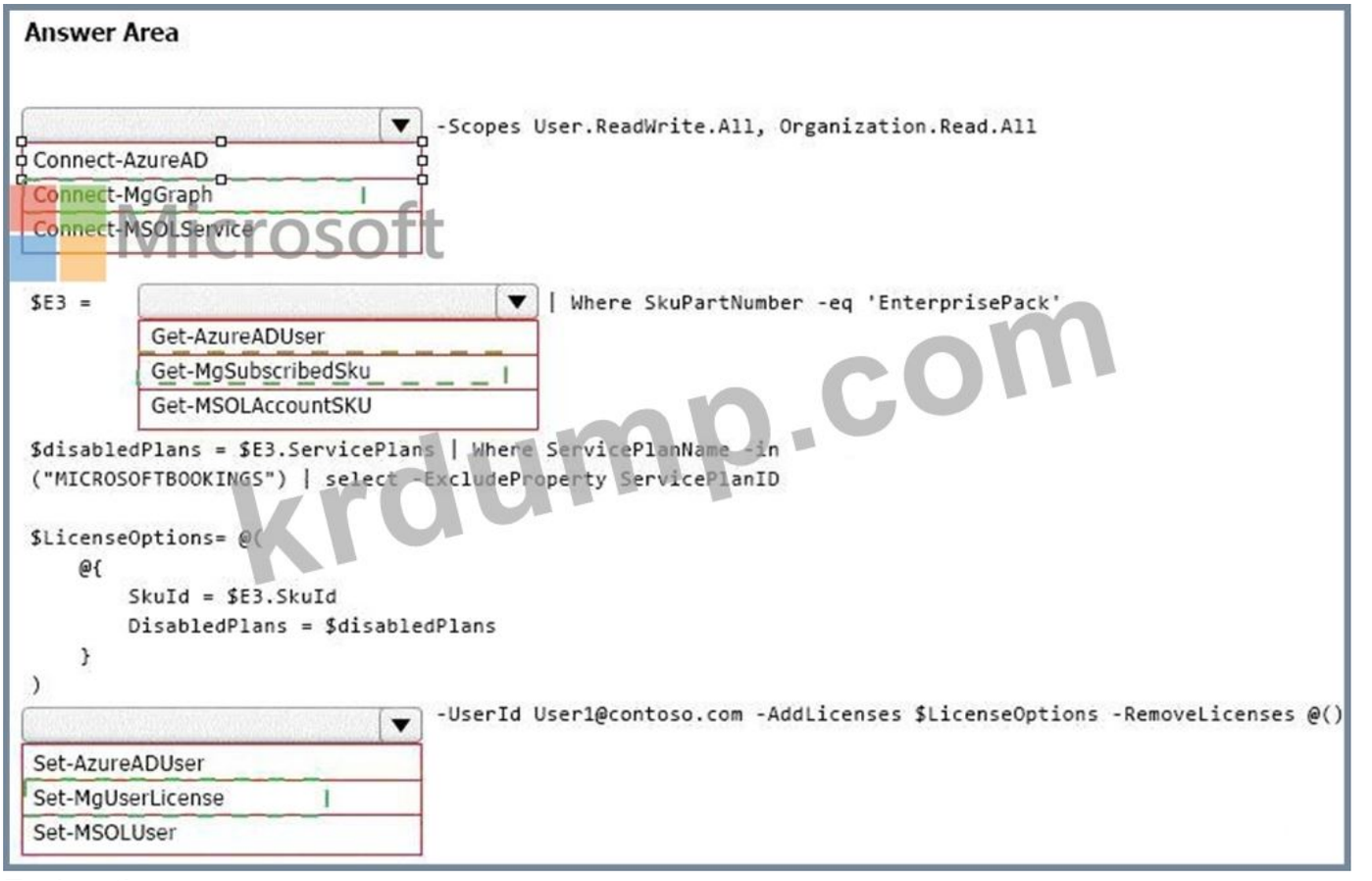
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 122
Microsoft Endpoint Manager□ □□□□ □□□□ Windows 10 □□□ □□□□.
Microsoft Edge□□ □□ □□□ □□□□ □□□.
Microsoft Endpoint Manager□□ □□□ □□□□ □□□?
A. □ □□ □□
B. □
C. □□ □□ □□□
D. □□ □□ □□
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

NEW QUESTION: 123
User1□□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□□□□ Microsoft 365 □□□ □□□□□□.
Cloud App Security □□ □□□□ □□ □□□ □□□ □□□ □□□□ □ □□□ □□□ User1 □□ □□□□□□ □□□□ □□□.
□□ □□: Azure Active Directory □□ □□□□ User1□□ □□ □□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: B (LEAVE A REPLY)

NEW QUESTION: 124
□□□
Microsoft 365 □□□ □□□□.
user1@contoso.com□□□ □□□□ □□ □□□□□□□□□□.
PowerShell□ □□□□ User1□ Microsoft Office 365 E3 □□□□□ □□□□ □□□. Microsoft Bookings□ □□□□□□□ □ □□□.
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:



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.

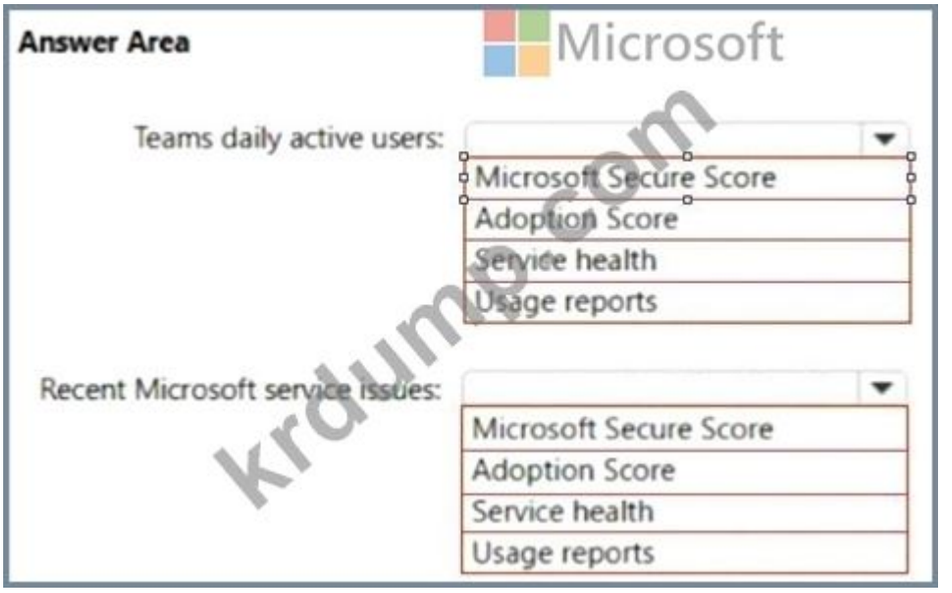
Set-MgUserLicense -UserId $userUPN -AddLicenses @{SkuId = "<SkuId>"} -RemoveLicenses @() This example assigns a license from the SPE_E5 (Microsoft 365 E5) licensing plan to the unlicensed user belindan@litwareinc.com:

$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'

Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId = $e5Sku.SkuId} - RemoveLicenses @() Reference:

https://learn.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-
365-powershell

NEW QUESTION: 125
□□□
Microsoft 365 □□□ □□□□.
□□ □□□ □□ □□□ □□□□ □□□.
Microsoft Teams□ □□ □□ □□□
□□ Microsoft □□□ □□
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:
Answer Area

Explanation:

Answer Area

Box 1: Usage reports
The daily active users in Microsoft Teams
Microsoft 365 Reports in the admin center - Microsoft Teams usage activity The brand-new Teams usage report gives you an overview of the usage activity in Teams, including the number of active users, channels and messages so you can quickly see how many users across your organization are using Teams to communicate and collaborate. It also includes other Teams specific activities, such as the number of active guests, meetings, and messages.
Box 2: Service Health
Recent Microsoft service issues
You can view the health of your Microsoft services, including Office on the web, Yammer, Microsoft Dynamics CRM, and mobile device management cloud services, on the Service health page in the Microsoft
365 admin center. If you are experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/microsoft-teams-usage-activity
https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health

NEW QUESTION: 126
□□ □□□□ □□□□ □□□ □□□□ □□ □□□□ □□ □□□ □□ □□(DLP) □□□ □□ □□□ □□□□.

□□□□□ □□ □□□□ □□□□ □□□□ □□ □□□□ □□ □□ □□□ □□□ □ □□□ □□ □□ □□□□□. □□□ □□□□ Microsoft SharePoint□ □□□□ □□ □□ □□□ □□ □ □□□ □□□ □ □□□□.
□□□□ □□□□ SharePoint□ □□□□ □□□□ □□□ □□□□ □□ □□□□ □□□.
□□□ □□□□ □□□?
A. DLP □□□ □□
B. DLP □□□ □□
C. □□□□ DLP □□ □□□ □□□□□□.
D. DLP □□ □□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 127
□□ □ □□ □□ □□ □□□ □□□□ Microsoft 365 □□□ □□□□.
□□ □□ □□□□□ □□□ □□ □□□ □□ □□□ □□□□□.
□□ □□□□ □□□ □ □□ □ □□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□ □.
□□□□: □□□ 1□□ 1□□□□.
A. □□□□□ □□□□□.
B. □□□□ □□ □□
C. □□ □□□□
D. □□□ □□ □□
E. □□ □□□ □□□□□
Answer: D,E (LEAVE A REPLY)

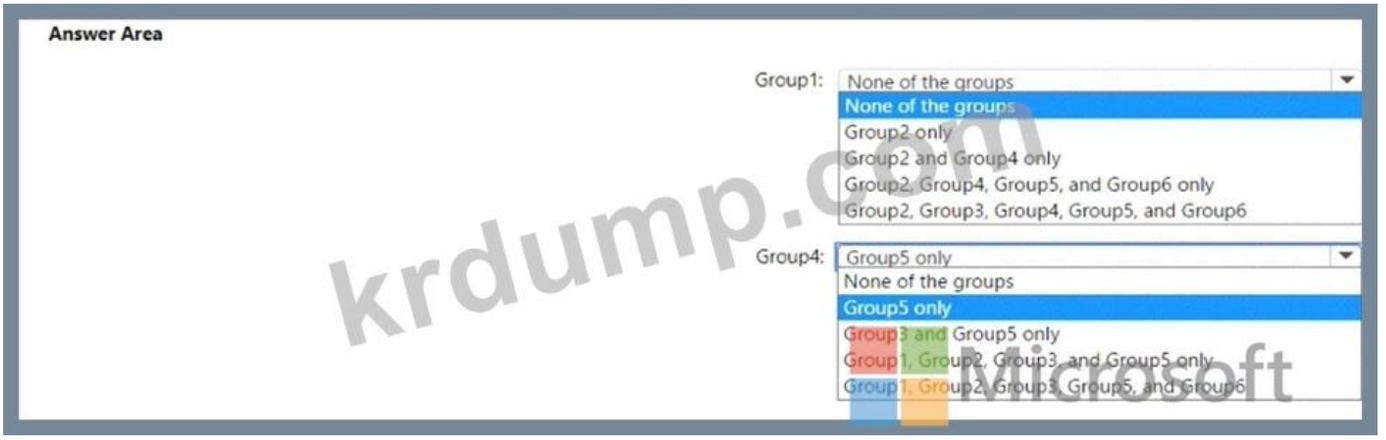
NEW QUESTION: 128
Windows 10 □□ 2004□ □□ □□□ □ □□□□ □□□□□□.
□□□□ □□ □□□□ □□□□ □□□. □□□□ □□□ □□□□ □□ □□□□□ □□□.
□□□□□ □□□ □□ □□□?
A. □□ □□ □□□□□ □□ □□ □□□□□ □□□□□.
B. 2004□□ □□□ □□□ □□ □□ □□□□□ □□ □□ □□□□□ □□□□□.
C. □□ □□ □□□□□ 2004□□ □□□ □□□ □□ □□ □□□□□ □□□□□.
D. 2004□□ □□□ □□□ □□ □□ □□□□□ 2004□□ □□□ □□□ □□ □□ □□□□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 129
□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

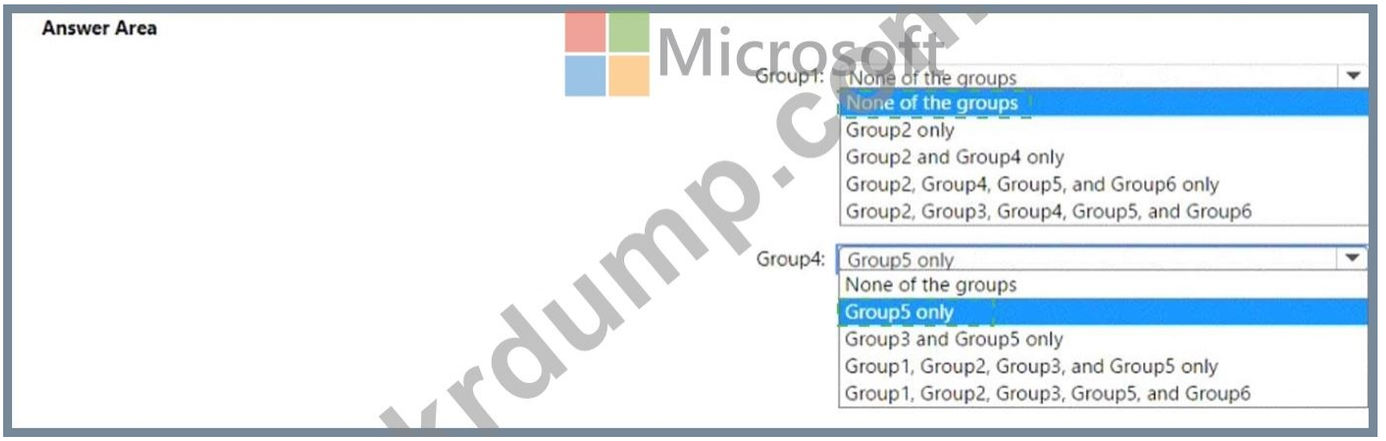
Name	Type	Security enabled	Role assignments allowed
Group1	Microsoft 365	No	No
Group2	Microsoft 365	No	No
Group3	Security	Yes	Yes
Group4	Security	Yes	No
Group5	Security	Yes	No
Group6	Distribution	No	No

□□ □□□ Group1□ Group4□ □□□ □ □ □□□□? □□□□□ □□ □□□□ □□□ □□ □ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 130

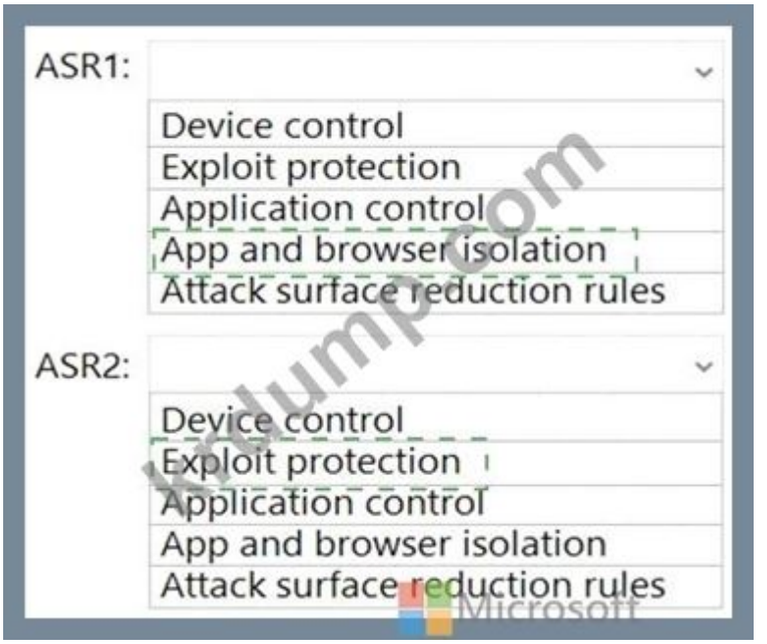
100□□ Windows 10 □□□□□ □□□□ Microsoft 365 □□□□ □□□□. □□□□□ Microsoft Endpoint Manager□ □□□□ □□□□□.

ASR1 □ ASR2□□ □ □□ □□ □□ □□(ASR) □□□ □□ □□□□□. ASR1□ Microsoft Defender Application Guard□ □□□□ □ □□□□□. ASR2□ Microsoft Defender SmartScreen □ □□□□ □ □□□□□.

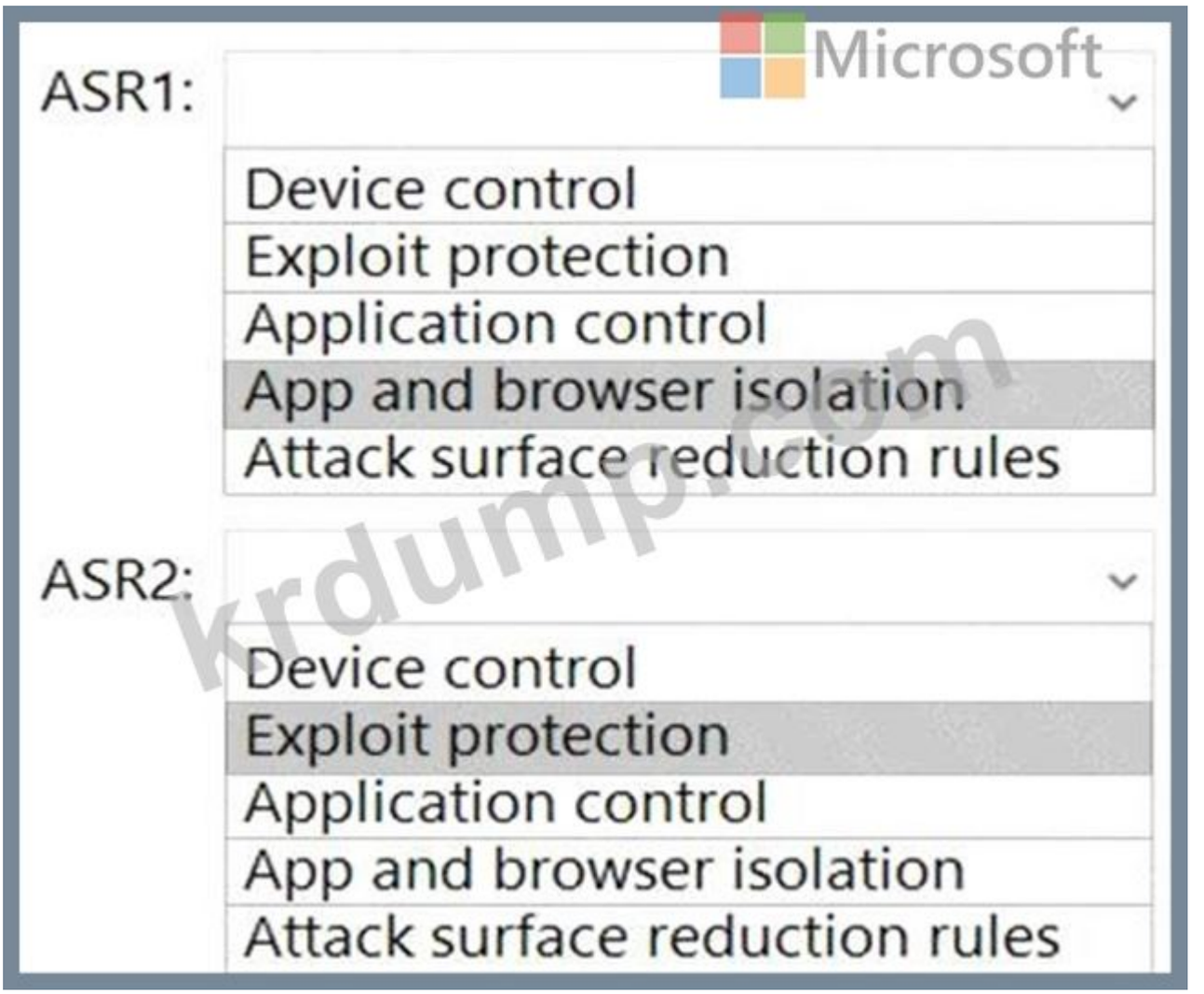
□ □□□ □□ □□ ASR □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□ □ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy

NEW QUESTION: 131
□□□ □□□□ □□ □□ □□ □□ □□□□ □□□ comoso.onmicrosoft.com□□□ Azure AD □□□□ □□□□.

Name	Role
User1	Password Administrator
User2	Security Administrator
User3	User Administrator
User4	None

□□ □□ □□□ □□□ □ □□ □□□□ □□□□ □□□.
* User4□ □□□□□ □□□□□□.
* User4□ □□□ □□ □□ □□□□□.

□ □□□ □□ □□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□ □□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 132
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows Server 2019□ □□□□ □□□ □□□□□ □□□□. □□□□□ □□□□ □□ □□□ Windows Server 2012 R2□□□.
□ □□□□□ Windows 10□ □□□□ 100□□ □□□□ Windows Server 2012 R2□ □□□□ Server1□□□ □□ □□□ □□□□ □□□□.
Server1□ □□□□ □□□□ □□□□ Windows 10 □□ □□ □□□ □□□ □□□□□.

Server1□ □□ □□ □□ □□(GPMC)□ □□□□□.
Server1□□ □□□□□ Windows □□□□ □□ □□ □□□ □□□□ □□□.
□□ □□: □□□□ □□ □□□ Windows Server 2016□□ □□□□. Windows 10 □□□□□ □□ □□□ □□□□□ Netlogon □□□ □□ □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?

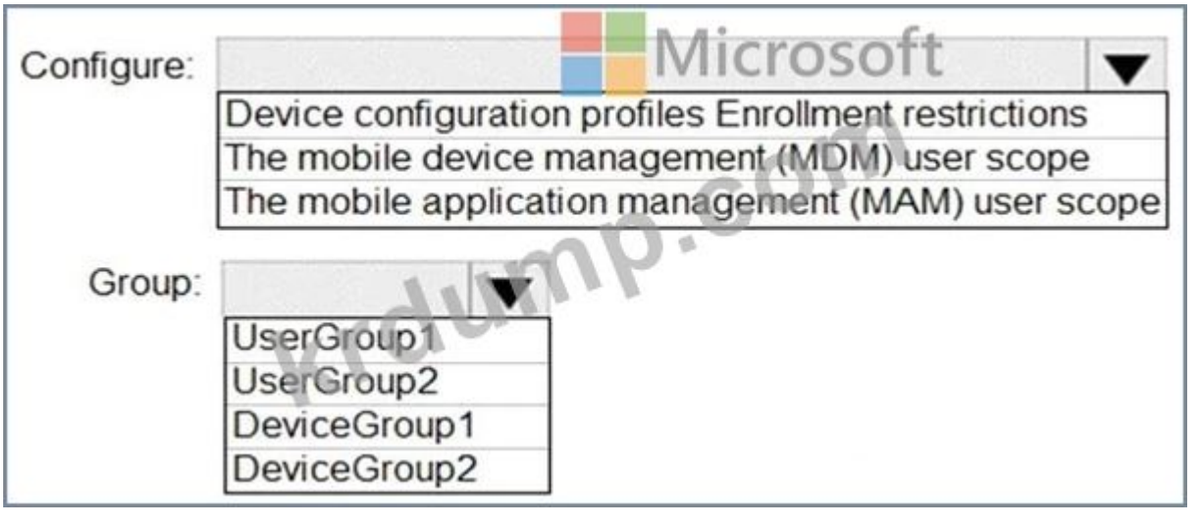
A. □□□

B. □

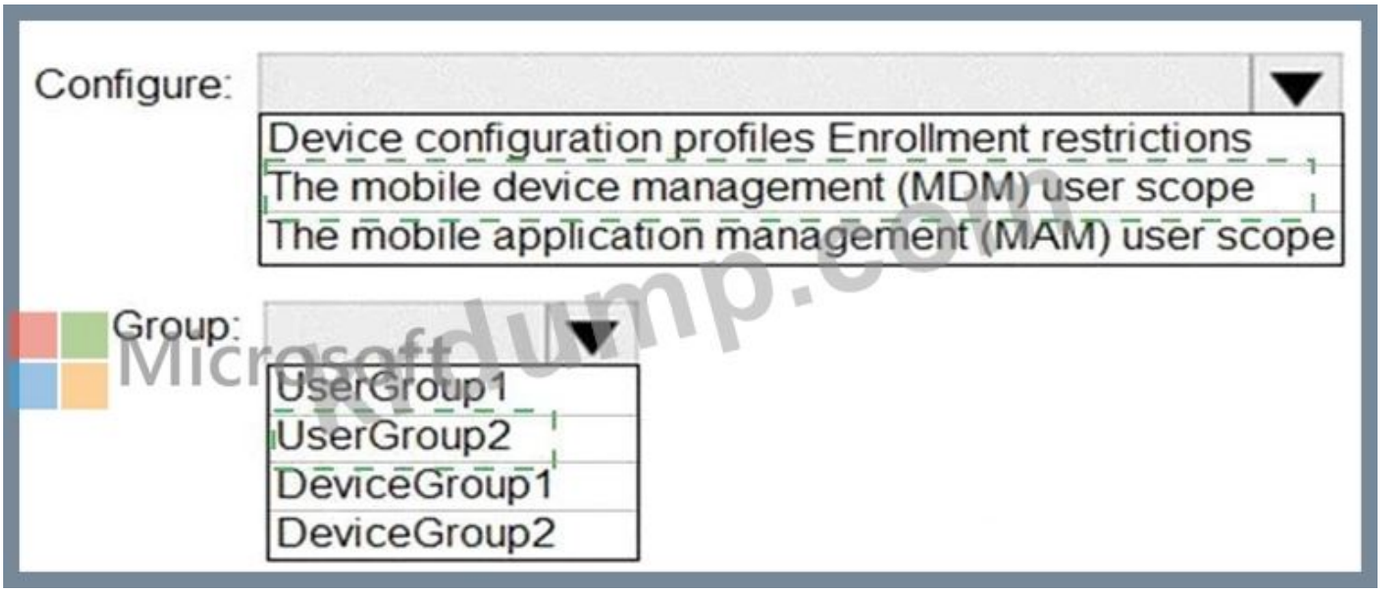
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133

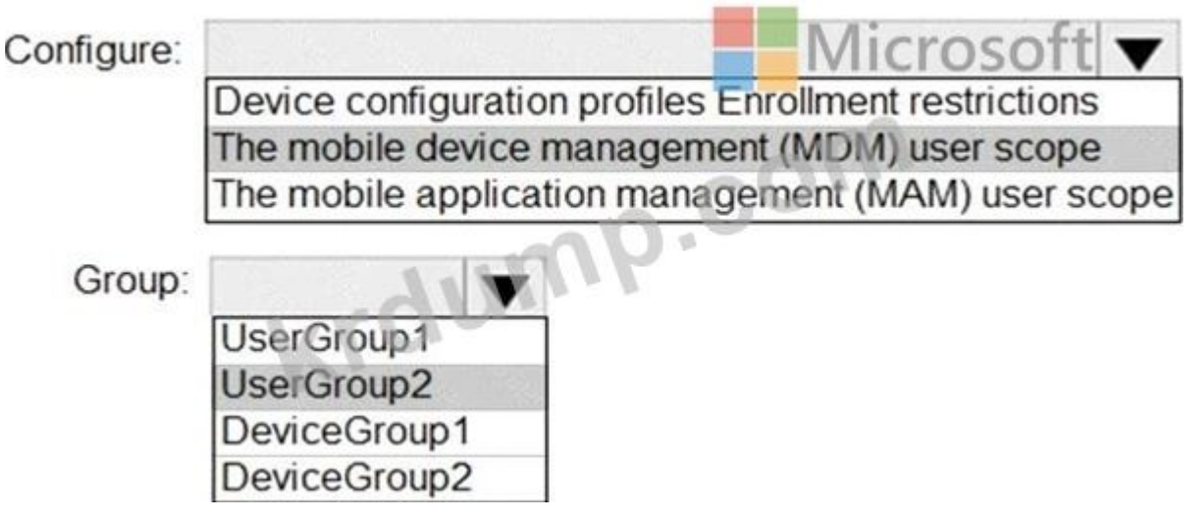
Intune□□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□, □□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □ □□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

NEW QUESTION: 134
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Windows 10□ □□□□ □□□□ □□□□.
□□□ Windows 10 □□□ □□□□ □□□.
□□□: □□ □□□□□□ winver.exe □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-
628bec99-476a-2c13-5296-9dd081cdd808

NEW QUESTION: 135
□□□
Azure Active Directory(Azure AD) □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □□□□ □ Group1□□□ □□□ □□ □□ □□□ □□□□ □□□□□.

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

□□□□□ □□□ □□ □□□ □□ □□□ □□□ □□□ □□□□.

□□: □□1

□□:

- □□□ □ □□: Group1
- □□□□ □ □□ □□: □□ □□□□ □

* □□ □□:

* □□ □□ □□ □□, □□

* □□ □□□: □□□ □□

□□□□ □□ □□ □□□□ '□'□ □□□□□.

□□ □□ □□□ □□ □□□ □□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

Answer:

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

Explanation:

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:
* Conditional Access policies can be enabled in report-only mode.
* During sign-in, policies in report-only mode are evaluated but not enforced.
* Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
* Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report- only

NEW QUESTION: 136
□□□
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

□□□ □□□ □□□ □□ □□ □□□ □□□□□.
* □□ □□: □□□□
* □□□□ : Group1
* □□ □□ : □□
* □□ □□□: 2023□ 3□ 15□
* □□ □□□: 2023□ 8□ 15□
Exchange □□□ □□□ □□ □□ □□□ □□□□□.
* □□ □□: □□□□
* □□□ □□ : Group2
* □□ □□ : □□
* □□ □□□: 2023□ 6□ 15□
* □□ □□□: 2023□ 10□ 15□
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

Box 1: Yes

Admin1 is member of Group1.

The User Administrator role assignment has Group1 as a member.

The assignment type: Active

July 15, 2023 is with the assignment period.

A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.

Box 2: No

Admin2 is member of Group2.

The Exchange Administrator role assignment has Group2 as a member.

The assignment type: Eligible

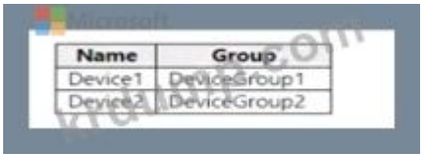
June 20, 2023 is with the assignment period.

The assignment must be approved.

Note: Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.
Box 3: Yes
Admin3 is member of Gropu1 and Group2.
The User Administrator role assignment has Group1 as a member.
The assignment type: Active
May 1, 2023 is with the assignment period.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-assign- member-owner

NEW QUESTION: 137
Microsoft 365 E5 □□□ □□□□.
□□□□ Android □□ iOS □□□ □□□ □□□, Windows 11 □□ MacOS□ □□□□ □□□□ □ Microsoft 365 □□□□ □□□□□□.
□□□□ □□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□?
A. Microsoft Authenticator □
B. FID02 □□ □□ □
C. □□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 138
□□ □□ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.



08:00□ □□ □□□ □□ □□□□ □□ □□□ □□□□□.
* □□ : □□!
* □□ □□
o □□ □ □□ 70: □□

o □□ □□ □□: □□(3)
o □□ □□: □□□ □ □□ □□
* □□□: Userl@contoso.com, User2@contoso.com
08:02□ □□ □□□ □□ □□□□ □□ □□□ □□□□□.
* □□ : □□
* □□ □□
o □□ □□□□ □□ □□: □□. □□
o □□ □□ □□: DevtceGroup1, DeviceGroup2
* □□□: Userl@contoso.com
Microsoft 365 Defender□□□ □□ □□ □□ □□□ □□□□□.

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

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□1. □□□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	○	○
User2@contoso.com will receive an incident notification email for the alert at 08:07.	○	○
User1@contoso.com will receive an incident notification email for the alert at 08:20.	○	○

Answer:

Answer Area

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	○	○
User2@contoso.com will receive an incident notification email for the alert at 08:07.	○	○
User1@contoso.com will receive an incident notification email for the alert at 08:20.	○	○

Explanation:

NEW QUESTION: 139

Microsoft 365 F5 □□□ □□□□.

100□□ □□□ Windows 10 □□□ □□□ □□□□□.

□□□ □□□ □□□ Windows 10 □□□ □□□□ □□□. □□□ □□ □□ □□□ □□□□ □ □□.

□□ 24□□ □□ □□□□ □□□□.

Microsoft □□□□□□ □□□(App-V) □□

□□ □□□ □□□□ □□□?

A. □□□ 10 □□, □□ 1909

B. □□□ 10 □□, □□ 2004

C. □□□ 10 □□, □□ 1909

D. Windows 10 Enterprise, □□ 2004

Answer: D (LEAVE A REPLY)

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: 140

Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□□.

□□ □□ □□□ □□ Intune□ □□□ □□□ □□□□.

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

□□ □□ □□□ □□ □□ □□□□ □□□□.

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

□ □□□ □□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

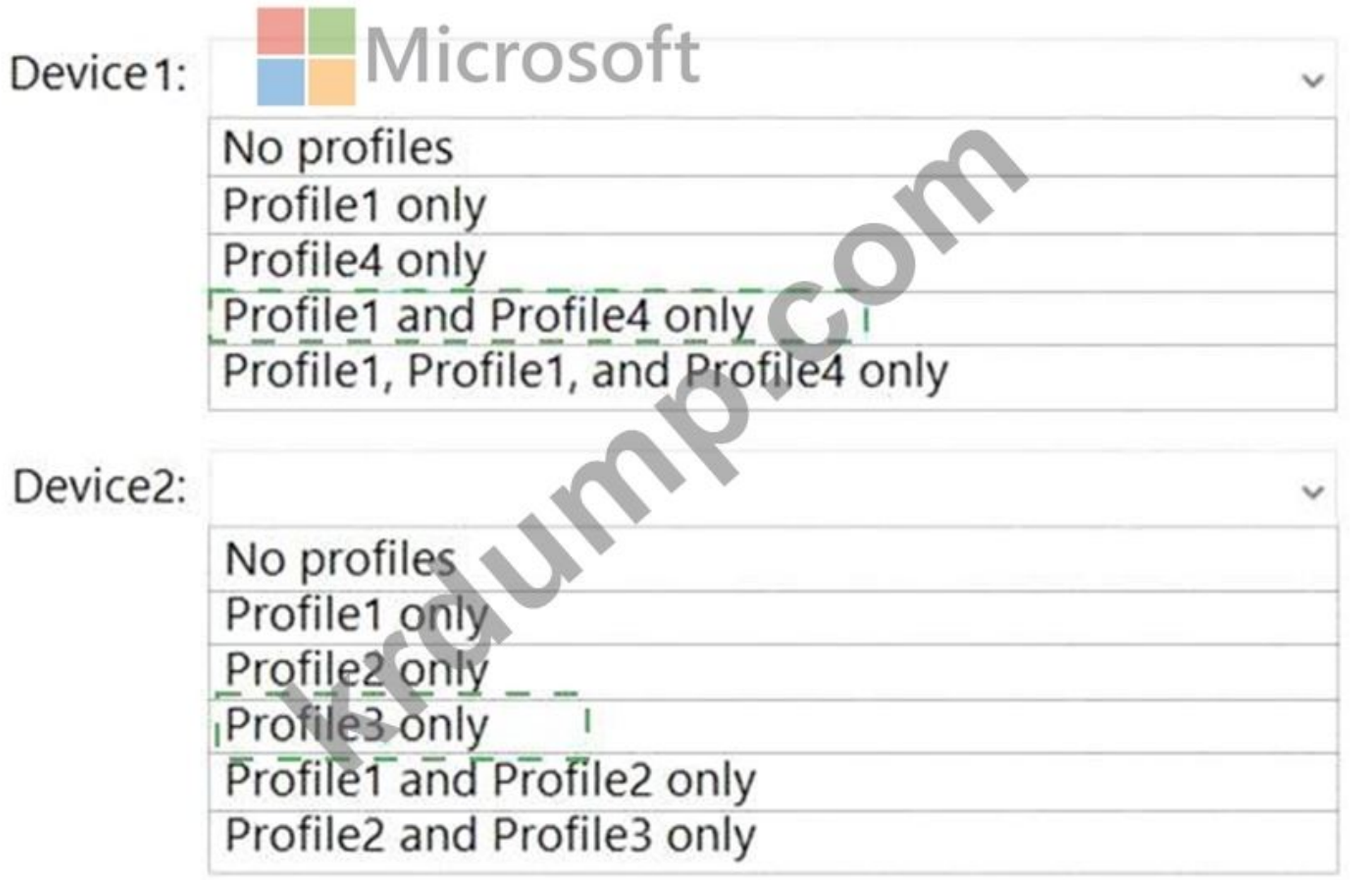
Device1:

- 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

Answer:



Explanation:

NEW QUESTION: 141

□□□ Microsoft 365 E5 □□□□ □□□□.

Microsoft Exchange Online □□□ □□ □□□ □□□□ □□□□□ □□ □□□ □□□□□ □ □□.

□□ □□ □□□ □□ □□□?

A. □□□ □□□□□□.

B. Microsoft 365 □□ □□□ □□□□□□.

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

NEW QUESTION: 142
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows Server 2019□ □□□□ □□□ □□□□□ □□□□. □□□□□ □□□□ □□ □□□ Windows Server 2012 R2□□□.
□ □□□□□ Windows 10□ □□□□ 100□□ □□□□ Windows Server 2012 R2□ □□□□ Server1□□□ □□ □□□ □□□□ □□□□.
Server1□ □□□□ □□□□ □□□□ Windows 10 □□ □□ □□□ □□□ □□□□□.
Server1□ □□ □□ □□ □□(GPMC)□ □□□□□.
Server1□□ □□□□□ Windows □□□□ □□ □□ □□□ □□□□ □□□.
□□ □□: Windows 10 □□□□□ Server1□ □□ □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 143

Microsoft 365 E5 □□□ □□□□.
□□□ □□□ □□□□ □□□□ □□□.
□□ □□□ □□□□ □□□?
A. Microsoft Purview □□ □□ □□
B. SharePoint □□ □□
C. Microsoft Entra □□ □□
D. Microsoft 365 □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 144
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□ □□ □□(DLP) □□□ □□□ □□□□□.

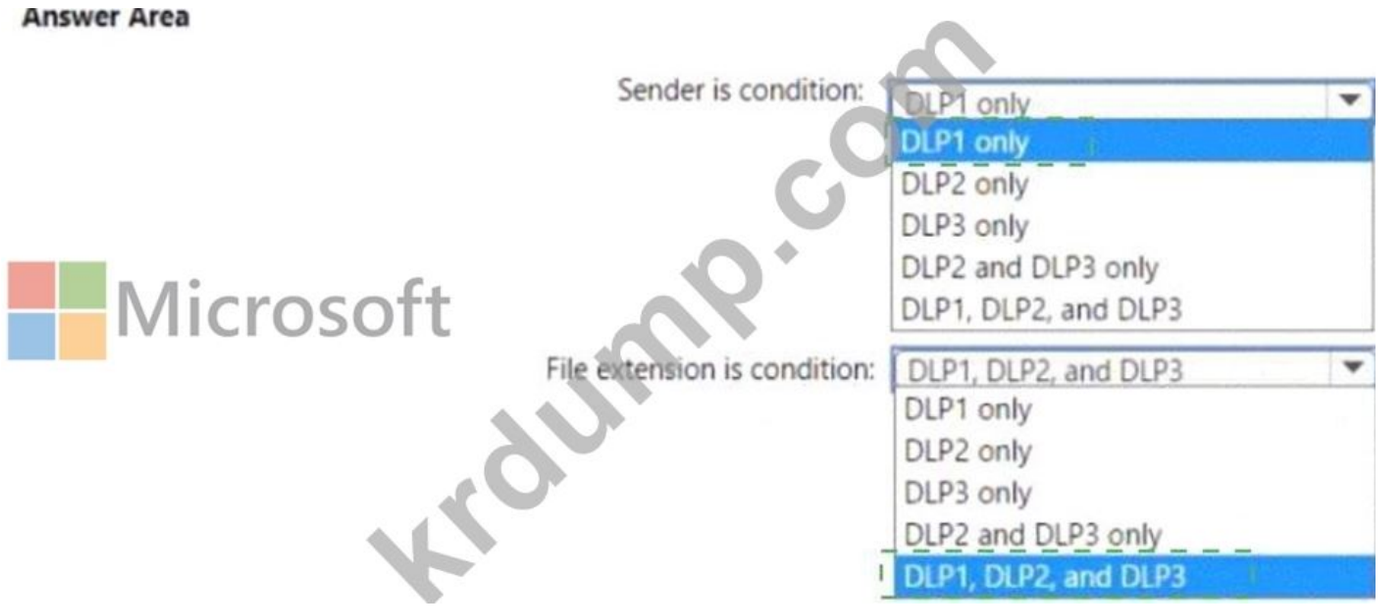
Name	Apply to location
DLP1	Exchange email
DLP2	SharePoint sites
DLP3	OneDrive accounts

□ □□□ □□ DLP □□□ □□□□ □□□.
□□ □□□ □□□ □□□ □□ □□□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □ □□ □□□□□.
□□□□: □□ □□□ 1□□□□.
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

Answer:



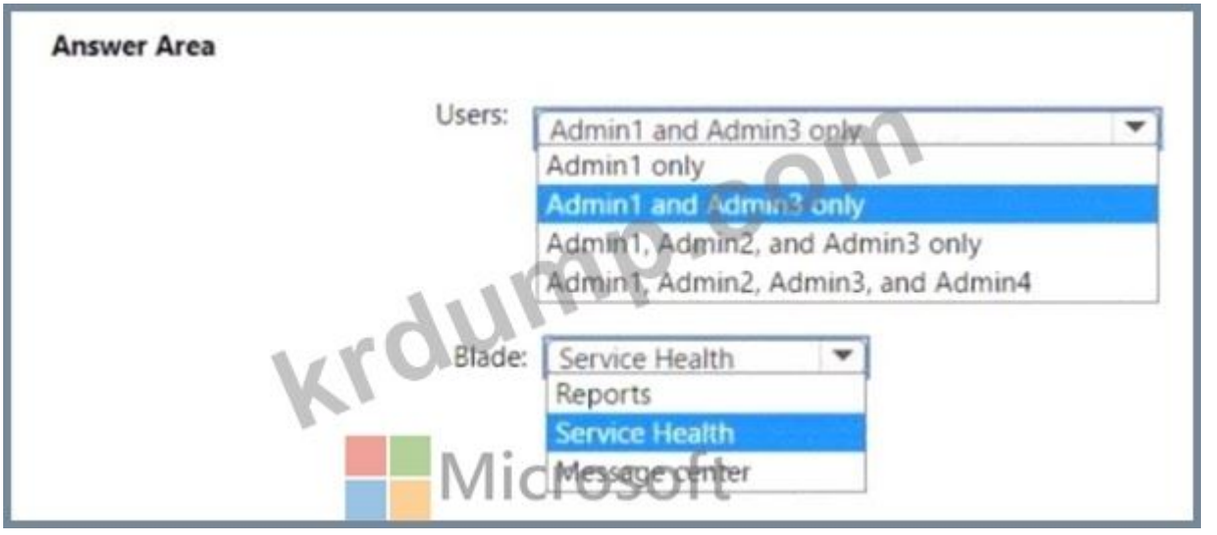
Explanation:

NEW QUESTION: 145

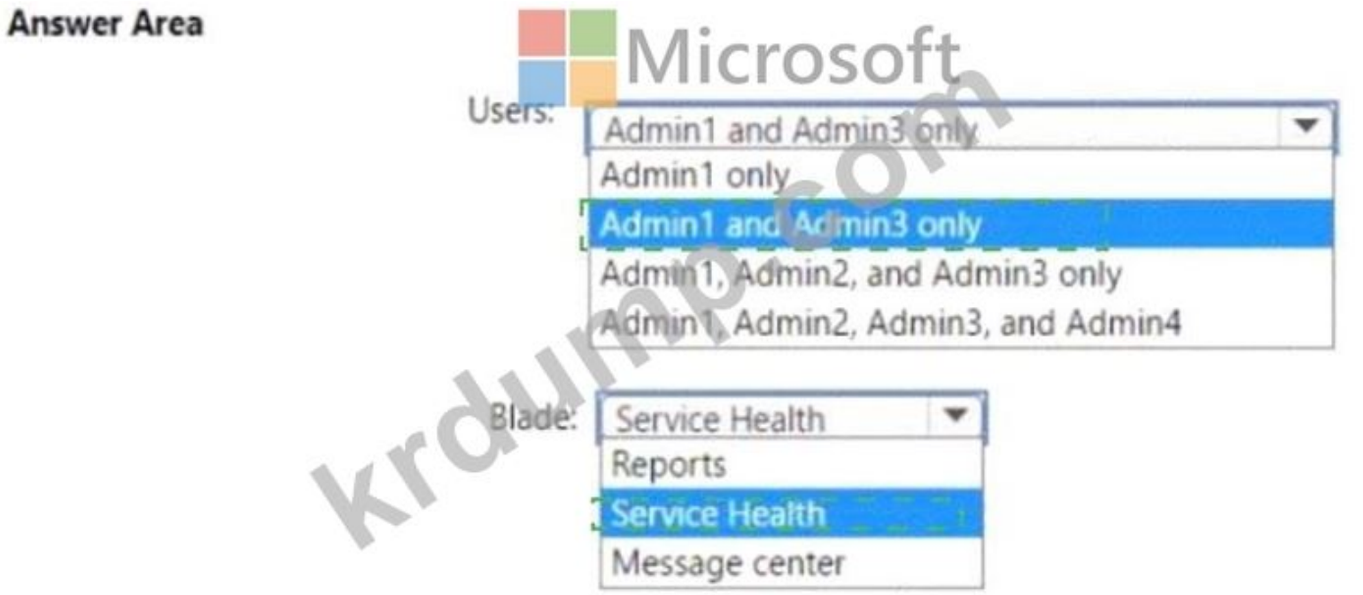
Microsoft 365 □□□□ □ □□ □□□ □□ □□□□ □□□.

□□ □□□□ □□□ □□□ □□□ □ □□□, □□□□ □□ □□□□□ □□□□ □□□? □□ □□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 146

500□□ Windows 10 □□□□□ □□□□ Microsoft 365 E5 □□□□ □□□□. □□□□□ Microsoft Intune□ □□□□ □□□□.

Endpoint □□□ □□□□ □□□□ □□□ □□□ □□□□□.

Endpoint □□□ □□□□□ □□□□ Windows □□ □□□□□ □□□□□ □□□. □□□ □□ □□□?

A. □□ □□□□ □□□□.

B. Endpoint □□ □□ □□ □□□□ □□□□□.

C. Windows 10 □□ □□ □□□□ □□□□.

D. □□ □□ □□□ □□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 147

Microsoft 365 E5 □□□□ □□□□.

□□□□ □□□□ □□□ □□□ □□□□ □□ □ □□□□□ □□□ □□□ □□□. □□□□ □□ □□□ □□□ □□□□ □□□.

□□ □□□ □□□ □□□□ □□, □□□ □□□□ □□ Microsoft 365 □□ □□ □□ □□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

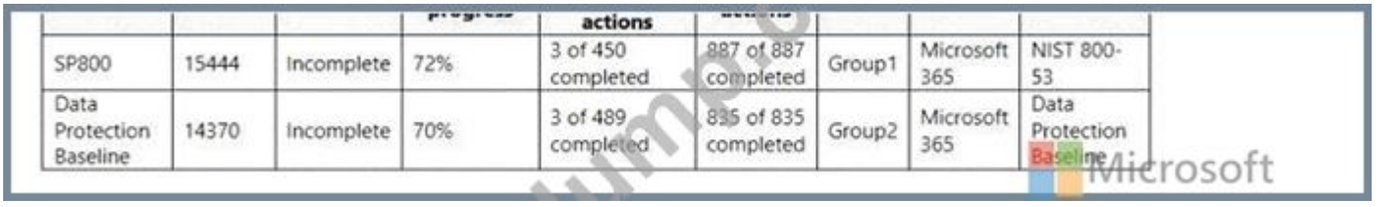
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

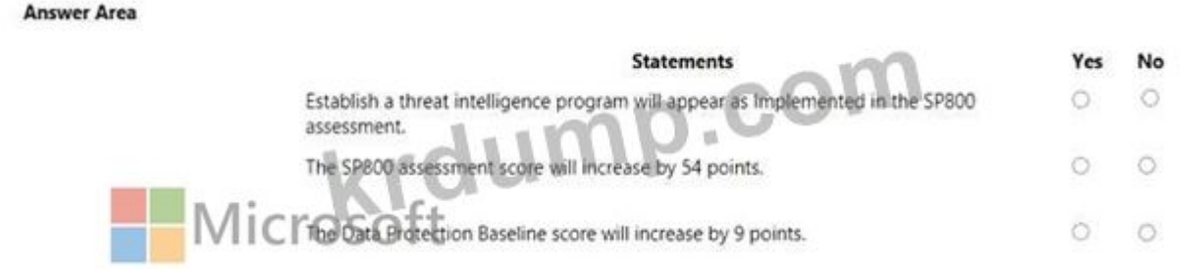
NEW QUESTION: 148

□□□



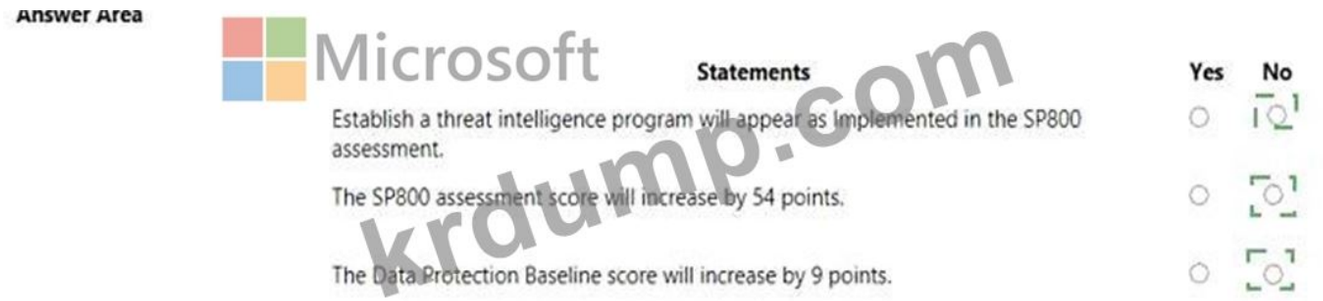
				actions				
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

SP800 □□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.



Answer:

Answer Area



Explanation:

NEW QUESTION: 149

Microsoft 365 □□□ □□□□.

DLP(□□□ □□ □□) □□□ □□□□□.

□□□□ □□□□ □□ □□□□ □□□□ DLP □□□ □□□□ □□□ □□□ □□□□□□.

□□□□ DLP □□□ □□□□ □□□□ □□□□ □□□.

□□□ □□□□ □□□?

A. □□

B. □□ □□□

C. □□

D. □□□□ □□□□

Answer: D (LEAVE A REPLY)

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: 150

□□□

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

User4□□ Microsoft 365 □□ □ □□□ □□□□□ □□ □□ □□□ □□□ □□□ □□□□□.
□□ Microsoft 365 □□□ □□□□ □□□, □□□ □□ □□□□ □□□ □□□ □ □□□ □□ □□ □□□.
□□□□ □□ □□□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

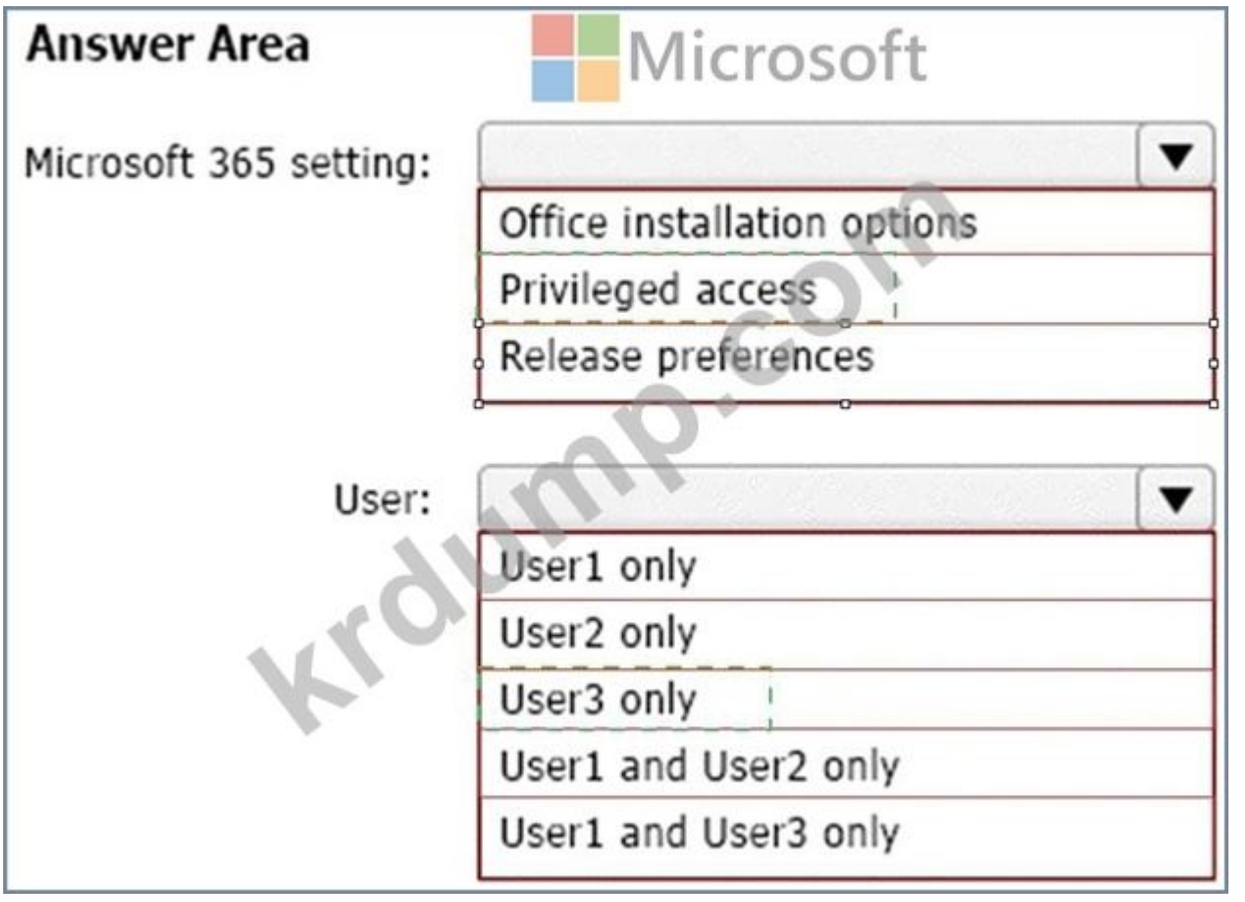
Microsoft 365 setting:

- Office installation options
- Privileged access
- Release preferences

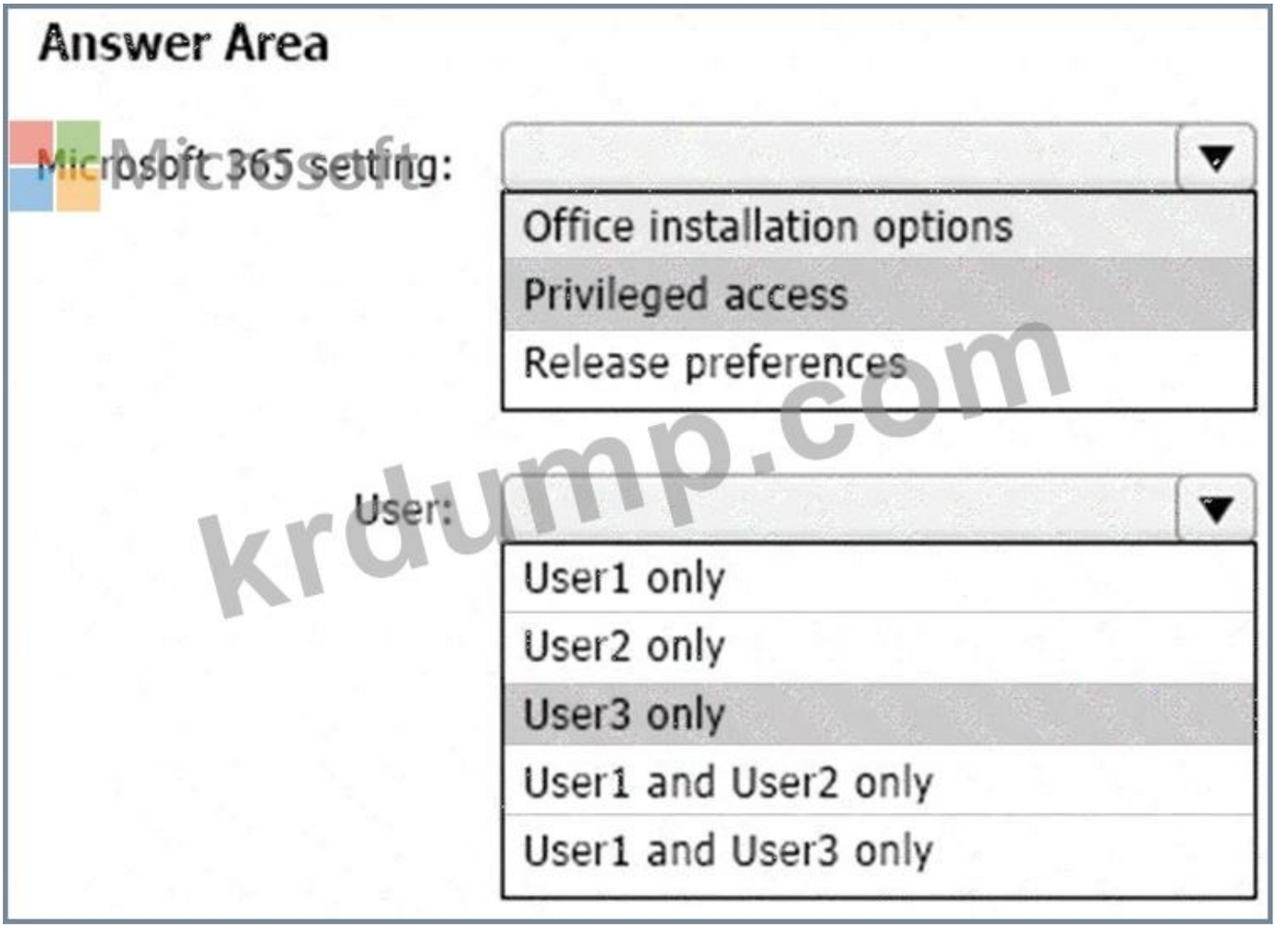
User:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

Answer:



Explanation:



NEW QUESTION: 151
□□ □□□ Azure ATP □□□ □□□□ □□□?
A. □□ 1
B. □□ 2
C. □□ 3
D. □□ 4
E. □□ 5
Answer: A (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning
However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

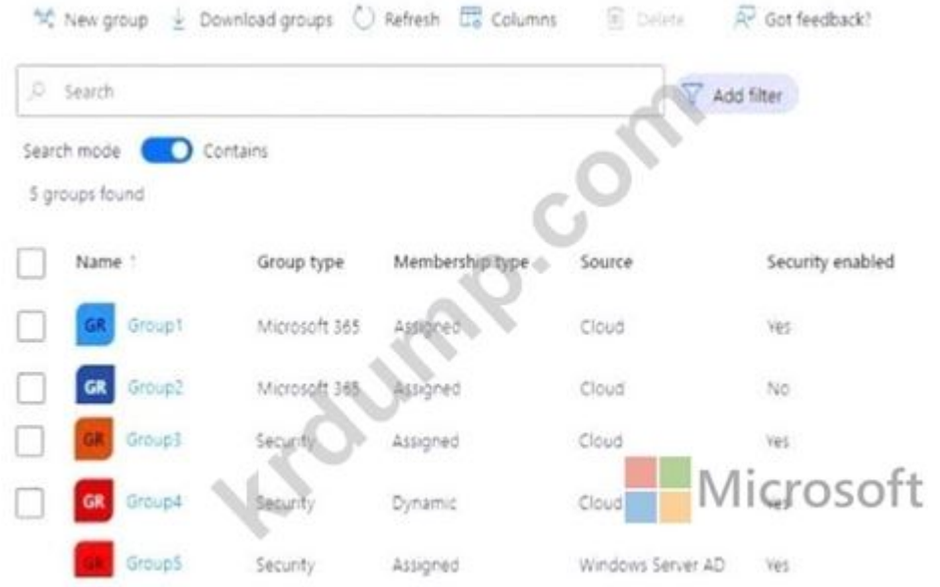
NEW QUESTION: 152
□□□ Contoso, Ltd.□□ □□□□ □□□□.
Contoso□ □□ □□ □□□ DNS □□□□ □□□□□ □□□ Microsoft 365 □□□ □□□□ □ □□□.
Contoso□ Fabrikam, Inc.□□ □□□ □□□□□.
Contoso□ □□ □□□□ Microsoft 365 □□□ □□□ □□□□□.
* □□□□□□
* □□□.□□□□□□
* □□□.□□□.com
□□ □□□ □□□□ □ □□□□ □□□ □□□ □ □□□ □□□□ □□□.
□ □□ □□□□ □□□□ □□, □□□□ □□ □□ □□□□□□ □□ DNS □□□ □□ □□□ □□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

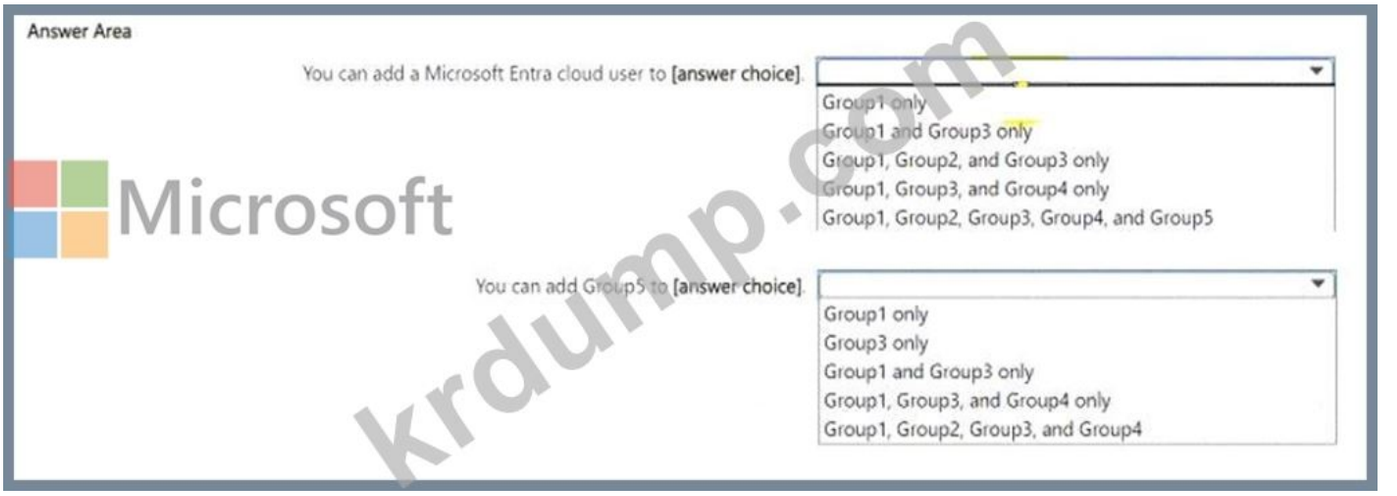
NEW QUESTION: 153

□□ □□□ □□□ □□□ □□□ Microsoft Entra □□□□ □□□□.

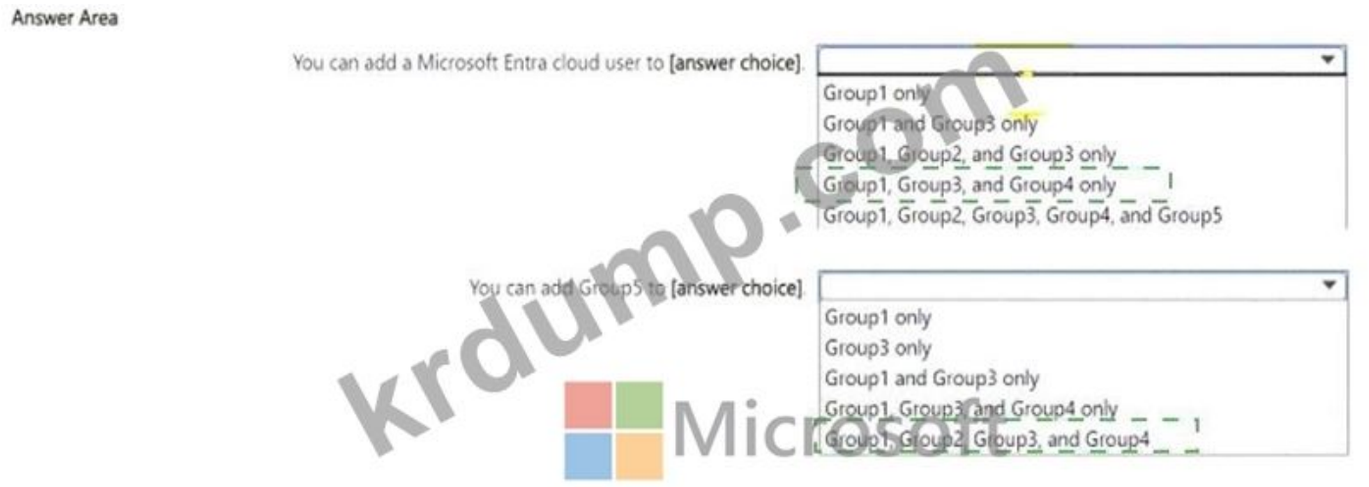


□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.

□□□□: □□ □□ □□□ 1□□ □□□ □□□□.



Answer:



Explanation:

You can add a Microsoft Entra cloud user to: Group1, Group3, and Group4 only

* Group1: Microsoft 365 group with assigned membership type and security enabled.
* Group3: Security group with assigned membership type and security enabled.
* Group4: Security group with dynamic membership type and security enabled.
* Group2 is not security enabled, so it cannot have security-related tasks assigned.
* Group5 is sourced from Windows Server AD, which may limit direct cloud user additions.

You can add Group5 to: Group1, Group2, Group3, and Group4

* Group5 can be added to other groups regardless of the membership type or source, as long as those groups (Group1, Group2, Group3, and Group4) are security-enabled and support such additions.

NEW QUESTION: 154

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

Label1□□□ □□□ □□□ □□□□ □□□□.
□□ □□□□ Label1□ □□□ □ □□□?
A. □□1□
B. □□2□
C. □□□ □□
D. Groupl □ Group2□
E. □□1, □□2, □□□ □□□
Answer: E (LEAVE A REPLY)
Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.
In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.
When you configure a label policy, you can:
Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

NEW QUESTION: 155
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
□□□□□ Active Directory □□□□ □□□□ □□□□.
Azure AD □□□□ □□□□□.
□□ □□□□ □□□□ Azure AD□ □□□□□□ □□□□□.
□□ □□(OU)□ 10□ □□□ □□□ Azure AD□ □□□□□ □□ □□ □□□□□□. □□ □□ □□□ □□□ □□□□□ □□□□□□□□.

Azure AD Connect Health□ □□□□ □□ □□□ □□ □□□□ □□□□□ □□□□□□ □□ □□□.
10□□ □□□ □□□ Azure AD□ □□□□□□□ □□□□ □□□.
□□ □□: Azure AD Connect□□ Azure AD □□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
The question states that "all the user account synchronizations completed successfully". Therefore, the Azure AD credentials are configured correctly in Azure AD Connect. 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: 156
Microsoft 365 E5 □□□ □□□□.
Policy1□□□ □□□ □□□ □□□ □□□ □□ □□□□□ Policy1□ □□□□□.
□□□ □□ □□□ □□ □□ □□ □□ □□(MFA)□ □□□□□ Policy1□ □□□□ □□□.
Policy1□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

Answer:

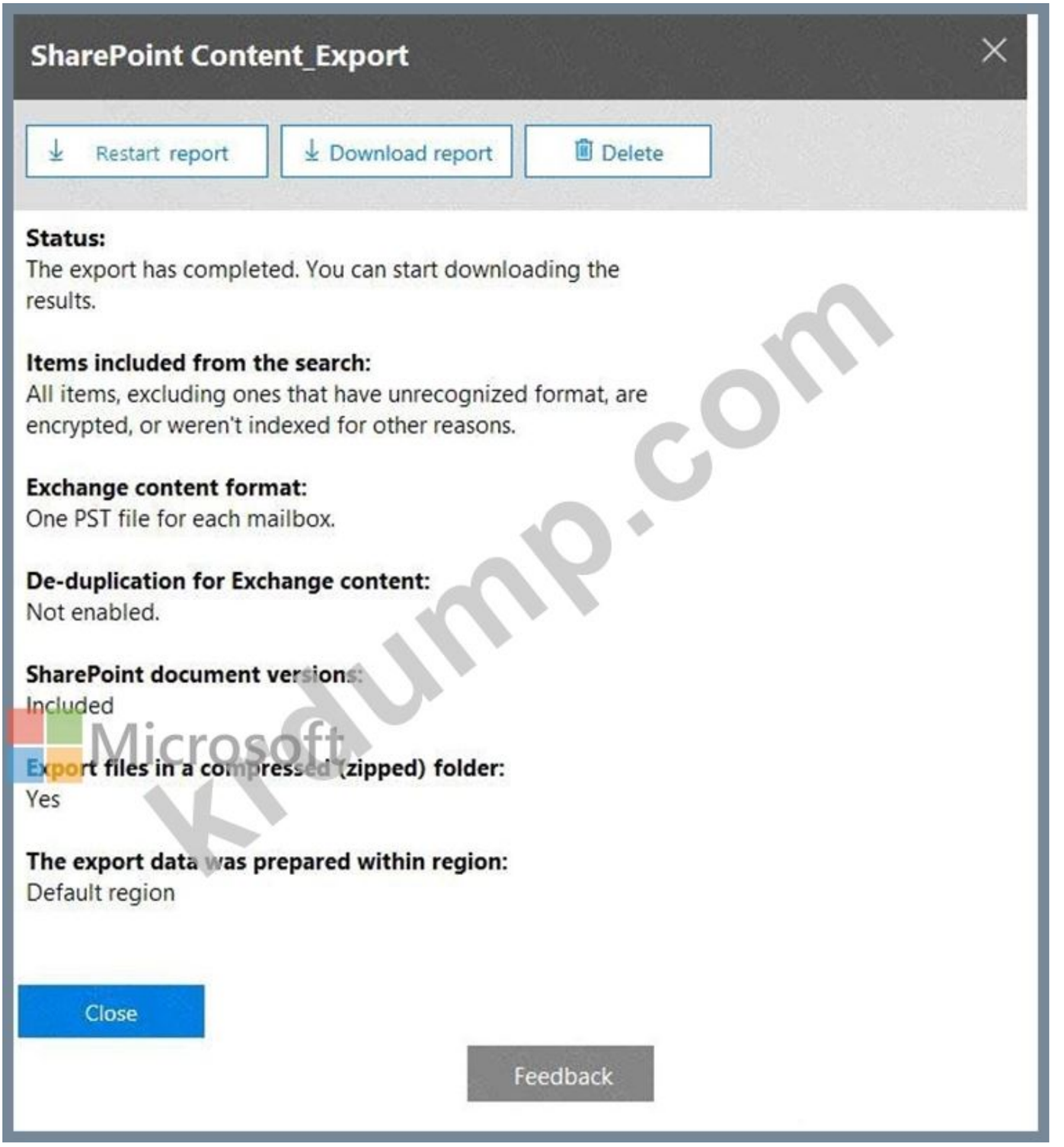
Answer Area

Explanation:
Conditions: Set "User risk" to "High"To enforce MFA based on user risk, you need to configure the Conditional Access policy to trigger when the user risk level is high. This setting ensures that the policy is applied only to users who have a high-risk level.
Grant: Require multi-factor authenticationThis setting enforces MFA for users who meet the condition set (high user risk). Requiring MFA ensures that users must provide additional verification, enhancing security for high-risk sign-ins.

NEW QUESTION: 157
□□: □ □□□□ □□□ □□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□ □ □□□ □□□.
□□□ □□ □ □ □□□ □□□□ □□□ □□□ □ □□□□. □□□ □□ □□□ □ □□ □□ □□□ □□□□ □□ □□ □□□□.
□ □□□ □□□ □□ □□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft 365 E5 □□□ □□ Office 365□ Microsoft Defender□ □□□□ □□□□.

□□, □□, □□□□□□ □□□□ □□ □□ □□ □□ □□ □□□□ □□□□ □□ □□□ □□ □□ □□□.
□□□: □□□ □□ □□ □□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 158
□□ □ □□ □□ □□ □□□□ □□□ □□□ □□ □□□ □□□□□ □□□□. (□□ □□ □ □□□□.)



□□□□ □□□□ □□□ □□□□□?

A. 10MB XLSX □□

B. 5MB MP3 □□

C. 5KB RTF □□

D. 80MB PPTX □□

Answer: B (LEAVE A REPLY)

Unrecognized file formats are excluded from the search.

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

NEW QUESTION: 159
□□□
Microsoft 365 E5 □□□ □□□□.
Azure AD Privileged Identity Management(PIM)□□ □□ □□□ □□ □□□ □□□ □□□ □□ □□ □□□ □□□□□.

Activation

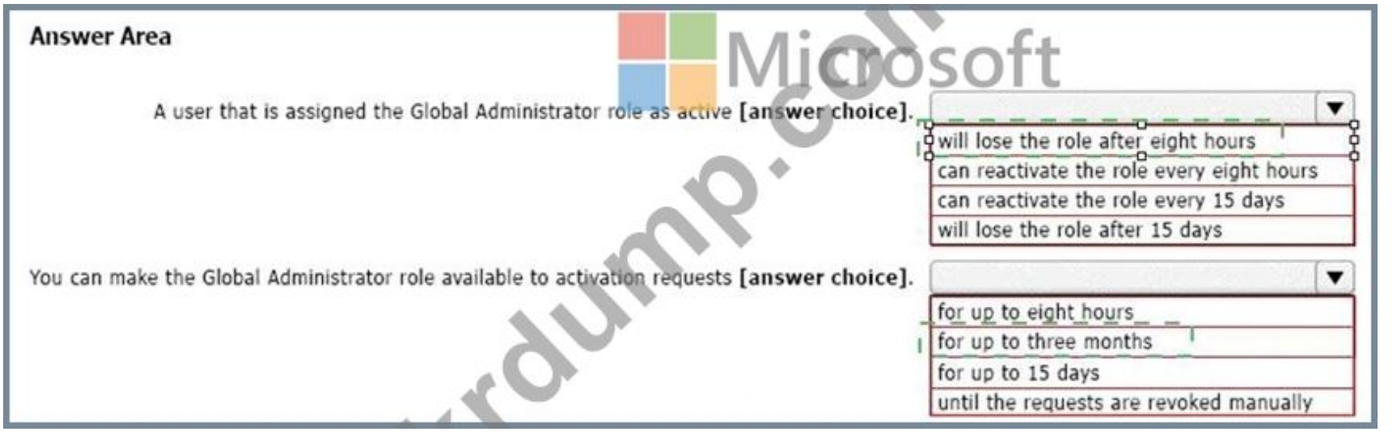
Setting	State
Activation maximum duration (hours)	8 hour(s)
On activation, require	Azure MFA
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

Assignment

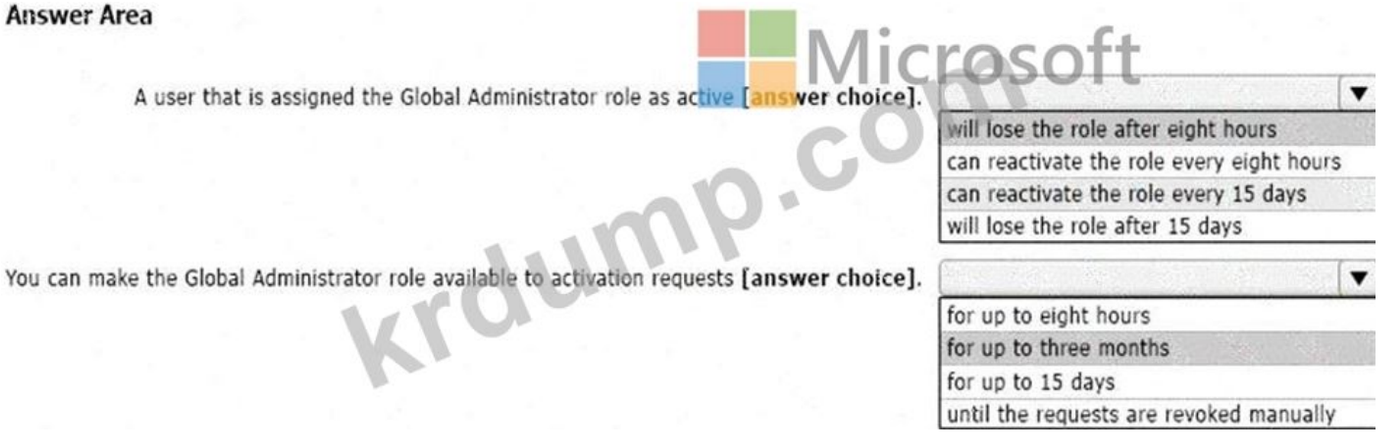
Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	15 day(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:



Explanation:



Box 1: will lose the role after eight hours

From exhibit: Activation, Activation maximum duration (hours): 8 hour(s) Box 2: for up to three months We see from exhibit: Assignment, Expire eligible assignment after: 3 month(s)

NEW QUESTION: 160

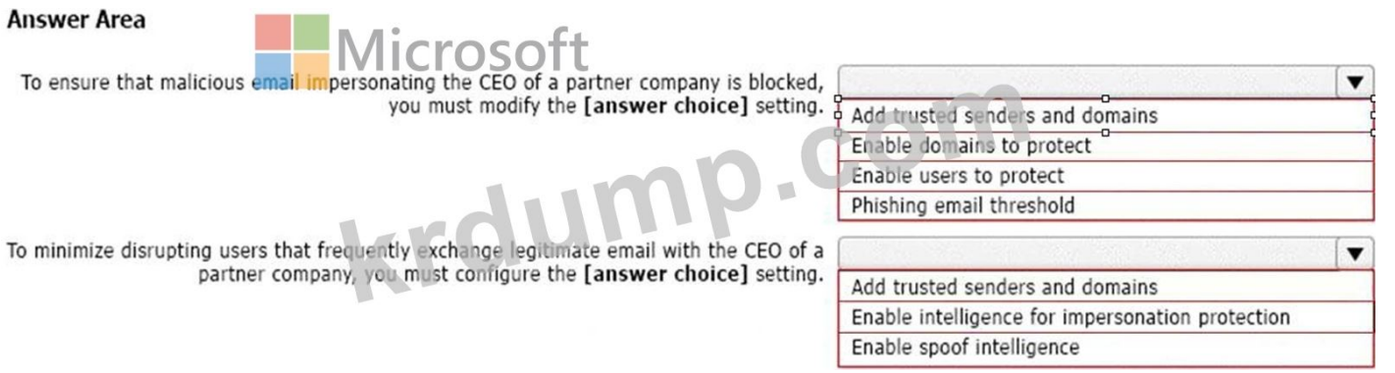
□□□

Microsoft 365 □□□ □□□□.

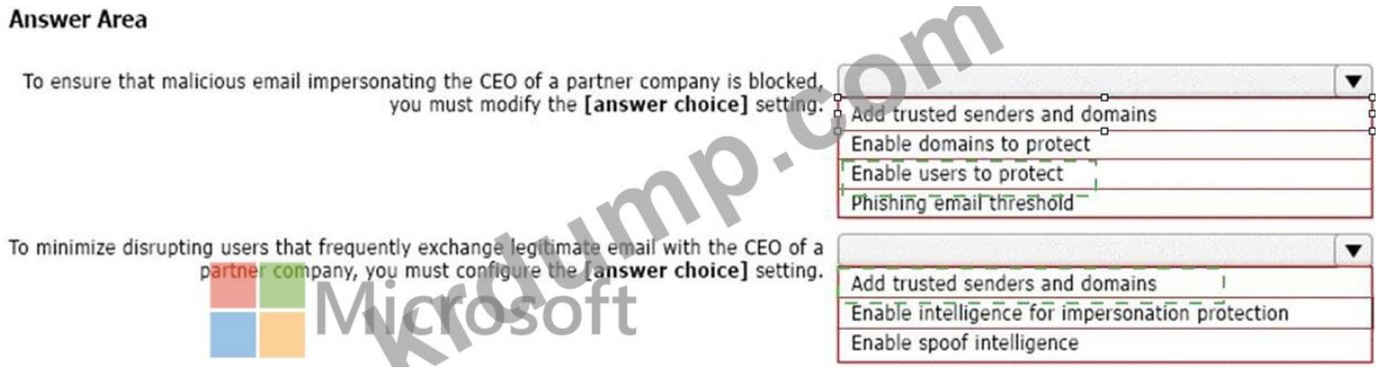
□□ □□□ □□□ □□ □□ □□ □□□ □□□□□.

□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.

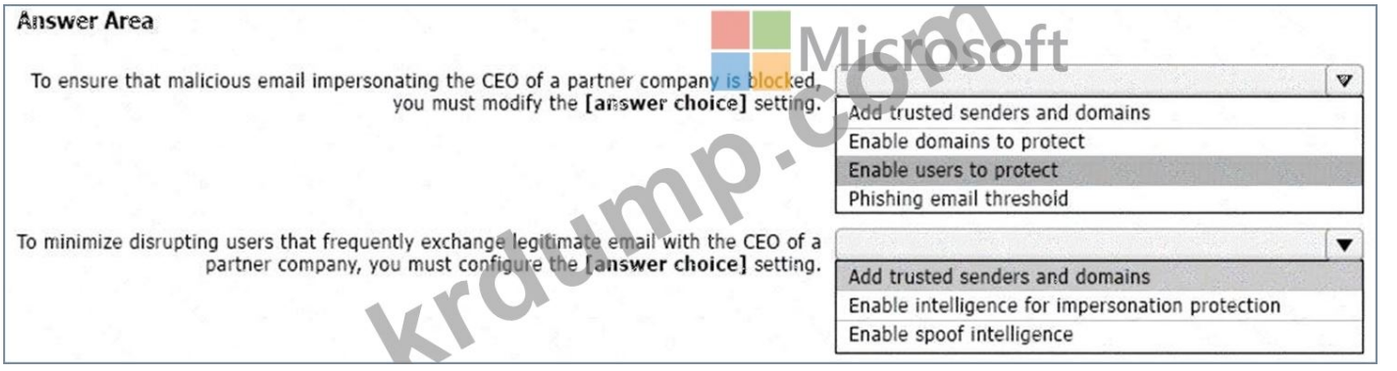
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Box 1: Enable users to protect

Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.

User impersonation protection

User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.

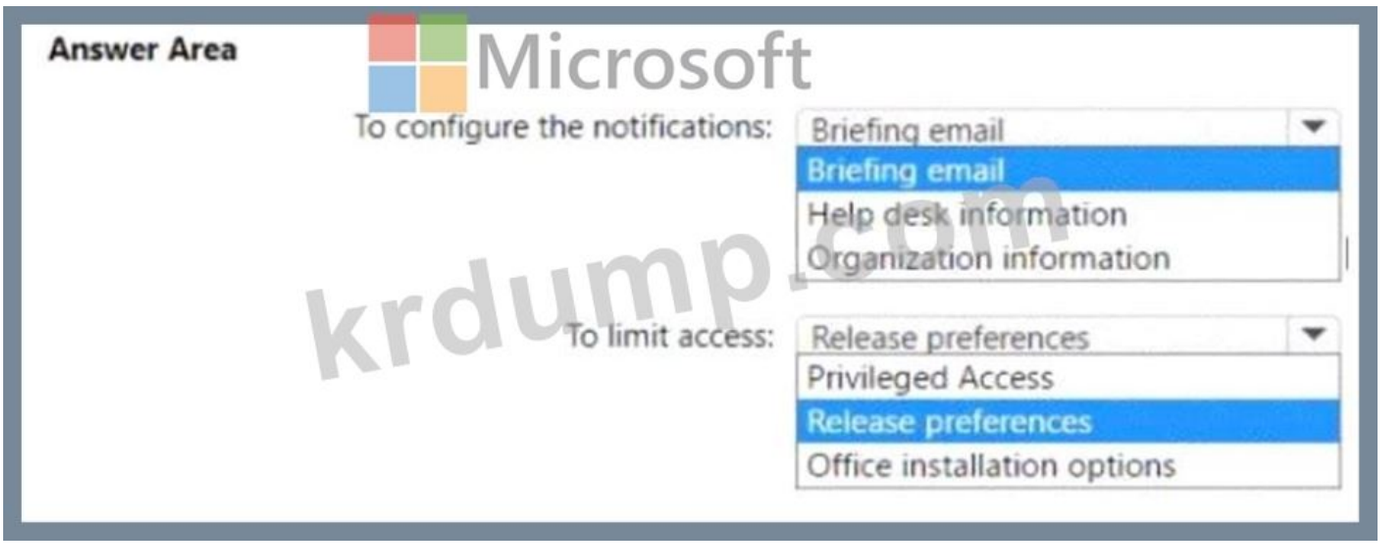
You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).

When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the

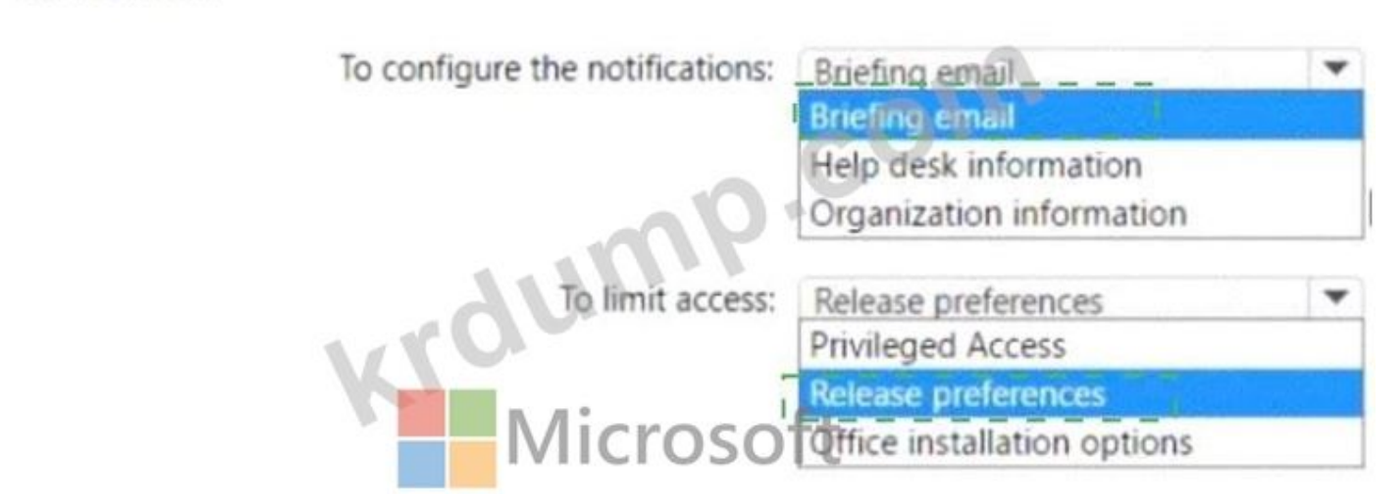
default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender's email address, the action for impersonated users is applied to the message.
Box 2: Add trusted senders and domains
Trusted senders and domains
Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren't applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.
eference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about

NEW QUESTION: 161
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Compliance Manager □□□ □□□□□ User1□ □□□□□ □□□.
□□ □□: Microsoft 365 □□ □□ □□□□ User1□ □□ □□ □□□ □□□ □□ □□□ □□ □□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)
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: 162
Office 365 □□□ □□ □□□ □□□□ □□□ □ □□ □□□□□ □□ □□□□ □□□□ □□ □. □□□□ □□ □□ □□□ □□□□ □□□.
Microsoft 365 □□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 163

500□□ Windows 10 □□□□□ Microsoft Endpoint Manager □□□□ □□ □□□ □□□ Microsoft 365 □□□□ □□□□.

□□□ □□□□ □□□ □□□ □□□ Microsoft Office 365 □□ □□□□ □ □□□ □□ □□□.

□□ □□ □□□ □□□□ □□□?

A. □□ □□ □□(ASR)

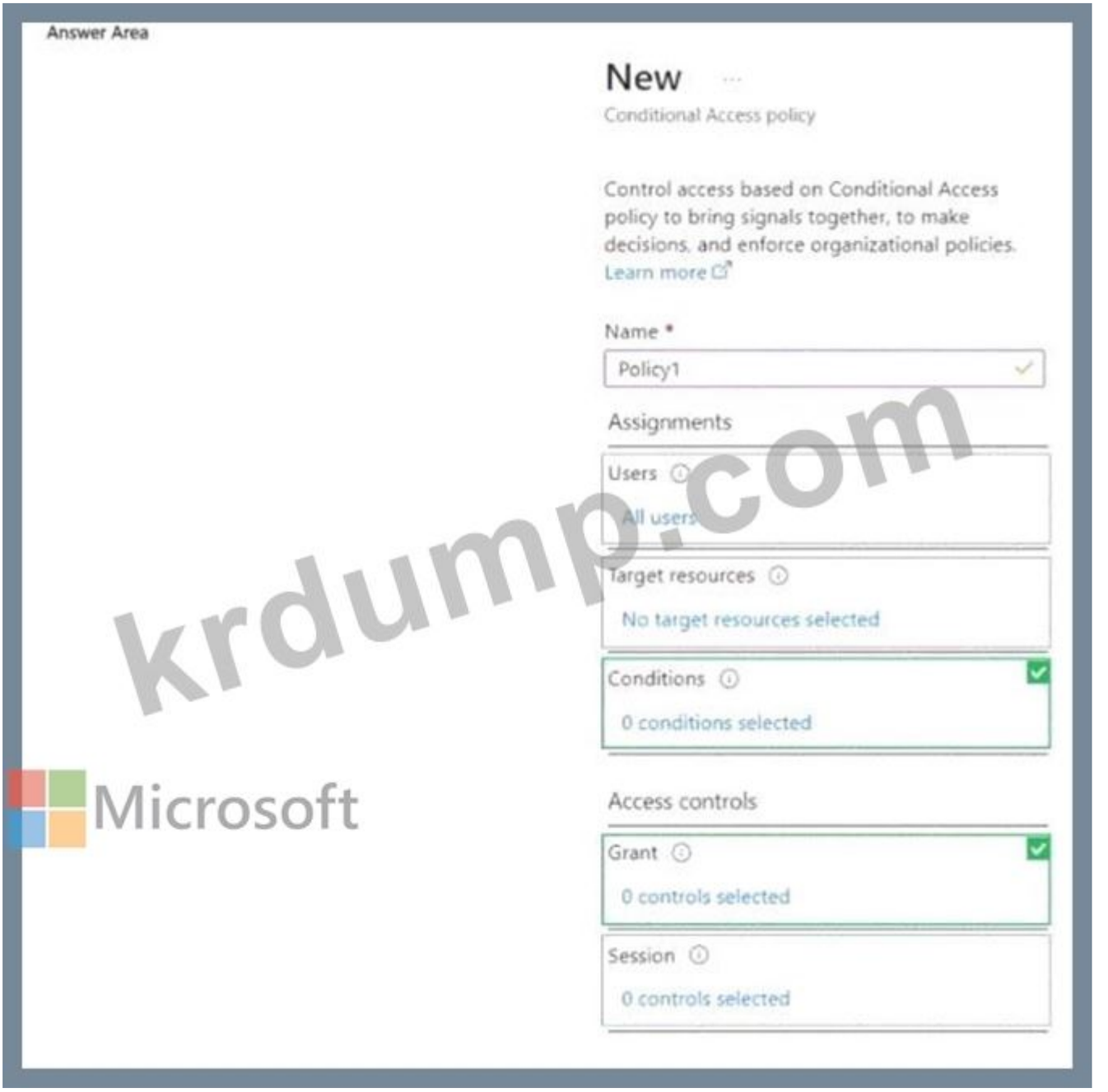
B. □□ □□

C. □□□ □□

D. □□□□□ □□ □ □□

Answer: (SHOW ANSWER)

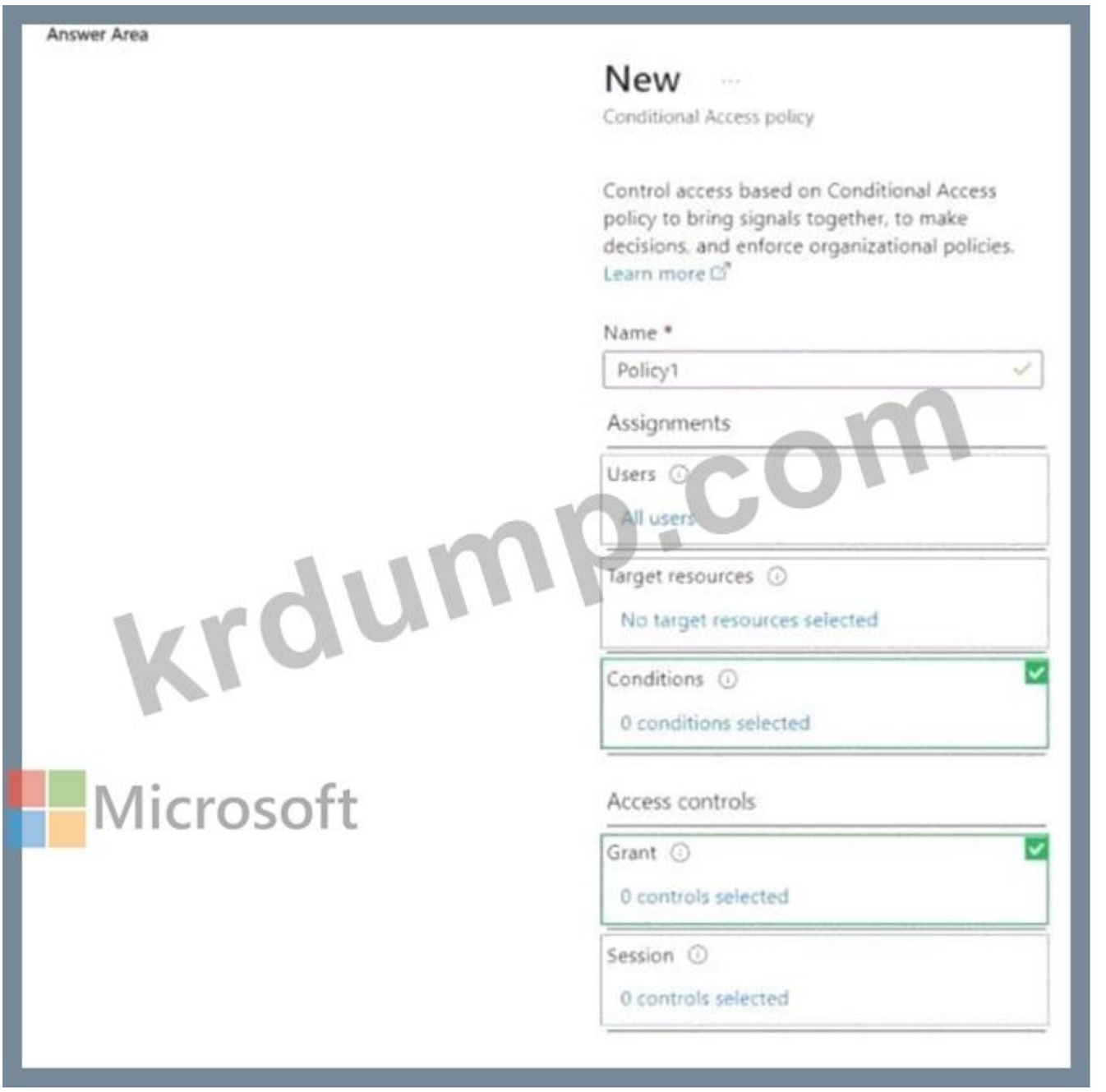
NEW QUESTION: 164
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□ Policy□□ □□□ □□□ □□□ □□□□ □□□.
* □□□ □□□□□ □□□□□.
* □□ □□(MFA)□ □□□□□.
□□ □ □□ □□□ □□□□ □□□? □□□□ □□□ □□□ □□□ □□□□□□. a. □□: □ □□□ 1□□□□.



Answer:

Answer Area

Explanation:



NEW QUESTION: 165

□□□

□□ □□ □□ □□ □□□□ □□□ contoso.com□□□ Azure AD □□□□ □□□□.

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

□□ □□ □□(MFA)□ 131.107.5.0/24□ □□□ □ □□ IP□ □□□□□ □□□□ □□□□.

□□□□ □□ □□ □□□ □□□ □□□ □□□□□.

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

□□ □□□ □□ □□□ □□□ □□□ □□□□.

* □□□ □□ □□ ID □□: □□ □□□
* □□□□ □ □□ □□ □□: App1
* □□: □□□ □ □□ □□ □□ □□
* □□□ □□: □□ □□ □□ □□

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

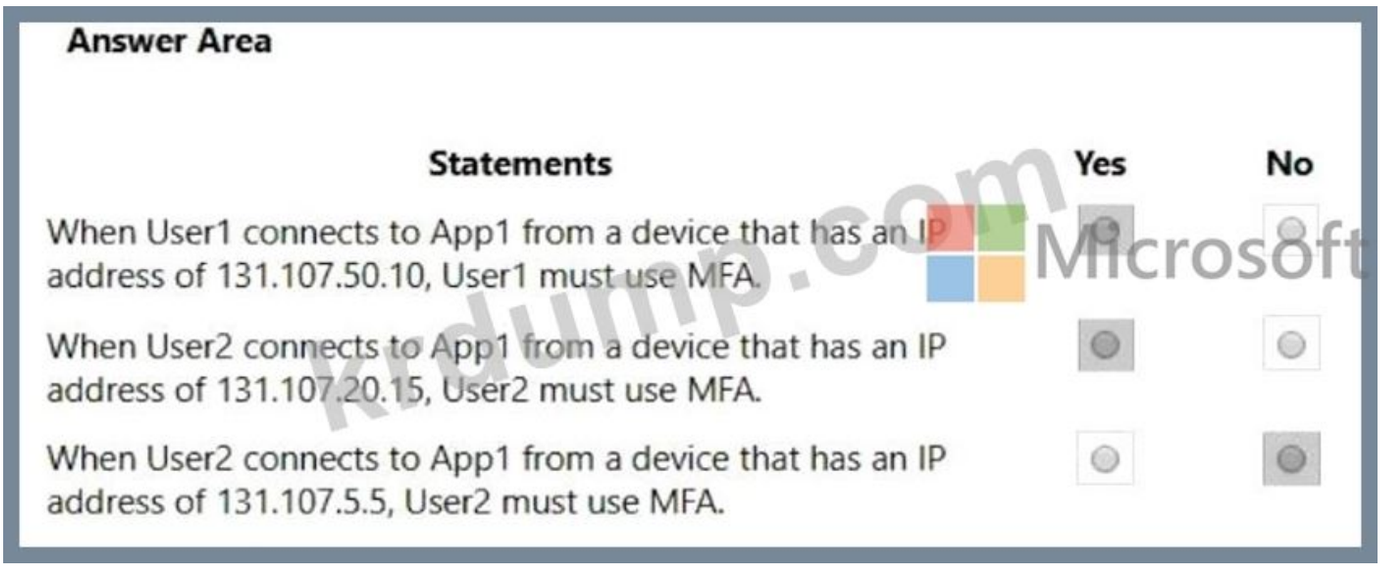
Statements	Yes	No
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.5.5,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

Answer:

Answer Area

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

Explanation:



Box 1: Yes

131.107.50.10 is in a Trusted Location so the conditional access policy applies. The policy requires MFA.

However, User1's MFA status is disabled. The MFA requirement in the conditional access policy will override the user's MFA status of disabled. Therefore, User1 must use MFA.

Box 2: Yes.

131.107.20.15 is in a Trusted Location so the conditional access policy applies. The policy requires MFA so User2 must use MFA.

Box 3: No.

IP not from Trusted Location so Policy does not apply, Subnet 131.107.5.5 is not in the range of 131.107.50.0

/24

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

NEW QUESTION: 166

Microsoft 365 E5 □□□ □□□□.

□□□□ □□ □□ □□□ □□□ □□□ □□□□.

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

Microsoft Endpoint Manager□ □ □□ □□□ □□□□ □□ □□□ □ □□ □□□ □□□□□?

A. Device1, Device4, Device6

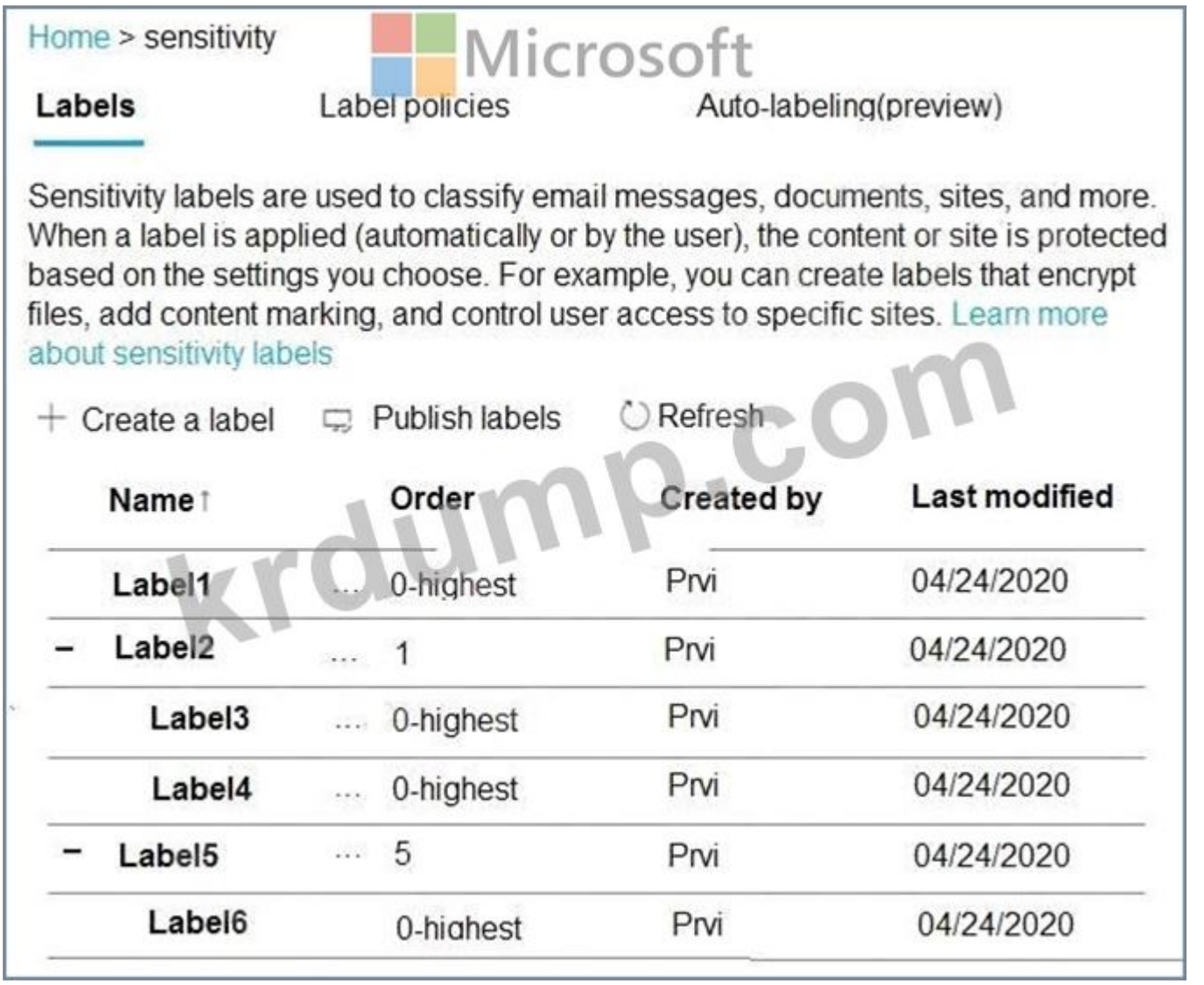
B. Device2, Device3, Device5

C. Device1, Device2, Device3, Device6
D. Device1, Device2, Device4, Device5
Answer: C (LEAVE A REPLY)
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: 167
1,000□□ Windows 10 □□□□□ □□□□ Microsoft 365 □□□□ □□□□. □□□□□ Microsoft Intune□ □□□□ □□□□.
□□ □□□ □□ □□□ □□□ □□ □□□ □□□ □□□.
* □□□ □□□□□ □□□□□.
* □□□ □□□ □□ □□□ □□□□ □□□□□.
* Microsoft Defender Antivirus □□□ □□ □□□ □□□□□□.
□□ □□□ □□□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □ □□ □□
B. □□ □□
C □□ □□ □□□
D □□□ □□□ □□

Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION: 168
□□ □□□□ □□□ □□□ □□□□□.



□□□□ □□□□ □□ □□□ □□□ □ □□□?

A. Label3, Label4, Label6□

B. □□1, □□2. □□3. □□4. □□5. □□□ □□6

C. Label1, Label2, Label5□

D. Label1, Label3, Label4, Label6□

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 169

2,500□□ Windows 10 □□□□□ User1□ User2□□ □ □□ □□□□ □□□□ Microsoft 365 E5 □□□□ □□□□. □□□□□ Microsoft Intune□ □□□□ □□□□□.
Microsoft Endpoint Manager□□ □□ □□□ □□ □□ □□□ □□ □□□□□.

Azure Active Directory(Azure AD)□□ □□ □□□ □□ □□□ □□ □□□□□.

Microsoft Endpoint Manager□□ User2□ □□ □□ □□□(DEM)□ □□□□□.

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□. □□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 170

User1□ □□ □□ □□□ □□□□□ □□□ □□□ □ □□□ □□□□ □□□. □□□ □□ □ □□?

A. Azure Active Directory □□ □□□□ User1□□ □□□□ □□ □□□ □□□ □□□□□.

B. Azure Active Directory □□ □□□□ □□□□ □□ □□ □ □□□ □□□□□.

C. Intune □□ □□□□ User1□ □□ □□ □□□□ □□□□□.

D. Intune □□ □□□□ □□ □□□ □□□□□.

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 171

Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□□□ □□□□ □□□ □□ □□□□ □□□ □ □□□ □ □□□□□.
□□ □□□ □□ □ □□□□ □□ □□□□ □□□□ □□□ □□□□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?

A. □□□ □□ □□ □□□ □□□□□.

B. □□□ □□□ □□(EDM) □□□□ □□□□.

C. Sec-RegulacoryComplianceUI cmdlet□ □□□□□.

D. Sec-LabelPolicy cmdlet□ □□□□□.

Answer: C (LEAVE A REPLY)

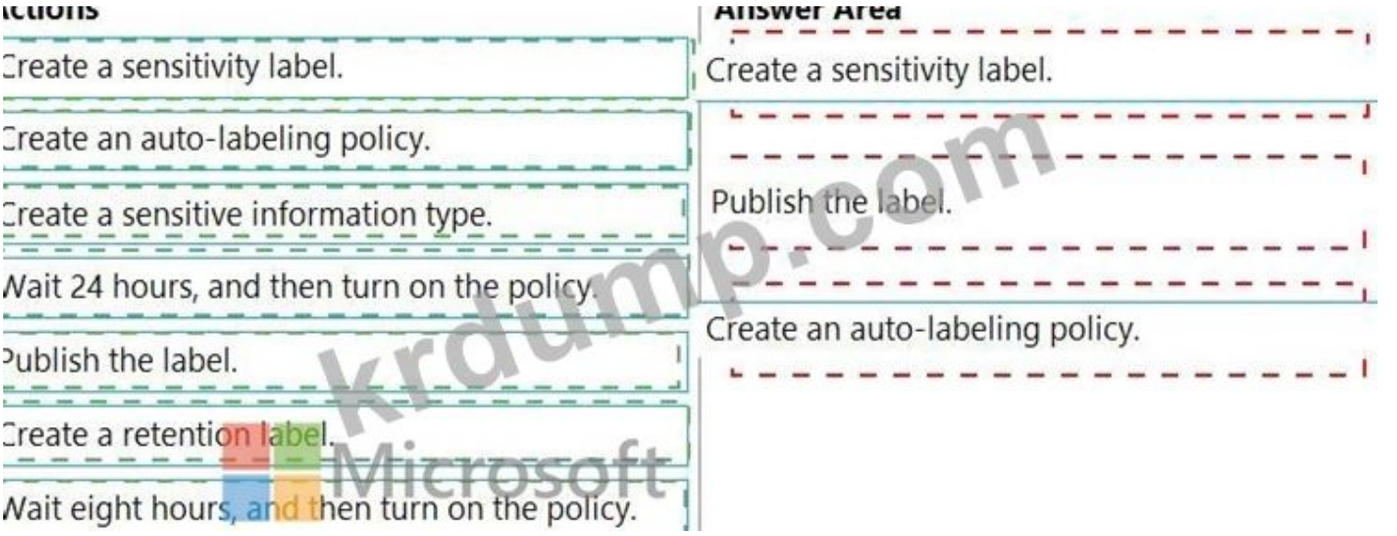
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide

NEW QUESTION: 172

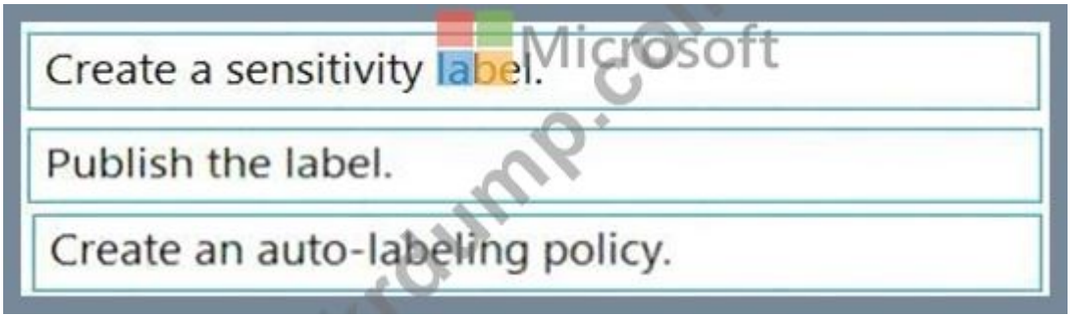
Site1□□□ Microsoft SharePoint Online □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Site1□□ □□□□ □□□ □□□ □□□ □□□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □ □□□ □□□ □□□ □□□ □□□□□.

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

Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what- label-policies-can-do
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365- worldwide

NEW QUESTION: 173

□□□

Microsoft 365 E5 □□□ □□□□.

□□ □□□ □□ Windows 11 □□□ Microsoft Defender for Endpoint□ □□□□□.

□□ □□ □□□ □□□□□ Defender for Endpoint□ □□□□ □□□.

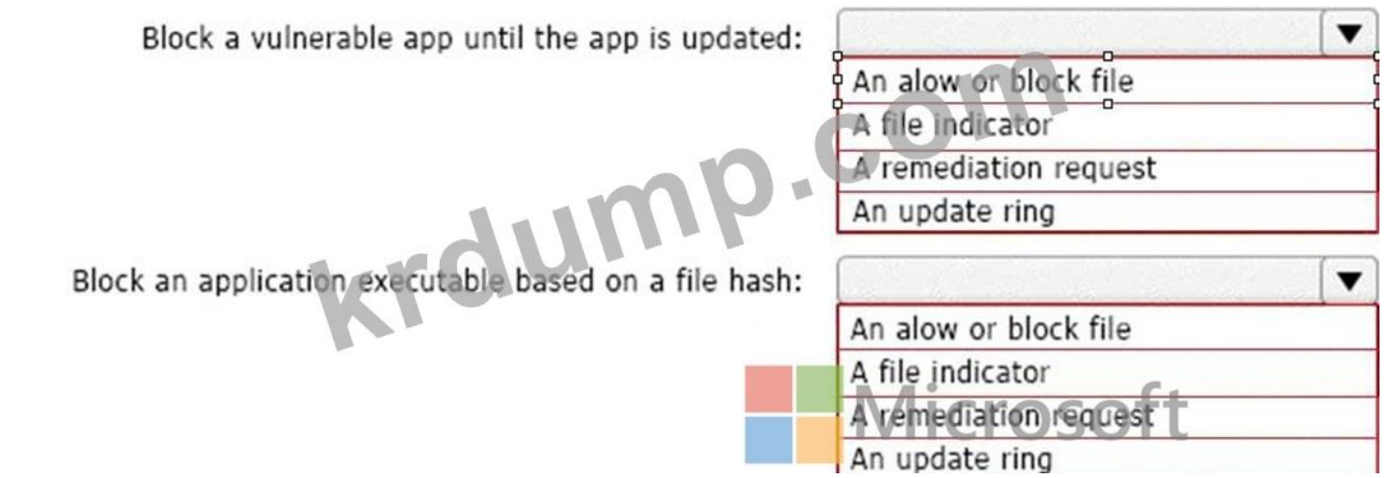
* □□ □□□□□ □□□ □□□ □□ □□□□□.

* □□ □□□ □□□□ □□□□□□ □□ □□□ □□□□□.

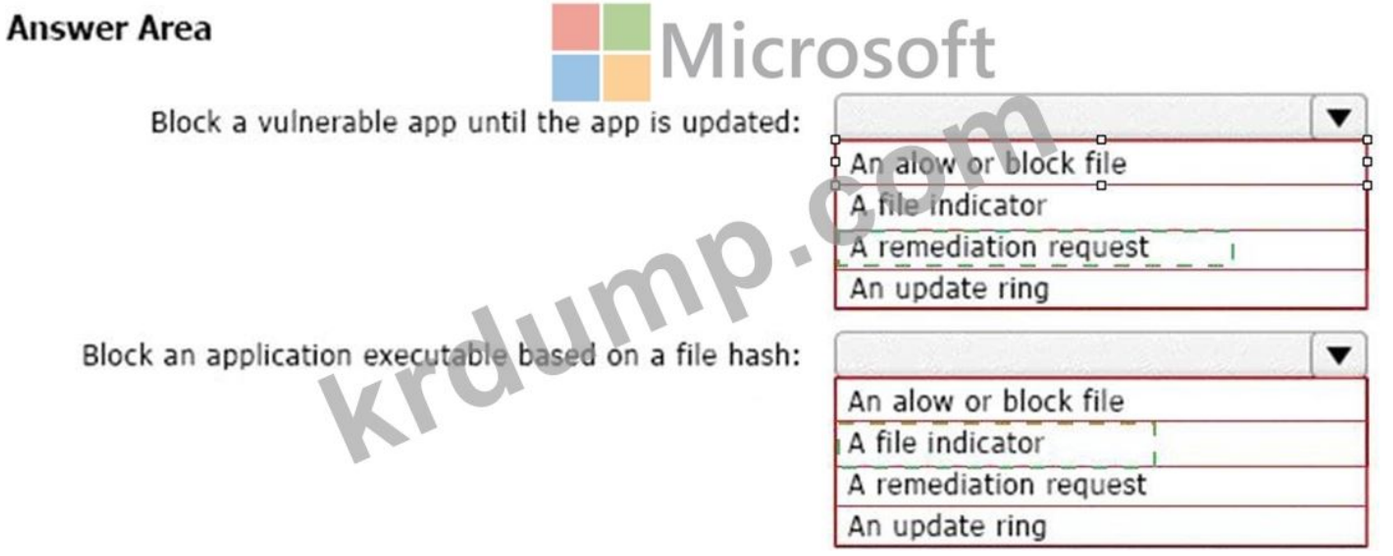
□□□□ □□□ □□□ □□□□□ □□□.

□ □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□ □.

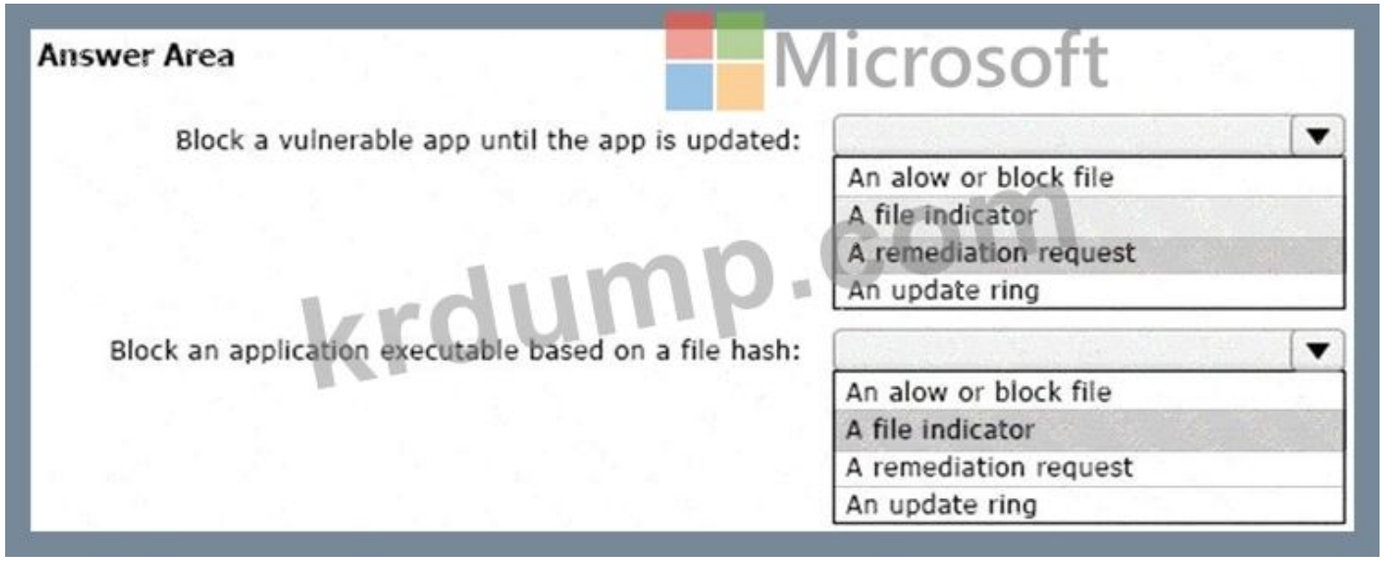
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



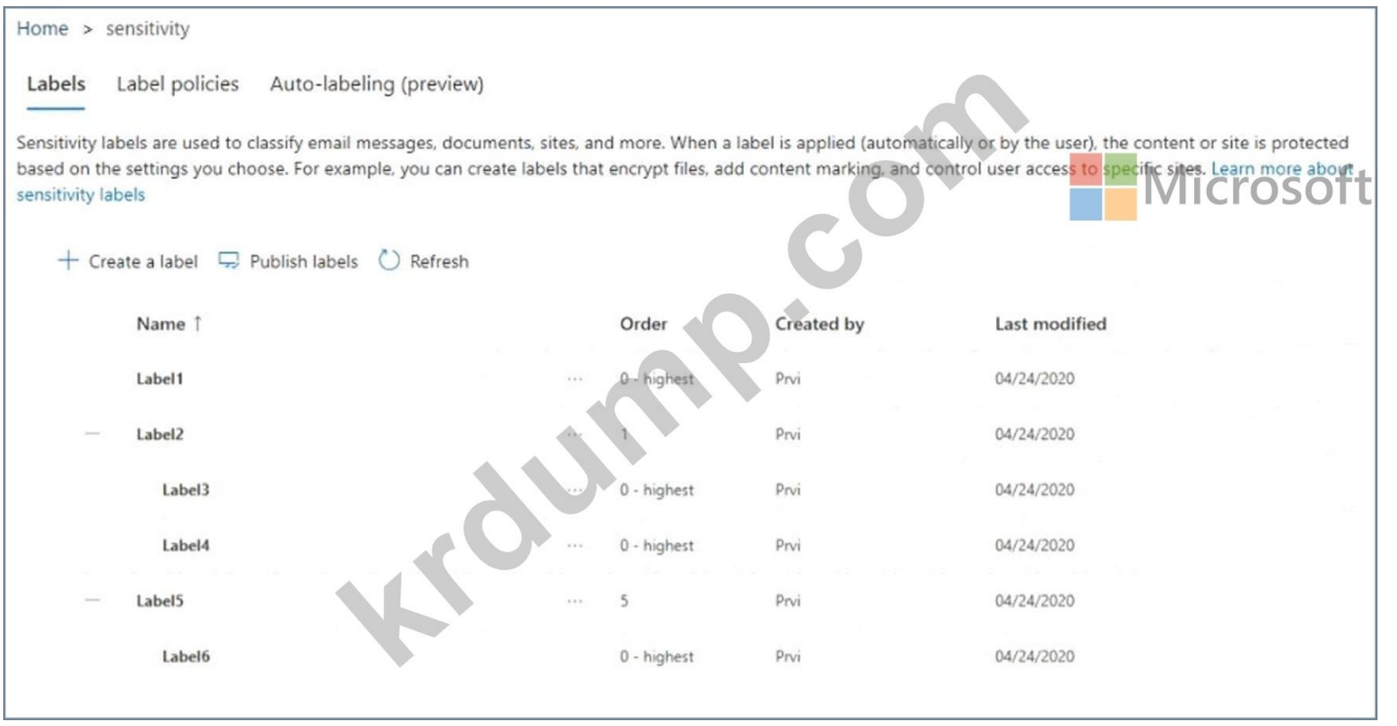
Box 1: A remediation request

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.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-block-vuln- apps

NEW QUESTION: 174
□□ □□ □□□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.



□□□□ □□□□ □□ □□□ □□□ □ □□□?

A. Label1, Label2, Label5□

B. Label1, Label2, Label3, Label4, Label5 □ Label6

C. Label3, Label4, Label6□

D. Label1, Label3, Labe2, Label6□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 175

User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □□ □□□ □□□□ Retention1□□□ □□□ □□ □□□□ □□□□.

User1□ □□□ □ □□ Retention1□ □□□□ □□□ □□□□ □□□□ □□□ □ □□□ □□ □□□.

Microsoft Exchange Online PowerShell□□ □□ cmdlet□ □□□□ □□□?

A. □□ □□□□

B. Start-AppBackgroundTask

C. Start-ManagedFolderAsslstant

D. Start-MpScan

Answer: C (LEAVE A REPLY)

NEW QUESTION: 176

□□□□□ Active Directory □□□□□ □□□□ □□□□.

Microsoft 365□ □□□□□.

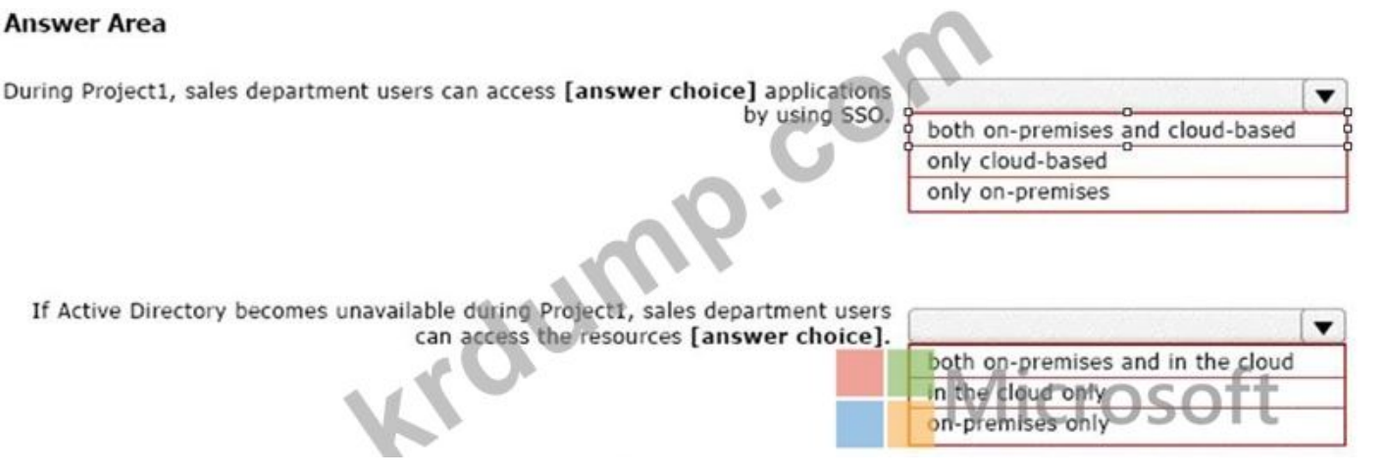
□□□□ □□□□ □□□ □□□□□.

□□□□ ID□ □□ □□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

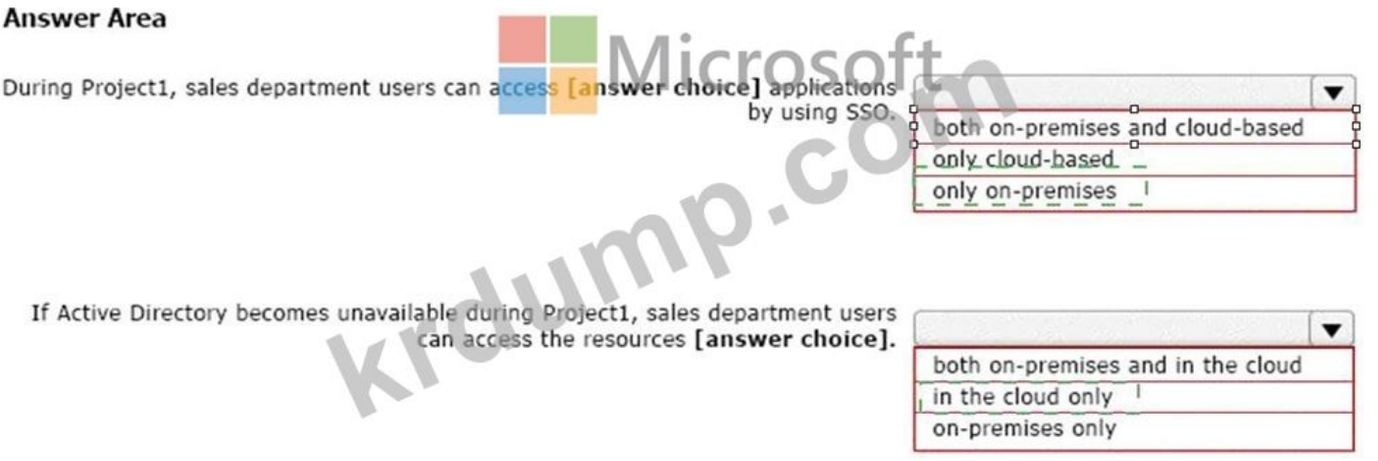
* Active Directory□ □□□ □ □□ □□ □□□□ Microsoft 365 □□□□ □□□□□ □□□ □ □□□ □□□.
* □□□ □□□□□ 10□ □□□□□ □□□.
□□□: □□□□ □□□ □□□□ Microsoft Entra Password □□□ □□□□□. □□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 177
□□□
Microsoft 365 □□□□ □□□□.
□□ □□□ □□ Azure AD Connect□ □□□□□.

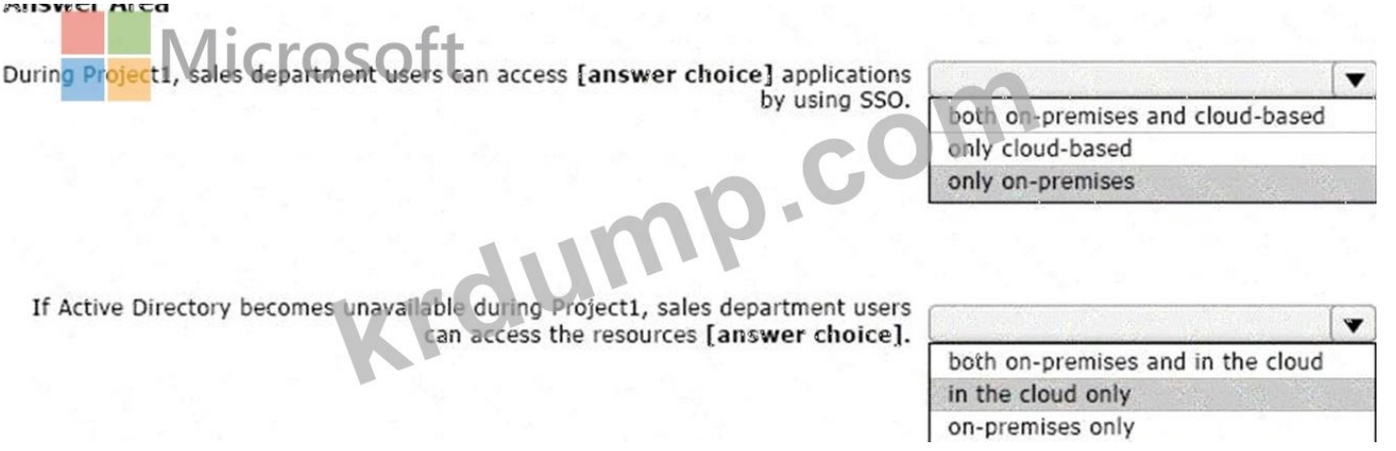
□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



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.

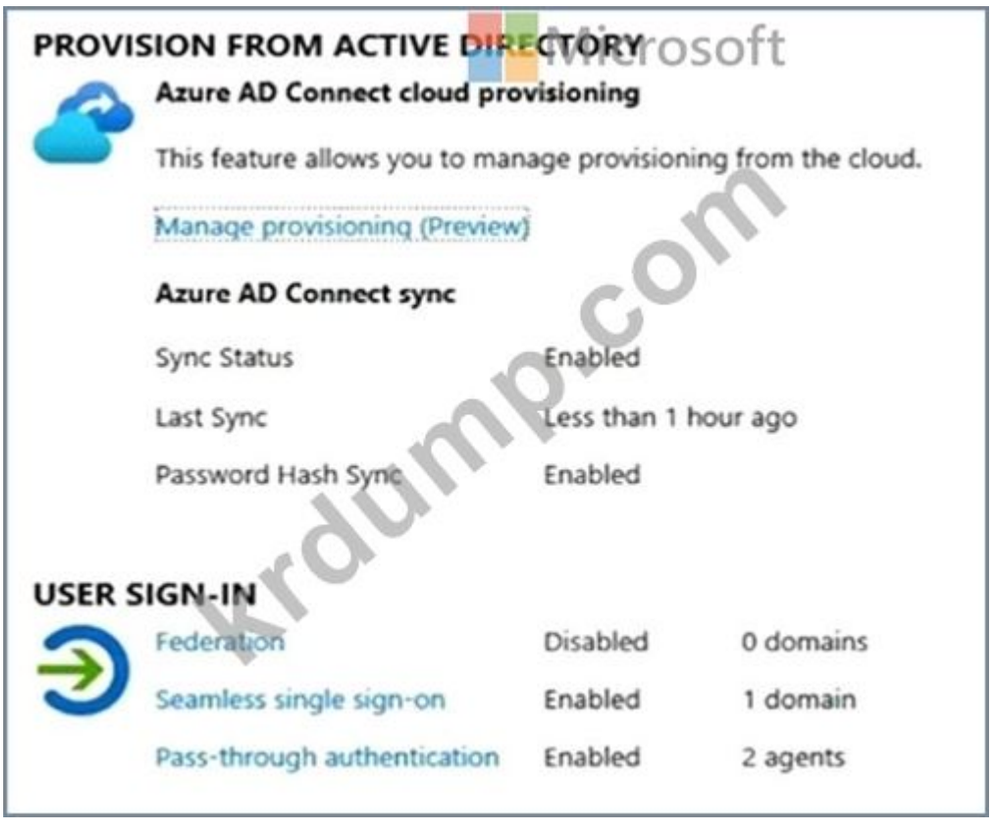
Box 2: in the cloud only

NEW QUESTION: 178
Microsoft 365 □□□□ □□□□.
Endpoint Protection □□ □□ □□□□ □□□ □□□□□.
□□□□ □□□□ □□ □□□□ □□□ □ □□□?
A. □□□ □□□
B. □OS
C. iOS
D. □□□□□
Answer: (SHOW ANSWER)
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: 179
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
□□□ □□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□ □□□ □. □ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

□□□□ □□□ □□□ □□ contoso.com□□□ Azure AD □□□□ □□□□□□. (□□ □□ □□□□□.)



User2□ user2@fabrikam.com□□ □□□□□□ Azure AD□ □□□□ □□□□□.
User2□ Azure AD□ □□□□ □□□□ □ □□□ □□□□ □□□.
□□□: □□□□□ Active Directory □□□□□ User2□ UPN □□□□ @contoso.com□□ □□ □□□. User2□□ user2@contoso.com□□ □□□□□□ □□□□□.
□□□ □□□ □□□□□?

A. □

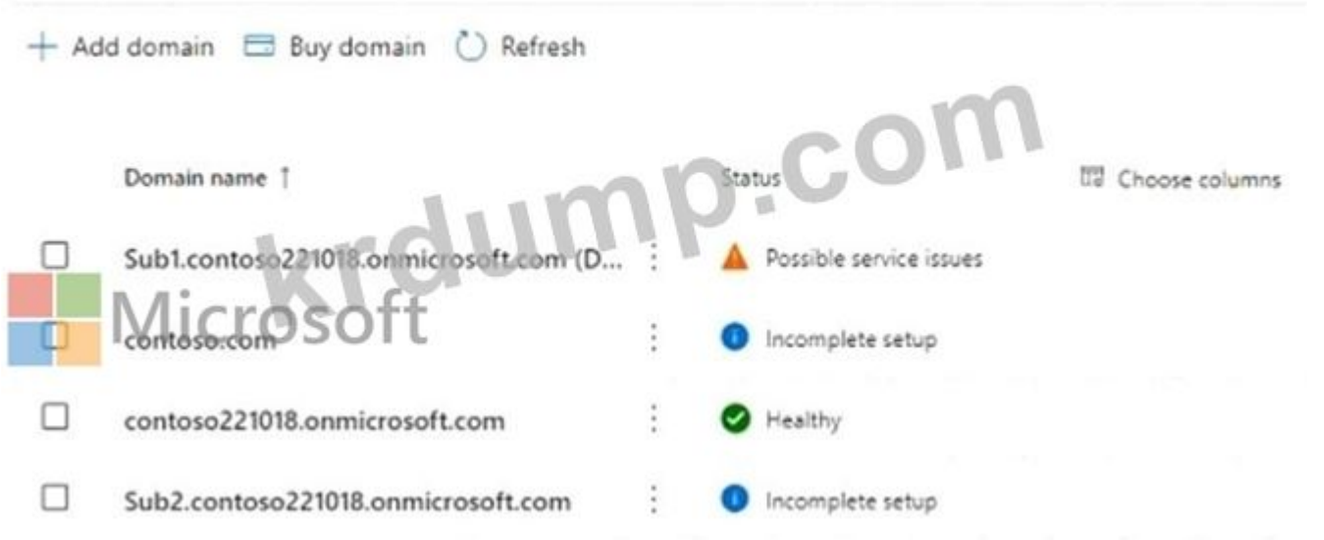
B. □□□

Answer: (SHOW ANSWER)

The on-premises Active Directory domain is named contoso.com. You can enable users to sign on using a different UPN (different domain), by adding the domain to Microsoft 365 as a custom domain. Alternatively, you can configure the user account to use the existing domain (contoso.com).

NEW QUESTION: 180

□□ □□□ □□□ □□□□ □□□ Microsoft 365 □□□ □□□□.



□□□□ □□□ □ □□ □□□ □□ □□□□ □□□ □ □□□?

A. □□□ □□ □□□

B. onlvcontoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com □ Sub2.contoso221018.onmicrosoft.com

C. Sub1.contoso221018.onmicrosoft.com□

D. onlycontoso.com □ Sub2.contoso221018.onmicrosoft.com

Answer: (SHOW ANSWER)

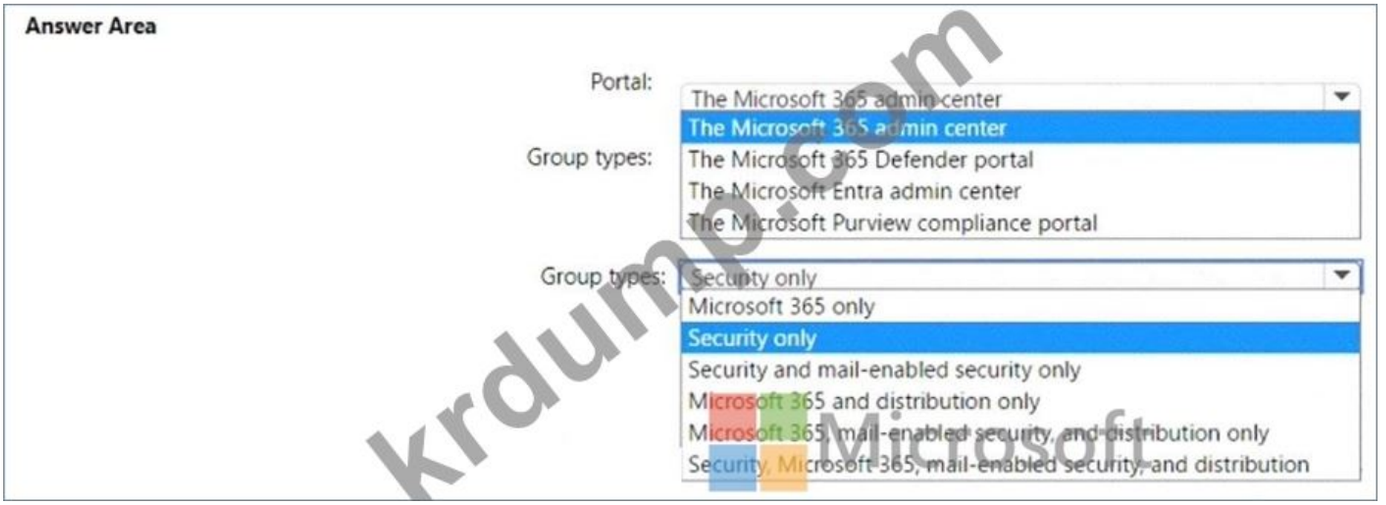
NEW QUESTION: 181

Microsoft 365 E5 □□□ □□□□.

□□ □□ □□□ □□□□ □□□.

□□ □□□ □□□□ □□, □□ □□□ □□□ □□□ □□□□□? □□□□□ □□ □□□□ □ □□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

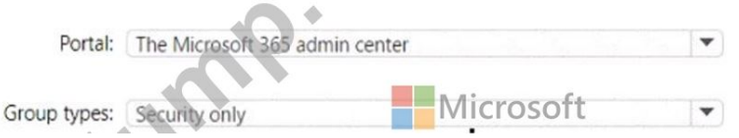


Answer:

Answer Area

Explanation:

Answer Area



NEW QUESTION: 182

Microsoft 365 E5 □□□□ □□□□.

□□ □□□□ □□ □□□□ □□□□ □□ □□□ □□□□□ □□□□ □□□.

Microsoft 365 □□ □□ □□□□ □□□ □□ □□□?

A. □□□ □□ □□(DSR) □□

B. □□ □□□ □□ □□(GDPR) □□□□ □□ □□□ □□ □□(DLP) □□□ □□□□.

C. EU GDPR □□ □□□□ □□□□ □□ □□

D. □□□ □□ □□ □□ □□□□ □□□□ □□ □□

Answer: C (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan

NEW QUESTION: 183

User1□□ □□ □□□ □□□□ □□□?

□□ □□□ □□ □□ (□□□ □□ □□ □□□ □□□□□)

A. □□□□

B. □□ □□

C. □□ □□□

D. □□ □□

Answer: C (LEAVE A REPLY)

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

Topic 5, Litware, Irk

Litware, Irk. is a consulting company that has a main office in Montreal and a branch office in Seattle?

Ltware collaborates with a third-party company named A. Datum Corporation.

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

* Password hash synchronization is enabled.
* Synchronization is enabled for the UtwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk Administrator
Admin3	Security Administrator
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure AD tenant has Security defaults enabled.
Litware identifies the following issues:
* Admin1 cannot create conditional access policies.
* Admin4 receives an error when attempting to use SSPR.
* Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.
Litware plans to implement the following changes:
* Implement Microsoft Intune.
* Implement Microsoft Teams.
* Implement Microsoft Defender for Office 365.
* Ensure that users can install Office 365 apps on their device.
* Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
* Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.
Litware identifies the following technical requirements:
* Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
* Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
* Litware users must be able to invite A. Datum users to participate in the following activities:
o Join Microsoft Teams channels,
o Join Microsoft Teams chats,
o Access shared files.
* Just in time access to critical administrative roles must be required.
* Microsoft 365 incidents and advisories must be reviewed monthly.
* Office 365 service status notifications must be sent to Admin2.
* The principle of least privilege must be used.

NEW QUESTION: 184
Microsoft 365 □□□ □□□□.
□□□ □□ Microsoft Office 365 □□□□□□□□ □□□□ □□□□□□□ □□□ □□□□□.
□□□ □□□□□ □□□□□□□□ □□□□ □□□□ □□□.
□□□ □□□ □ □□ □ □□ □□□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□ □.

□□□□: □□ □□□ 1□□□□.

A. Microsoft 365 □□ □□□□ □□□ □□ □□□□□ □□□□□.

B. Microsoft 365 □□ □□□□ □□□ □□ □□□□□ □□□□□.

C. Microsoft 365 □□ □□□□ □□ □□□□□ □□□□□.

D. Microsoft 365 □□□ □□□ agg□□ □□□□ □□□□□.

Answer: B,D (LEAVE A REPLY)

The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where Microsoft posts official messages with information including new and changed features, planned maintenance, or other important announcements.

The messages displayed in the Message center can also be viewed by using the Office 365 Admin mobile app.

Reference:

https://docs.microsoft.com/en-us/office365/admin/manage/message-center

https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app

NEW QUESTION: 185

100□□ Windows 10 □□□ □□□ Microsoft 365 E5 □□□□ □□□□.

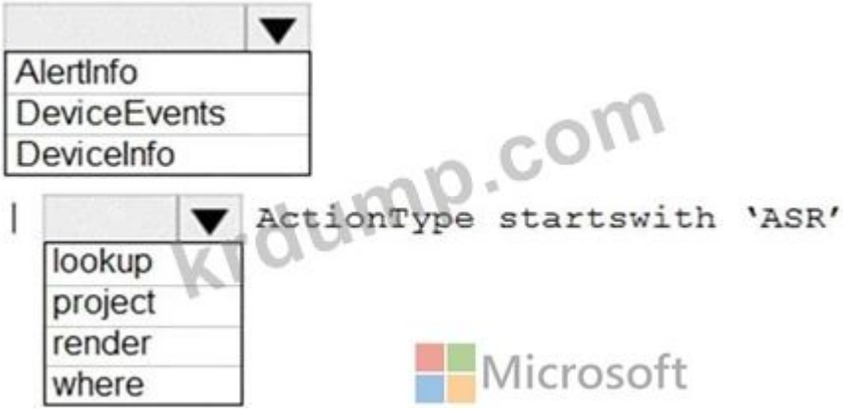
Windows 10 □□□ □□ □□ □□(ASR) □□□ □□□ □□□□□.

□□ □□□□ ASR □□□ □□□□ Log Analytics □□ □□□□ □□ □□□□ □□□□□.

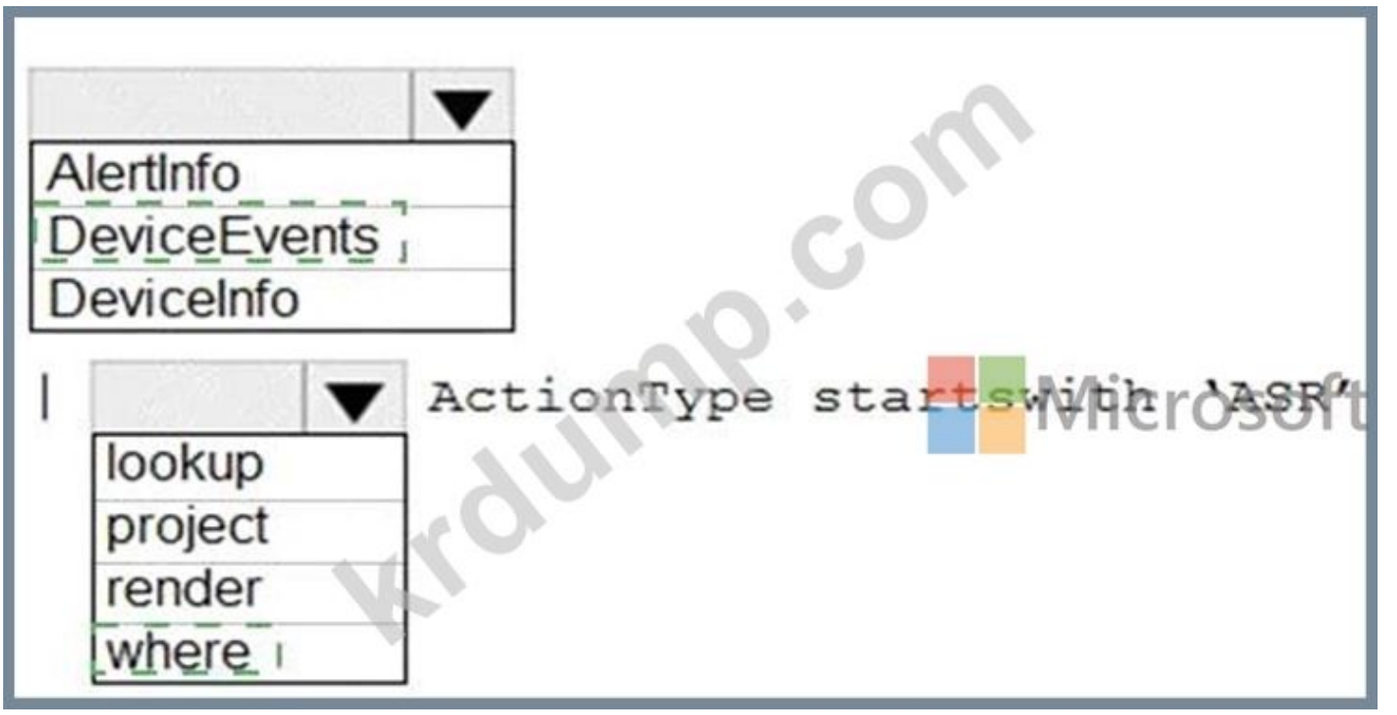
□□□ □□□ □□□□ ASR □□□ □□□ □□□.

Kusto □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

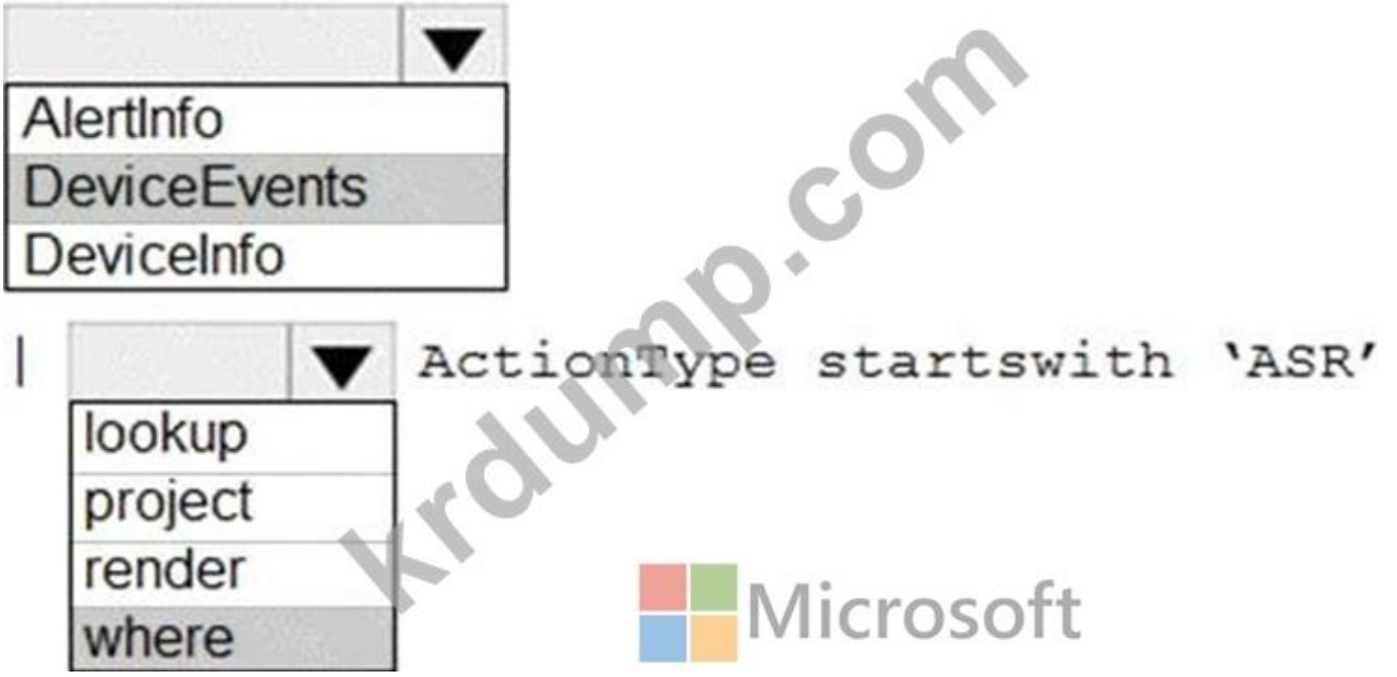
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Reference:
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface- reduction-rules-part-3/ba-p/1360968

NEW QUESTION: 186
□□□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□□□ □□□ □□□□ □□□□□.
□□ □□ □□□□ □□□ □□□□ □□□ □□□ □□□□□□ □□□□ □□□□□ □□□□ □□ □□□□□ □□□□□ □□ □□□□ □□□. □□ □□□ □□□□ □□□□□□ □ □□ □.

□□□ □□ □□□?
A. □□□□ □□□ □□□ □□ □□□ □□ □□(DLP) □□□ □□□□.
B. □□□ □□ □□ □□□ □□□ □□□□□.
C. □□□□ □□□□ □□ □□□ □□ □□□ □□ □□(DLP) □□□ □□□□.
D. □□□ □□□ □□ □□□ □□□□.
Answer: (SHOW ANSWER)
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: 187
Microsoft 365 □□□ □□□□.
Microsoft 365 Defender□□ eDiscovery Manager □□ □□□ □□□□ US eDiscovery Managers□□ □□ □□□ □□□□.
□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□□□ □□□ □□□ □□□ □ □□ □ □□ □□□.
□□ □□: Windows PowerShell□□ □□□ □□ □□□ □□ New-complianceSecurityFilter cmdlet□ □□□□□.
□□□ □□□ □□□□□?
A. □□□

B. □

Answer: (SHOW ANSWER)

NEW QUESTION: 188

□□□ □□□ Microsoft 365□ □□□□ □□□□.

□□□ □□□ □□□ □□ □□□ □□□□ □□□□□.

□□ □□ '□□'□□□ □□□ □□□ □□□ □□□□ □□□□ □□□□ □□□.

□□□ □□□□ □□□?

A. Microsoft 365 □□ □□□ Dace □□□

B. Exchange □□ □□□ □□ □□

C. Microsoft 365 □□ □□ □□□ □□□ □□ □□(DLP) □□

D. Exchange □□ □□□ □□ □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 189

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.

Microsoft 365 E5 □□□ □□□□.

SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.

SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Microsoft Defender for Office 365 □□ □ □□□ □□□ □ □□□ □□□□ □□□.

□□ □□: Microsoft 365 □□ □□□□ SecAdmin1□□ Exchange □□□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

You need to assign the Security Administrator role.

Reference:

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

NEW QUESTION: 190

Microsoft 365 ES □□□ □□□□.

Microsoft 365 Defender □□□□ □□□ Microsoft Secure Score□ □□□□□.

□□ □□ □□□□ □□□ □□□□ □□□□□.

□□ □□ □□□ □□□□ □□□ □□□□ □ □□□ □□□.

□□ □□□ □□□□ □□□?

A. □□

B. □□ □□ □□
C. □□□ □□ □□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 191
Youi □□□□□□ Active Directory □□□□ □□□□ □□□□.
□□ □□□□ □□□□□ Microsoft Entra □□□□ □□□□.
Microsoft Entra Connect Sync□ □□□□ □□□□ □□ □□□□□□□. □□ □□ □□□ □ □ □□□ □□□ □□□□□□□□□.
□□□ □□ □□□ □□□□□ Microsoft Entra ID Protection□ □□□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Microsoft Entra Connect□□ □□□□ □□□ □□□□□□.
B. Microsoft Entra □□ □□□□ □□ □□□ □□ □□□ □□□□□.
C. Microsoft Entra □□ □□□□ □□ □□□□ □□□□□□.
D. Microsoft Entra Connect□□ □□□□ □□ □□□□ □□□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 192
□□□ □□□□□□ □ □□ Active Directory □□□□□ □□□□. □□□□ □□□ □□□□ □ □ □□□ □□□□.
Microsoft Entra □□□□ □□□□.
□+□□□□ Active Directory□ Microsoft Entra □□□□ □□□□□□ □□□.
□□□ □□□□ □□□□ □□□. □□□□ □□ □□□ □□□□□□ □□□□ □□□ □ □□ □□□ □ □□ □□□ □ □□□ □□ □□□.
□□□□□ □□□ □□□□ □□□?
A. 3□□ Microsoft Entra Connect □□□ □□□ □□□□ □□□ 3□□ Microsoft Entra Connect □□□ □□
B. □□□□ □□□ 6□ Microsoft Entra Connect □□□ □□□ 3□ Microsoft Entra Connect □□ □ □□
C. □□□□ □□□ □ □□ Microsoft Entra Connect □□□ □□□ □□□ Microsoft Entra Connect □□□ □□
D. □□□ Microsoft Entra Connect □□□ □□□ □□□□ □□□ □□□ Microsoft Entra Connect □□□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 193
Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□ □□□ □□ □□□ □□□□□.


How do you want the alert to be triggered?
Every time an activity matches the rule
When the volume of matched activities reaches a threshold
More than or equal to 15 activities
During the last 60 minutes
On All users
When the volume of matched activities becomes unusual
On All users

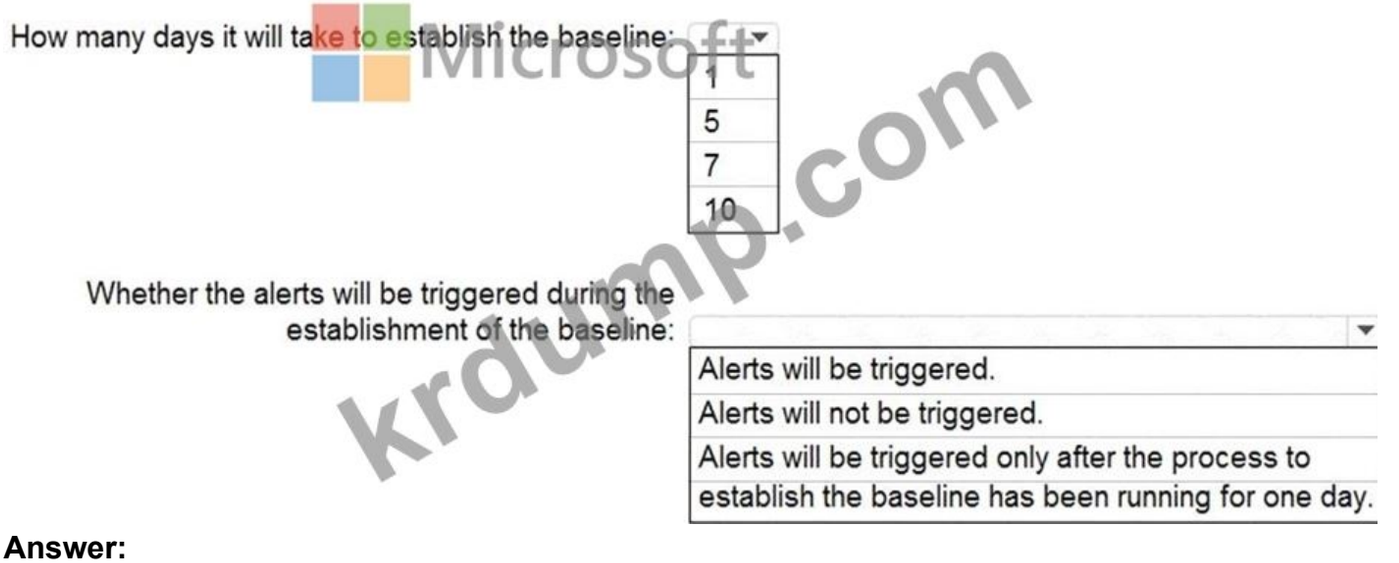
□□ □□□ □□□□ □□□.

* □□□□□ □□□ □□ □□□□ □□□□ □ □□□ □□□□?

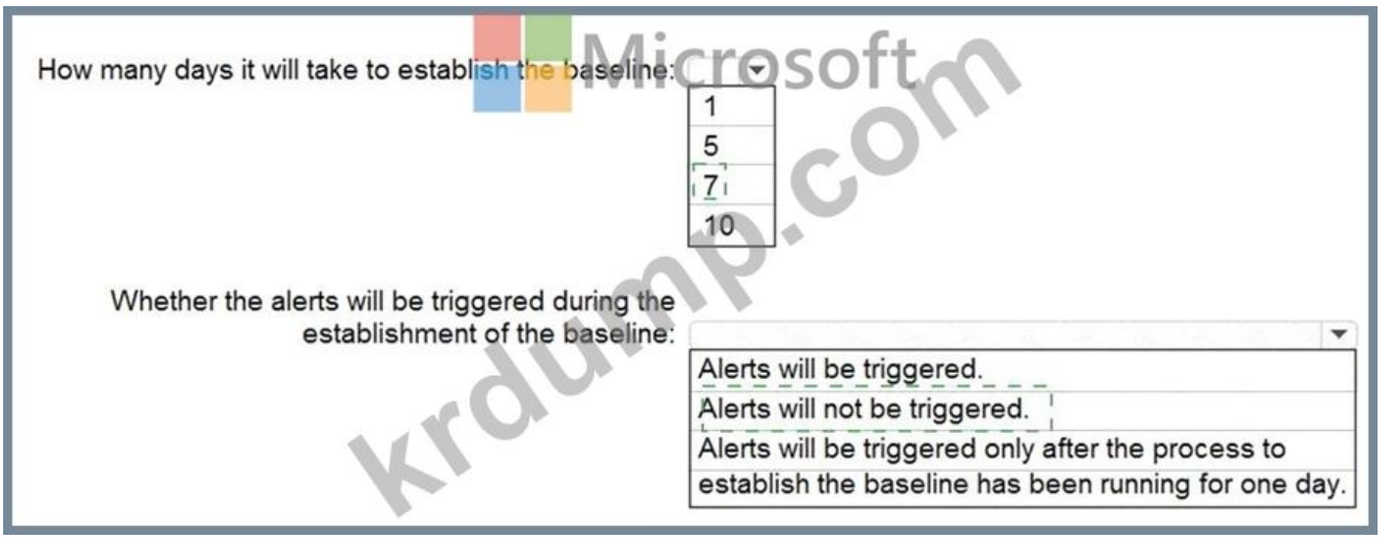
* □□□□ □□□□ □□ □□□ □□□□□ □□.

□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

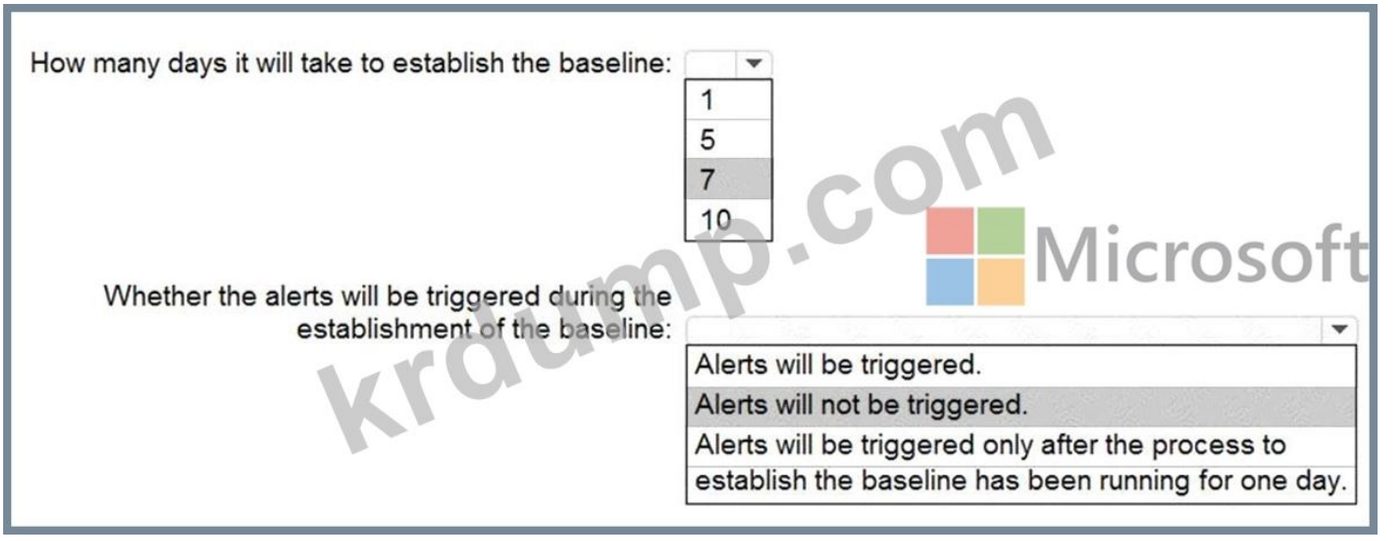
□□□□: □□ □□□ 1□□□□.


How many days it will take to establish the baseline:
1
5
7
10
Whether the alerts will be triggered during the establishment of the baseline:
Alerts will be triggered.
Alerts will not be triggered.
Alerts will be triggered only after the process to establish the baseline has been running for one day.

Answer:



Explanation:



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

NEW QUESTION: 194
Microsoft Defender for Endpoint□ □□□□ Microsoft 365 □□□ □□□□.
□□□ □□ □□□ Microsoft Defender for Endpoint□ □□□□ □□□□.
□□ 24□□ □□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□ □□□.
□□□ □□ □□□?
A. □□ □□□□ □□□ □□ □□□ □□□□.
B. Microsoft Purview □□ □□ □□□□ □□ □□ □□□ □□□□.
C. Microsoft Purview □□ □□ □□□□ DLP(□□□ □□ □□) □□□ □□□□.
D. □□ □□□□□ □□ □□□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 195

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □ □□ □□ □□□□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
□□□□□ Active Directory □□□□□ □□□□ □□□□.
Microsoft 365□ □□□□□.
□□□□ □□□□ □□□ □□□□□.
□□□□ ID□ □□ □□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Active Directory□ □□□ □ □□ □□ □□□□ Microsoft 365 □□□□ □□□□□ □□□ □ □□□ □□□.
* □□□ □□□□□ 10□ □□□□□ □□□.
□□□: Azure AD □□□□□ □□ □□ □□□□ □□□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

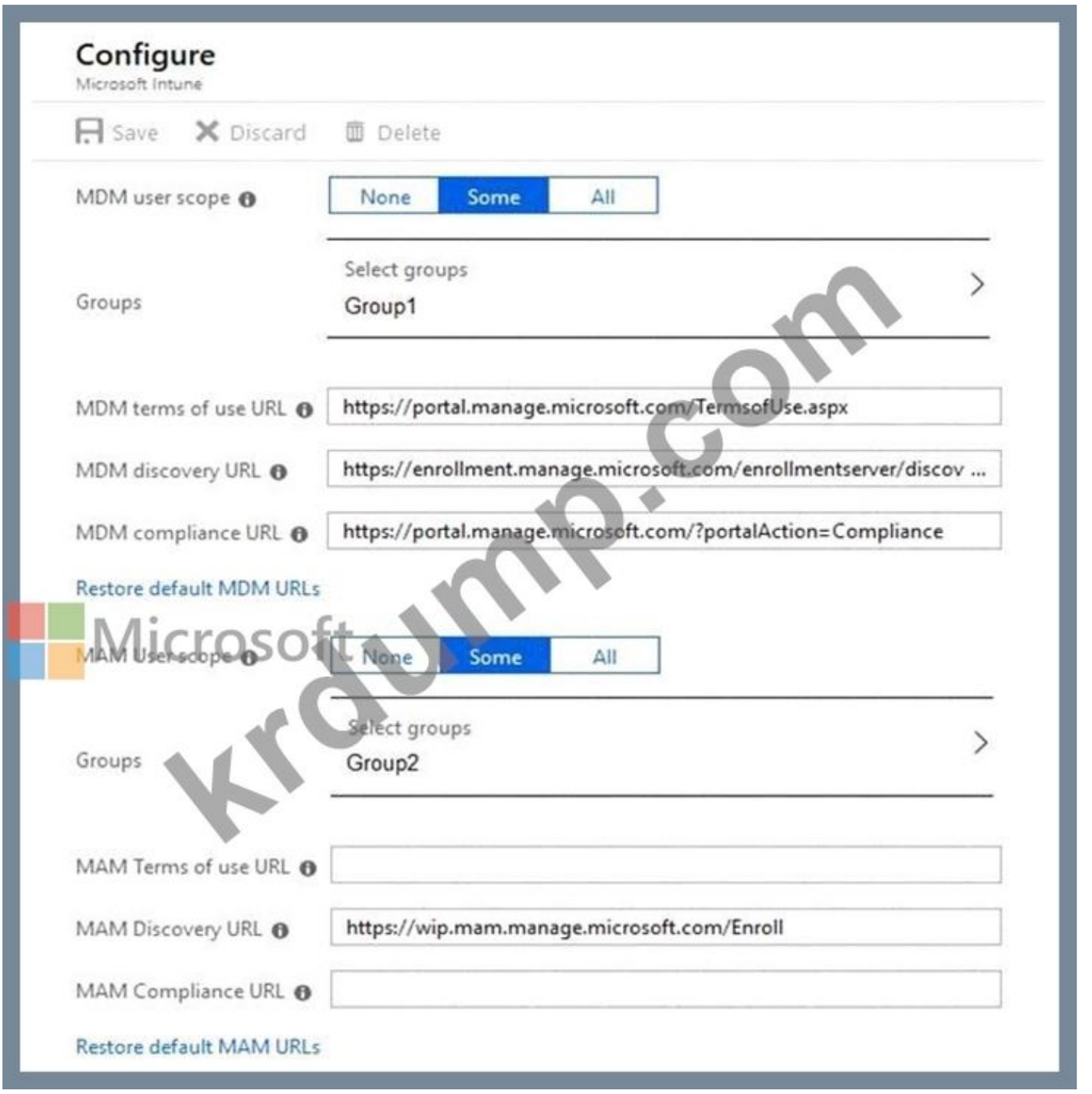
Answer: B (LEAVE A REPLY)

NEW QUESTION: 196

□□ □□ □□ □□ □□□□ □□□ contoso.com□□□ Azure Active Directory(Azure AD) □□ □□ □□□□.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

□□ □□□ □□ Microsoft Intune□ contoso.com□ □□□□□.



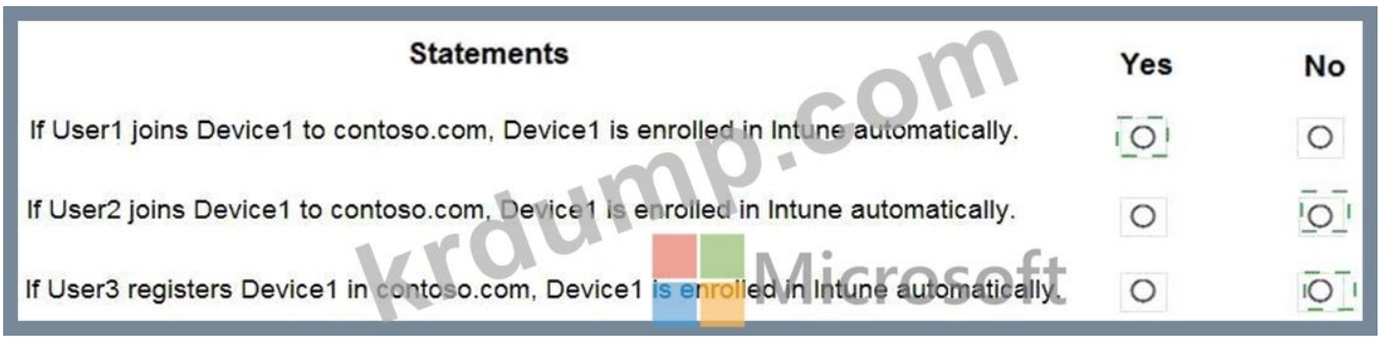
Device1□□□ Windows 10 □□□ □□□□□□.

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

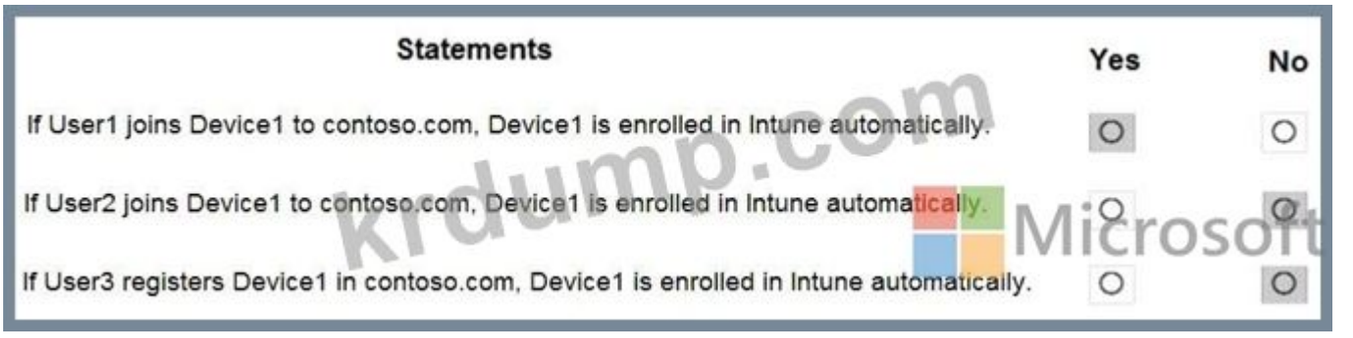
□□□□: □□ □□□ 1□□□□.

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

Answer:



Explanation:



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

NEW QUESTION: 197
□□ □□ □□□ □□□ User1, User2□□ □ □□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.

Name	Members
Group1	User1
Group2	User2, Group1

□□ □□□ □□□ Microsoft Intune □□ □□□ □□□□.
* MDM □□□ □□ : □□
* □□ : □□1
* MAM □□□ □□ : □□
* □□ : □□2
□□ □□ □□□ □□□ □□□□□.

Name	Platform
Device1	Windows 10
Device2	Android

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

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	○	○

Answer:

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	○	○

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	○	○

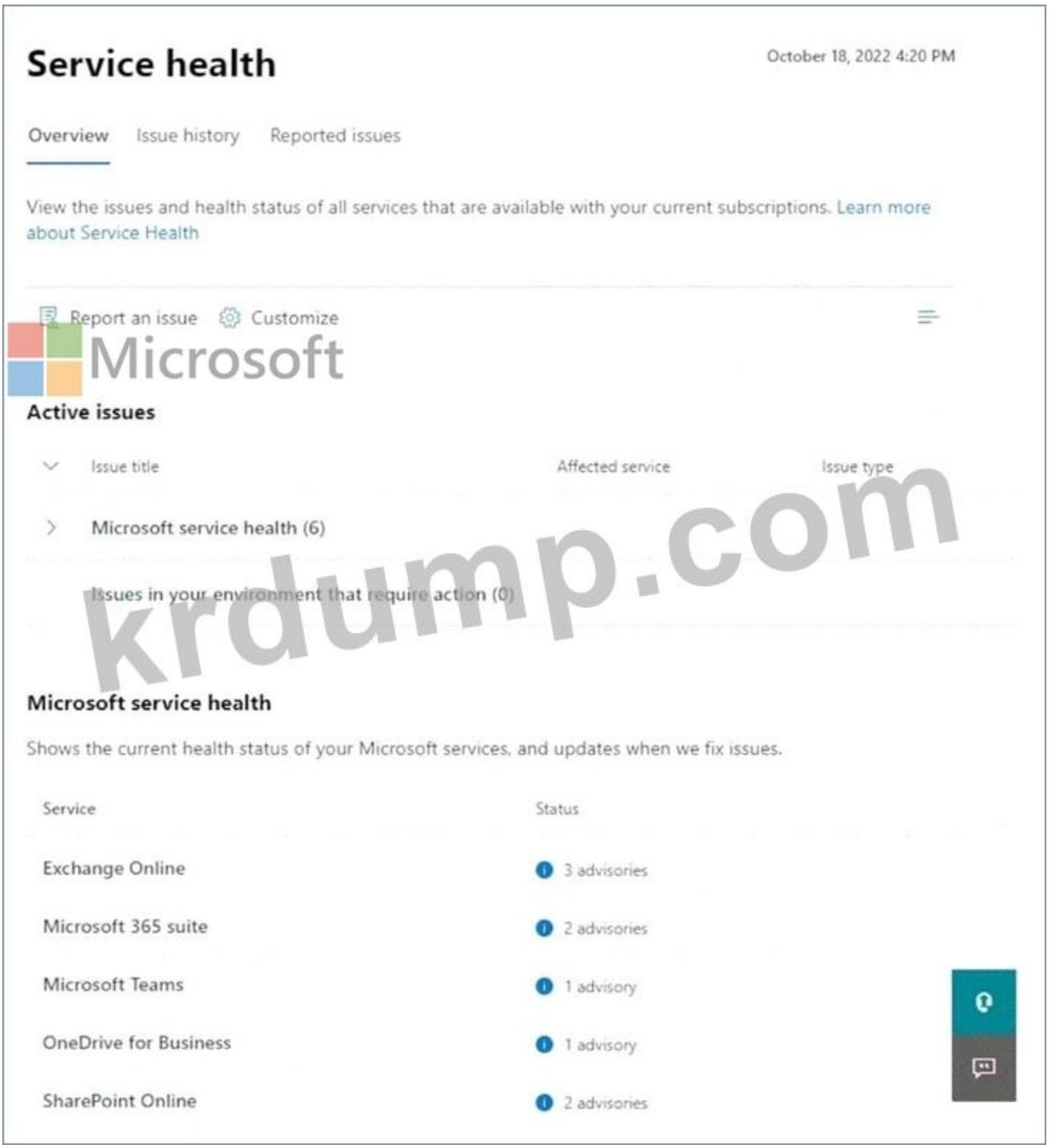
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll
https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll-device-administrator

NEW QUESTION: 198
Microsoft 365 E5 □□□□ □□□□.
□□□ □□ □□□ □□□ □□□□ □□□□□ □□ □□ □□□ □□□ □□□□. □□□ □□ □ □□□ □□□□□.

□□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. □□ □□□□□ □□□ □□□ □□□□□.
B. □□□ □□□
C. □□□□□ □□□□ □□ □□
D. Azure Information Protection □□ □□
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365- worldwide

NEW QUESTION: 199
Microsoft Defender for Office 365□ □□□□ User1□□□ □□□□ □□□ Microsoft 365 E5 □ □□ □□□□.
User1□ PDF □□□ □□ □□□□□ 300□ □□□□□ □□□□ □□□□. 200□ □□□□□ □□□ □□□□ □□, User1□ □□ □□□ □□□□ □□□ □□ □□□□□.
□ □□□ □□ □□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□ □□
B. □□ □□ □□
C. □□□ □□ □□ □□
D. □□□ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 200
Microsoft 365 □□□ □□□□.
□□ □□□ □□ □□□ □□ □□□ □ □ □□□□.



User1□□□ □□□□ □□□ □□ □□□ □□□□ □□ □□ □□□ □ □ □□□ □□□□ □ □□.

User1□□ □□ □□□ □□□□ □□□?

A. □□□ □□ □□

B. □□ □□□

C. □□□ □□ □□□

D. □□ □□ □□□

Answer: (SHOW ANSWER)

Service Support admin

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

NEW QUESTION: 201
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft 365 E5 □□□ □□□□.
SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.
SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Microsoft Defender for Office 365 □□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Microsoft 365 □□ □□□□ SecAdmin1□□ Exchange □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
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: 202

□□ □□ □□ □□ □□□□ □□□ Microsoft 365□ □□□□□ □□□ □□□□.

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□ □□□ □□□ □□□□.

□□□□ □□ □□□: □□□□

□□□□ □□: □□□□

□+□□□□ Active Directory□ □□□ □□ □□□ □□□ □□ Azure AD□ □□□□ □□□ □ □□ □□□□ □□□□ □□□.

□□ □□□□ □□□□ □□□?

A. □□

B. □□1 □□□

C. User1□ User2□

D. User1, User2, User3

Answer: D (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 203

□□□ □□□ Microsoft 365□ □□□□ □□□□.

□□ □□□□ □□ Office 365□ □□ □□□□□ □□ □□□ □□ □□□□ □□□□ □□□. □ □□□□ □□□□□ □□□□ □ □□□ □□□ □□□ □□□□□ □□□.

□□□ □□□□ □□□?

A. Microsoft 365 □□ □□□ □□ □□□

B. Microsoft Purview □□ □□ □□□ □□□

C. Microsoft Entra □□ □□□ □□□□ □□□□

D. Microsoft 365 □□ □□□ □□□

Answer: (SHOW ANSWER)

Microsoft 365 Reports in the admin center

You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.

Which activity reports are available in the admin center

Depending on your subscription, here are the available reports in all environments.

Report	Public	GCC	GCC-High	DoD	Office 365 operated by 21Vianet
Microsoft browser usage	Yes	No[1]	No[1]	No[1]	No[1]
Email activity	Yes	Yes	Yes	Yes	Yes
Email apps usage	Yes	Yes	Yes	Yes	Yes
Mailbox usage	Yes	Yes	Yes	Yes	Yes
Office activations	Yes	Yes	Yes	Yes	Yes

Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports

NEW QUESTION: 204
Microsoft 365 □□□ □□□□.
□□ □□ □□□ □□□□ □□□ Azure AD □□□□ □□□□.

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

□□ □□□ □□ □□□ □□□ □□□□□.

□□□□□ □□□ □□□ □□□□ □□ Microsoft□□ □□□ □□ □□□□ □□□□□?
A. □□□ □□
B. User2□

C. User3☐
D. ☐☐ ☐☐☐ User2☐ ☐☐
E. User2☐ User3☐
Answer: B (LEAVE A REPLY)
Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified.
Reference:
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365

NEW QUESTION: 205
Microsoft 365 E5 ☐☐☐ ☐☐☐☐.
☐☐ ☐☐☐☐ Mac ☐☐☐☐ ☐☐☐ ☐☐☐☐. ATI ☐☐☐☐ Microsoft Endpoint Manager☐ ☐☐ ☐☐ Microsoft Defender for Endpoint☐ ☐☐☐☐☐☐.
☐☐☐☐☐ Endpoint☐ Microsoft Defender☐ ☐☐☐☐ ☐☐☐.
Endpoint Management ☐☐ ☐☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐?
A. ☐☐ ☐☐ ☐☐☐
B. iOS ☐☐☐☐ ☐☐
C. ☐☐☐ ☐☐ ☐☐(MDM) ☐☐ ☐☐ ☐☐☐
D. Microsoft Defender for Endpoint ☐☐ ☐☐☐
Answer: (SHOW ANSWER)

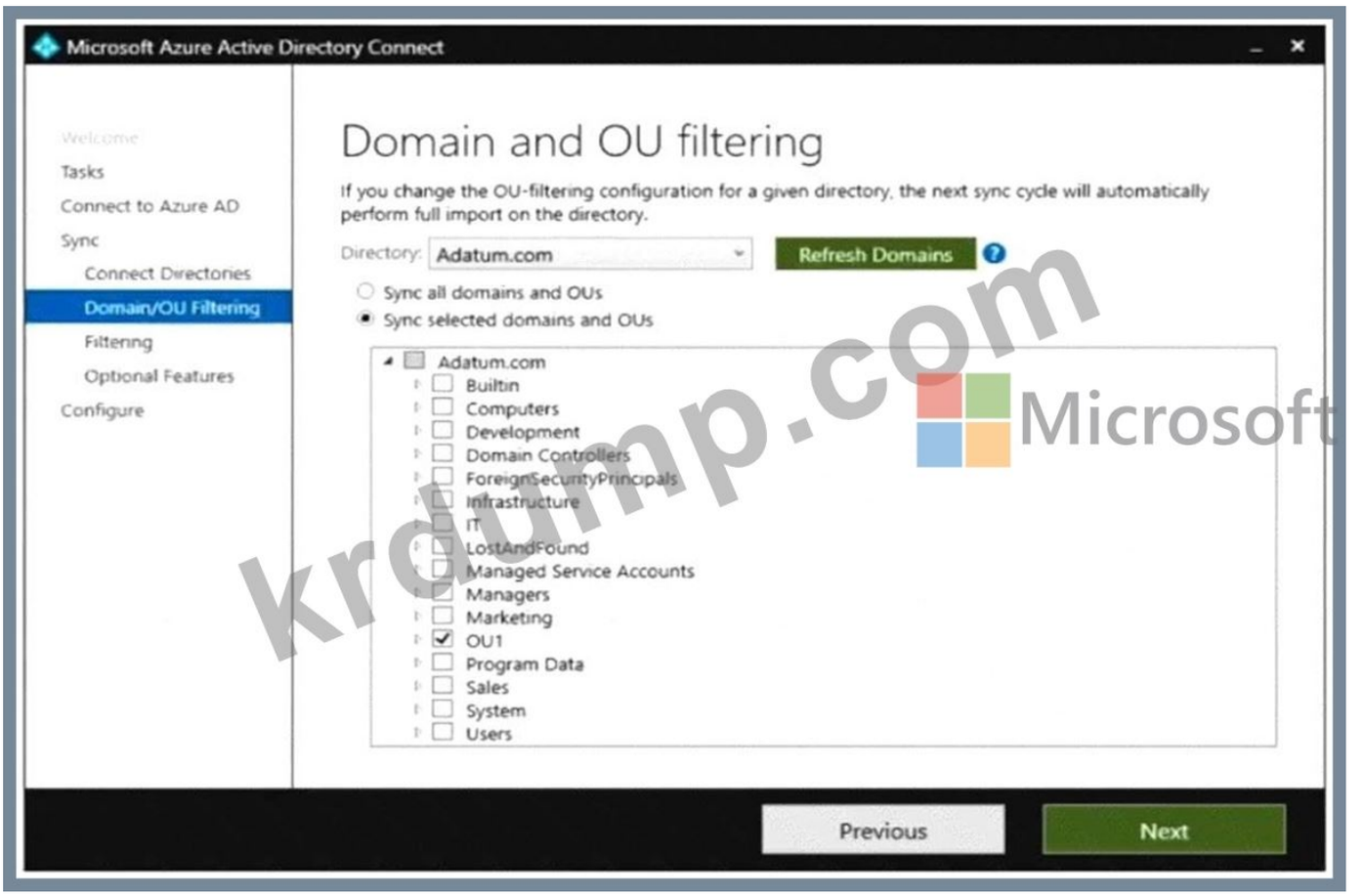
NEW QUESTION: 206
☐☐☐
☐☐☐☐☐ ☐-☐☐☐☐ Active Directory ☐☐☐☐ Microsoft 365 ☐☐☐ ☐☐☐☐ ☐☐☐☐.
☐☐ ☐☐☐☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐.

Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

☐☐ ☐☐☐☐☐ ☐☐ ☐☐ ☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐.

Name	Member of	In OU
Group1	*None*	Sales
Group2	Group1	OU1

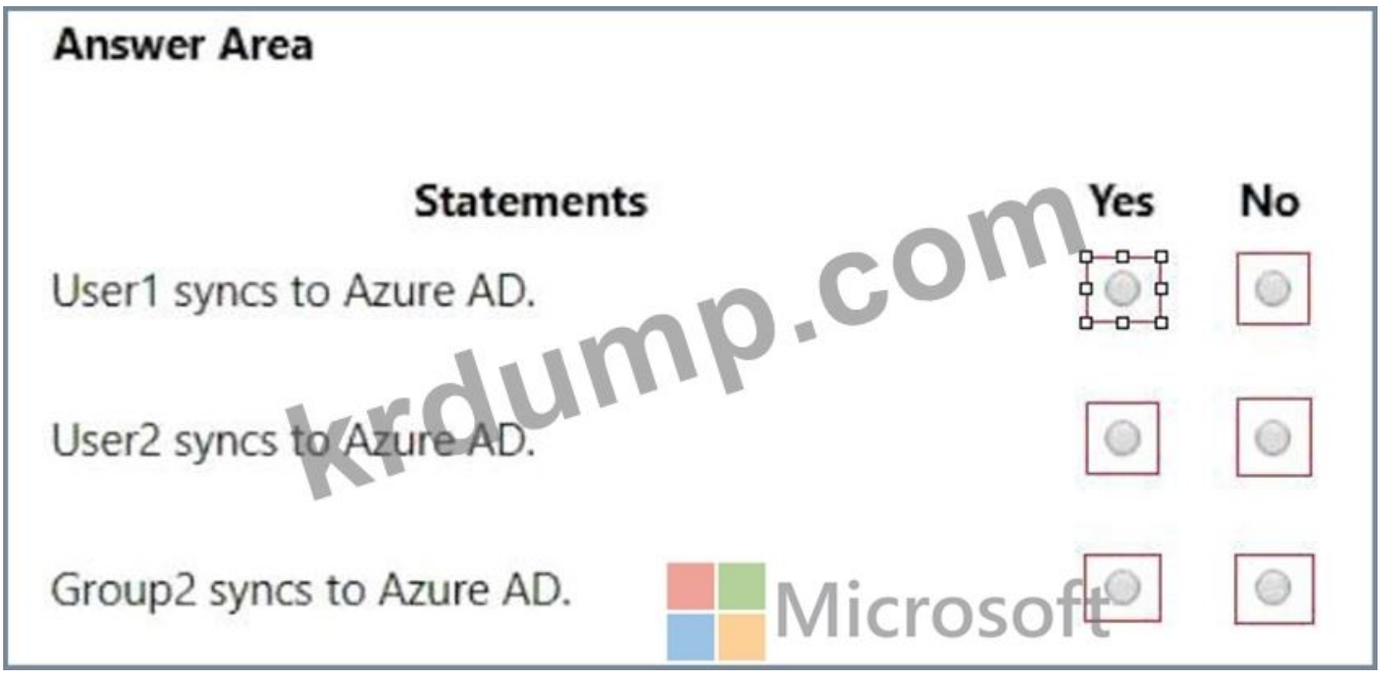
Azure AD Connect☐ ☐☐☐☐ ☐☐☐☐.
☐☐ ☐☐☐ ☐☐ ☐☐☐ ☐ OU ☐☐☐☐ ☐☐☐☐☐.


Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Domain/OU Filtering
Filtering
Optional Features
Configure
Domain and OU filtering
If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.
Directory: Adatum.com
Refresh Domains
Sync all domains and OUs
Sync selected domains and OUs
Adatum.com
Builtin
Computers
Development
Domain Controllers
ForeignSecurityPrincipals
Infrastructure
IT
LostAndFound
Managed Service Accounts
Managers
Marketing
OU1
Program Data
Sales
System
Users
Previous
Next

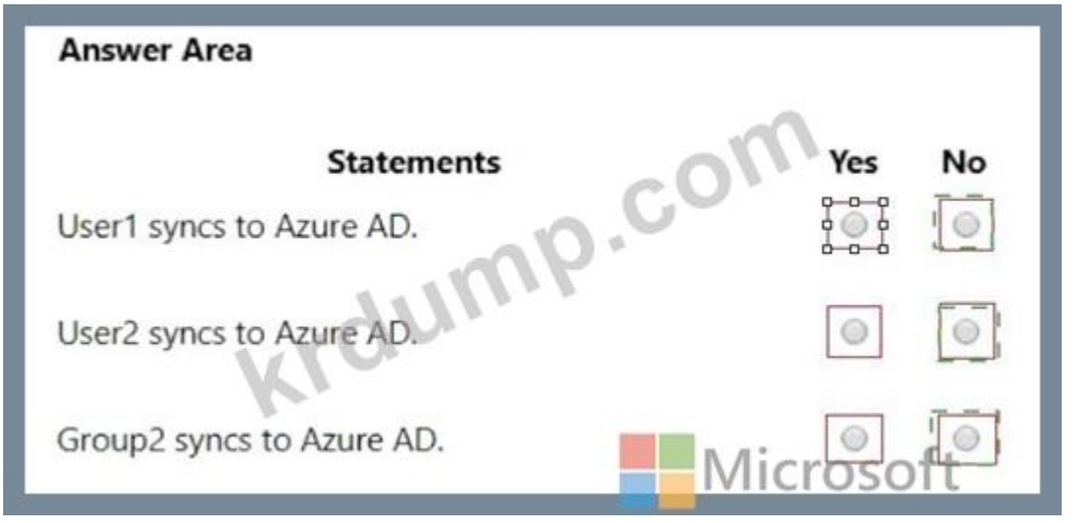
□□ □□ □□ □□ □□□ □ □□□ □□□□□.


Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Domain/OU Filtering
Filtering
Optional Features
Configure
Filter users and devices
For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.
Synchronize all users and devices
Synchronize selected
FOREST
GROUP
Adatum.com
CN=Group1,OU=Sales,DC=Adatum,DC=com
Resolve
Previous
Next

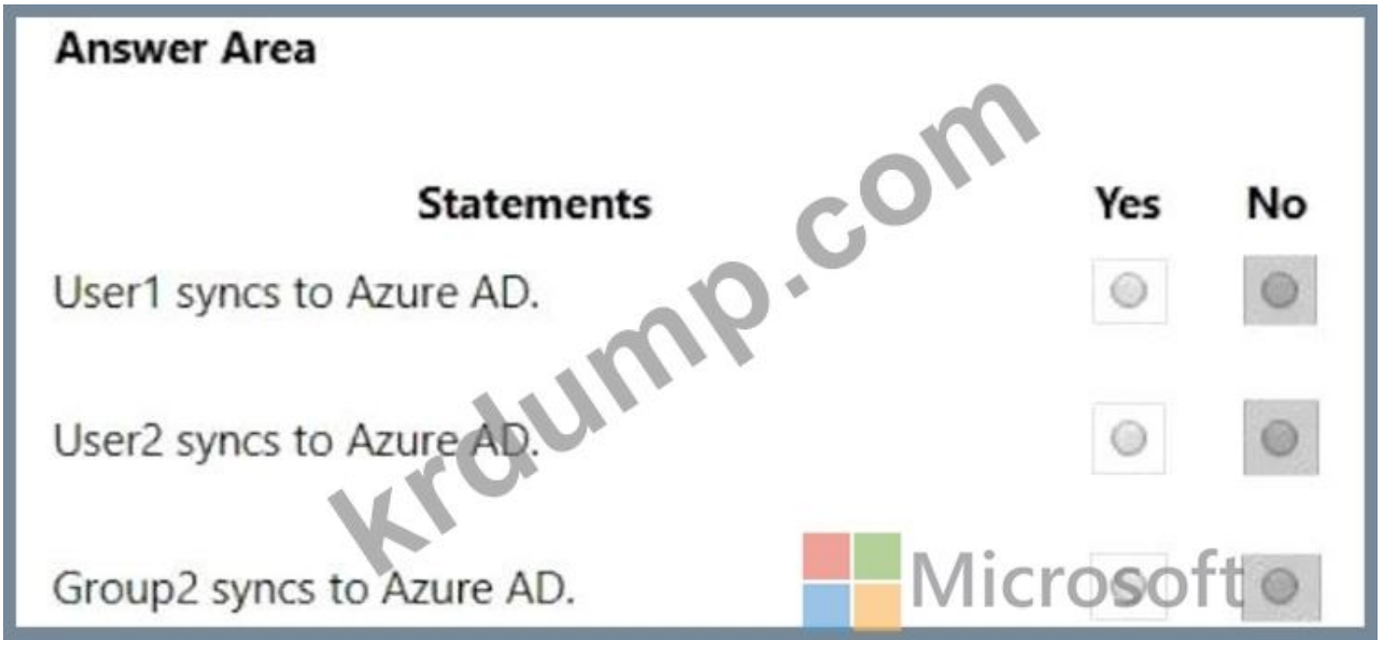
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 207

□□□ □□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□. □□□ □□ 1,000□□ Windows 10 □□□ □□□□.

10□□ □□□ □□□□□ □□ Microsoft Defender for Endpoint□ □□ □□(PoC) □□□ □□□ □□. □□□ □□□□ □□ Microsoft Defender for Endpoint □□ □□□□ □□□ □□□□□ □ □□□□.

□□ □□□ Microsoft Defender for Endpoint□ □□□□ □□□□□.

Microsoft Defender for Endpoint □□□□ □□□ □□□□ □□□.

□□ □□ □□□ □□ □□□?

A. □□ □□□ □□□□□.

B. □□□□□ □□□□.

C. □□□ □□□ □□□□□.

D. □□□ □□□ □□□□ □□□□.

Answer: (SHOW ANSWER)

Storage locations

Understand where Defender for Cloud stores data and how you can work with your data:

* Machine information

- Stored in a Log Analytics workspace.

- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.

:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace

NEW QUESTION: 208

□□□ □□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□ □□□ □. □ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

□□□□ □□□□ □□□ □□□ contoso.com□□□ Microsoft Entra □□□□ □□□□□□. (□□ □ □□ □□□□□.) User2□ usef2@fabfikam.com□□ □□□□ □ Microsoft Entra □□□□ □ □□□ □□□□. User2□ Microsoft Entra ID□ □□□□ □□□□ □ □□□ □□□□ □□□.

□□ □□: Microsoft Entra □□ □□□□ <abrlkam.com>□ □□□ □□ □□□□□ □□□□□.

User2□□ user2@fabrikam.com□□ □□□□□□ □□□□□. □□□□ □□□ □□□ □ □□ □?

A. □

B. □□□

Answer: (SHOW ANSWER)

NEW QUESTION: 209

Microsoft 365 E5 □□□ □□□□.

Microsoft 365 Defender□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□.

□□□ □□□□ □□□?

A. □□ □□

B. □□ □□

C. □□□ □□ □□ □□

D. □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 210

□□□

Microsoft 365 □□□ □□□□.

□□□ □□□ □□ □□ □□ □□□□ □□□□ □□□□.

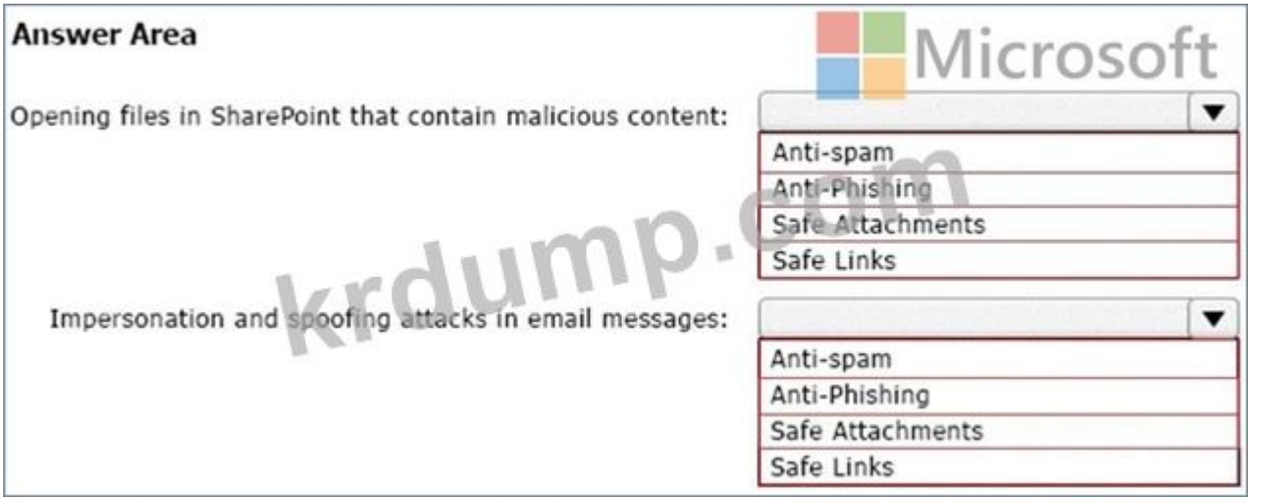
□□□□ □□□ □□ □□□□□□ □□□ □□ □□□□ □□□□□ □□□.

* □□ □□□□ □□□ Microsoft SharePoint□ □□ □□

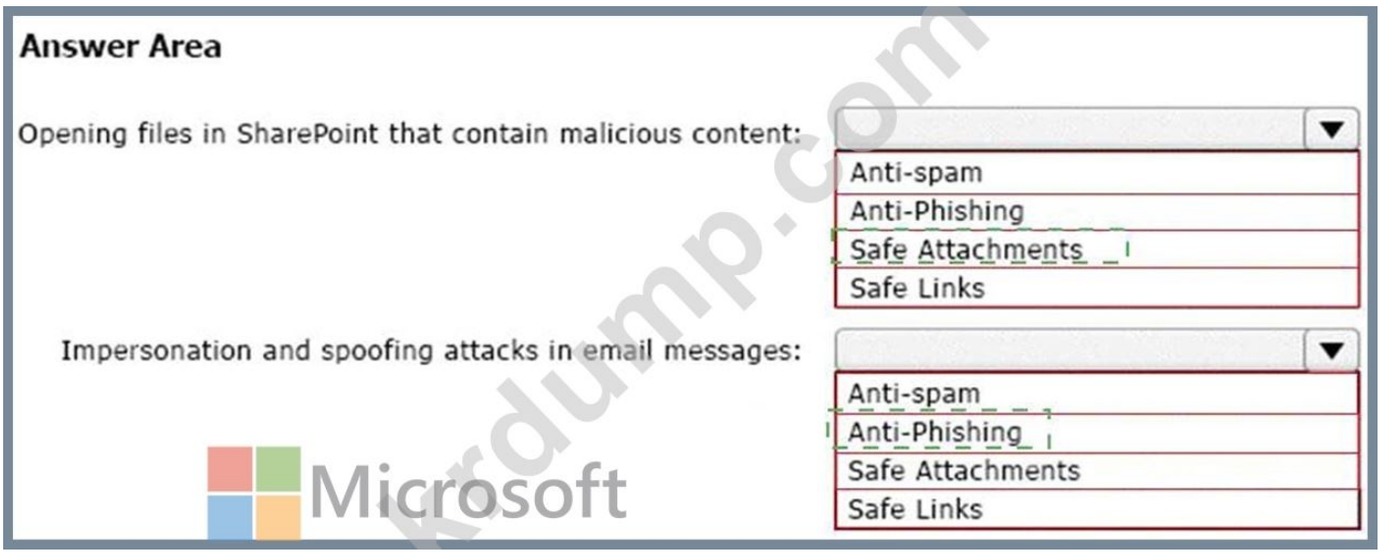
* □□□ □□□□□□ □□ □ □□□ □□

Microsoft 365 Defender□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □ □□ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 211

Microsoft 365 E5 □□□ □□□□.

Microsoft Defender for Endpoint□ Microsoft Intune□ □□□□□.

Intune□ □□□ □ □□□ Defender for Endpoint□ □□□□ □□□□□□ □□ □□□.

□□□: □□ □□ □□□ □□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: A (LEAVE A REPLY)

NEW QUESTION: 212

Microsoft 365 □□□ □□□□.

□□ □□ □□□ □□□ Retention1□□□ □□□ □□ □□□ □□□□.

□□ Microsoft OneDrive □□□□ □□ □□□ □□□□□.

2020□ 1□ 1□□ □□□□ OneDrive□ File1□□□ □□□ □□□□□.

2020□ 1□ 10□□ □□□□ File1□ □□□□□.

2020□ 2□ 1□□ □□□□ File1□ □□□□□.

File1□ OneDrive□□ □□□□□ □□□□ □□□ □ □□ □□ □□□ □□□□□?

A. 2020□ 7□ 1□

B. 2020□ 2□ 1□

C. 2020□ 7□ 10□

D. 2020□ 8□ 1□

Answer: (**SHOW ANSWER**)

NEW QUESTION: 213

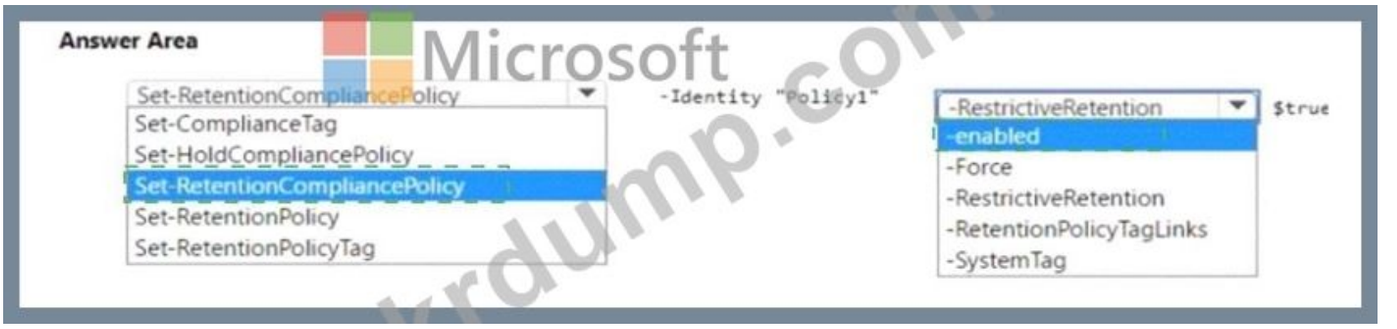
Microsoft Purview □□ □□□□ □□ 1□□□ □□□ □□ □□□ □□□□.

□□ □□□□ □□□ □□□□□□□ □□ □□□ □□□ □□ □□□□ □□□.

Azure PowerShell □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □ □□□□.

□□□□: □□ □□□ 1□□□□.

Answer:



Explanation:

NEW QUESTION: 214

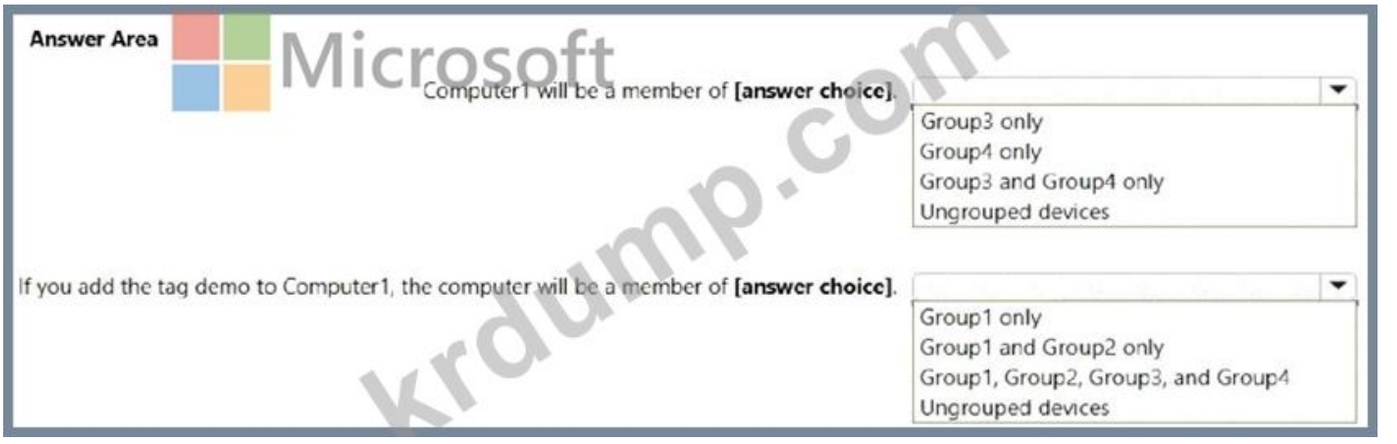
□□□

□□□ Microsoft Defender for Endpoint□ □□□□□. Microsoft Defender for Endpoint□□ □□ □□ □□□ □□ □□□ □□□□□.

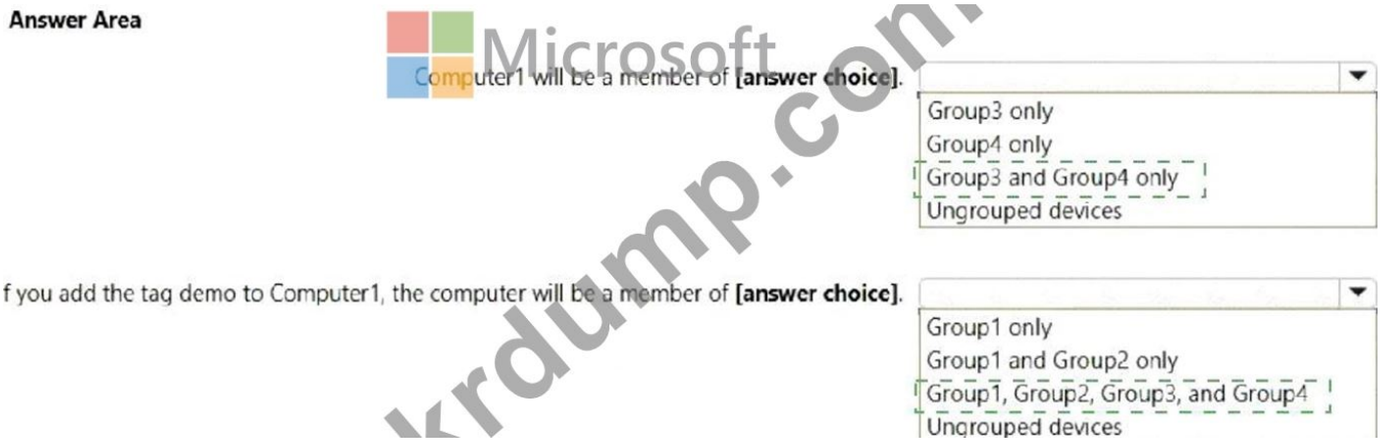
Rank	Device group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped devices (default)	*Not applicable*

□□ □□□ □□ Microsoft Defender for Endpoint□ computer1□□□ □□□□ □□□□□□.

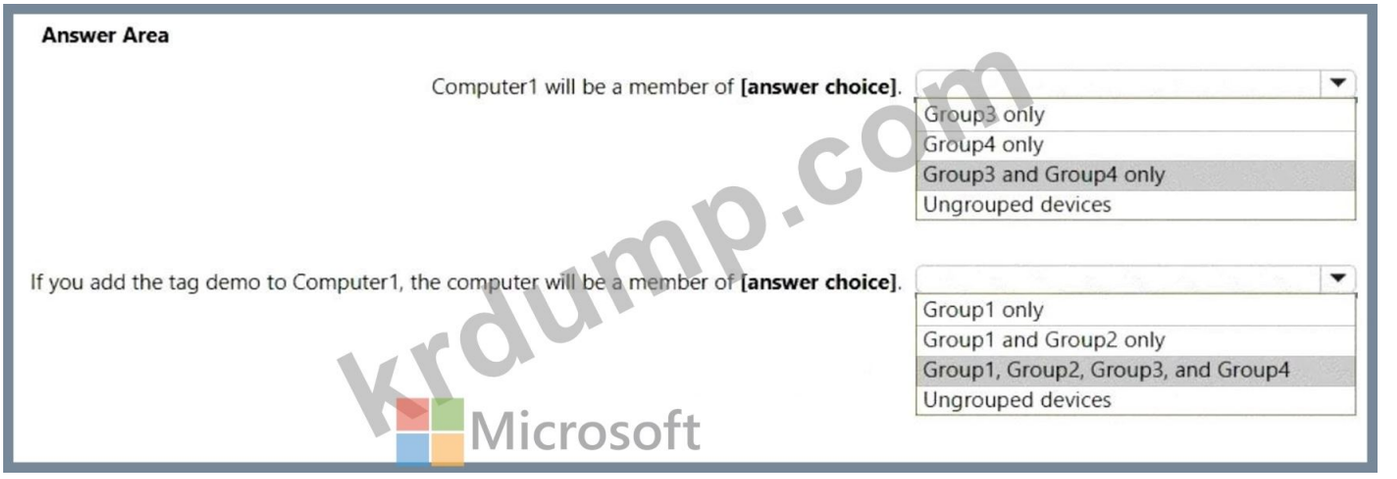
□□□□ □□□ □□□ □ □□□ □□□□ □□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Box 1: Group3 and Group4 only

Computer1 has no Demo Tag.

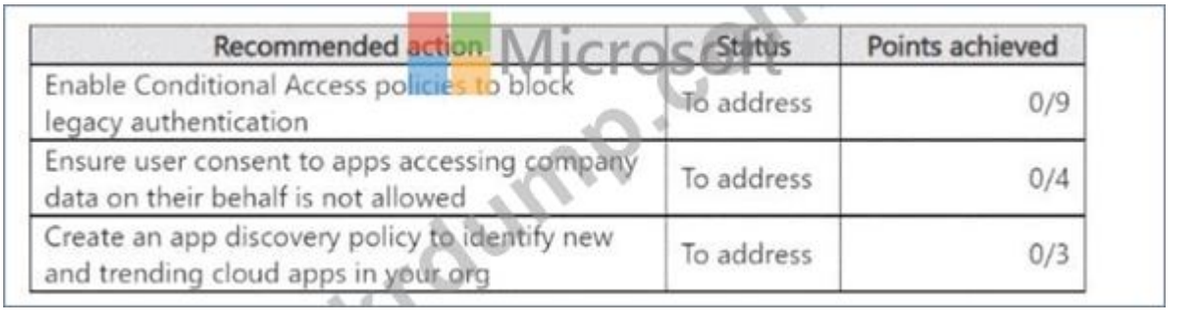
Computer1 is in the adatum domain and OS is Windows 10.

Box 2: Group1, Group2, Group3 and Group4

NEW QUESTION: 215

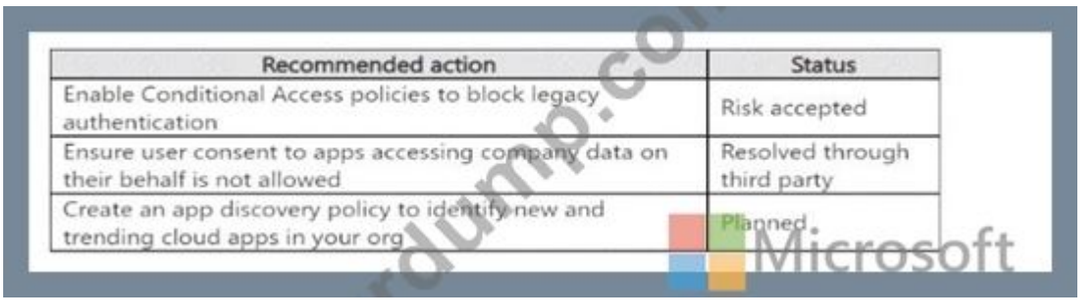
Microsoft Defender XDR□ □□□ Microsoft 365 □□□ □□□□.

Microsoft Defender □□□□ □□ □□ □□□ Microsoft Secure Score □□ □□□ □□□□□.



Recommended action	Status	Points achieved
Enable Conditional Access policies to block legacy authentication	To address	0/9
Ensure user consent to apps accessing company data on their behalf is not allowed	To address	0/4
Create an app discovery policy to identify new and trending cloud apps in your org	To address	0/3

□□ □□ □□□ □□ □□ □□□ □□□ □□□□□ □□□□□.



Recommended action	Status
Enable Conditional Access policies to block legacy authentication	Risk accepted
Ensure user consent to apps accessing company data on their behalf is not allowed	Resolved through third party
Create an app discovery policy to identify new and trending cloud apps in your org	Planned

□□□□ □ □□ □□□ □□□ □□□□□?

A. 0

B. 16

C. 7

D. 4

E. 13

Answer: C (LEAVE A REPLY)

NEW QUESTION: 216

Microsoft 365 E5 □□□□ □□□□.

□□□ □□□ □□□ □□□ □□ □□□ □□□□ □□□□ □□□□. (□□□ □□□ □□ □□ □□□.)


Review your settings and finish
Name
Sensitivity1
Display name
Sensitivity1
Description for users
Sensitivity1
Scope
File,Email
Encryption
Content marking
Watermark: Watermark
Header: Header
Auto-labeling
Group settings
Site settings
Auto-labeling for database columns
None

□□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□□. (□□ □□□ □□ □□ □□ □□□.)

Auto-labeling policy

Edit Policy Delete Policy

Policy name
Auto-labeling policy

Description

Label in simulation
Sensitivity

Info to label
IP Address

Apply to content in these locations
Exchange email All

Rules for auto-applying this label
Exchange email 1 rule

Mode
On

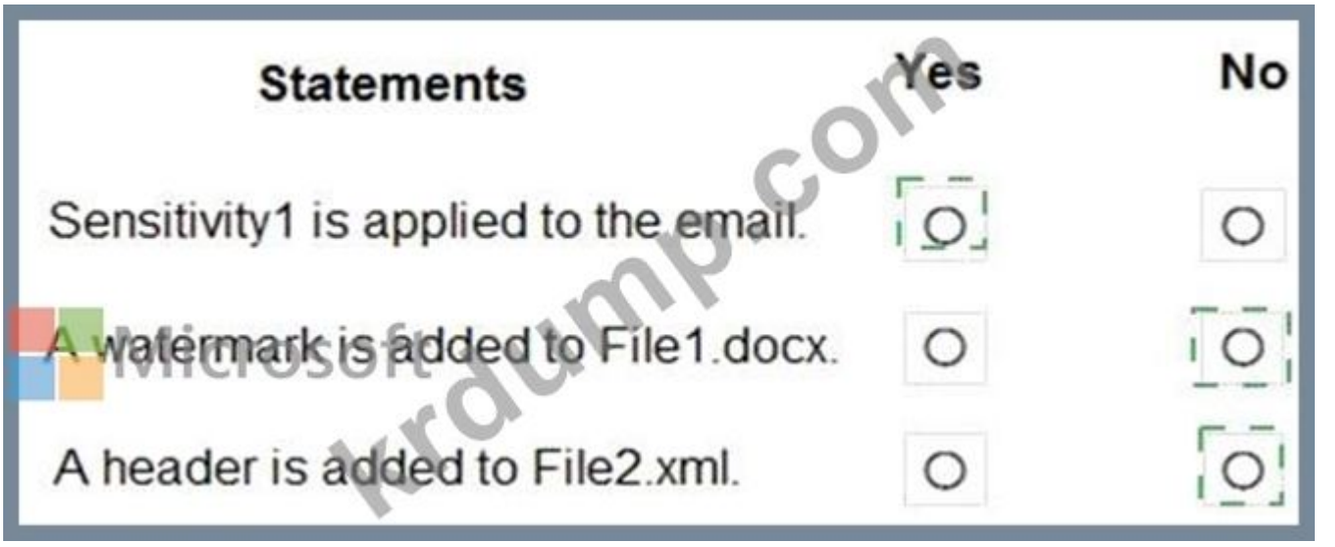
Comment
□□□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□□.

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

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

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

Answer:



Explanation:

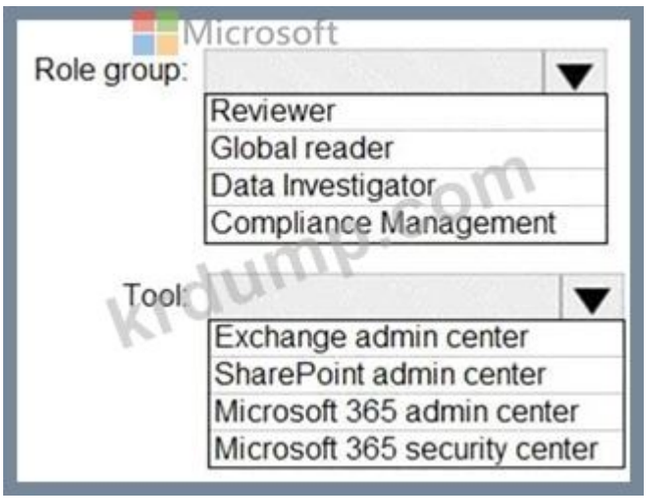
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365- worldwide

NEW QUESTION: 217

User2□ □□ □□□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □ □□.

User2□ □□ □□ □□□ □□□□ □□, □□□ □□□□ □□□? □□□□□ □□ □□□□ □ □□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?
view=o365-worldwide

NEW QUESTION: 218

□□□ □ □□

Group1□ Group2□□ □ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

□ □□□ □□ □□ □□□ □□□ □□□ □ □□□ □□□□ □□□.

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

□□□□ □□ □□□ □□□ □□□□ □□□.

□ □□□ □□ □□□ □□□□ □□□? □□□□ □□□ □□□ □□□ □□□□ □□□ □□□ □. □ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □□□ □□ □ □□□ □□□□□ □□□□ □ □ □□□□.

□□□□: □□ □□□ 1□□□□.

Roles

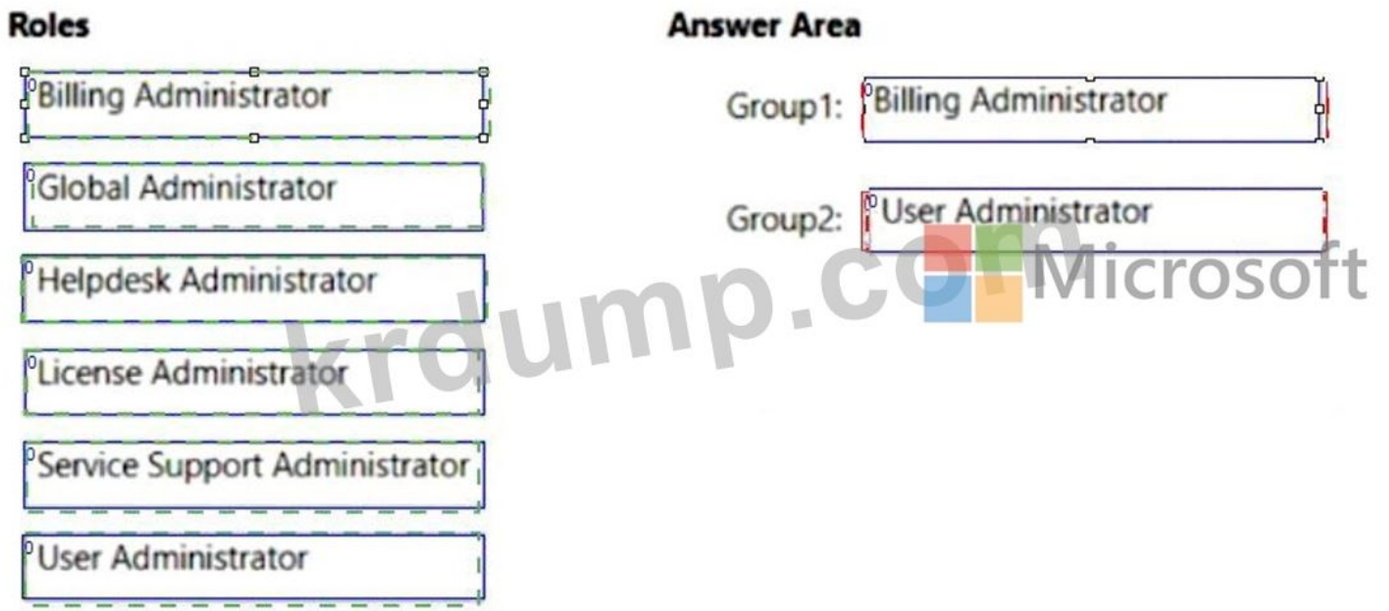
- Billing Administrator
- Global Administrator
- Helpdesk Administrator
- License Administrator
- Service Support Administrator
- User Administrator

Answer Area

Group1: Role

Group2: Role

Answer:



Explanation:

Box 1: Billing admin

manage service request

Purchase new services

Etc.

Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.

Box 2: User admin

User admin

Assign the User admin role to users who need to do the following for all users:

- Add users and groups
- Assign licenses
- Manage most users properties
- Create and manage user views

- Update password expiration policies
- Manage service requests
- Monitor service health

Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles

NEW QUESTION: 219

Microsoft 365 E5 □□□ □□□□.

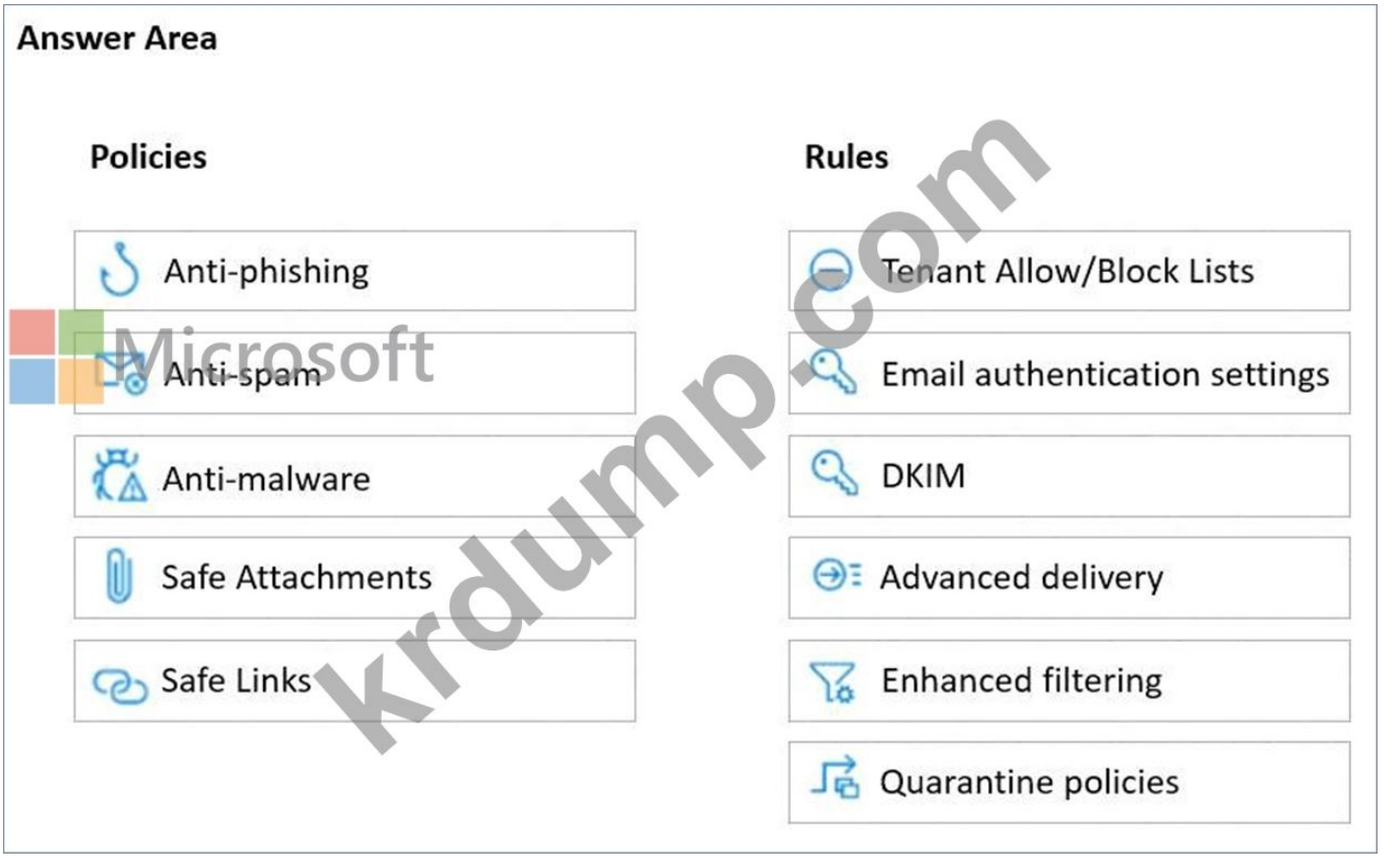
Mailbox1□□□ □□□□ □□□□ □□ □□□ □□□□ □□□ □□□□□.

□□ □□ □□□ □□□□□ Office 365□ Microsoft Defender□ □□□□ □□□.

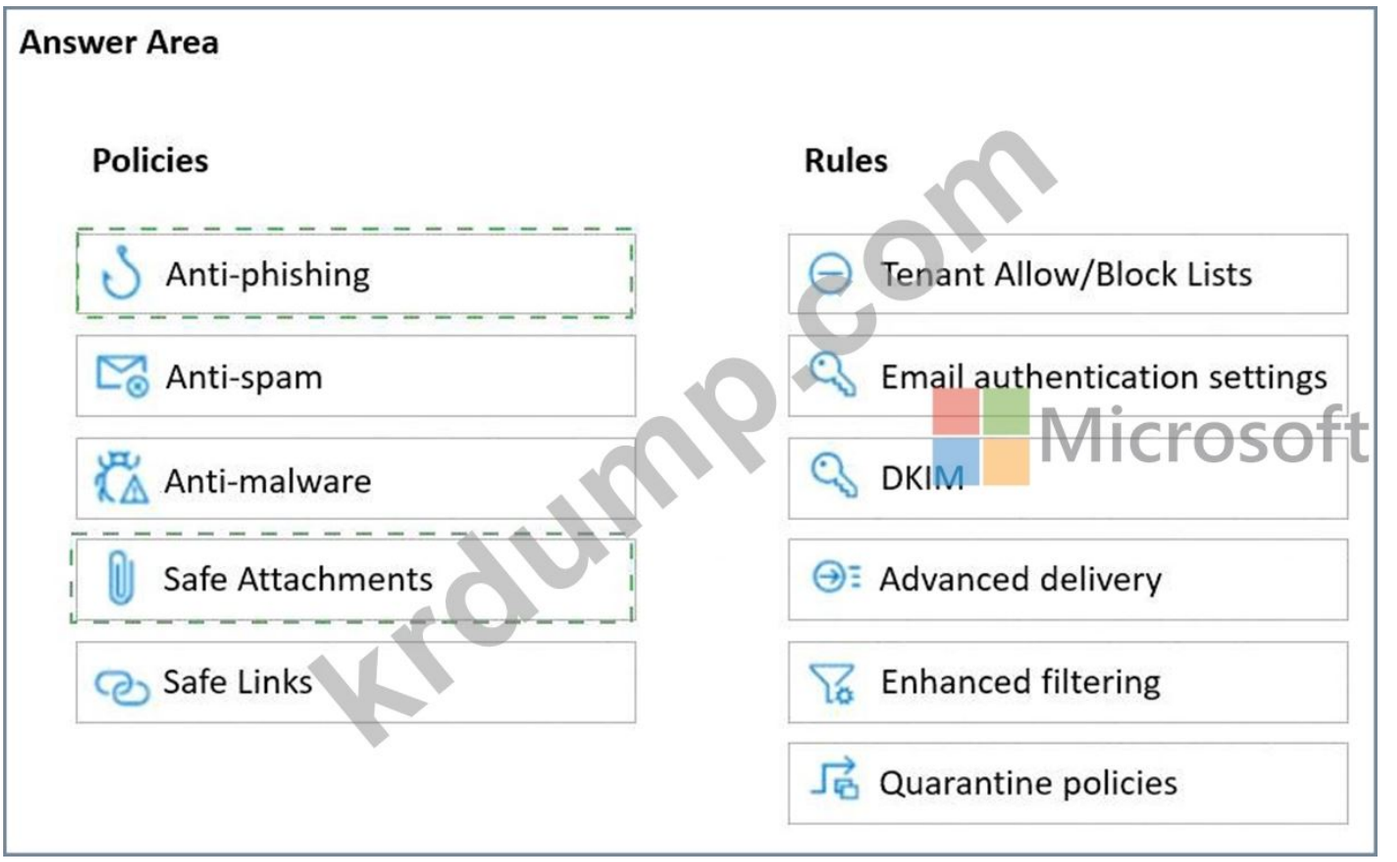
* Mailbox1□□ □□ □□□□ □□□□□ □□□□ □□□□□.

* □□□ □□ □□ □□ □□□□ □□ □□ □ □□□ □□□ □□□□□.

□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.



Answer:



* 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: 220

□□□

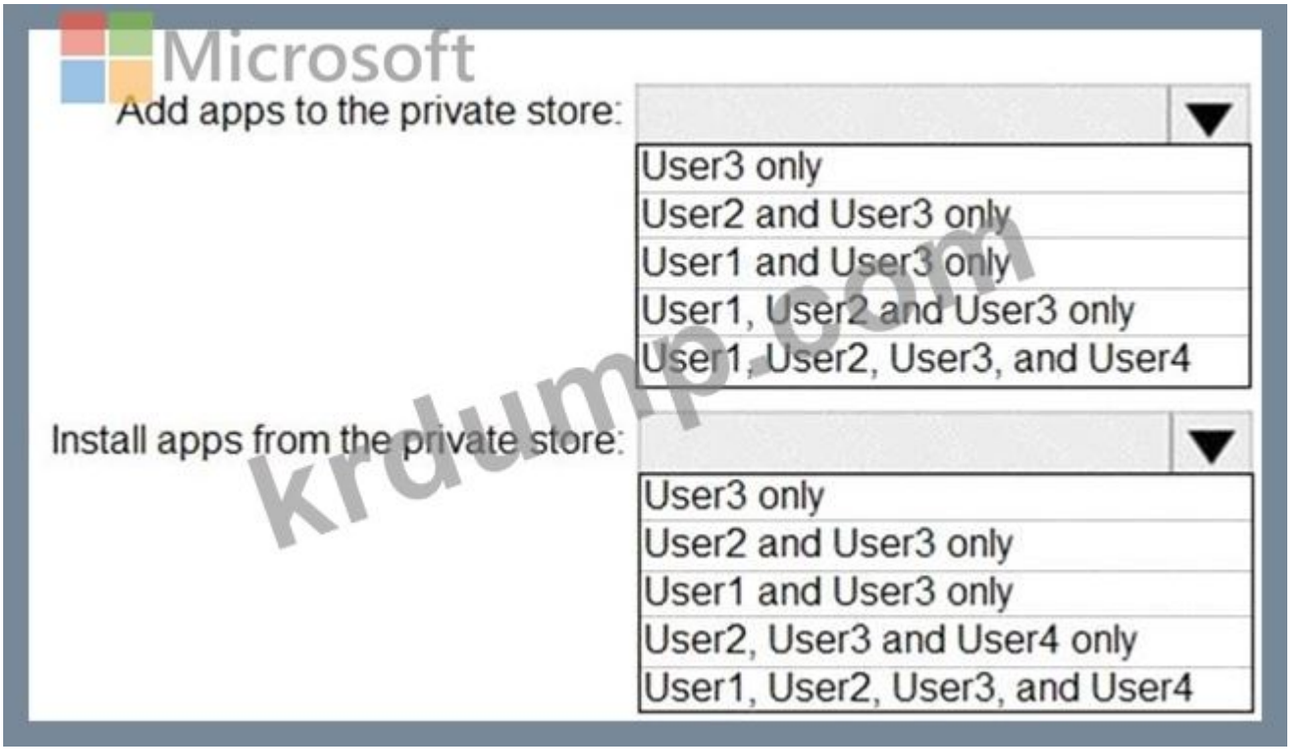
□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.

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

□□ □□ □□□ □□ □□□□□ Microsoft Store for Business □□□ □□□□□.

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

□□ □□□□ Microsoft Store for Business□ □□ □□□□ □□ □□□ □ □□, □□ □□□□ □□ □□□□□ □□ □□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□. □□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business
https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

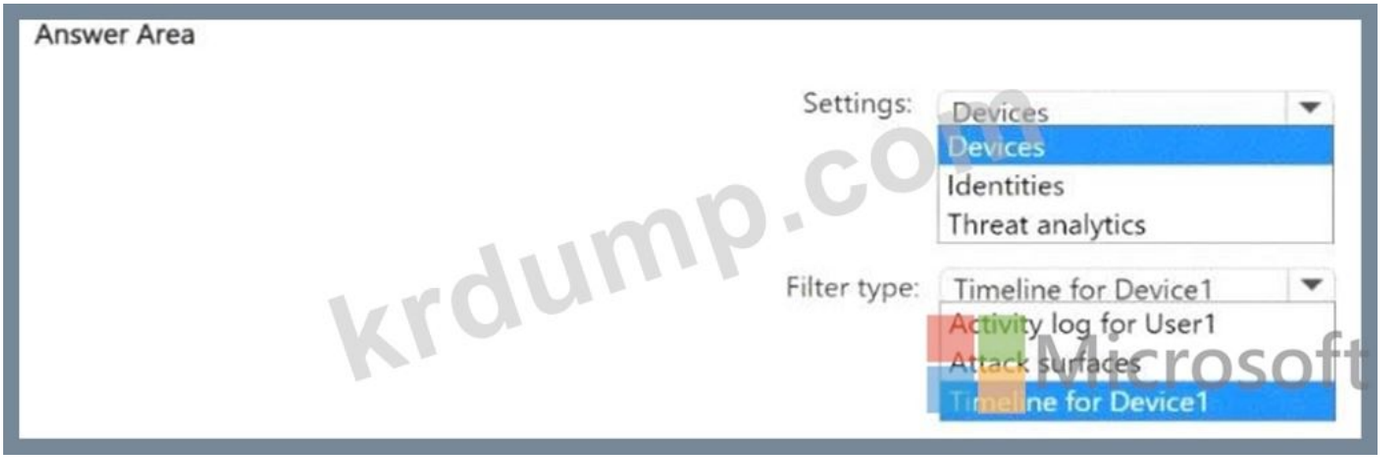
NEW QUESTION: 221
contoso.com□□□ Azure AD □□□□ □□□ Microsoft 365 □□□ □□□□.
□□ □□□ □□□ □□□ □□□□□□ Contoso□□ □□□ □□□□□□ □ □□□.
□□ □□□ □□□□□ □□□ □□ □□□?
A. Microsoft Entra □□ □□□□ □□ □□ □□□ □□□□□.
B. Microsoft Entra □□ □□□□ □□□ □□□ □□□ □□□□.
C. Azure AD Identity Protection□□ □□□ □□ □□□ □□□□□.
D. Microsoft 365 □□ □□□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 222
Microsoft J65 E5 □□□ □□□□.
Microsoft Defender for Endpoint□ Microsoft Intune□ □□□□□.
Intune□ □□□ □ □□□ Defender for Endpoint□ □□□□ □□□□□□ □□ □□□.
□□ □□: □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)

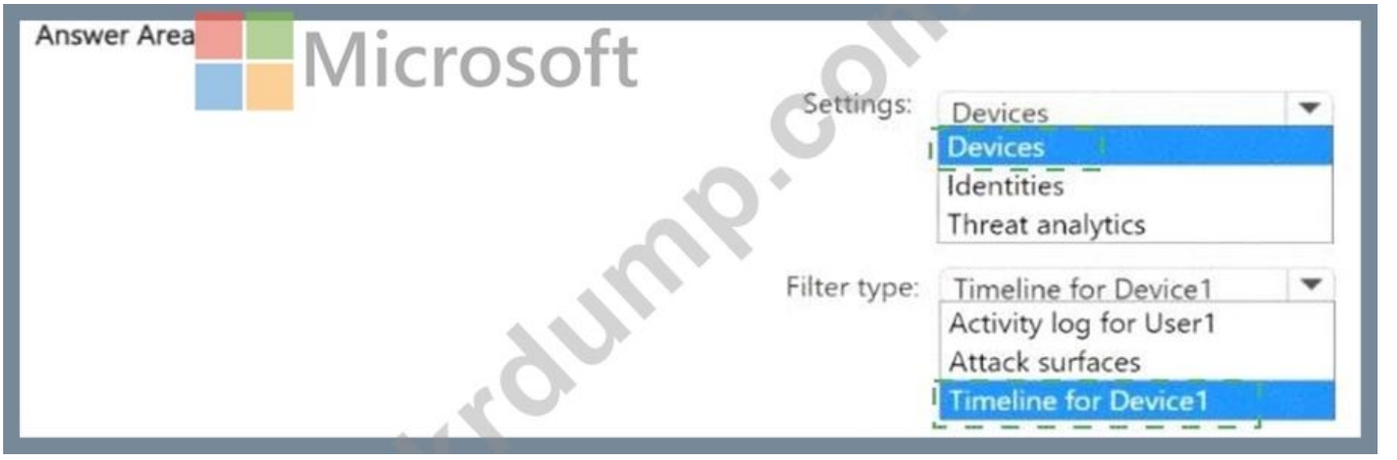
NEW QUESTION: 223
Microsoft 365 □□□ □□□□.
App1□□□ □ Azure AD □□□□□□ □□□□□□□ □□□□□. App1□ □□□□□ □□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□□ □□□□ App1□ □□□□□□ □□ □□□ □□□ □□□□ □□□?
A. □□□□ □□□ Microsoft 365 □□
B. □□ □□□ □□□□ □□ Microsoft 365 □□
C. □□□□ □□□ □□ □□
D. □□ □□□ □□□□ □□ □□ □□
Answer: C (LEAVE A REPLY)
To grant permissions to assignees to manage users and group access for a specific enterprise app, go to that app in Azure AD and open in the Roles and Administrators list for that app. Select the new custom role and complete the user or group assignment. The assignees can manage users and group access only for the specific app.
Note: You can add the following types of groups:
Assigned groups - Manually add users or devices into a static group.
Dynamic groups (Requires Azure AD Premium) - Automatically add users or devices to user groups or device groups based on an expression you create.
Note:
Security groups
Security groups are used for granting access to Microsoft 365 resources, such as SharePoint. They can make administration easier because you need only administer the group rather than adding users to each resource individually.
Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.
Security groups can be configured for dynamic membership in Azure Active Directory, allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device attributes such as operating system version.
Security groups can be added to a team.
Microsoft 365 Groups can't be members of security groups.
Microsoft 365 Groups
Microsoft 365 Groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 Group, members get a group email and shared workspace for conversations, files, and calendar events, Stream, and a Planner.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps
https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?
https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy

NEW QUESTION: 224

User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□. User1□ Microsoft Defender for Endpoint□ □□□□ Device1□□□ Windows 11 □□□ □□□ □□□□.
User1□ Device1□□ □□□ □□□ □□□□□□ □□□□□.
□□□ □□□ □□□□ □□□□□ □□□ □□□□ □□□.
Microsoft Defender □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□? □ □□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 225
Contoso.com□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.
Contoso□ ID □□□□□ □□ Microsoft Defender□ □□□□.
□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□□ □□□□□ Defender□ □□□ □□□□ □□□.

□□□: User3□□ ID □□ □□□ □□ Defender□ □□□□□ □□□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: B (LEAVE A REPLY)

NEW QUESTION: 226

□□ □□ □□□ □□□ Microsoft Endpoint Manager□ □□□ □□□ 3□ □□□□.

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

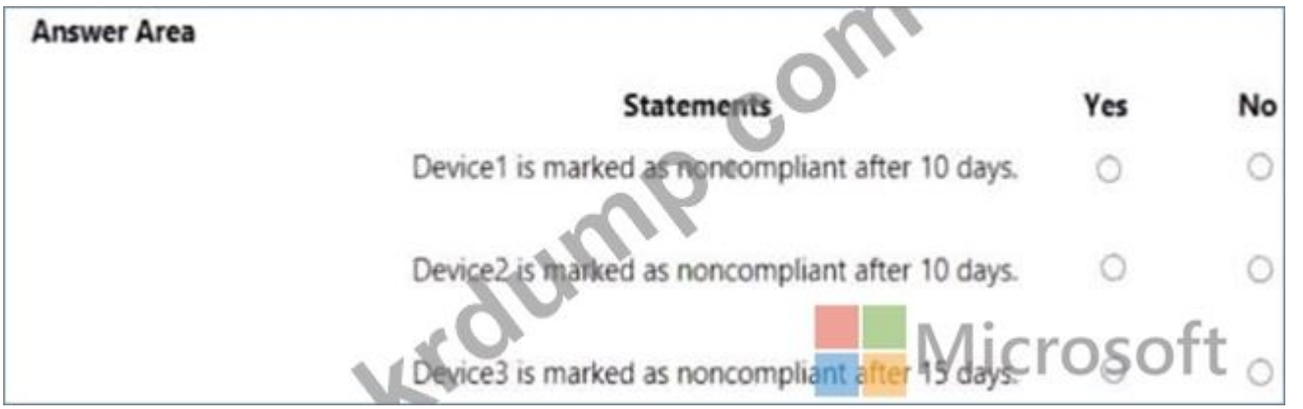
Endpoint Manager□ □□ □□ □□□ □□ □□ □□ □□□□□.

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

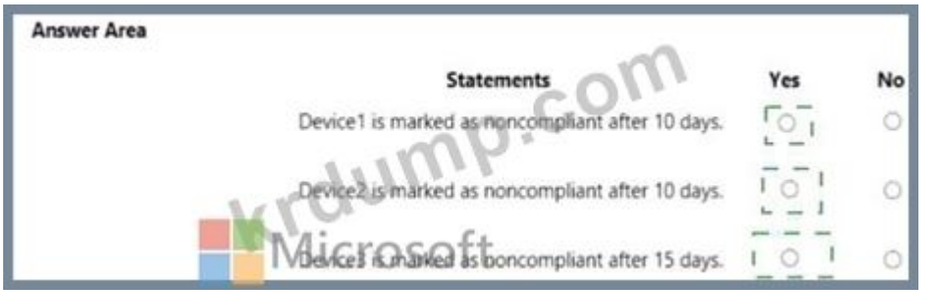
□□ □□ □□□ □□□ □□ □□ □□□□ □□□□.

Name	Assigned to
Policy2	Group2
Policy3	Group3

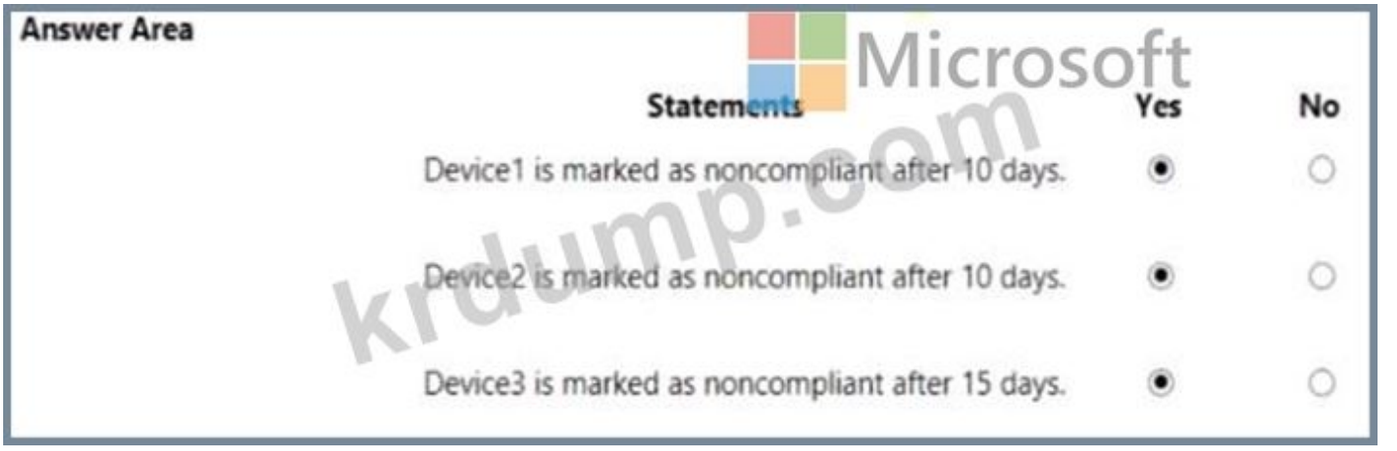
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□□. □□□ □□□ □□□□ □□□□□ □. □□: □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 227

□□□

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Member of	Multi-factor authentication (MFA) method registered
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1	*None*

□□ □□□ □□ □□ □□ □□□ □□□□□□ Microsoft Authenticator □□ □□ □□□ □□ □□□.

□□□1□ □□□2□ □□ Microsoft Authenticator □□□ □□□□ □□ □□□□□□ □□□□ □□□□ □□□□ □□□□□.

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.	○	○
User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.	○	○
User3 can use passwordless authentication without further action.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.	○	○
User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.	○	○
User3 can use passwordless authentication without further action.	○	○

Explanation:

Answer Area

Box 1: Yes
User1 is member of Group1.
User1 has MFA registered method of Microsoft Authenticater app (push notification) The Microsoft Authenticator authentication method policy is configured for Group1, registration is optional, authentication method is any.
Note: Microsoft Authenticator can be used to sign in to any Azure AD account without using a password.
Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology.
This authentication technology can be used on any device platform, including mobile. This technology can also be used with any app or website that integrates with Microsoft Authentication Libraries.
Box 2: No
User2 is member of Group2.
The Microsoft Authenticator authentication method policy is configured for Group1, not for Group2.
Box 3: No
User3 is member of Group1.
User3 has no MFA method registered.
User3 must choose an authentication method.
Note: Enable passwordless phone sign-in authentication methods
Azure AD lets you choose which authentication methods can be used during the sign-in process. Users then register for the methods they'd like to use.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless- phone

NEW QUESTION: 228
□□ □□□ □□ □□ □□ □□□ □□ □□□□.

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

□□ □□□□ □ □□□ □□ □□ □□ □□□ □□□□□.

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

□□□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 229

□□□

□□□ □□□□□□ fabrikam.com□□□ Active Directory □□□□ □□□□. □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

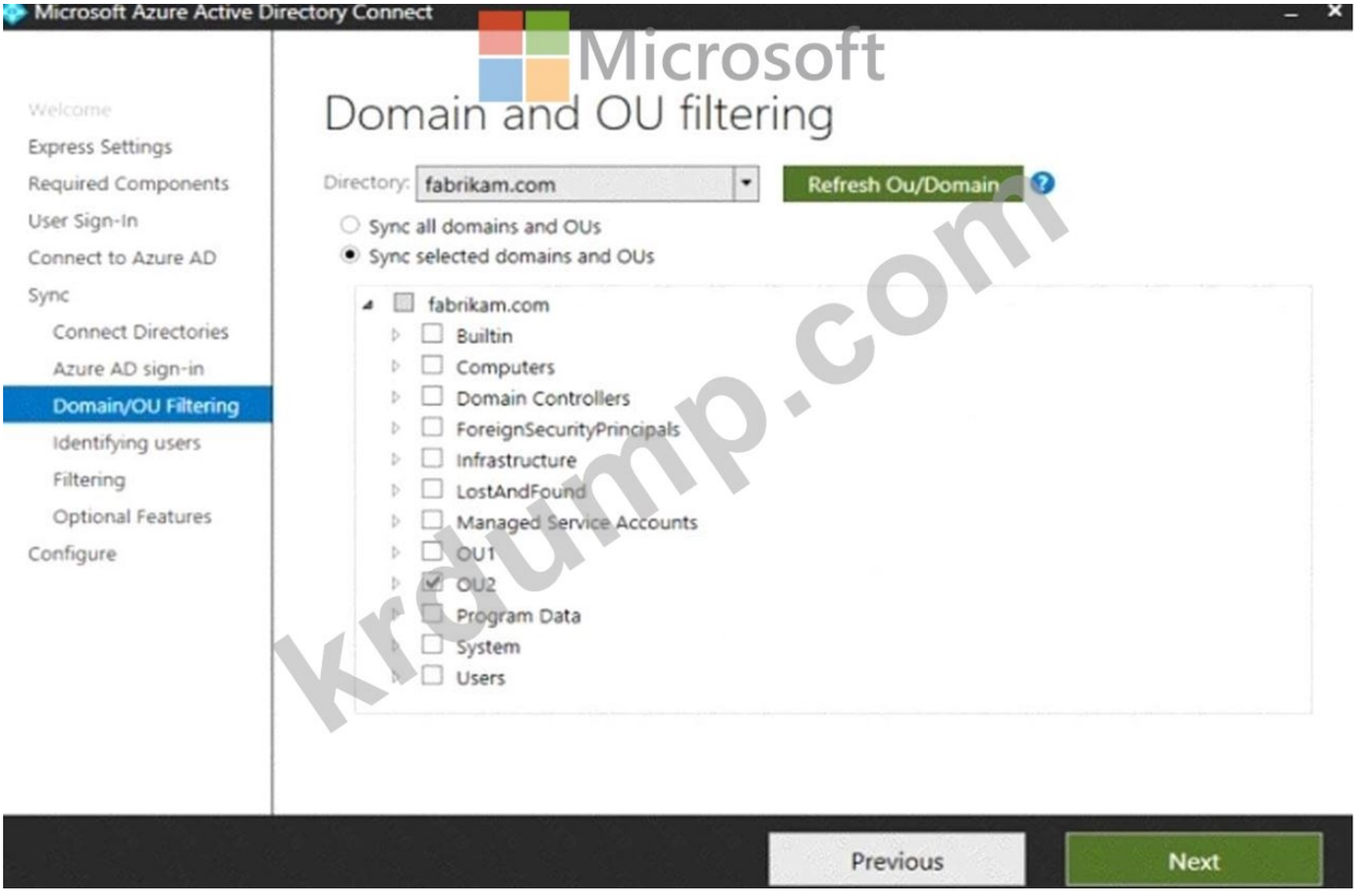
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

□□□ □□□□ □□ □□ □□ □□□□.

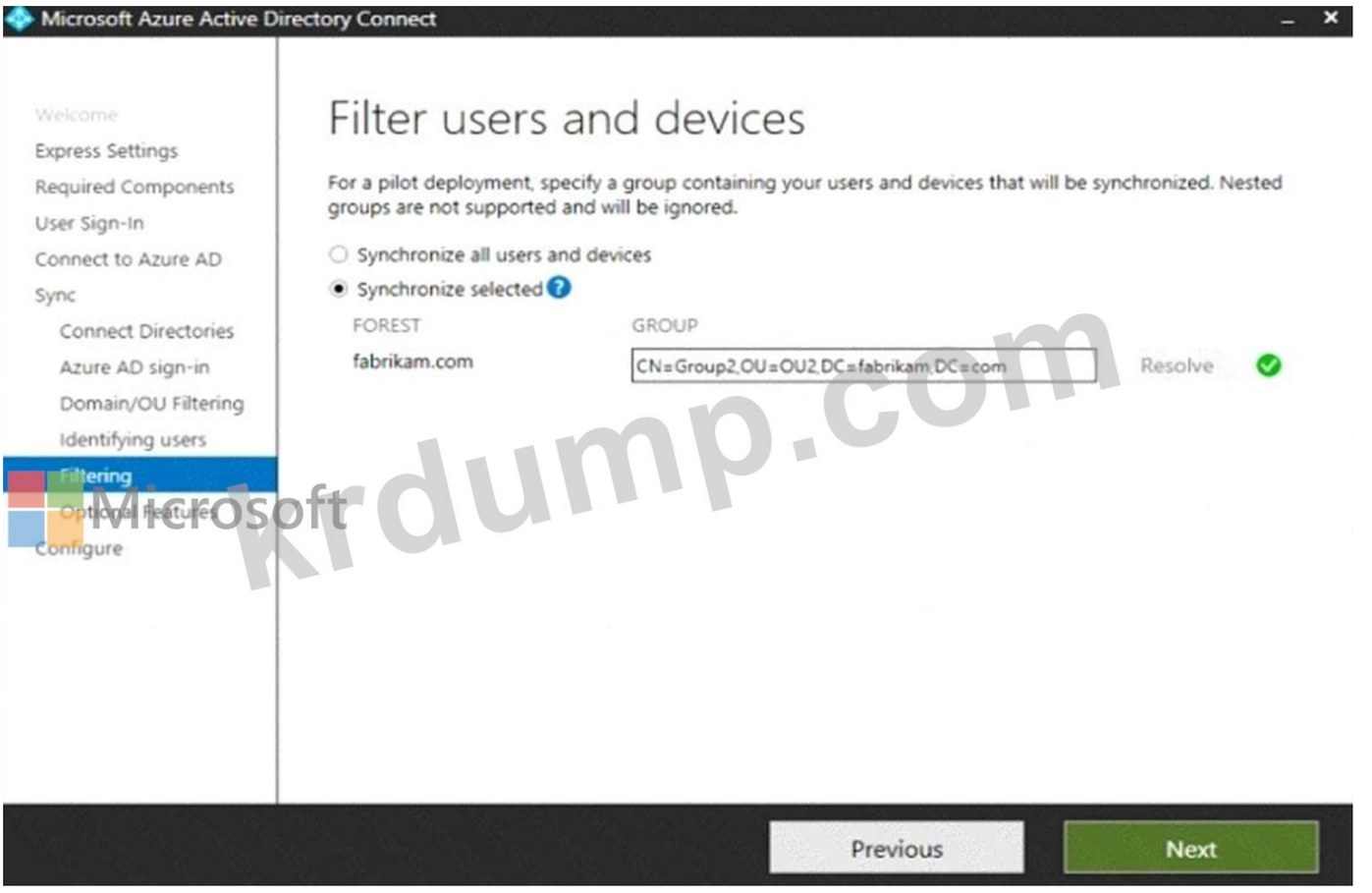
Group	Members
Group1	User1
Group2	User2, User3, Group1

fabrikam.com□ Azure AD □□□ □□ □□□□ □□□□ □□□□.

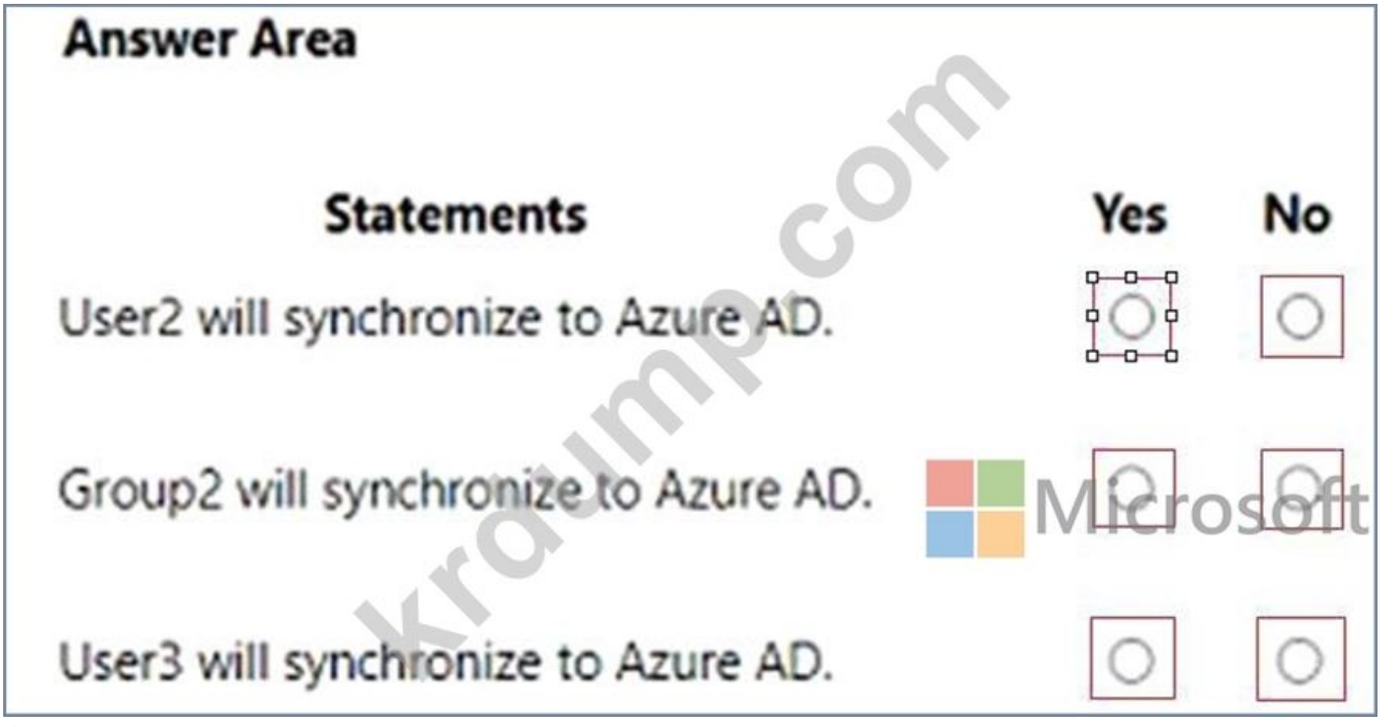
□□□/OU □□□ □□□ □□□ □□ Azure AD Connect□□ □□□/OU □□□ □□□ □□□ □□(□□□/OU □□□ □□ □□□□□.)



Azure AD Connect□□ □□□ □□□ □□□ □□□ □□□ □□ □□□□□. (□□□ □□ □□ □□□.)

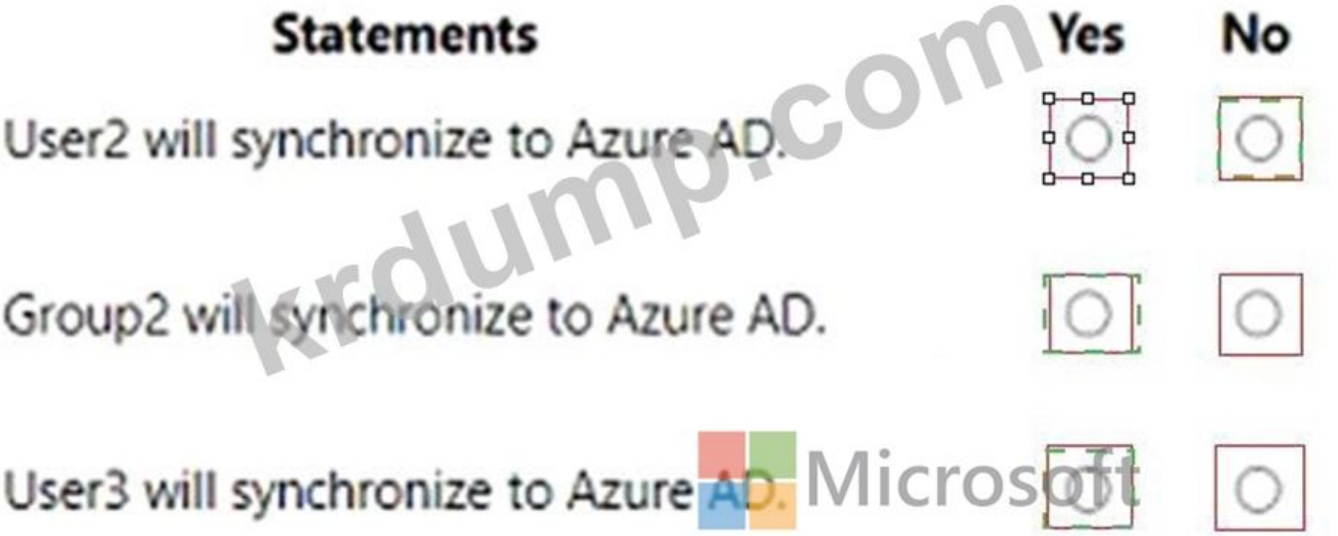

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional features
Configure
Filter users and devices
For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.
Synchronize all users and devices
Synchronize selected
FOREST
GROUP
fabrikam.com
CN=Group2,OU=OU2,DC=fabrikam,DC=com
Resolve
Previous
Next

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□. □□□□: □□ □□□ 1□□□□.


Answer Area
Statements
Yes
No
User2 will synchronize to Azure AD.
Group2 will synchronize to Azure AD.
User3 will synchronize to Azure AD.

Answer:

Answer Area



Explanation:

Box 1: No

The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.

User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD.

Box 2: Yes

Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.

Box 3: Yes

User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#group-based-filterin

NEW QUESTION: 230

Microsoft Intune□ □□□ Microsoft 365 □□□ □□□□.

Intune□ □□□□ □□ iOS □□□ □□□ □ □□□□.

Microsoft Defender for Endpoint□ □□□□ □□ □□□ iOS □□□ □□□ □□□□□. Intune□ Defender for Endpoint □□ □□□ □□□□□.

Endpoint□ Defender□ □□□ □□□□□ □□□.

□□□ □□ □□□?

A. □□□ □□□□ □□□□□□□.

B. □ □□ □□□ □□□□.

C. Intune□ □□ □□□□□.

D. □□□□□ Microsoft Defender□ □□□□□□.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 231

□□ □□ □□ □□ □□ □□ □□□ □□□ Microsoft 365 □□□□ □□□□.

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

□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

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

Answer:

Explanation:

NEW QUESTION: 232

Microsoft 365 E5 □□□ □□□□. □□□□ Site1□□□ Microsoft SharePoint Online □□□□ □□□□ □□□□. Site1□□ □□ □□□ □□□□ □□□□.

* □□.docx
* □□□□.docx
* □□jmportant.docx

Microsoft Defender Cloud □□□ □□ □□□ □□□ □□□ □□ Policy1□□□ □□ □□□ □ □□□.

Policy1□ □□ □□□ □□□□□?

A. □□.docx□

B. ImportantFile.docx□

C. File.docx, ImportantFile.docx, Filejmportant.docx

D. Filejmportant.docx□

E. ImportantFile.docx □ Filejmportant.docx□

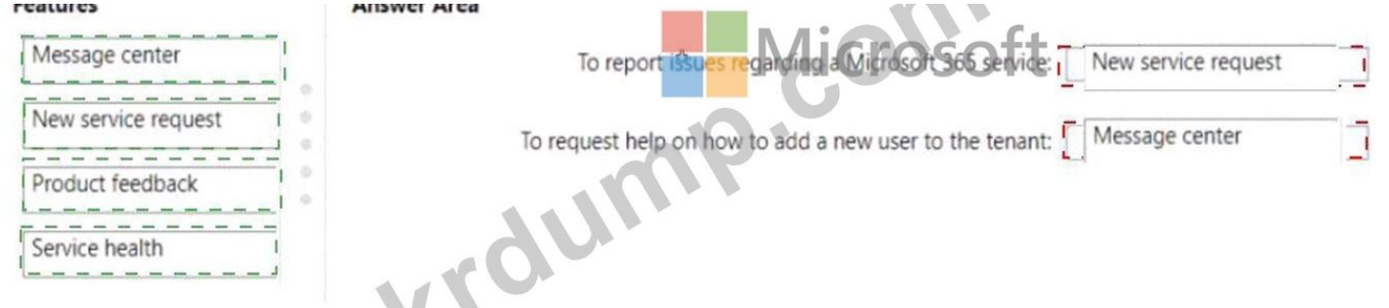
Answer: D (LEAVE A REPLY)

NEW QUESTION: 233

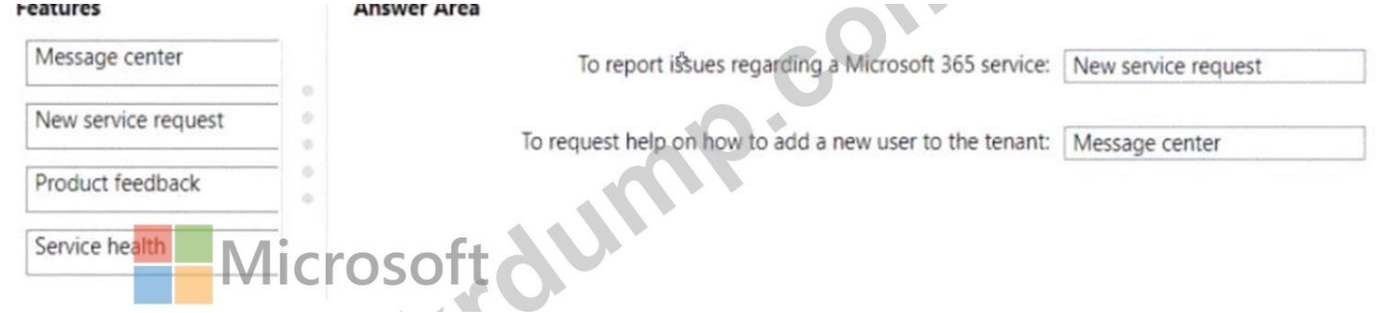
Microsoft 365 □□□ □□□□.

□□ □□ □□□ □□□□ □□□.
* Microsoft 365 □□□ □□□ □□□□□.
* Azure AD □□□□ □ □□□□ □□□□ □□□ □□ □□□ □□□□□.
Microsoft 365 □□ □□□□ □□□ □□□□ □□□? □□□□□ □□□ □□□ □□□ □□ □ □□□ □□□ □□□□. □ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □ □□ □□ □□□ □□□ □□□ □□□□ □□□ □□□□□ □ □□ □□□□.
□□□□: □□ □□□ 1□□□□.

Answer:



Explanation:



NEW QUESTION: 234
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□ Policy1□□□ □□□ □□□□□ □□ □□ □□□ □□□□.

Policy1□ User1□ □□□□□.
User1□ 24□□ □□ □□ □ □□ □□ □□□ □□□ □□ □□□□□?
A. 720
B. 30
C. 1000
D. 1030
Answer: A (LEAVE A REPLY)

NEW QUESTION: 235
Microsoft 365 E5 □□□□ □□□□.
□□□□□ 1,000□□ □□□ iOS □□□ □□□ □□□□□. □□□ □□□□□□ □□□□□ □ □ □□□□□.
□□ □□ □□□ □□□□ Microsoft Intune □□ □□□ □□□□ □□□.
* □□□ □□□□□ □□□□□□
* □□□ □□□ □□□□□□
* □□□ □□ □□□□ □□□□□.
□□□ □□□□ □□□?

A. □□ □□ □□(ADE)
B. BYOD(Bring Your Own Device) □□□ □ □□ □□
C. Apple Configurator □□
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll