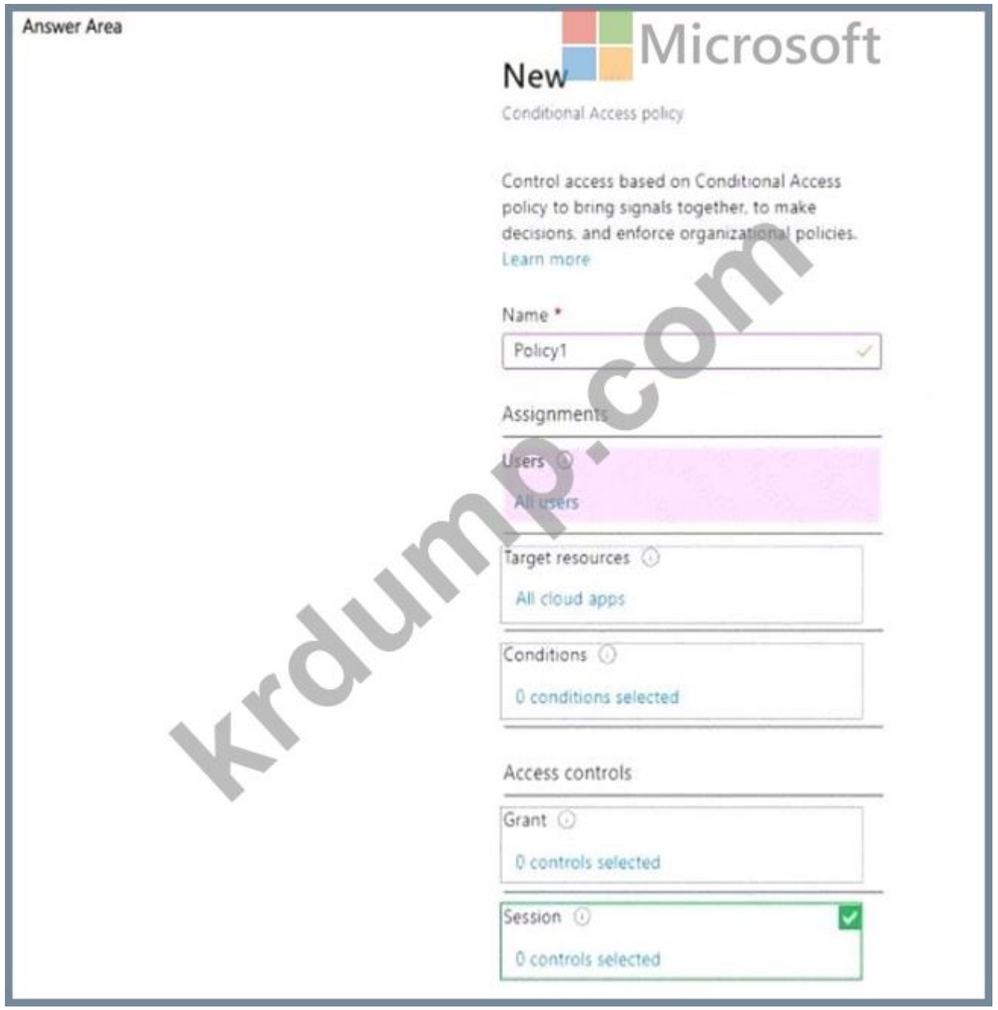
Microsoft.MS-102-KR.v2026-09-01.q239

□□□□:	MS-102-KR
□□□□:	Microsoft 365 Administrator (MS-102 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	239
□□:	v2026-09-01
# □□ □:	489
# □□ □□□:	2390
https://www.krdump.com/Microsoft.MS-102-KR.v2026-09-01.q239.html	

NEW QUESTION: 1
Microsoft 365 E5 □□□ □□□□.
Policy1□□□ □□□ □□□ □□□ □□□ □□ □□□□□ Policy1□ □□□□□.
□□□ □□ □□□ □□ □□ □□ □□ □□(MFA)□ □□□□□ Policy1□ □□□□ □□□.
Policy1□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area



Answer:

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 authentication

This 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: 2

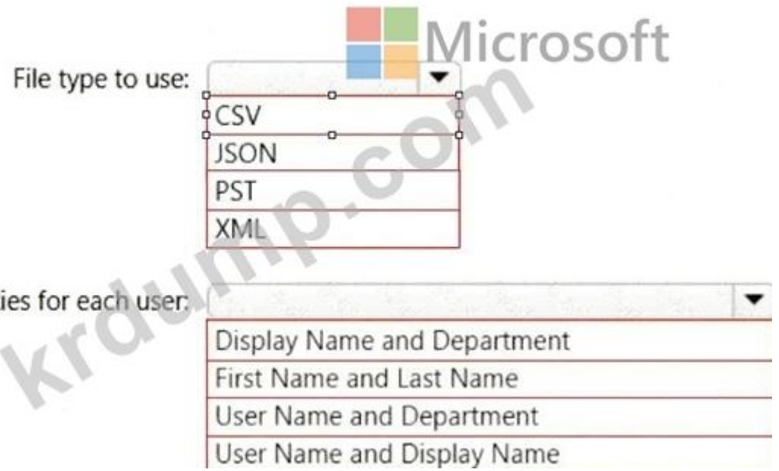
□□□

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

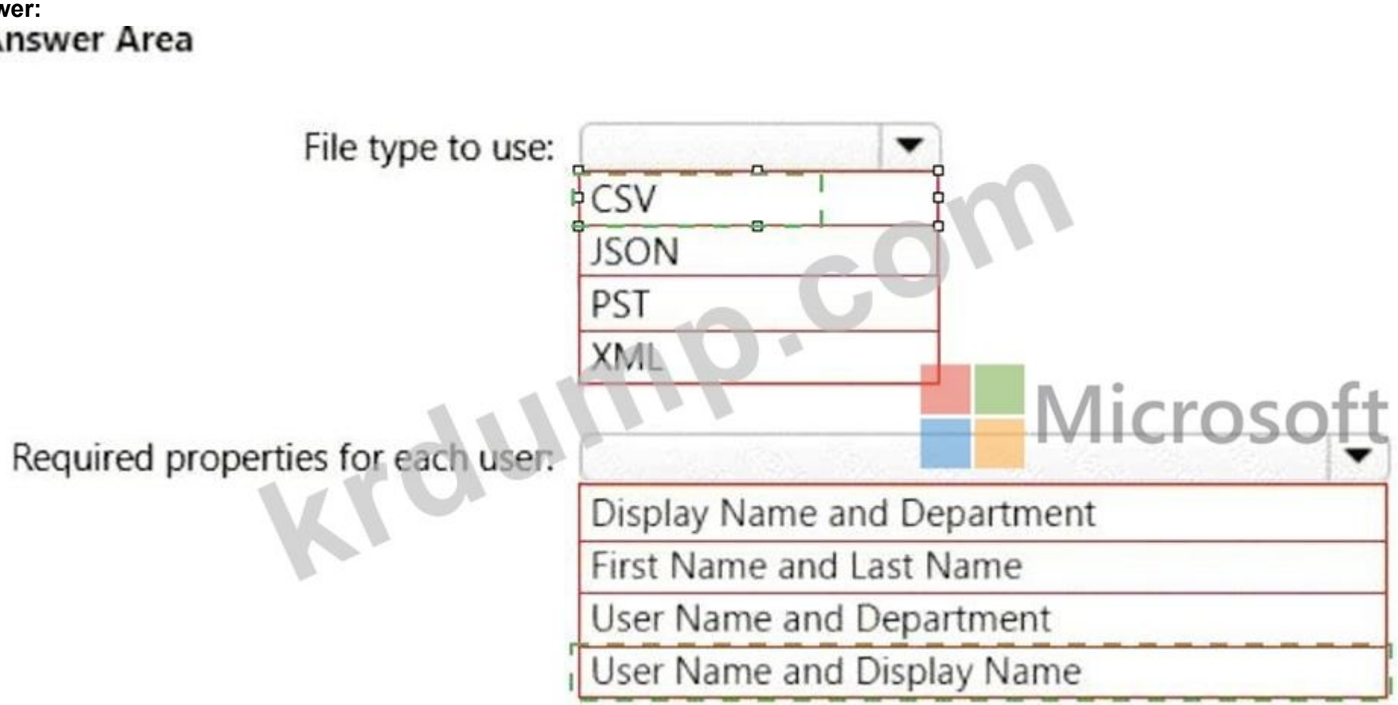
□□□ Microsoft 365 □□□ □□□□□.

Microsoft 365 □□ □□□ □□□□ 100□□ □□□□ Microsoft 365□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

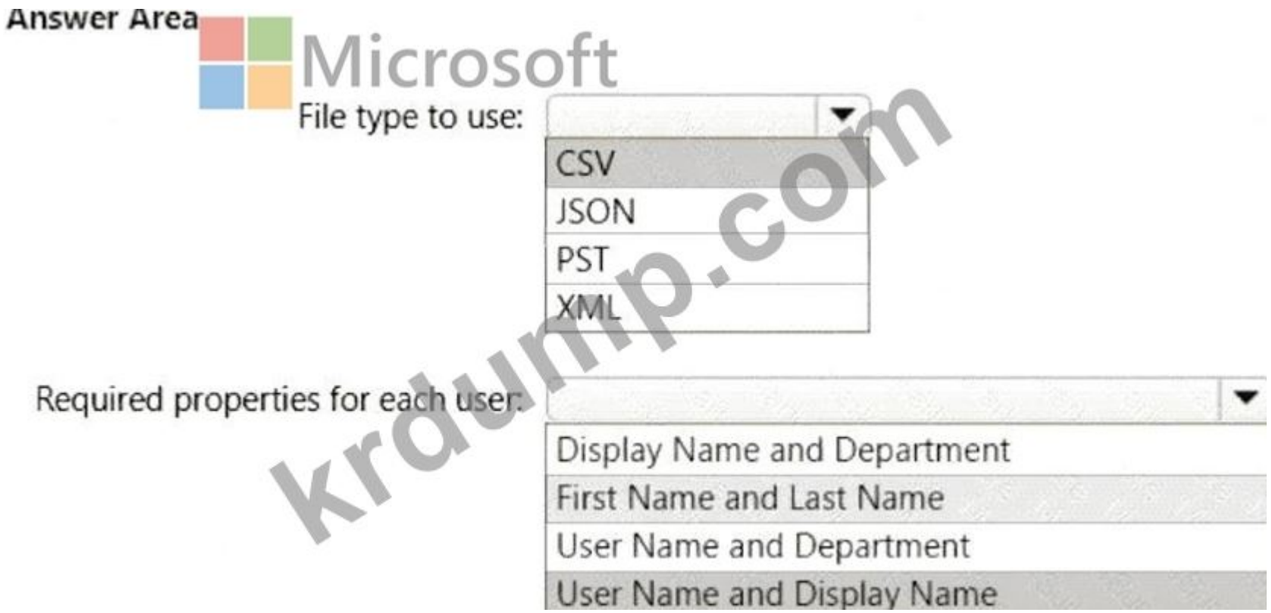
Answer Area



Answer:



Explanation:



Box 1: CSV

Add multiple users in the Microsoft 365 admin center

Sign in to Microsoft 365 with your work or school account.

In the admin center, choose Users > Active users.

Select Add multiple users.

On the Import multiple users panel, you can optionally download a sample CSV file with or without sample data filled in.

Etc.

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

Not sure what CSV format is?

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

Box 2: User Name and Display Name

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

Reference:

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

NEW QUESTION: 3

□□□ Microsoft 365 □□□ □□□□ □□□□.

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

User1□□□ □□□□ □□□□□ "ProjectX"□□ □□□ □□□ □□ □□□ □□□□ □□□ □□□□ □□□.

□□□ □□ □□ □□□?

A. Microsoft Defender for Cloud Apps□□ □□ □□□ □□□□□.

B. Microsoft Defender XDR□□ □□□ □□□ □□□□□.

C. Exchange □□ □□□□ □□ □□ □□□ □□□□□.

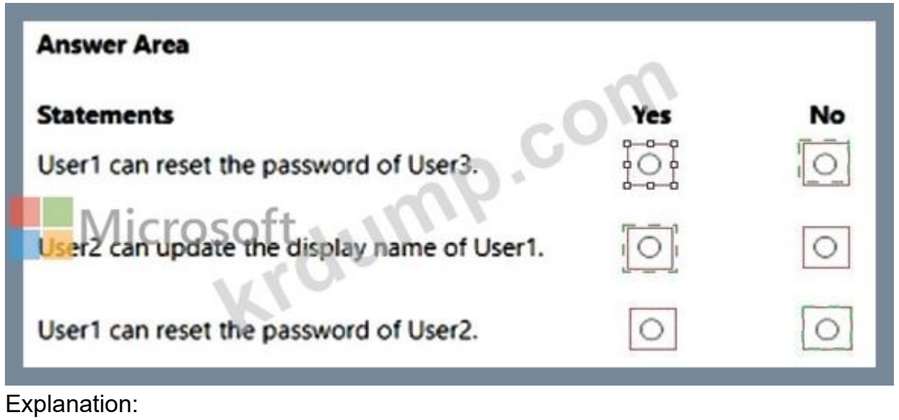
D. Microsoft Purview □□ □□ □□□□ □□□□ □□□ □□□ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
□□□
□□□ □□ □□ □□□ □□ □□□ □□□□ Microsoft Entra □□□□ □□□□ □□□□.

Name	Members
AU1	User1, User2
AU2	User3

□□□ □□ □□□□ □□□□:
User1□□□ □□□ □□□□□ AU1 □ AU2□ □□ □□□□ □□□ □□□ □□□□□□□.
AU1□ □□ □□□ □□□□ □□□ User2□□ □□□□□□.
□□□□ □□ □□□ □□□□ □□□ User3□□□ □□□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:



Explanation:

Box 1: No

User1 is assigned the Password Administrator for AU1 and AU2.

User3 is in AU2. User3 is User Adminstrator.

Password administrators cannot reset User Administrators passwords.

Note: Password Administrator

Users with this role have limited ability to manage passwords. This role does not grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user ' s password depends on the role the user is assigned.

Box 2: Yes

Box 3: No

User1 is assigned the Password Administrator for AU1 and AU2.

User2 is in AU1. User2 is User Adminstrator.

Password administrators cannot reset User Administrators passwords.

Note: User Administrator

Can manage all aspects of users and groups, including resetting passwords for limited admins.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

NEW QUESTION: 5

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

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

□□ 24□□ □□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□ □□□.

□□□ □□ □□□?

A. □□ □□□□ □□□ □□ □□□ □□□□.

B. Microsoft Purview □□ □□ □□□□ □□ □□ □□□ □□□□.

C. Microsoft Purview □□ □□ □□□□ DLP(□□□ □□ □□) □□□ □□□□.
D. □□ □□□□□ □□ □□□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 6
□□□ □□ □□□ □□□ □□□ □□□□ Microsoft 365 □□□□ □□□□. □□□ □□ □□ □□□ □□ □□□□□.

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

□□□ □□ VPN □□□□ □□□□ □□□□□.
□□□ □ □□ □□ □□□ □□□□□?
A. 4
B. 1
C. 3
D. 5
Answer: (SHOW ANSWER)

NEW QUESTION: 7
□□□ □□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

□□ 8□□ □□□ □□ □□□□ □□ □□ □□□ □□□□□.
* □□: □□!
* □□ □□
o □□ 70□ □□: □□
o □□ □□ □□: □□(3)
o □□ □□: □□□ □□ □□
* □□□: Userl@contoso.com, User2@contoso.com
□□ 8□ 2□□ □□□ □□ □□□□ □□□□ □□ □□□ □□□□□.
* □□: □□
* □□ □□
o □□ □□□: □□, □□□ □□ □□ □□
o □□ □□ □□: DeviceGroup1, DeviceGroup2
* □□□: Userl@contoso.com
Microsoft Defender XDR□□□ □□ □□ □□ □□□ □□□□□.

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□□□□.

Answer:

Explanation:

NEW QUESTION: 8

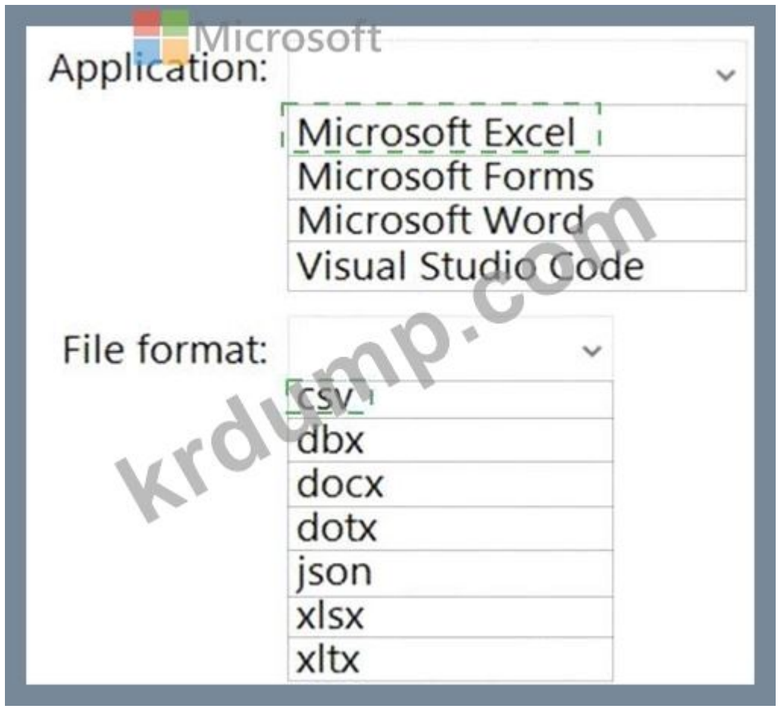
Microsoft 365 □□□□ □□□□.

□□□ □□ □□ □□□ □□ □□□□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.

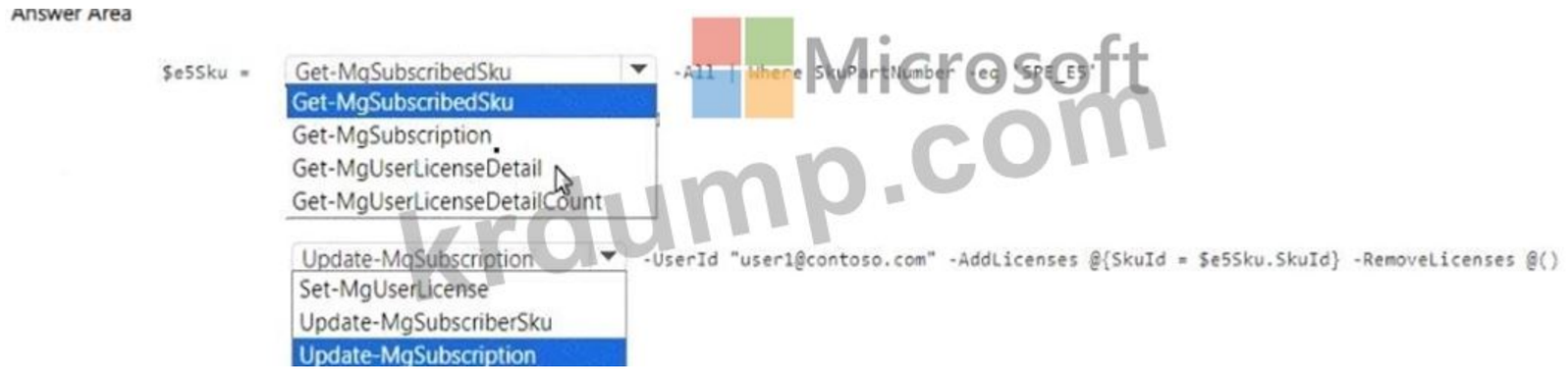
Answer:



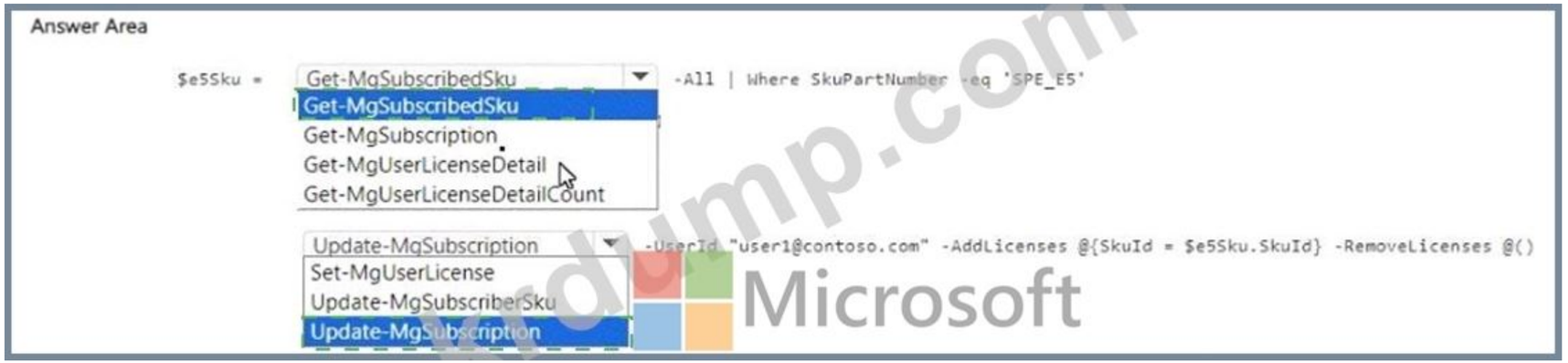
Explanation:

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

NEW QUESTION: 9
Microsoft 365 E5 □□□ □□□□.
user1□□□ □ □□□□□ Microsoft 365 E5 □□□□□ □□□□□ Microsoft Graph PowerShell□ □□□□ □□□.
@contoso.com.
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 10

Microsoft 365 □□□ □□□□.

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

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

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 11

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□

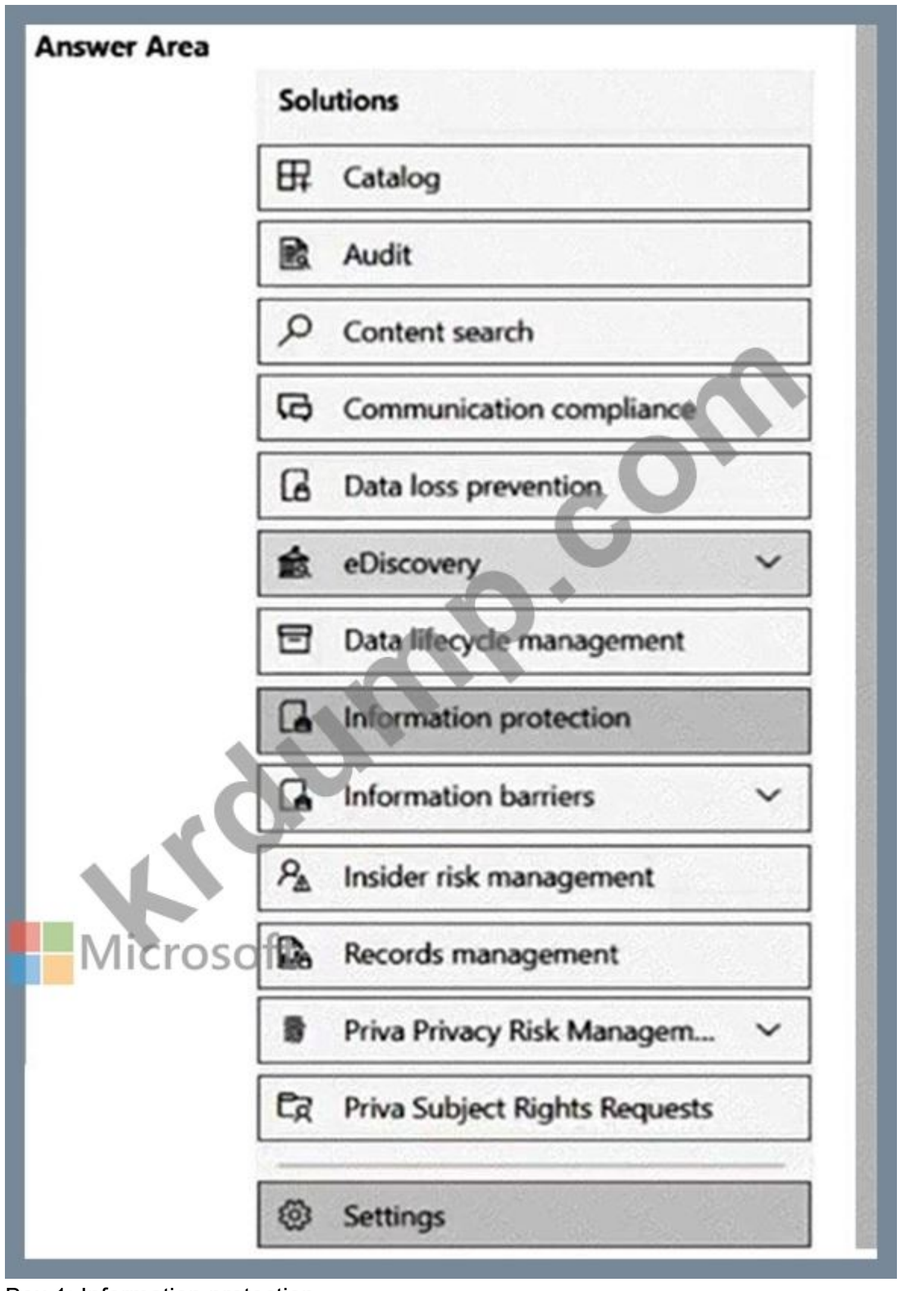
B. 2024□ 1□ 1□
C. 2023□ 1□ 31□
D. 2024□ 1□ 31□
E. □□ □□
Answer: (SHOW ANSWER)
Retention wins over deletion.
Note:
Explanation for the four different principles:
1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle 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: 12
□□□
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□ □□□.
Microsoft OneDrive □ SharePoint□ □□□ □□□ □□□□ □□□□□□.
□□□ □□□□ □□□□ □□□□ Microsoft Office □□□ □□ □□□ □□□□□□.
Microsoft Purview □□ □□ □□□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Explanation:



Box 1: Information protection

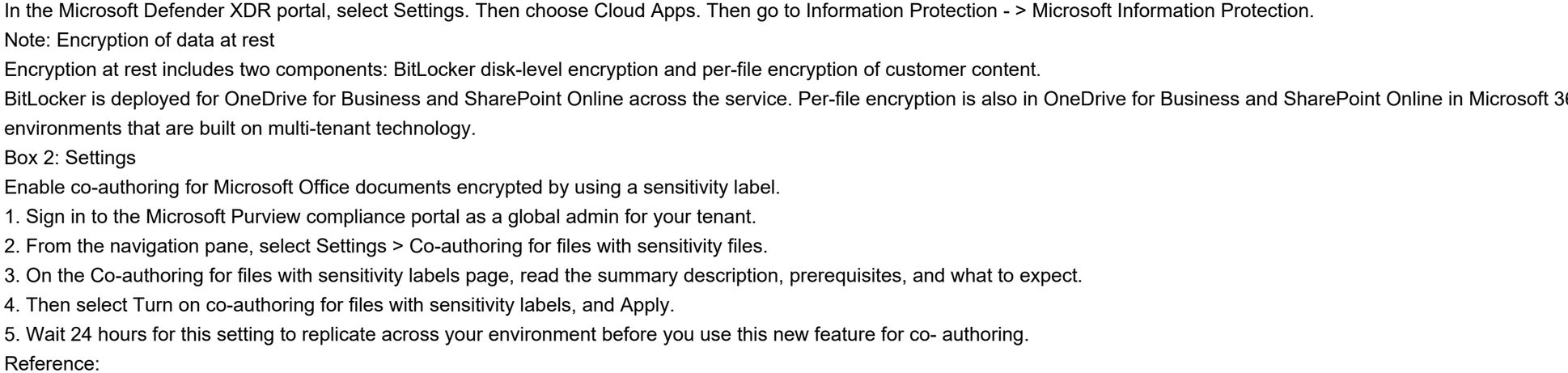
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you ' ll see them in Defender for Cloud Apps.

To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels:

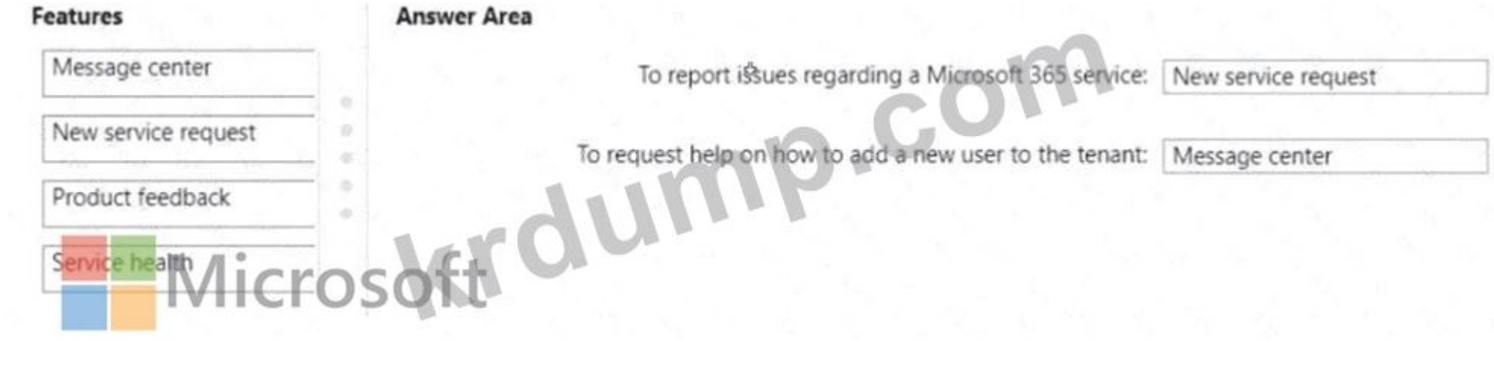
In the Microsoft Defender XDR portal, select Settings. Then choose Cloud Apps. Then go to Information Protection - > Microsoft Information Protection.
Note: Encryption of data at rest
Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.
BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology.
Box 2: Settings
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.
1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co- authoring.
Reference:
https://learn.microsoft.com/en-us/defender-cloud-apps/azip-integration
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-coauthoring

NEW QUESTION: 13
□□□ Microsoft 365 □□□ □□□□ □□□□.
□□ □□□ □□□□ □□□.
* Microsoft 365 □□□ □□□ □□□□□.
* Microsoft Entra □□□□ □ □□□□ □□□□ □□□ □□ □□□ □□□□□.
Microsoft 365 □□ □□□□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□ □□□ □□ □□□□□□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□ □ □□□□□□ □□□□□ □ □□ □□□□.
□□: □□ □□□ 1□□□□.



Answer:

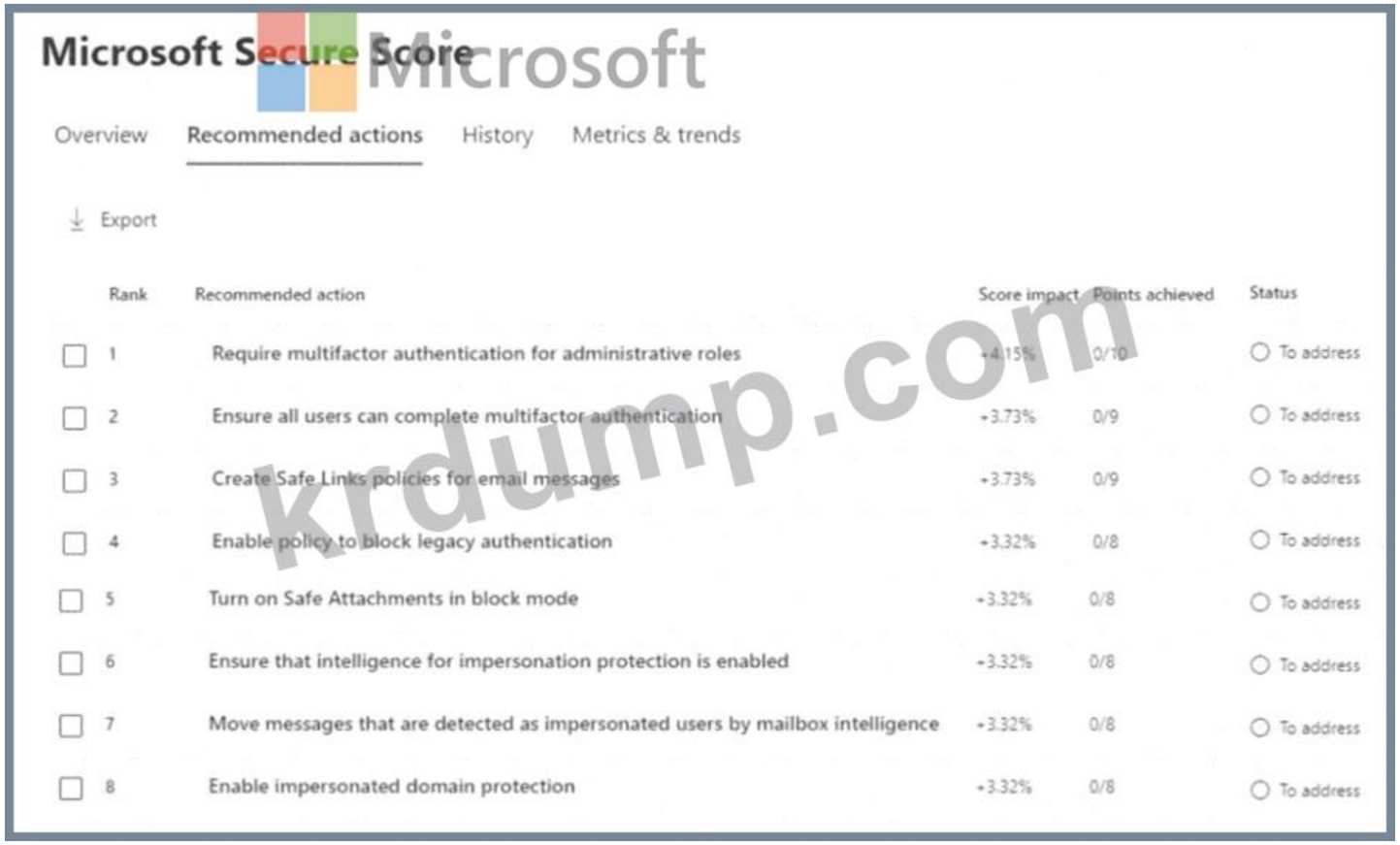
Explanation:



NEW QUESTION: 14

Microsoft 365 E5 □□□ □□□□.

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



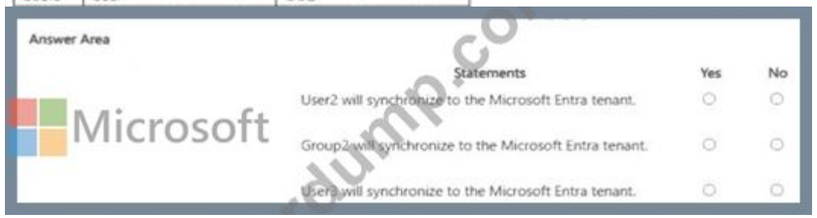
□□□ □□□□ □□ □□□ □□ □□ □□□□ □□□□ □□ □ □□ □□ □□□□ □□□ □□ □□□□ □□□□□.
□ □□ □□□ Secure Score□ □□ □□□ □□□□?
A. 9□□□ □□□□□.
B. □□□□ □□□□□
C. 9□□□ □□
D. 1□□□ □□
E. 1□□□ □□□□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
□□□ □□□□□□ Contoso□□ Active Directory □□□□□ □□□□ □□□□. □□.
Microsoft 365 □□□ □□□□.
□□□□ □□ □□□□ □□□□ □□□□ □□□ □□□□ □□□□□ □□□.
Microsoft 365 □□ □□□□ contoso.com □□□ □□□ □□□□□ □□□□□□.
□□□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Microsoft 365 □□ □□□□ Contoso.Local □□□ □□□ □□□□□.

B. Active Directory □□□ □ □□□□□□ contoso.com□ UPN □□□□ □□□□□.
C. Active Directory □□□ □ □□□□□ □□ □□□□ UPN □□□□ □□□□□.
D. contoso.com□ □□ DNS □□□□ □□□ □□ □□□(MX) □□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
□□□□□ contoso.com□□□ Active Directory □□□□ □□□□. □ □□□□□ □□ □□ □□ □□ □□□ □□□□ □□□□.

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

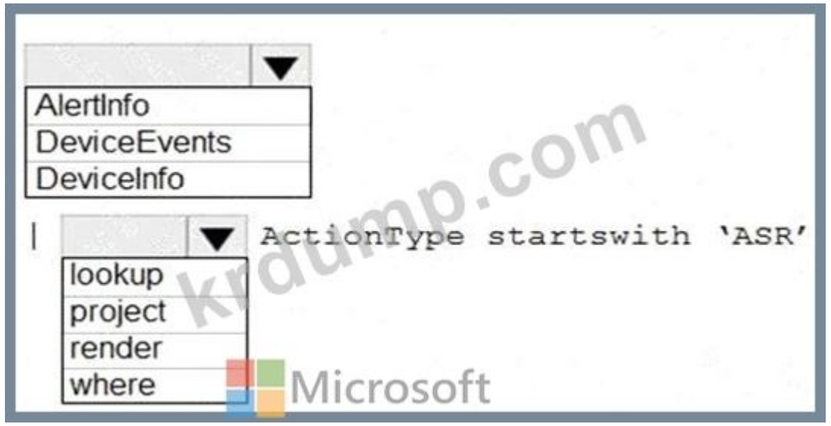


Answer:

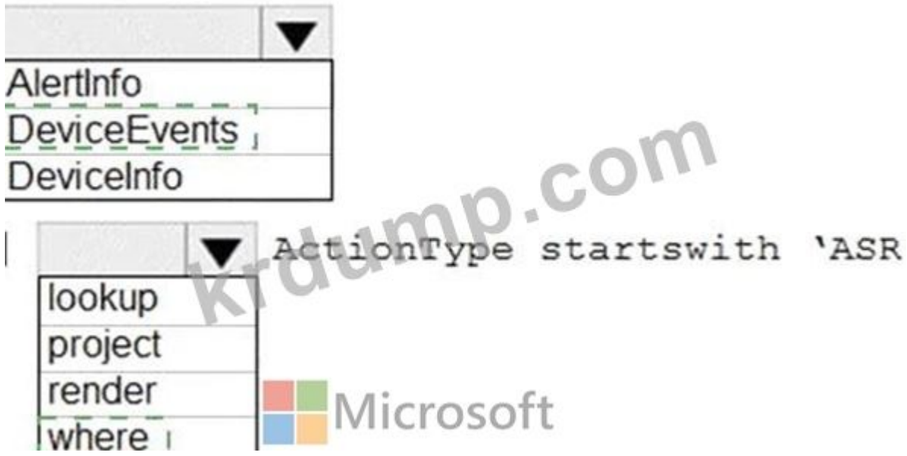
Explanation:

NEW QUESTION: 17
100□□ Windows 10 □□□ □□□ Microsoft 365 E5 □□□□ □□□□.
Windows 10 □□□ □□ □□ □□(ASR) □□□ □□□ □□□□□.
□□ □□□□ ASR □□□ □□□□ Log Analytics □□ □□□□ □□ □□□□ □□□□□.
□□□ □□□ □□□□ ASR □□□ □□□ □□□.

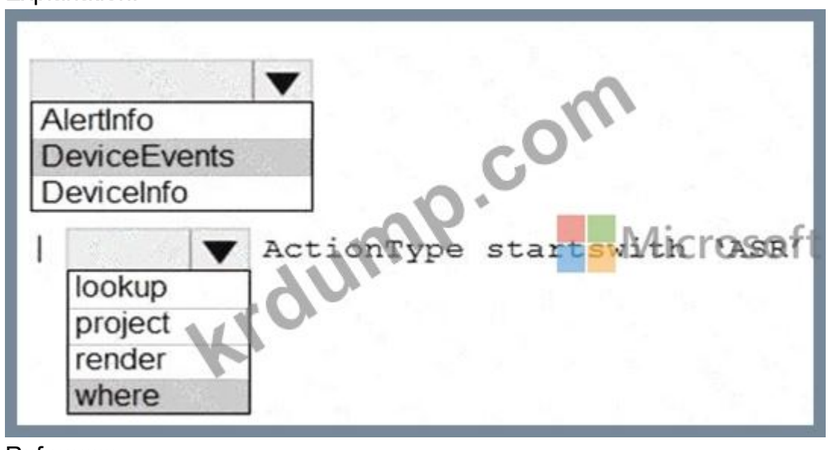
Kusto □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



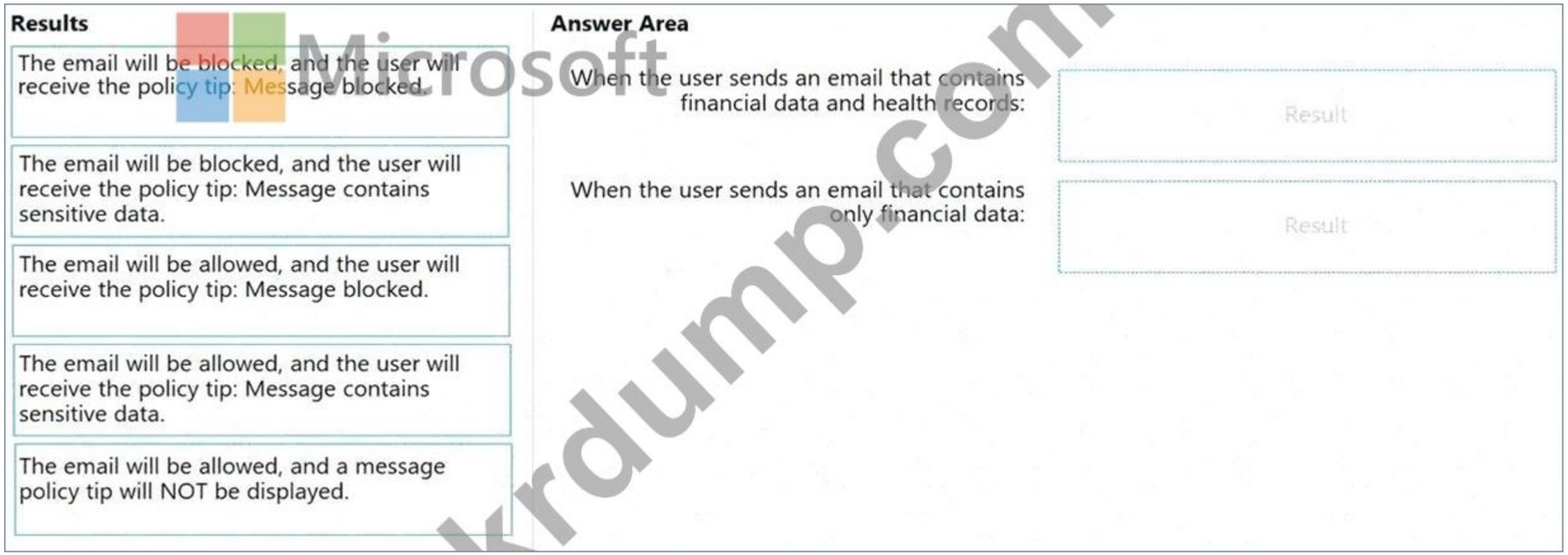
Explanation:



Reference:

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

NEW QUESTION: 18
Microsoft 365 □□□ □□□□.
Exchange □□ □□□□ □□ □□□ □□ Policy1□□□ DLP(□□□ □□ □□) □□□ □□□□.
* □□ □□□□ □□□ □□□□ □□□□□.
* □□ □□ □ □□□□ □□□□□: □□□□ □□□□□□□.
□□ □ □□ □□ □□ □□□□ □□ □□□ □□ Policy2□□ DLP □□□ □□□□.
* □□ □□□ □□□□□: □□□□ □□□□□.
* □□ □□ □ □□□□ □□□□□: □□□□ □□□ □□□□ □□□□ □□□□.
* □□□□ □□□□ □□ □, □□□□ □□ □□□ □□□□ □□ □□ □□□□□ □□□□.
□□□□ □□□□ □□ □ DLP □□□ □□□ □□□□□? □□□□□ □□□ □□□ □□□ □□□□□ □□□ □□□□□. □ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □□□ □ □□ □□□ □□□□□ □□□□ □ □ □□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Results

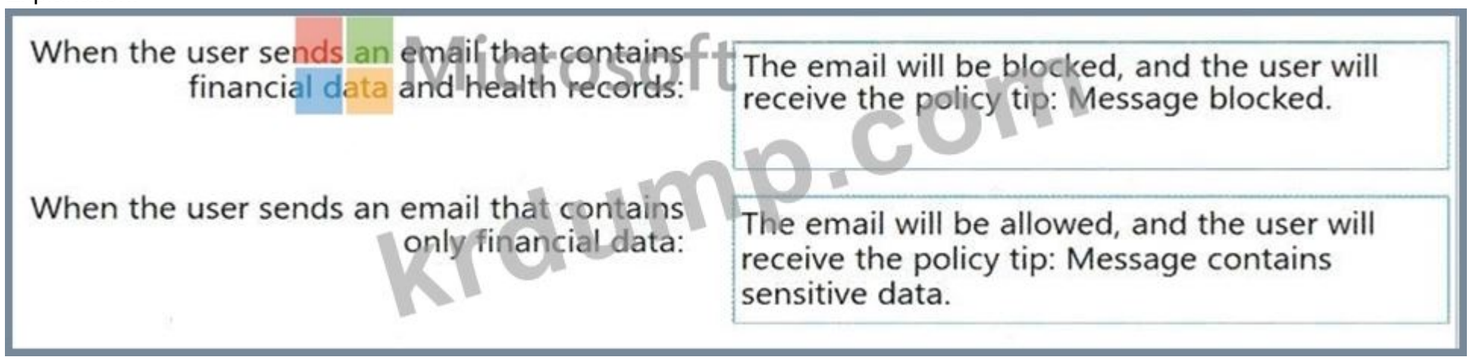
- The email will be blocked, and the user will receive the policy tip: Message blocked.
- The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.
- The email will be allowed, and the user will receive the policy tip: Message blocked.
- The email will be allowed,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

Answer Area

When the user sends an email that contains financial data and health records: The email will be blocked, and the user will receive the policy tip: Message blocked.

When the user sends an email that contains only financial data: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Explanation:



Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked.

If you ' ve created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.

Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Reference:

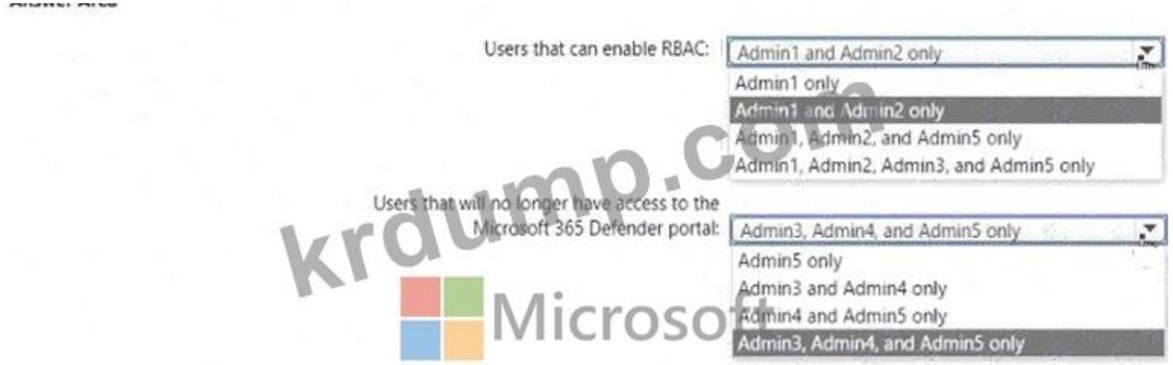
https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers

NEW QUESTION: 19

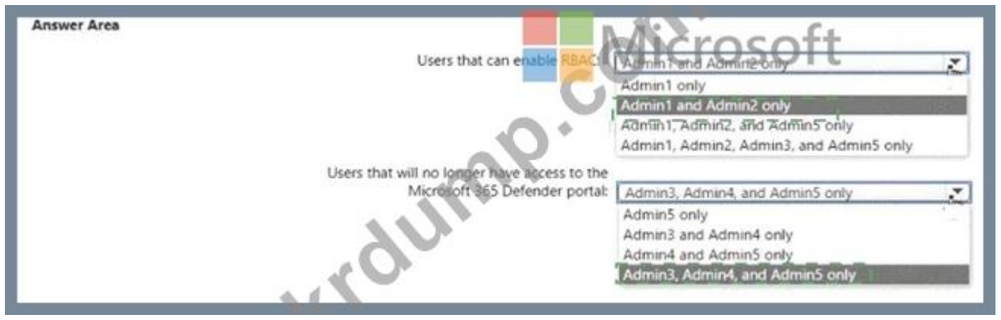
□□□ □□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

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

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



Answer:

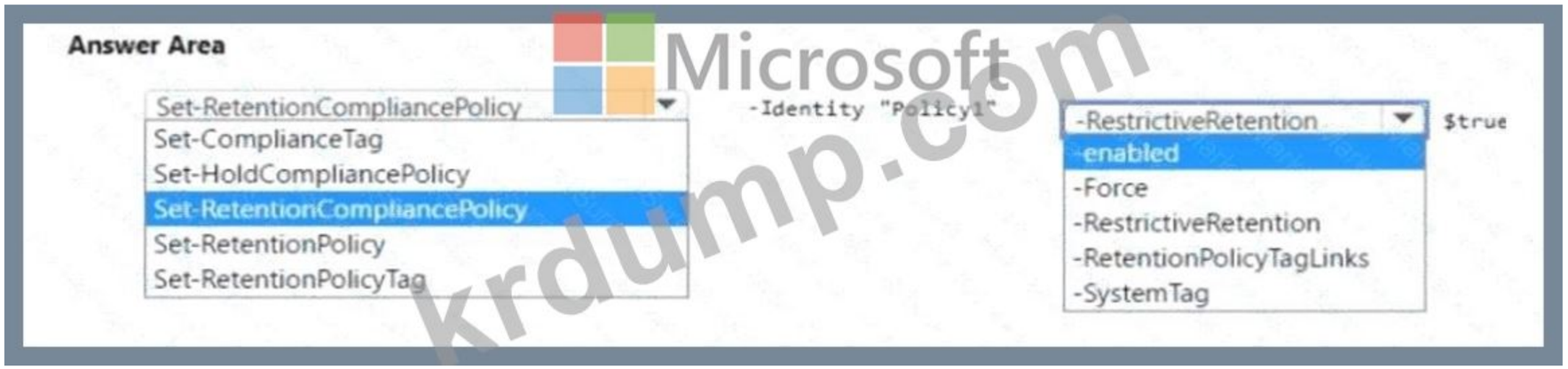


Explanation:

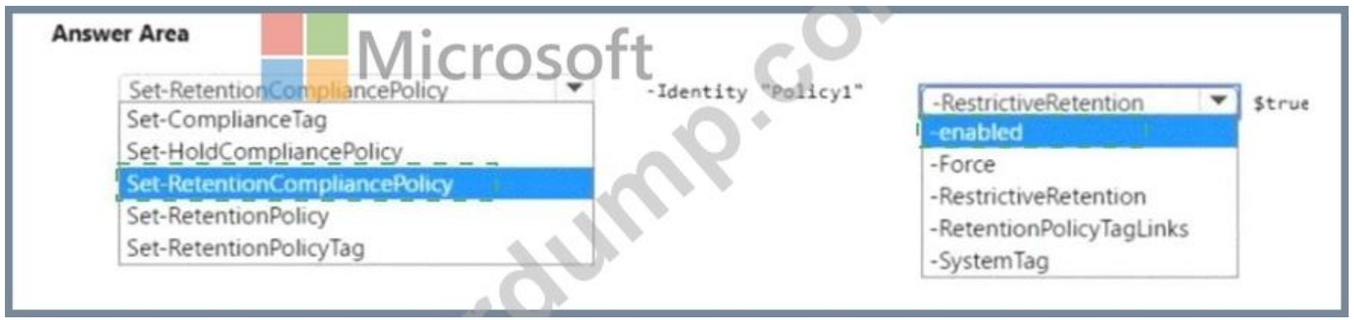
NEW QUESTION: 20
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □□ □□□ □□□□.
□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□, □□ □□□□ □□□□ □□□□.
□□□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft Entra □□□□ □□□□□.
□□ □□□□ □□□□ Microsoft Entra ID□ □□□□□□ □□□□□.
□□ □□(OU)□ □□ □□□ □□ 10□□ Microsoft Entra ID□ □□□□□ □□ □□ □□□□□□. □□□ □□□ □□□ □□ □□□□□ □□□□□□□□.
Microsoft Entra Connect □□□ □□□ □□ □□ □□□ □□ □□□□ □□□□□ □□□□□□ □□□□□□.
10□□ □□□ □□□ Microsoft Entra ID□ □□□□□□□ □□□□ □□□.

□□ □□: Microsoft Entra Connect Sync□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)

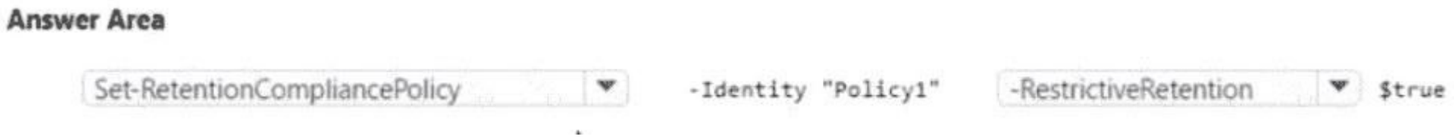
NEW QUESTION: 21
Microsoft Purview □□ □□□□ □□ 1□□□ □□□ □□ □□□ □□□□.
□□ □□□□ □□□ □□□□□□□ □□ □□□ □□□ □□ □□□□ □□□.
Azure PowerShell □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 22
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □ □, □□ □□□□ □□□ □□ □ □□□□.

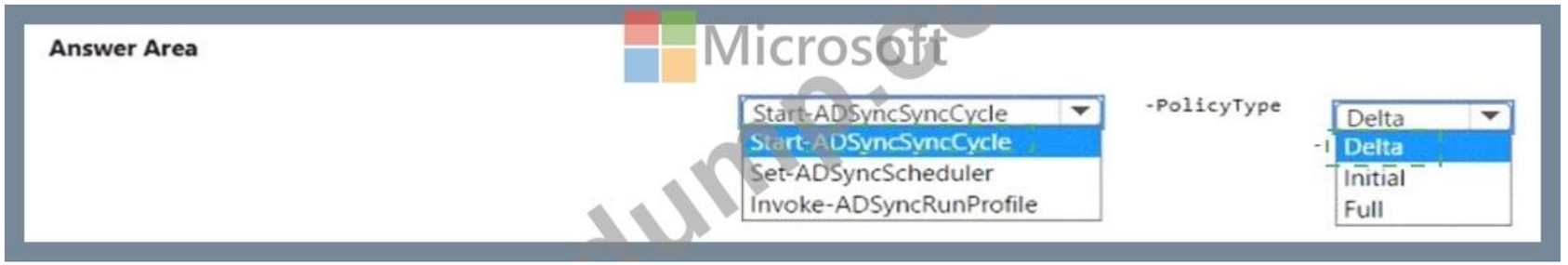
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Windows 10□ □□□□ □□□□ □□□□.
□□□ Windows 10 □□□ □□□□ □□□.
□□ □□: □□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

NEW QUESTION: 23
Microsoft 365 □□□□ □□□□.
Microsoft Defender XDR□ □□□□ □□□□□ □□□□□ □□□ □□□□□. Microsoft Defender □□□ □□□□ □□□□ □□ Microsoft □□□ □□□ □□□□□?
A. □□□□ □□ Microsoft Defender
B. □□□□□ Microsoft Defender
C. Azure Arc
D. Azure □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 24
□□□□□□ Active Directory □□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□ □ 10,000□□ □□ □□□□ □□□□ □□□□ □□□□ □□□□□.
100□□ □ □□□ □□ □□□ □□□□□□.
□ □□□ □□□ Microsoft Entra ID□ □□□ □□ □□□□□□ □□ □□□.
□□ □□□□ □□□□ □□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□.

Answer Area

Answer:



Explanation:

NEW QUESTION: 25

Microsoft 365 □□□ □□□□.

□□□ □□ onmicrosoft.com □□□□ □□□□ □□□. □□ □□□□ □□□□ □□□ □□□ □□□ □ □□□ □□□.

□□□ □□□ □ □□ onmicrosoft.com □□□□ □□ □□ □□□□□?

A. 1

B. 2

C. 5

D. 10

Answer: (SHOW ANSWER)

You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to create a new one.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq

NEW QUESTION: 26

Microsoft Entra ID □□ □□ □□(ATP)□ □□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Azure ATP□□ □□ □□ □□□ □□□□ □□□.

□□ □□□ □□□□ □□□?

A. □□ □ □□ □□ □□ □□

B. □□□□□□□ □□□ □□ □□

C. Microsoft 365 □□ □□

D. Microsoft Entra ID □□ □□ □□ □□

E. □□□□ □ □□ □□

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/what-is

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

NEW QUESTION: 27

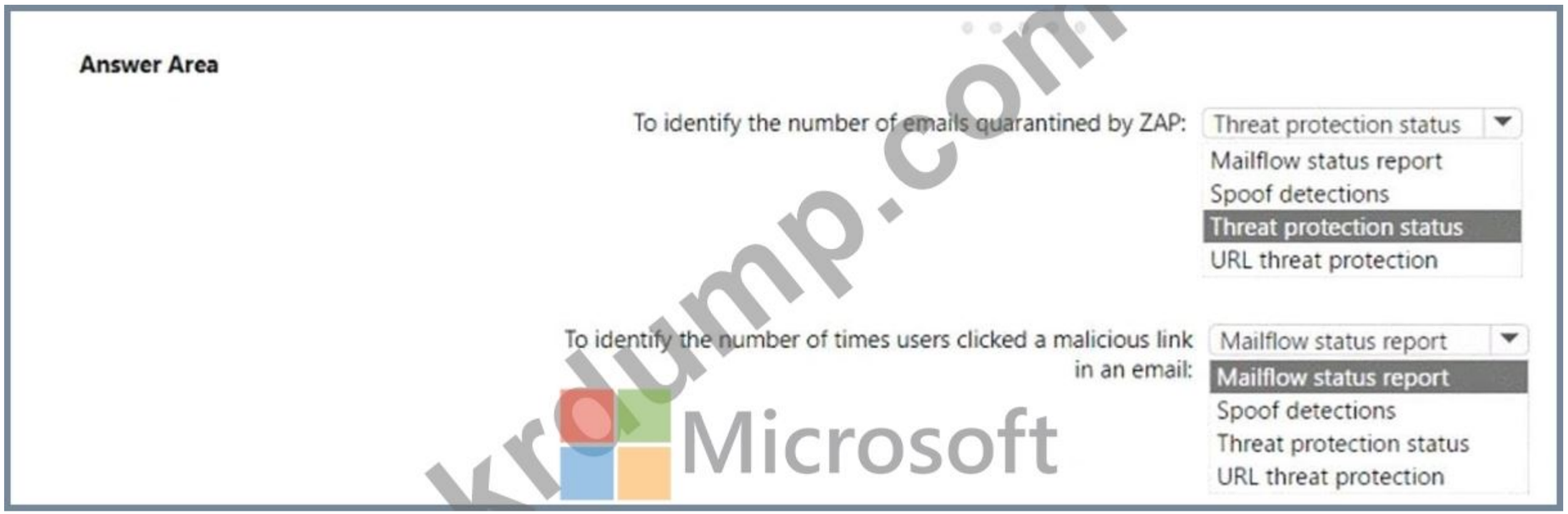
Office 365□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□ □□□□.

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

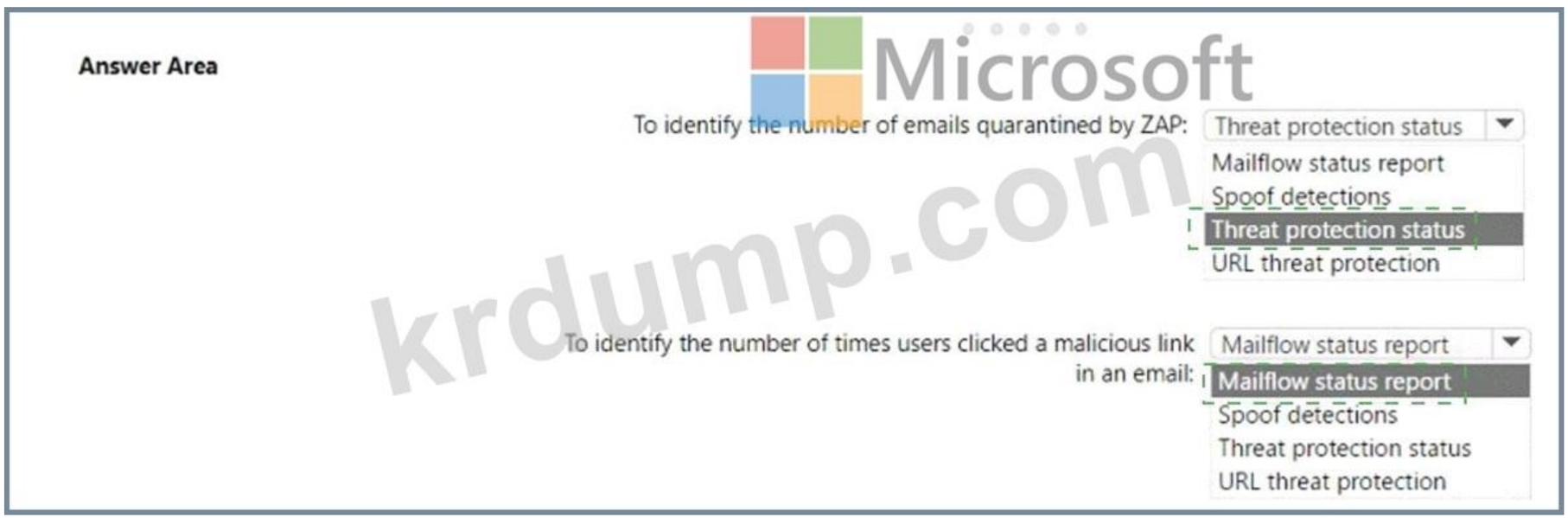
□□ □□□ □□□□ □□□.

* ZAP(□□□□ □□ □□)□ □□□ □□□ □□□ □

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

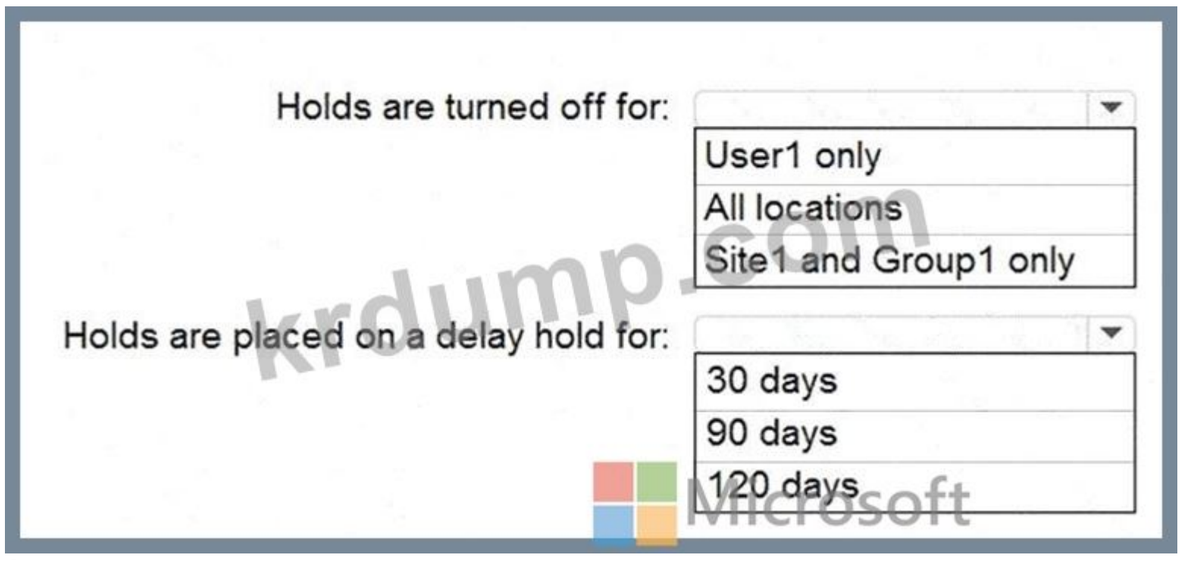


Answer:



Explanation:

NEW QUESTION: 28
□□ □□ eDiscovery □□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□ : Case1
□□□ □□□: Group1, User1, Site1
□□ □□: Exchange □□□, SharePoint □□□, Exchange □□ □□ Case1□ □□ □□□ □□□□ □□□ □□□□.
Case1□ □□ □ □□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/close-or-delete-case?view=o365-worldwide

NEW QUESTION: 29
Windows 10 □□□ 2,500□ □□, User1□ User2□□ □ □□ □□□□ □□ Microsoft 365 E5 □□□□ □□□□. □□ □□□ Microsoft Intune□ □□□□ □□ □□□□.
Microsoft Endpoint Manager□□ □□ □□□ □□ □□□ □□ □□□□□.

Microsoft Entra ID(Microsoft Entra ID)□□ □□ □□□ □□ □□□ □□ □□□□□.

Microsoft Endpoint Manager□□ User2□ □□ □□ □□□(DEM)□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 30
Office 365□ Microsoft Defender□ □□□□ Microsoft 365 □□□ □□□□.
□□ □□□ □□□□ □□□□ □□□□ □□□ □□ □□□ □□□□□ □□□ □ □□□ □□□□ □□ □□ □□□□?
□□□ □□□□□ 24□□ □□□ □□□ □□□ □□□.
A. □□ □□□ □□ □□□ □□□ □□□□□.

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

NEW QUESTION: 31
□□□□□ Endpoint□ Microsoft Defender□ □□□□ □□□□.
□□ □□□□ Microsoft Defender for Endpoint□ □□□□ □□□ □□□□□.

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

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

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

□□ □□□ □□□□ □□ □□□ □□□□.
* IOC □□□: □□ IOC
* □□: □□ □□□
* □□ □□: ATP1 □□ □□□ □□ □□
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□□. □□□ □□□ □□□□ □□□□□□. □□: □□□ □□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 32
Montreal Users □ Seattle Users OU□ □□ □□□ □□ □□□ □□□□□ Microsoft Entra Connect Sync□ □□□□ □□□.
□□□ □□ □□□?
A. PowerShell□□ Start-ADSyncSyncCycle cmdlet□ □□□□□.
B. PowerShell□□ Add-ADSyncConnectorAttributeInclusion cmdlet□ □□□□□.
C. Microsoft Entra Connect □□□□□ □□□□□ □□□ □□□□□.
D. Microsoft Entra Connect □□□□□ □□□ □□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 33
□□□□□□ □□ □□□ □□ Microsoft Entra ID□ □□□□ □□□□□ Active Directory □□□□ □□□□ □□□□.

□□□□□ Active Directory □□□ □□□ Allan You□ Microsoft Entra ID□ □□□□□□□□. Microsoft 365□□ Allan□ □□□ □□ □□□ □□□ Allan @ > ddatum□□ □□□□ □□ □□ □□□ □ □□□□.
onmicrosoft.com.

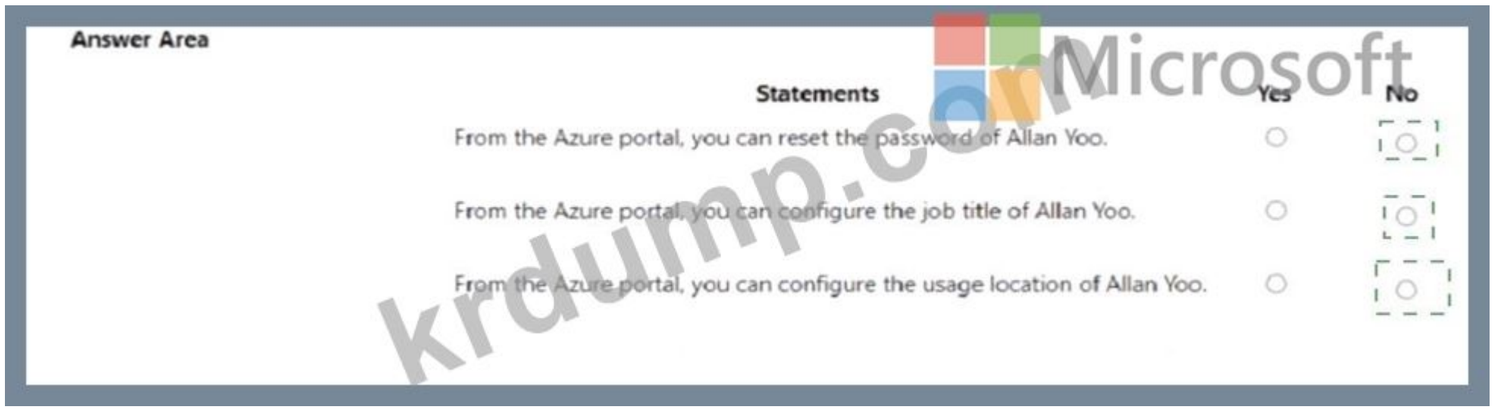
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:



Explanation:

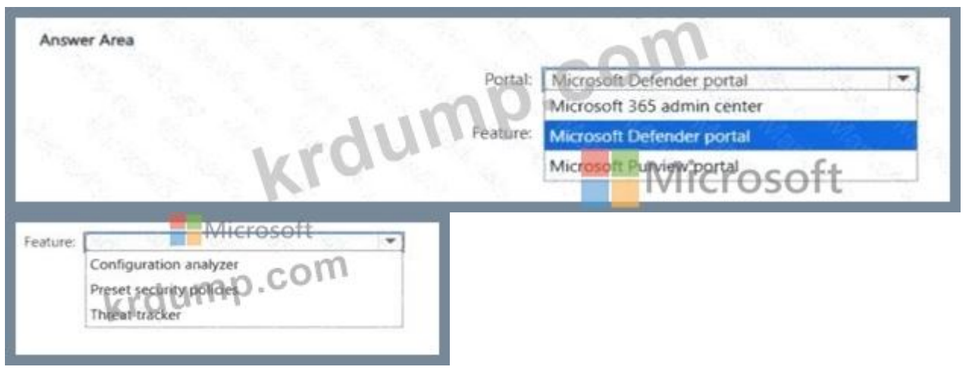
NEW QUESTION: 34

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

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

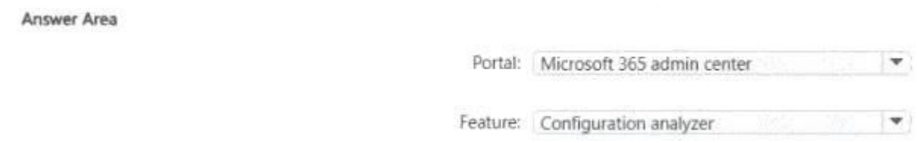
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.



Answer:

Explanation:



NEW QUESTION: 35

□□ □□ □□ □□ □□□□ □□□ 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 Microsoft Entra ID Microsoft Entra ID (Microsoft Entra ID), 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 Microsoft Entra ID.

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

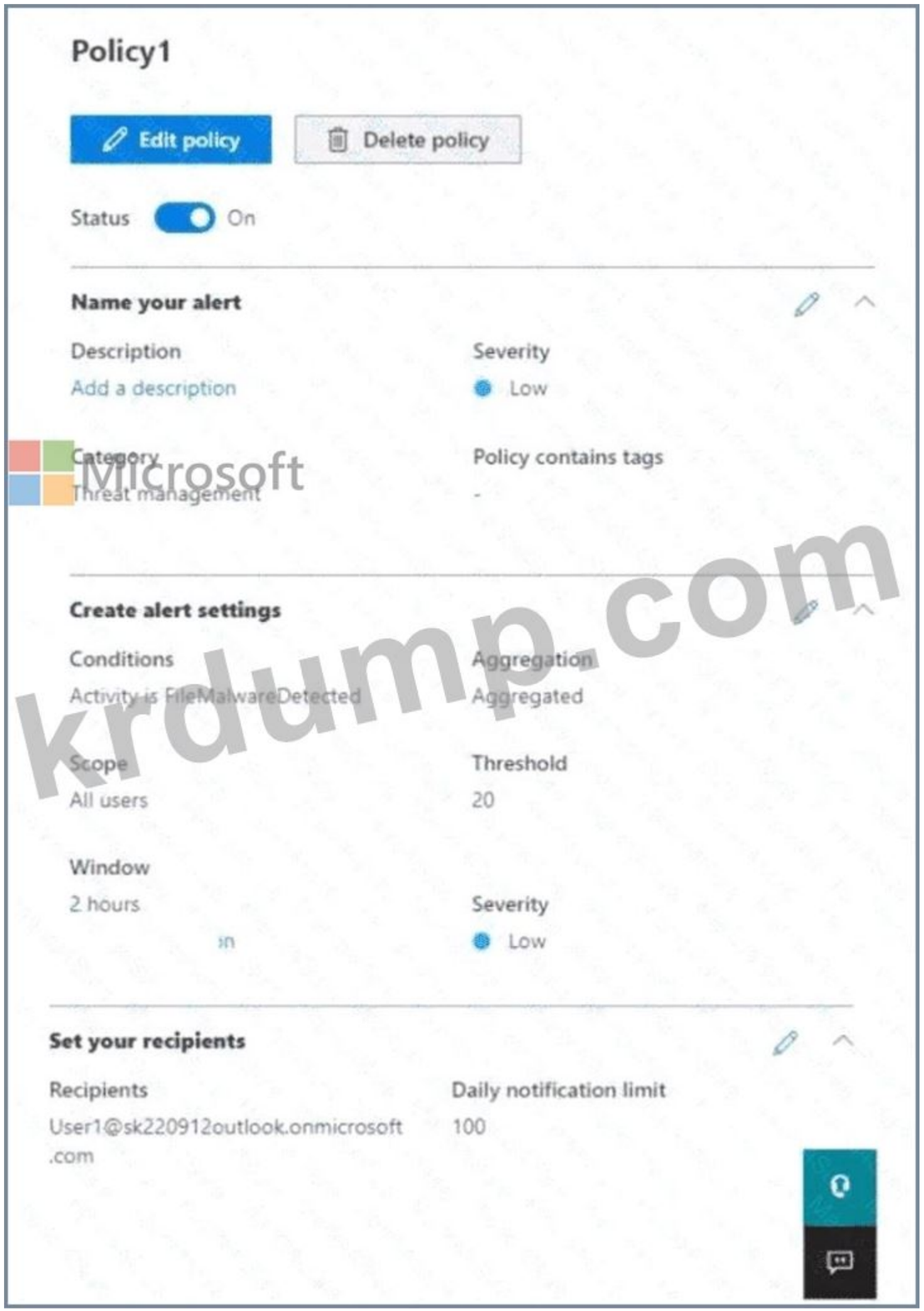
NEW QUESTION: 36

Microsoft 365 E5 □□□□ □□□□.

□□□□ □□ □□□ □□□□ □□□□□.

□□□□□□□ □
□□□□□□□ □□□□□
□□□□□□□ □□□□□ □□□
□□□□□□□ □□□□□ □□□
Microsoft 365 □□□□ 2□ □□ □□□□ □□□.
□□□ □ □□ □□ □□□ □□□□ □□□?
A. 1
B. 2
C. 3
D. 4
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide

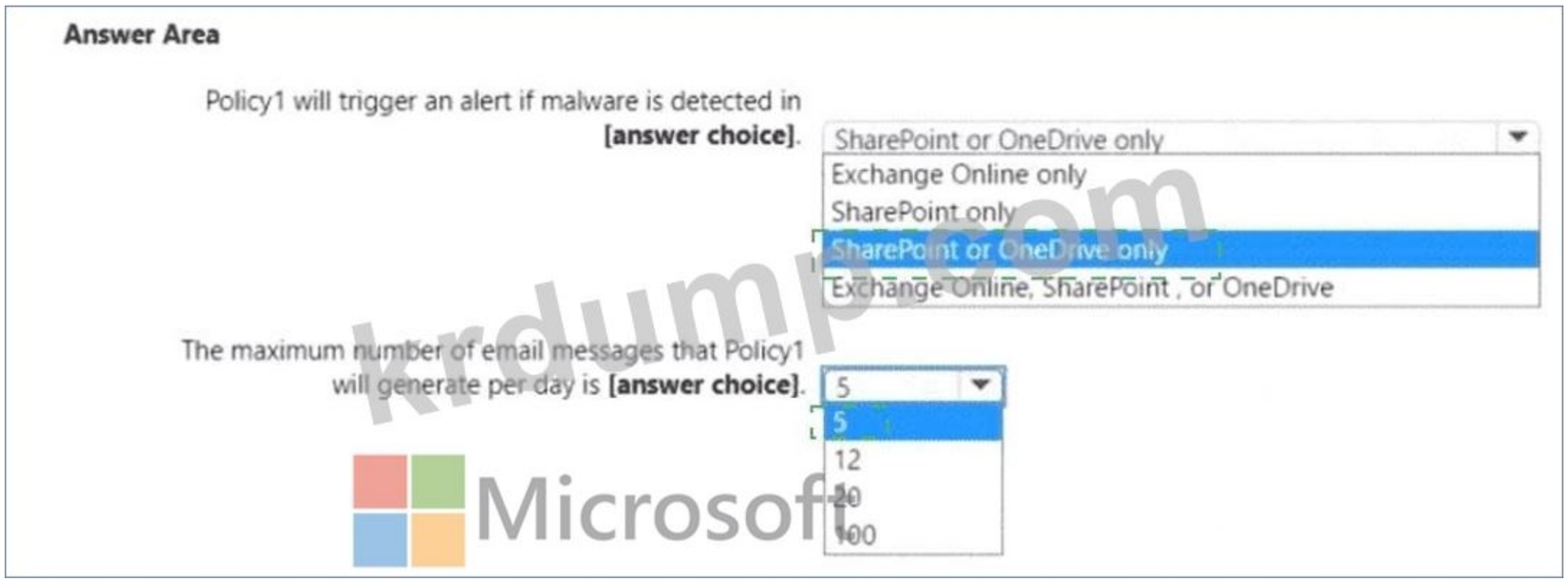
NEW QUESTION: 37
Microsoft 365 □□□ □□□□.
□□ □□□ □□ □□ □□□ □□□□.



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

Answer Area

Answer:



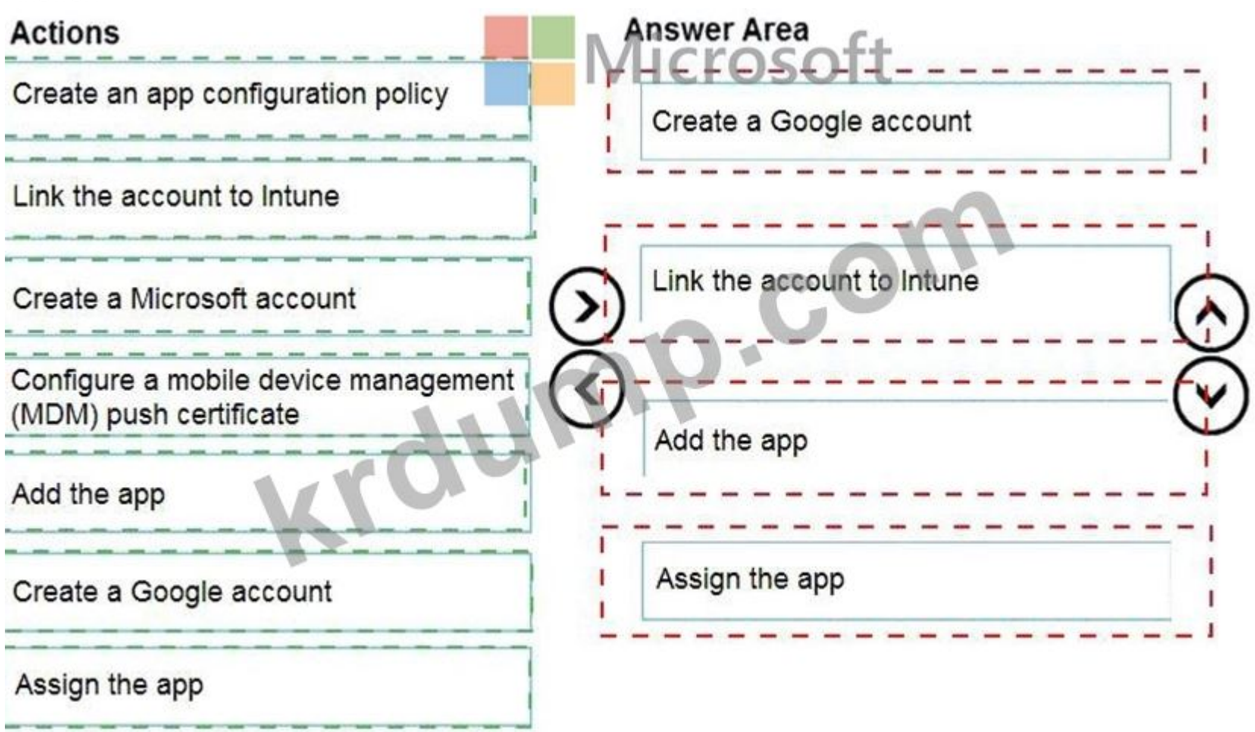
Explanation:

NEW QUESTION: 38
Microsoft 365 E5 □□□ □□□□. □□□□□ FID02 □□ □□ □□□□□.
FID02 □□ □□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□□ □□□. □□□ □□ □□ □□□ □□ □□□ □□□□ □□□?
A. □□ □□ □□
B. □□□ □□□□□ □□ □□□□□.
C. □□□ □□□ □□ □□ □□□ □□□□□.
D. □□ □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
Microsoft Intune□ □□□ Android □□ 500□□ □□ Microsoft 365 E5 □□□□ □□□□.
□□□□ Google Play □□ □□□ □□□□□ Microsoft Endpoint Manager□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□□.


Actions
Answer Area
Create an app configuration policy
Link the account to Intune
Create a Microsoft account
Configure a mobile device management (MDM) push certificate
Add the app
Create a Google account
Assign the app

Answer:


Actions
Answer Area
Create an app configuration policy
Link the account to Intune
Create a Microsoft account
Configure a mobile device management (MDM) push certificate
Add the app
Create a Google account
Assign the app
Create a Google account
Link the account to Intune
Add the app
Assign the app

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work#assign-a-managed-google-play-app-to-android-enterprise-fully-managed-devices

NEW QUESTION: 40
□□□ □□□□□□ contoso.com□□□ □□□ □□□□□ Active Directory □□□□ □□□□.
□□ □□□ □□□ □□ □□□ □□ □□□ □□ □□ □ □□□□ □□□□□ □□□□ □□□□.
contoso.com□ Microsoft Entra □□□□ □□□□ □□□□□.
□□□□ □□□□ Microsoft Entra ID□ □□□□ □ □□□ □□ □□□ □□□□□ □□ □□□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□□?
A. □□ □□
B. □□□ □□ □□
C. □□□□ □□□
D. Microsoft Entra ID □□ □□
Answer: A (LEAVE A REPLY)
Reference:
https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

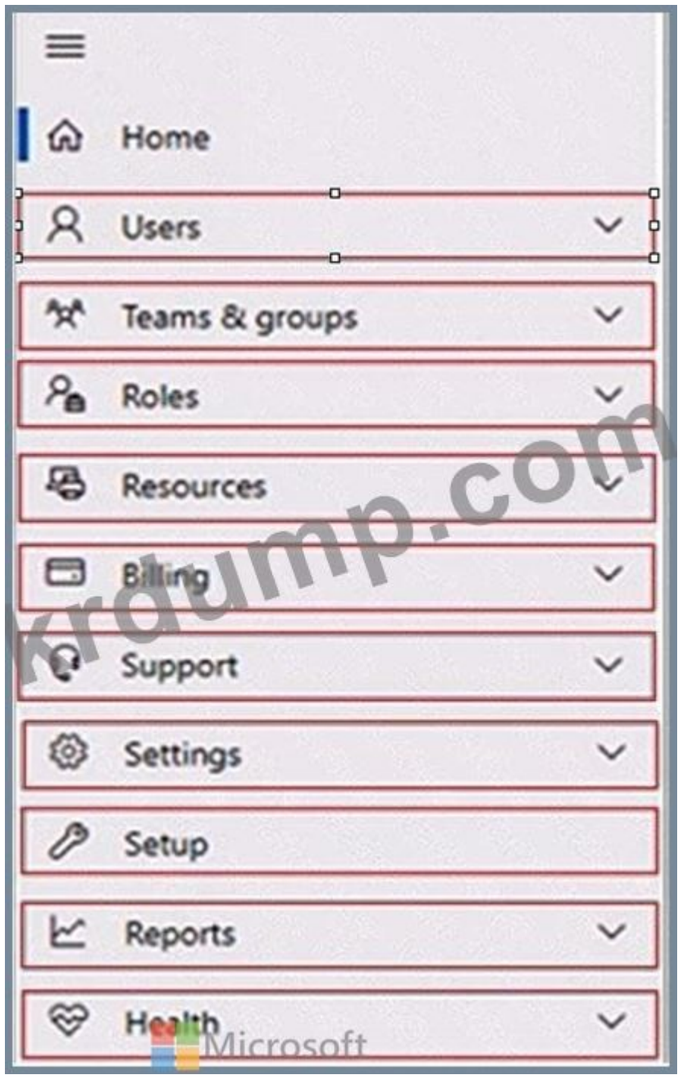
NEW QUESTION: 41
Microsoft 365 □□□ □□□□.
□□□ □□ Microsoft Office 365 □□□□□□□□ □□□□ □□□□□□□ □□□ □□□□□.
□□□ □□□□□ □□□□□□□□ □□□□ □□□□ □□□.
□□□ □□□ □ □□ □ □□ □□□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. Microsoft 365 □□ □□□□ □□□ □□ □□□□□ □□□□□.
B. Microsoft 365 □□ □□□□ □□□ □□ □□□□□ □□□□□.
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: 42
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

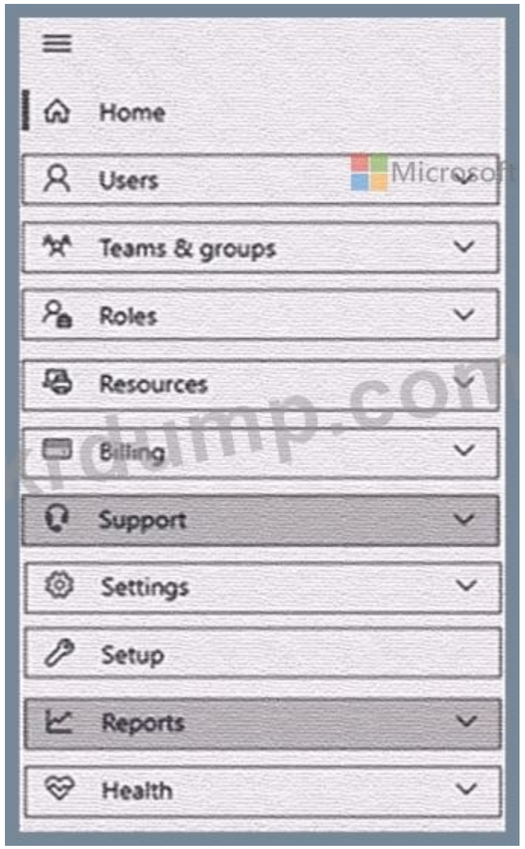
NEW QUESTION: 43
Windows 11 □□□□□ □□□ Microsoft 365 E5 □□□ □□□□. □□ □□□□□ Microsoft Defender for Endpoint□ □□□□□ □□□□.
□□ □□ □□□□□ □□ □□ □□□ □□□□ □□□. □□□ □□□□ □□□?
A. □□ □□ □□
B. □□□□□
C. □□□
D. □□ □□ □
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
□□□
□□□ □□□□ 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: 45

□□□ 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

Microsoft Entra ID(Microsoft Entra ID)□ □□□ □□□□□ □□□. Azure AU □□□ □□□□□ □ □□□□ □□□ □□ □□□? □□□□□ □□□ □□□ □□ □□ □□□□ □□□□□□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □ □□□□.
□□: □□ □□□ 1□□□□.

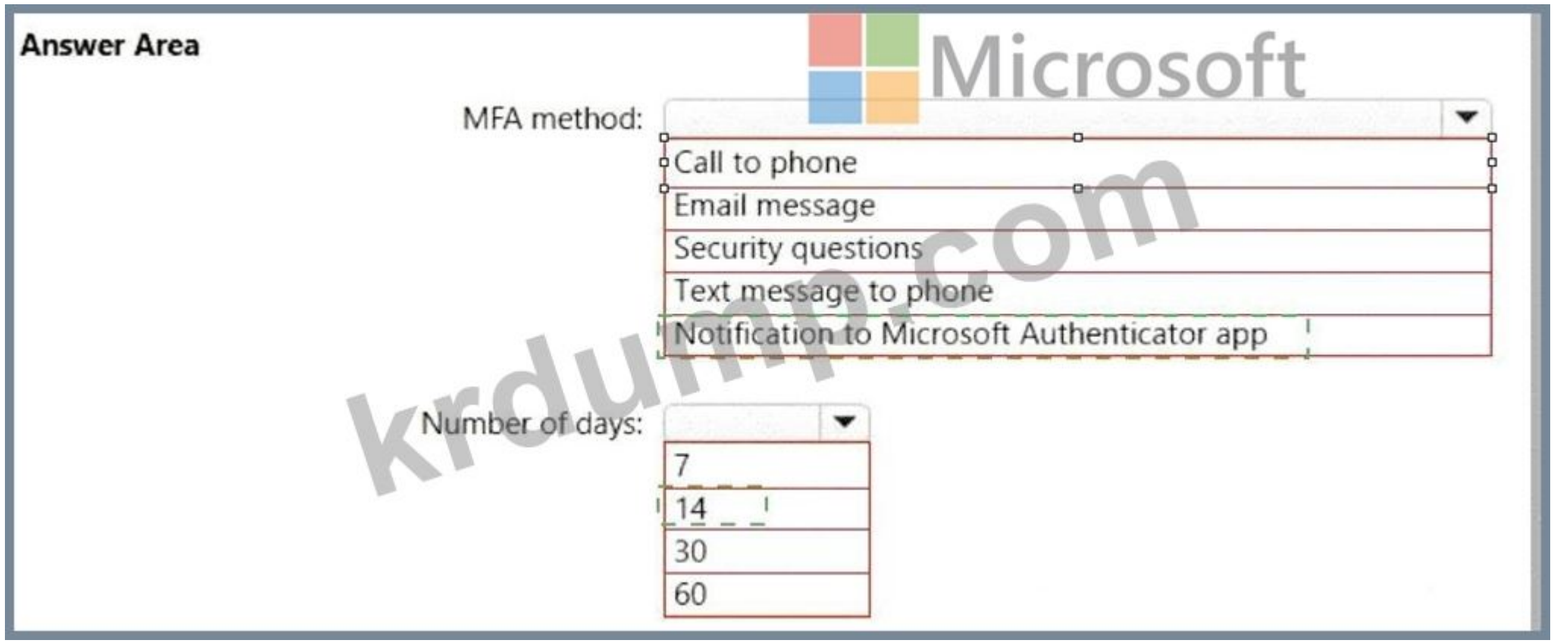
Answer:

Explanation:

NEW QUESTION: 46
□□□
□□□ Microsoft 365 E5 □□□□ □□□□.
□□ □□□ □□□ □□ □□□□□□□.
□□□□ □□□□ □□□□ □□□□□□.
□□□□ □□ □□ □□ □□(MFA) □□□ □□□ □ □□□, □□□□ MFA□ □□□□ □□ □□□ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□□□: □□ □□□ 1□□□□.

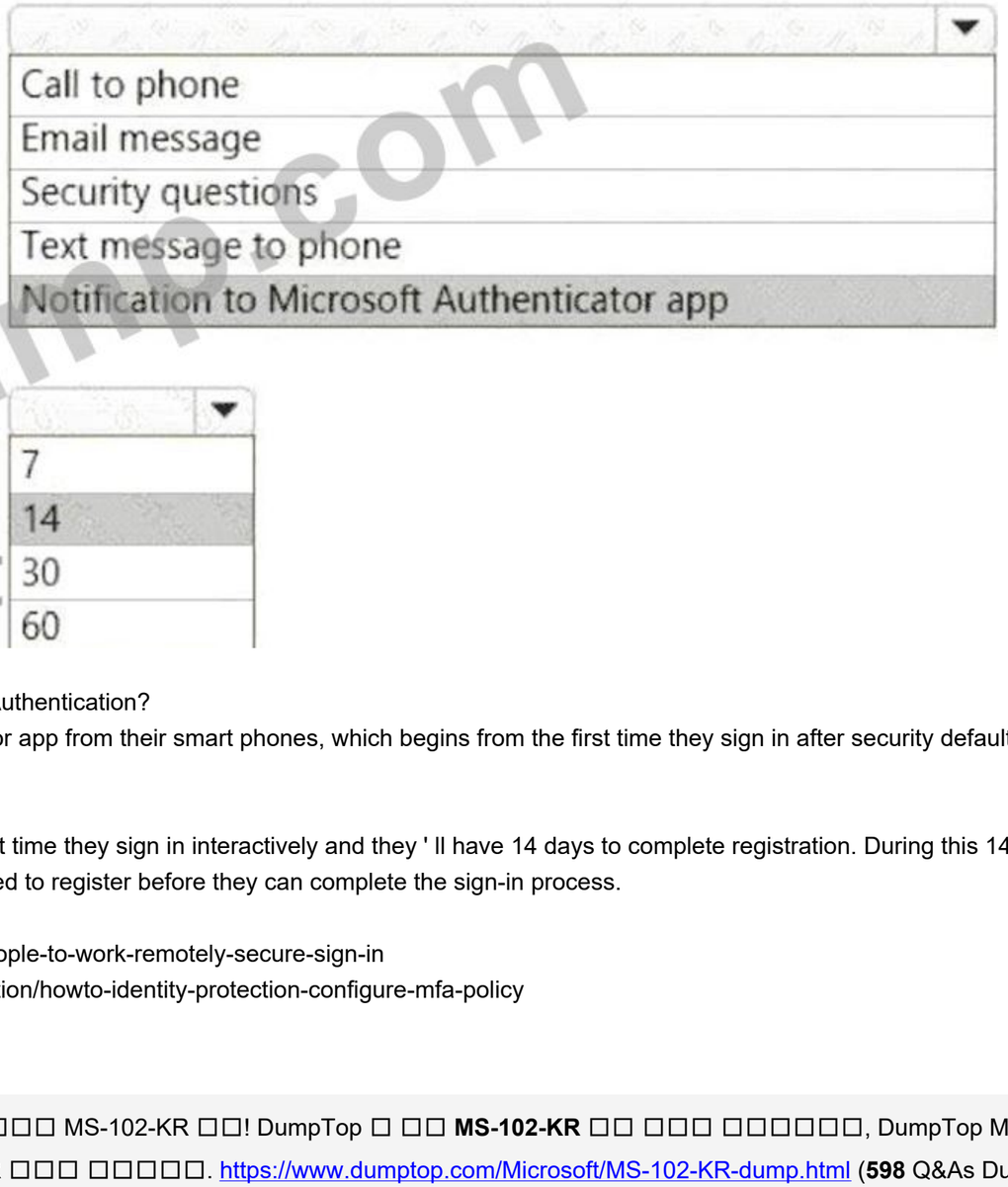
Answer Area

Answer:



Explanation:

Answer Area



Box 1: Notification to Microsoft Authenticator app

Do users have 14 days to register for Microsoft Entra ID 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

Microsoft Entra ID 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

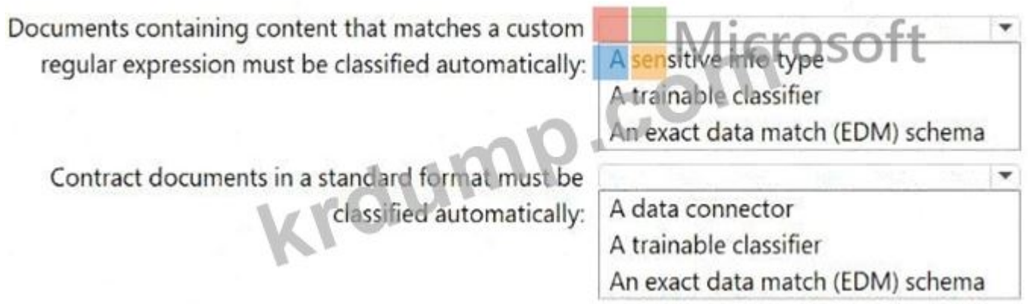
NEW QUESTION: 47

□□□ Microsoft 365 □□□ □□□□ □□□□.

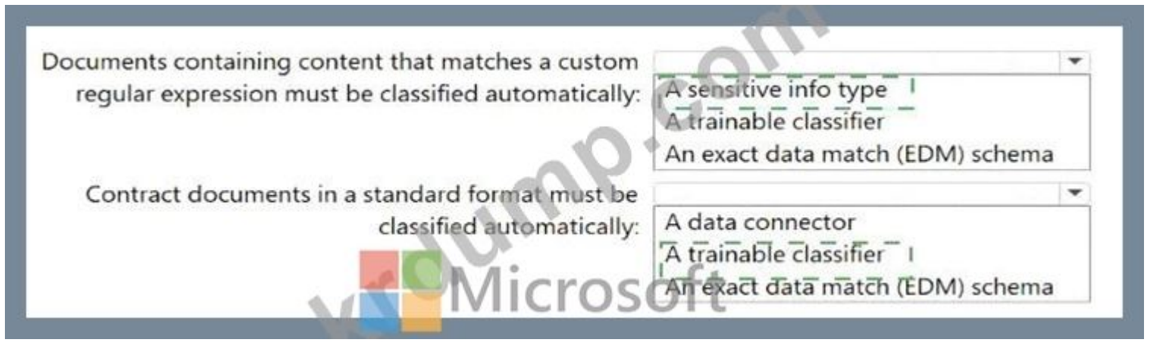
□□ □□□□ □□□□ □□ □□□ □□□□ □□ □□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

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

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



Answer:



Explanation:
Requirement
Correct selection
Documents containing content that matches a custom regular expression must be classified automatically.
A sensitive info type
Contract documents in a standard format must be classified automatically.
A trainable classifier
The first requirement must use a sensitive info type because Microsoft Purview sensitive information types are pattern-based classifiers. Microsoft states that sensitive information types detect sensitive content by using patterns, and custom sensitive information types can be created when the organization needs its own detection logic. A custom regular expression is exactly this kind of detection pattern, so it belongs in a custom sensitive information type rather than a trainable classifier or EDM schema.
The second requirement must use a trainable classifier. Contract documents in a standard business format are document-category classification problems, not exact-value matching problems. Microsoft Purview trainable classifiers are designed to recognize types of content by evaluating example content and can be used as conditions for auto-labeling Office files with sensitivity labels. Microsoft also provides built-in trainable classifiers for agreement and legal agreement content, including legal agreements, statements of work, leases, employment agreements, contracts, and nondisclosure agreements.
An exact data match schema is wrong here because EDM is used to match structured sensitive records from a data source, not to identify contract document format. A data connector is for ingesting external data into Microsoft Purview, not classifying Office documents.

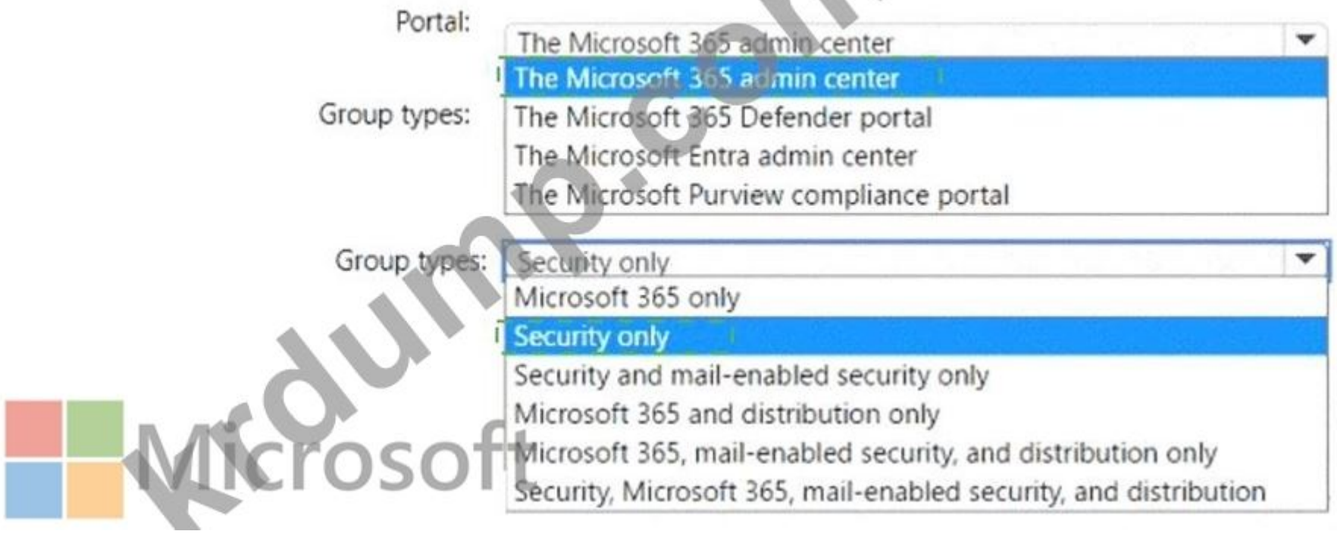
NEW QUESTION: 48
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□ □□□.
□□ □□□ □□□□ □□, □□ □□□ □□□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area



Explanation:

NEW QUESTION: 49

□□□□□□ □□□□□ Active Directory Domain Services(AD DS) □□□□ □□□□. □ □□□□□ UserI□□□ □□□□ □□□□.

Microsoft Entra □□□□ User2□□ □□□□ □□□□.

Microsoft Entra Cloud Sync□ □□□□ AD DS □□□□ Microsoft Entra □□□□ □□□□ □□□□□.

User1□ □□□□ Microsoft Entra Cloud Sync□ □□□ □ □□, User2□ □□□□ Microsoft Entra Cloud Sync□ □□□ □ □□□ □□ □□□. □ □□□□ □□ □□ □□□ □□□ □□□.

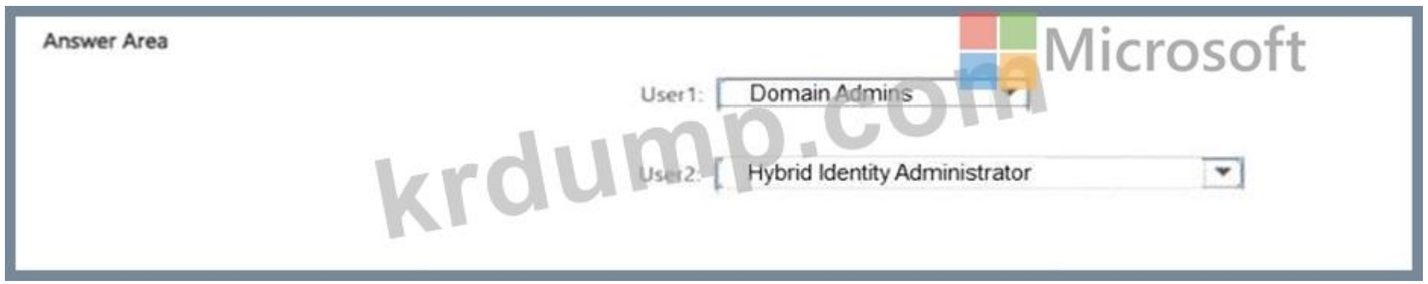
User1□ □□ □□□ □□□□ □□, User2□□□ □□ □□□ □□□□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.

Answer Area

Answer:

Answer Area

Explanation:



NEW QUESTION: 50
Microsoft 365 □□□□ □□□□.
□□ □□□ □□ □□ Windows 10 □□□ □□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□□ □□□□□.
□□□ □□ □□□ □□□□ □□□□□.
Microsoft Defender Antivirus □□□ □□ □□□ □□□□□□.
□□ □□□ □□□□ □□ □□□ □□□□ □□□□ □□□□□ □□ □□□□ □□□.
□□ □ □□ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. □□ □□
B. □□ □□
C. □□ □□ □□□
D. □□□ □□□ □□
E. □□ □□□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION: 51
Microsoft 365 □□□ □□□□.
□□ □□ □□□ □□□ Retention1□□□ □□□ □□ □□□ □□□□.

□□ Microsoft OneDrive □□□□ □□ □□□ □□□□□.
2020□ 1□ 1□□ □□□□ OneDrive□ File1□□□ □□□ □□□□□.
2020□ 1□ 10□□ □□□□ File1□ □□□□□.
2020□ 2□ 1□□ □□□□ File1□ □□□□□.
File1□ OneDrive□□ □□□□□ □□□□ □□□ □ □□ □□ □□□ □□□□□?
A. 2020□ 7□ 10□
B. 2020□ 7□ 1□
C. 2020□ 2□ 1□
D. 2020□ 8□ 1□
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□□ Microsoft 365□ □□ □□ □□□ □□□□ □□□.
* User 1□□□ □□□□ □□□ 30□□ □□ □□□ □□□□ □□□ □□□□ □□□□□.
* □□ □□□ □□□□ □□ □□□ □□□ □□□□□.
Microsoft Defender for Office 365□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

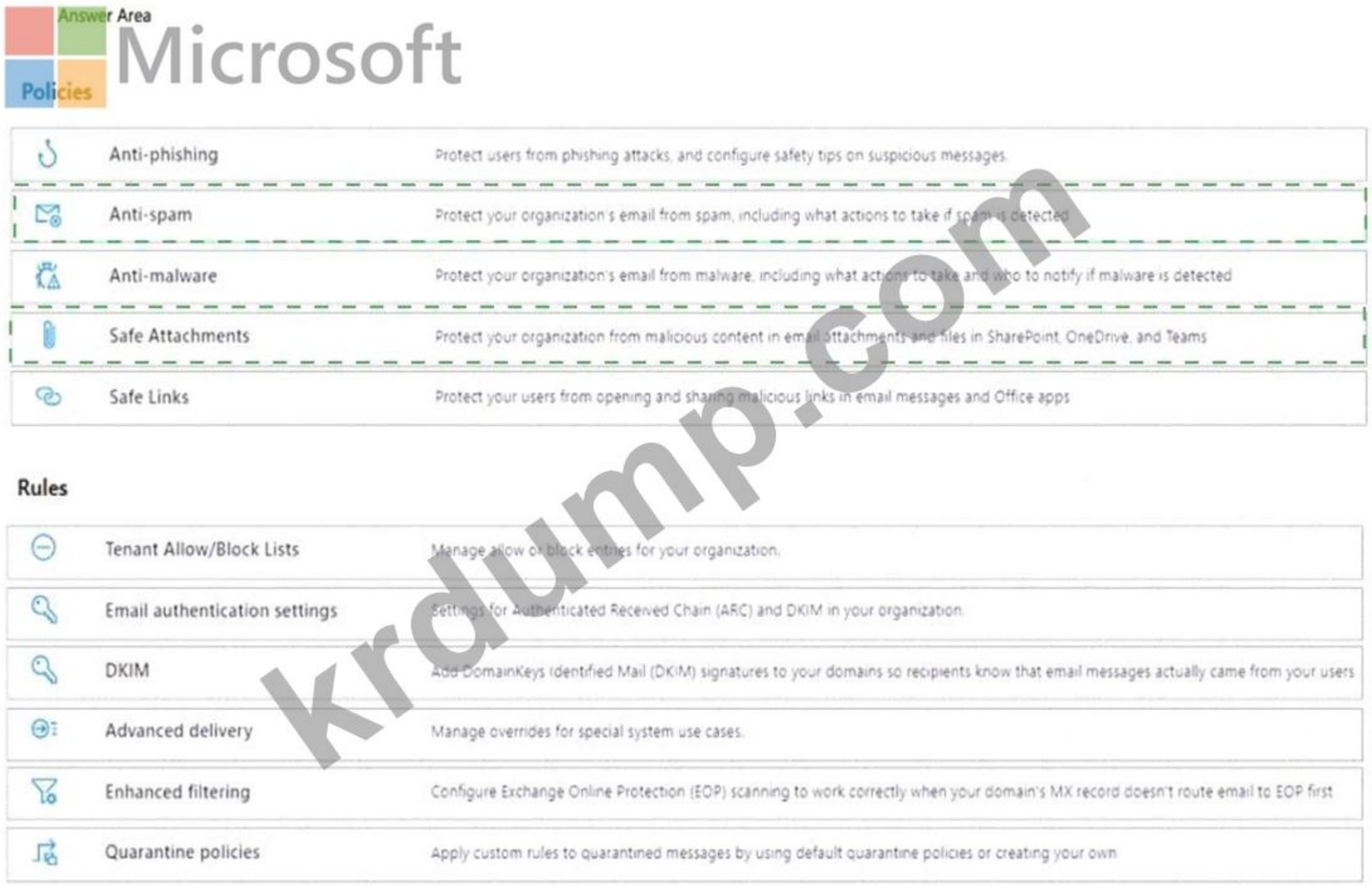
Policies

Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Rules

Tenant Allow/Block Lists	Manage allow or block entries for your organization.
Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization
DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users
Advanced delivery	Manage overrides for special system use cases.
Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own

Answer:

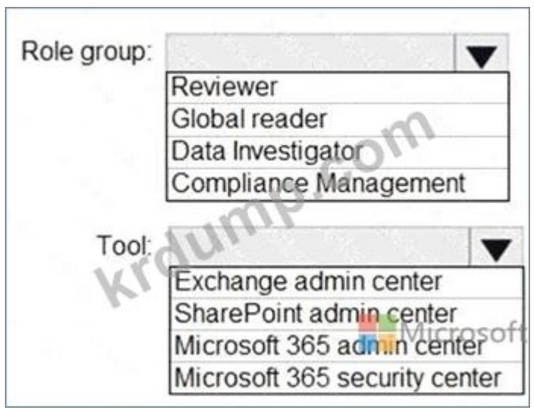


Explanation:
Limit a user named User 1 from sending more than 30 email messages per day: Anti-spam policy The anti-spam policy in Microsoft Defender for Office 365 allows you to configure outbound spam settings, including limiting the number of email messages a user can send per day. This helps prevent spam and potential email abuse within the organization.
Prevent the delivery of a specific file based on the file hash: Safe Attachments policy The Safe Attachments policy in Microsoft Defender for Office 365 can be configured to block or quarantine emails with attachments that match specific file hashes. This ensures that potentially malicious files are not delivered to users ' inboxes.

NEW QUESTION: 53
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□ 7□ □□ □□ IP □□□ □□ Microsoft Office 365□ □□□□ □□□□ □□□□ □□□.
□□□ □□ □□□?

A. Microsoft 365 □□ □□□□ □□ □ □□ □□ □□□□ □□□.
B. Microsoft Entra ID □□ □□□□ □□□ □□□ □□□□ □□□□□.
C. Microsoft 365 □□ □□□□ □□ □□□□ □□□□□.
D. □□□□ □ □□ □□ □□□□ □□□ □ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
User2□ □□ □□□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
User2□ □□ □□ □□□ □□□□ □□, □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

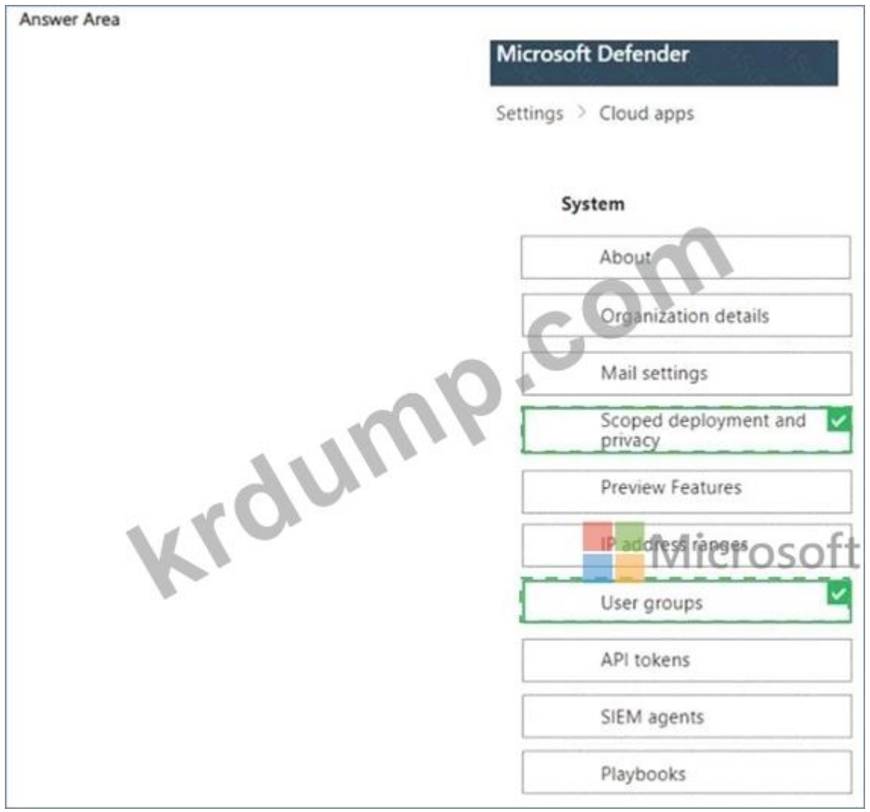
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

NEW QUESTION: 55
□□ □□ □□□ □□□□ User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
User1□ □□□ 1,000□□ □□□ □□□□ □□ □, □□□□ □□ □□□□ □□□ □□ □□□□□□ □□□□□. □□□ □□□□ □□□.
* User1□ □□□ □□□ □ □□ □□□□ □□□□□?
* User1□ □□□□ □□ □□□ □□ 2,000□□ □□□□ □□ □ □□□ □□□□ □□ □ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area



Explanation:

Answer Area

NEW QUESTION: 56

□□□ User1, User2, User3□□□ □□□ □□□ 3□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

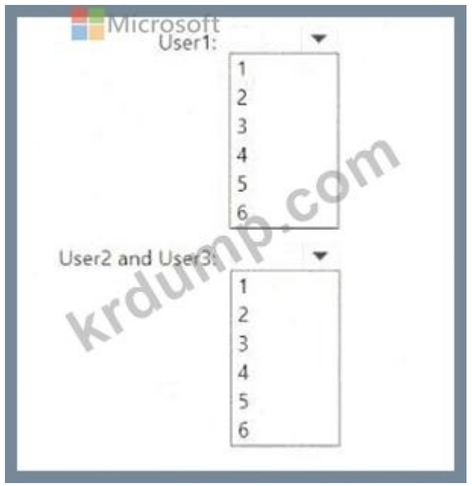
Microsoft Entra ID Protection□ □□□□ □□□□.

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

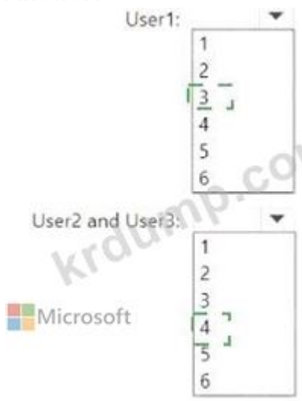
□□□□□□ □□ □□ □□□ □□ □□□ □□□□□.

Time	User	Risk level
8:00:00 AM	User2	Medium
8:00:00 AM	User3	High
8:00:10 AM	User1	Low
8:02:00 AM	User1	Medium
8:02:04 AM	User1	High
8:03:01 AM	User2	Medium
8:03:01 AM	User3	High
8:05:00 AM	User1	High
8:10:00 AM	User3	High
9:00:00 AM	User2	High

□□□ □□ □□, User1□ □□ □□□ □□□ □ □ □□□, User2□ User3□ □□ □□□ □□□ □□ □ □ □□□□?



Answer:



Explanation:

User1: 3

User2 and User3: 4

Microsoft Entra ID Protection generates a Users at risk detected email when a user's calculated risk level reaches the configured threshold. In this case, the threshold is Low or above, so Low, Medium, and High risk events all qualify. Microsoft states that the email is generated when the user's risk level reaches the configured risk level, and additional emails can be generated when later detections recalculate the user risk level at the configured level or higher. Microsoft also states that only one email is sent within a five-second period, and if multiple users move to the configured risk level during that same five-second period, the data is aggregated into one email.

For User1, alerts occur at 8:00:10, 8:02:00, and 8:05:00. The 8:02:04 High event is within five seconds of the

8:02:00 Medium event, so it does not create a separate alert. Therefore, User1 receives 3 alerts.

For User2 and User3, the 8:00:00 events are aggregated into one alert, the 8:03:01 events are aggregated into one alert, then User3 at 8:10:00 generates another, and User2 at 9:00:00 generates another. Total: 4 alerts.

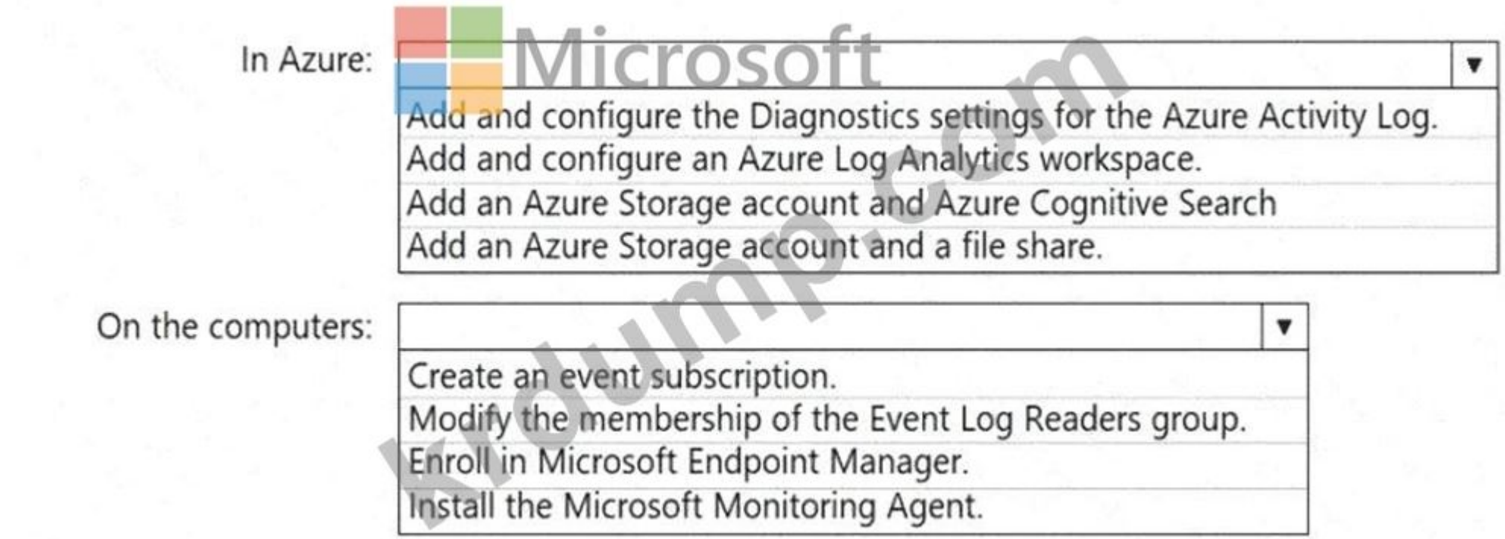
References/topics: Microsoft Entra ID Protection, Users at risk detected alerts, user risk threshold, alert aggregation window.

NEW QUESTION: 57

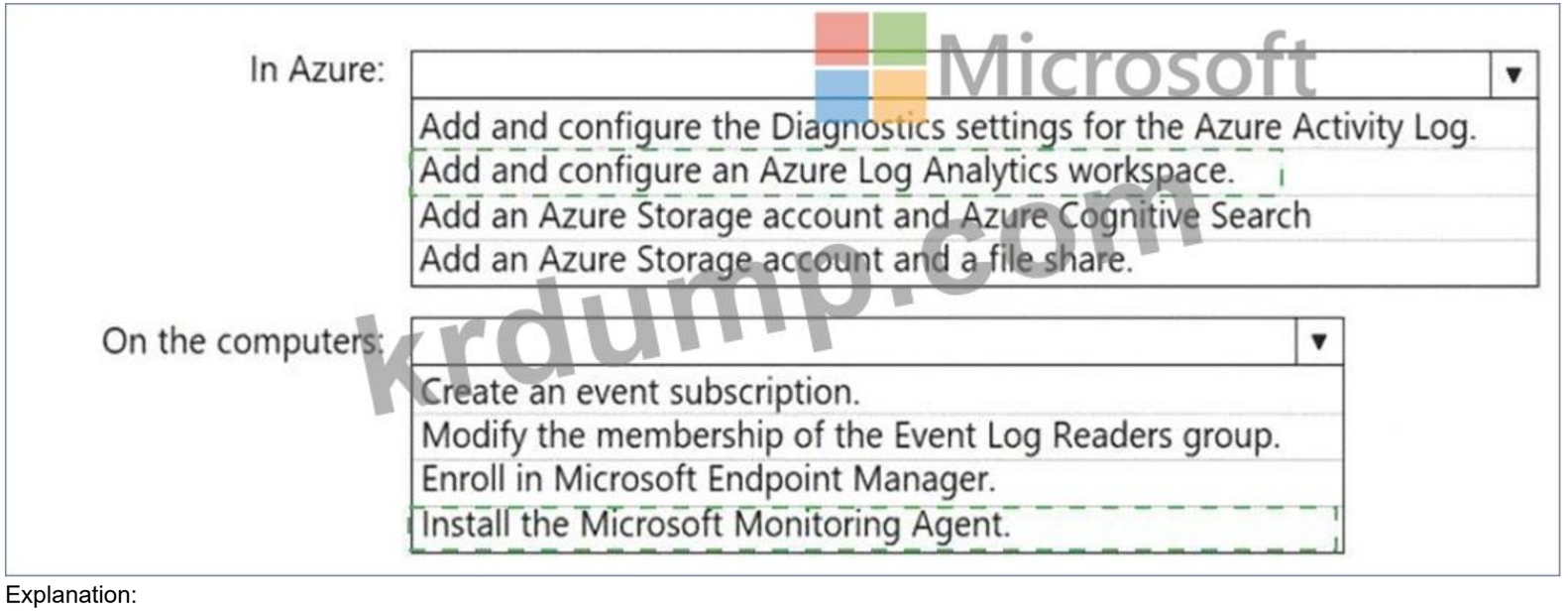
Azure □□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows 10□ □□□□ 50□□ □□□□ □□□□.

□□□□ □□□ □□ □□□□ □□□□ □□□□□□ □□□.

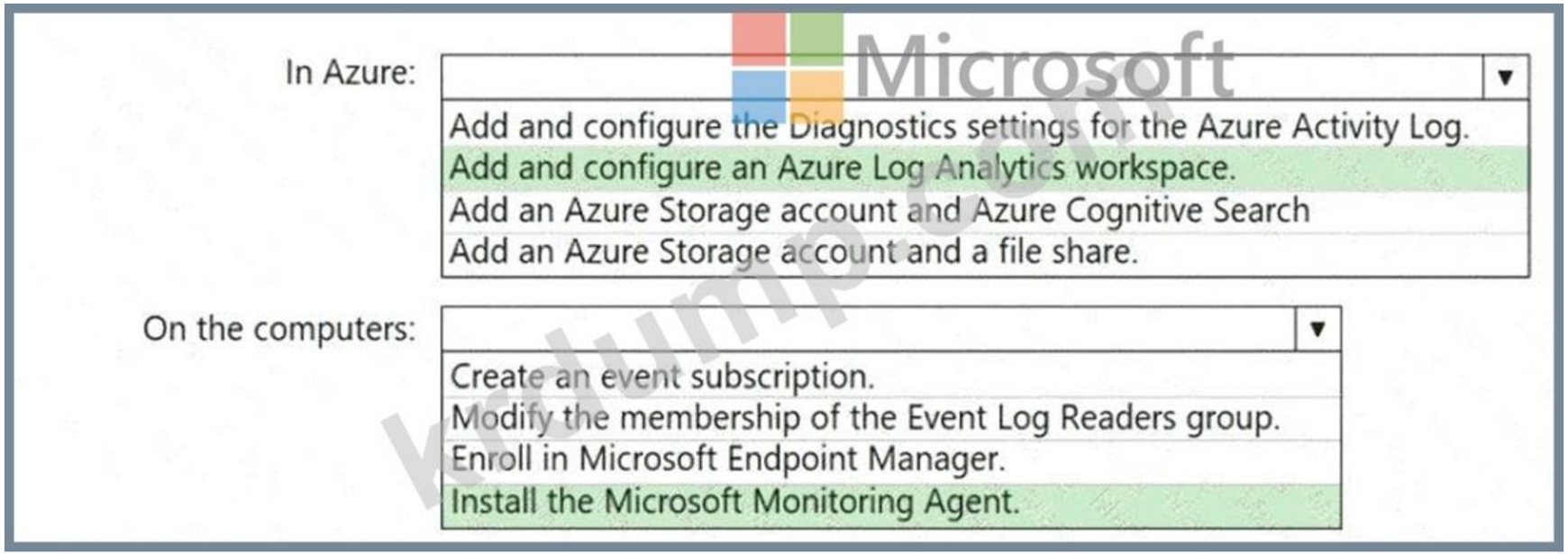
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

NEW QUESTION: 58
□□□ Microsoft 365 □□□ □□□□ □□□□.
□□ □□□ □□ Microsoft □□ □□□ 60□□□, □□ □□□ □□□ 75□□□□.
□□□ □ □□ □□□□ □□□□ □□□□□ □□□ □□(MFA)□ □□□□ □□□ □□□ □□□ □□□□ □□□.
□ □□□ □□□ □□ □□□ □□□□?
A. □□ □□□ □□□□ □□ □□ □□□ □□□□□.
B. □□ □□□ □□ □□ □□□ □□□□□.
C. □□ □□□ □□ □□ □□□ □□□□ □□□□.
D. □□ □□□ □□□□ □□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The correct exam selection is D. The Secure Score will increase, and the achievable score will decrease.
Microsoft Secure Score measures security posture, and Microsoft states that a higher score indicates that more recommended security actions have been taken. Microsoft also states that points are awarded for configuring recommended security features, and Conditional Access/MFA-related controls are part of the Microsoft 365 security posture model.
When you implement a Conditional Access policy requiring MFA from untrusted devices, you are applying a control that strengthens identity protection. That increases the current Secure Score because the tenant has completed or partially completed a recommended security action. The "achievable score" represents the remaining score opportunity available from your current licenses and risk posture. After you complete an improvement action, the remaining achievable gap is reduced, so the achievable score decreases in the exam's scoring logic. Microsoft's Secure Score documentation confirms that completed actions grant points and that Secure Score views include current score, current license score, planned score, and achievable score.

NEW QUESTION: 59
Microsoft J65 E5 □□□ □□□□.
Microsoft Defender for Endpoint□ Microsoft Intune□ □□□□□.

Intune□ □□□ □ □□□ Defender for Endpoint□ □□□□ □□□□□□ □□ □□□.
□□ □□: □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 60
Microsoft Entra ID(Microsoft Entra ID)□□ □□ □□ □□ □□□ '□□□'□ □□□ 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

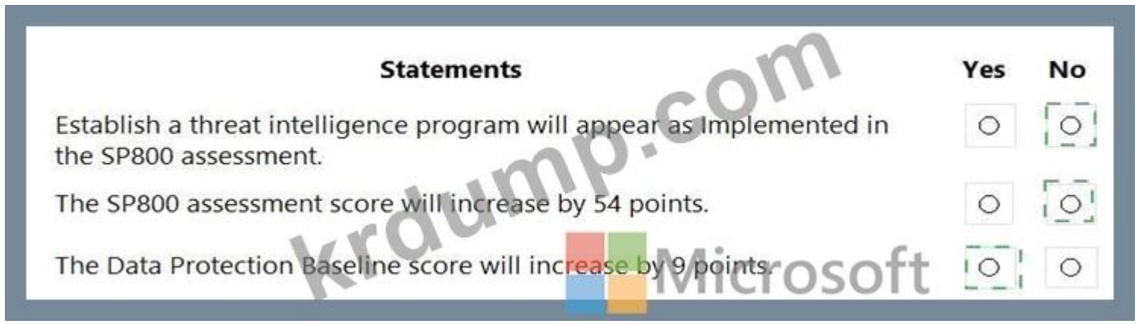
SP800 □□□ □□ □□ □□□ □□ □□ □□ □□□□.

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

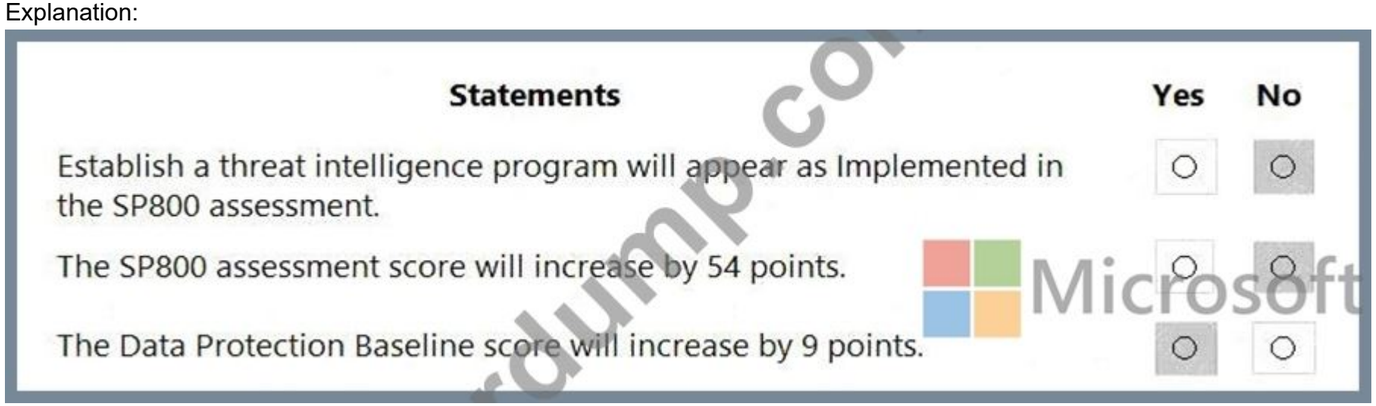
□□□ □□ □□□ □□□□□.
□□□ □□ □□□ □□□□ '□□ □□□□□ □□□□ □□' □□□ □□□ '□□□'□□ □□□□□□.
□□ □□□□□ □□□ □□(MFA)□ □□□□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

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:



Explanation:



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: 61
Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□□□ □□□ □□ □□□ □□□□□ □□□.
□□□ □□□□ □□□?
A. Intune □
B. Microsoft 365 □□□ □□□ □
C. Microsoft Authenticator □
D. Intune □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 62
□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□□ □□□□.

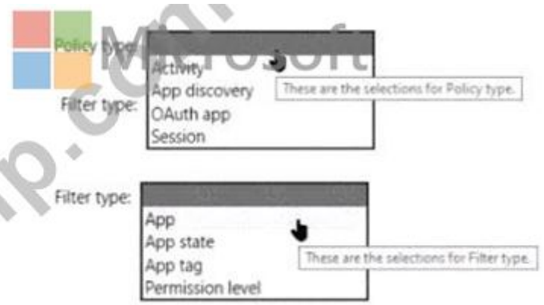
Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

□ □□□ Microsoft Intune□ □□□□ □□□□□.
□□ □□□ □□□ □□□□□ □□ □□□□ □□□□□ □□□.
□□ □□□ □ □□□ □□□□□?
A. Device1□
B. Device1, Device2, Device3, Device4
C. Device1, Device3, Device4
D. Device1□ Device4
Answer: A (LEAVE A REPLY)

NEW QUESTION: 63
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: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

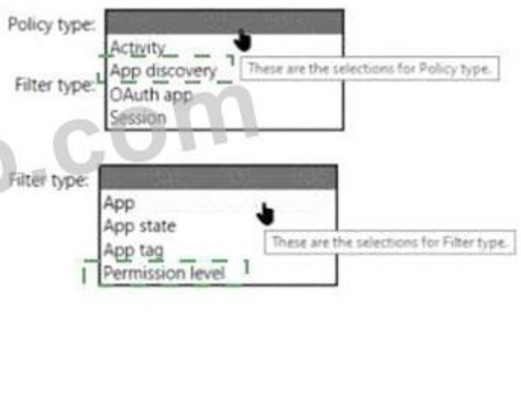
NEW QUESTION: 64
□□□□ □□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□ □□□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□ □□ □□□□ □□□ □□□ □□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



Explanation:

NEW QUESTION: 65

□□□ □□ □□□ □□□□□ □□ PII □□□□ □□□□ □□□.

□□□ □□□□ □□□?

A. □□□ □□□ □□□□ □□□ □□ □□(DLP) □□

B. □□□ □□□□ □□□ □□□□ □□□□ □□ □ □□ □□ □□ □□

C. □□□ □□□□ □□□□ □□□ □□ □□(DLP) □□

D. □□□ □□□□ □□ □ □□ □□ □□ □□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 66

Endpoint□ Microsoft Defender□ □□□□□.

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

Name	Rank	Membership
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	*Not applicable*

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

Answer:

Explanation:

NEW QUESTION: 67

□□□□□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□□ □□□□ □□□□.

□□□ Microsoft Entra □□□□ □□□□ □□□□.

Microsoft Entra Connect □□□□ □□□□□.

□□□□ □□□□ □□□□□.

□□□ □□□ □□ □□□ □□ □□ □□□□ □□□□□□.

"Microsoft Entra Connect Sync□ □□□□ □ □□□□ □□□ □□□□ □□□ □□□□□□□." □□□□ □□□□□ □□□□□ □□ □□□. □□ □□□ □□□□ □□□ □□□□□ □□□.

□□□ □□ □□□?

A. PowerShell□□ Repair-AADCloudSyncToolsAccount cmdlet□ □□□□□.

B. PowerShell□□ Set-ADSyncScheduler cmdlet□ □□□□□.

C. Active Directory □□□ □ □□□□□ ADSync □□□ □□□ □□□ □□□□□□.

D. Microsoft Entra □□ □□□□ Microsoft Entra Connect Sync □□□ □□□ □□□□□□□.

Answer: A (LEAVE A REPLY)

The correct answer is A. From PowerShell, run the Repair-AADCloudSyncToolsAccount cmdlet. This is the least administrative effort because the cmdlet is designed specifically to repair the synchronization service account used by Microsoft Entra synchronization services. Microsoft documents Repair- AADCloudSyncToolsAccount as a cmdlet that deletes the current sync account if present and then resets the sync account authentication by creating or using a new sync account in Microsoft Entra ID. That directly matches the error indicating an issue with the service account used for synchronization.

Microsoft's troubleshooting guidance also states that when you need to repair the cloud sync service account, you should run Connect-AADCloudSyncTools and then Repair-AADCloudSyncToolsAccount from an elevated PowerShell session, after which the account should be repaired successfully.

Set-ADSyncScheduler is wrong because it controls the synchronization schedule; it does not repair service account authentication. Resetting the ADSync service account password manually is risky because Microsoft warns that changing ADSync service account credentials after installation can cause the sync service to fail, lose database access, and stop synchronization until the original credentials are restored. Resetting the account from the Entra admin center is not the documented repair path.

NEW QUESTION: 68

□□□ contoso.com□□□ Microsoft Entra □□□□ □□□□ Microsoft 365 □□□ □□□□ □□□□. □□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

Label 1□□□ □□□ □□ □□□□ □□□□ □□□ □□ □□□ □□□□□.

* □□□□ 5□□ □□□□□.
* 5□ □□ □ □□ □□□□ □□□□ □□□□□.

Policy1□□□ □□□ □□□□ Label1□ □□ □□ □□□□□ □□□□□□. Policy1□□ □□□ □□ □□□ □□□□.

* '□□'□□□ □□□ □□□ □□□□ □□□□□.
* 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:

Answer Area

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

NEW QUESTION: 69

Microsoft Purview□□ eDiscovery Manager □□ □□□ Lynne Robbins□ □□□□ □□□.

Answer:

See the solution below:

Explanation:
Add Lynne Robbins to the eDiscovery Manager subgroup of the built-in eDiscovery Manager role group. Do not add her as an eDiscovery Administrator because that would provide organization-wide access to all eDiscovery cases.
Step-by-Step Solution with Explanation:
* Sign in to the Microsoft Purview portal with an account assigned the Role Management role or membership in Organization Management .
* Select Settings .
* Navigate to:
Roles and scopes # Role groups
Some tenant interfaces display this directly as Settings # Role groups .
* On Role groups for Microsoft Purview solutions , search for:
eDiscovery Manager
* Select the eDiscovery Manager role group.
* Select Edit .
* On the Manage eDiscovery Manager page, select Choose users .
* Search for and select Lynne Robbins .
* Select Select , and then select Next .
* When the eDiscovery Administrator membership page appears, do not add Lynne. Continue by selecting Next .
* If administrative-unit scoping is presented, retain organization-wide or Full directory access unless the task environment specifies an administrative unit.
* Select Next # Save # Done .
* Reopen the role group and verify that Lynne appears under eDiscovery Managers , not eDiscovery Administrators .
An eDiscovery Manager can create and manage cases, run searches, manage holds, and access cases they create or to which they are assigned. An eDiscovery Administrator can access all cases, which exceeds this requirement. Microsoft: Assign permissions in eDiscovery

NEW QUESTION: 70
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □ □, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Windows 10□ □□□□ □□□□ □□□□.
□□□ Windows 10 □□□ □□□□ □□□.
□□ □□: □□ □□□□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
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: 71
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Microsoft Defender XDR□□ □□□□ □□ □□ □□□ □□□ □ □□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?

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

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

NEW QUESTION: 73
2,000□ □□□ □□□ □□□□ □□ Microsoft 365 □□□ □□□□.
□□□□ Microsoft 365 □□□ □□□ □□□□ □□□□ □□ □□□□ 30□□□ □□ □□□□ □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□□ □□
B. □□ □□
C. □□ □□
D. □□ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 74
□□ □□ □□ □□ □□□□ □□□ 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

Statements	Yes	No
User1 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.	○	○
User3 will be required to register for MFA on the next sign-in.	○	○

Answer:
Answer Area

Statements	Yes	No
User1 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.	○	○
User3 will be required to register for MFA on the next sign-in.	○	○

Explanation:
User1 will be required to register for MFA on the next sign-in: Yes
User1 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: No
User2 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: No
User3 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: 75
□□ □□ □□□ □□□ 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 Area

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

Answer:

Explanation:

Answer Area

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

NEW QUESTION: 76

□□ □□ □□□ □□ □□□ □□□ 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 Area

Statements	Yes	No
User2 can reset the password of User1.	○	○
User2 can reset the password of User4.	○	○
User3 can assign licenses to User1.	○	○

Answer:

Answer Area

Statements	Yes	No
User2 can reset the password of User1.	○	○
User2 can reset the password of User4.	○	○
User3 can assign licenses to User1.	○	○

Explanation:

Answer Area

Statements	Yes	No
User2 can reset the password of User1.	●	○
User2 can reset the password of User4.	○	●
User3 can assign licenses to User1.	●	○

NEW QUESTION: 77

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

User1□ Device1□□ □□□ □□□ □□□□□□ □□□□□.

□□□ □□□ □□□□ □□□□□ □□□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.

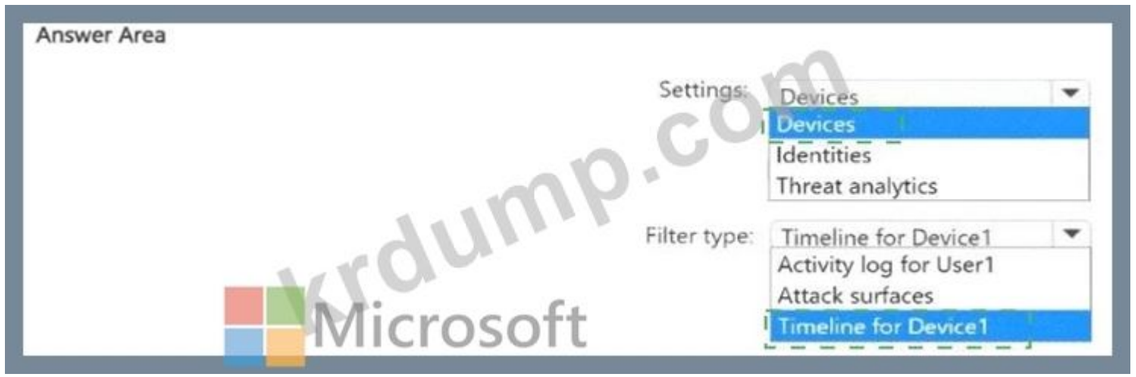
Answer Area

Microsoft

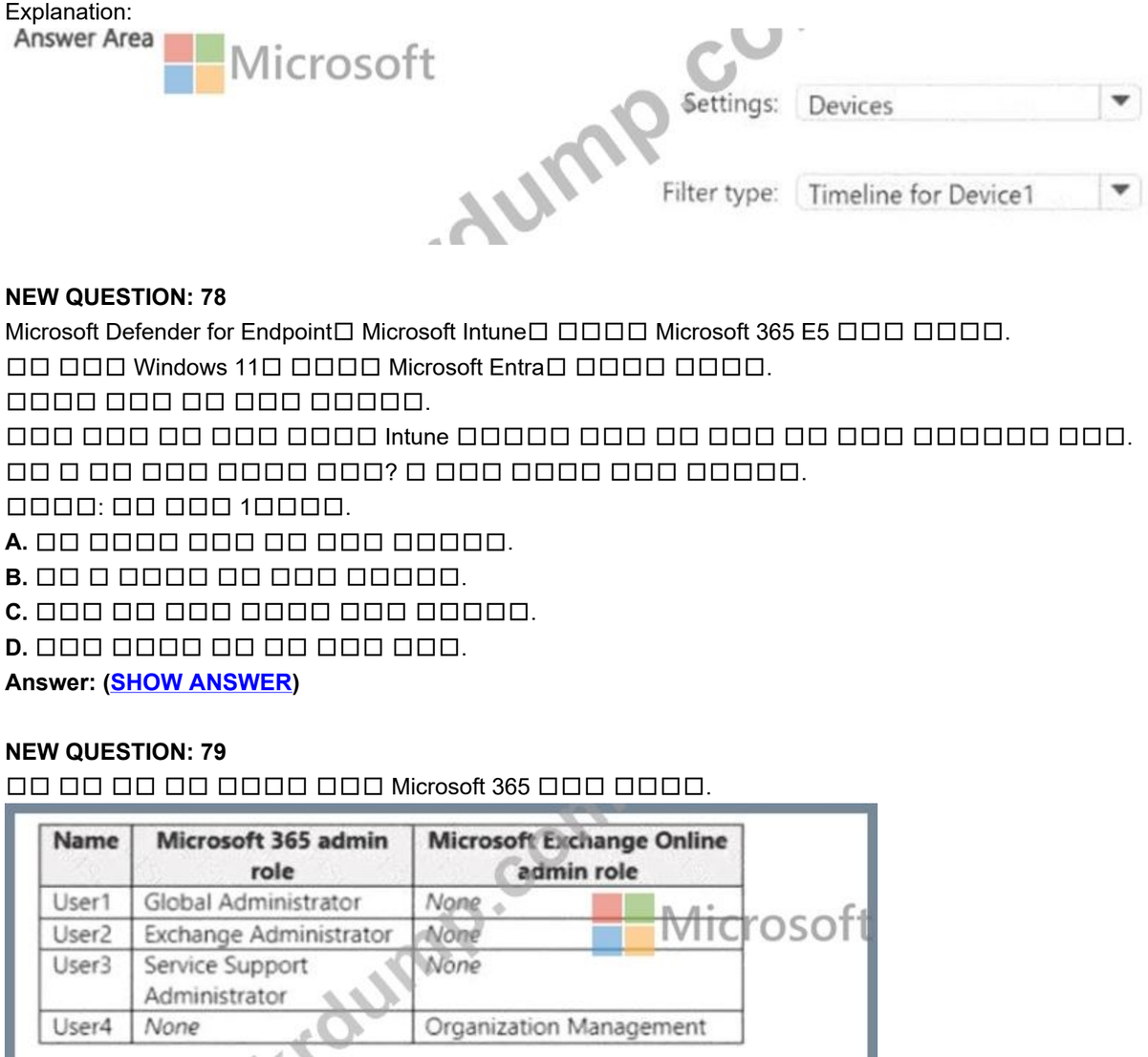
Settings: Devices
- Devices
- Identities
- Threat analytics

Filter type: Timeline for Device1
- Activity log for User1
- Attack surfaces
- Timeline for Device1

Answer:



Explanation:



NEW QUESTION: 78

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

□□ □□□ Windows 11□ □□□□ Microsoft Entra□ □□□□ □□□□.

□□□□ □□□ □□ □□□ □□□□□.

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

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

□□□□: □□ □□□ 1□□□□.

A. □□ □□□□ □□□ □□ □□□ □□□□□.

B. □□ □ □□□□ □□ □□□ □□□□□.

C. □□□ □□ □□□ □□□□ □□□ □□□□□.

D. □□□ □□□□ □□ □□ □□□ □□□.

Answer: (SHOW ANSWER)

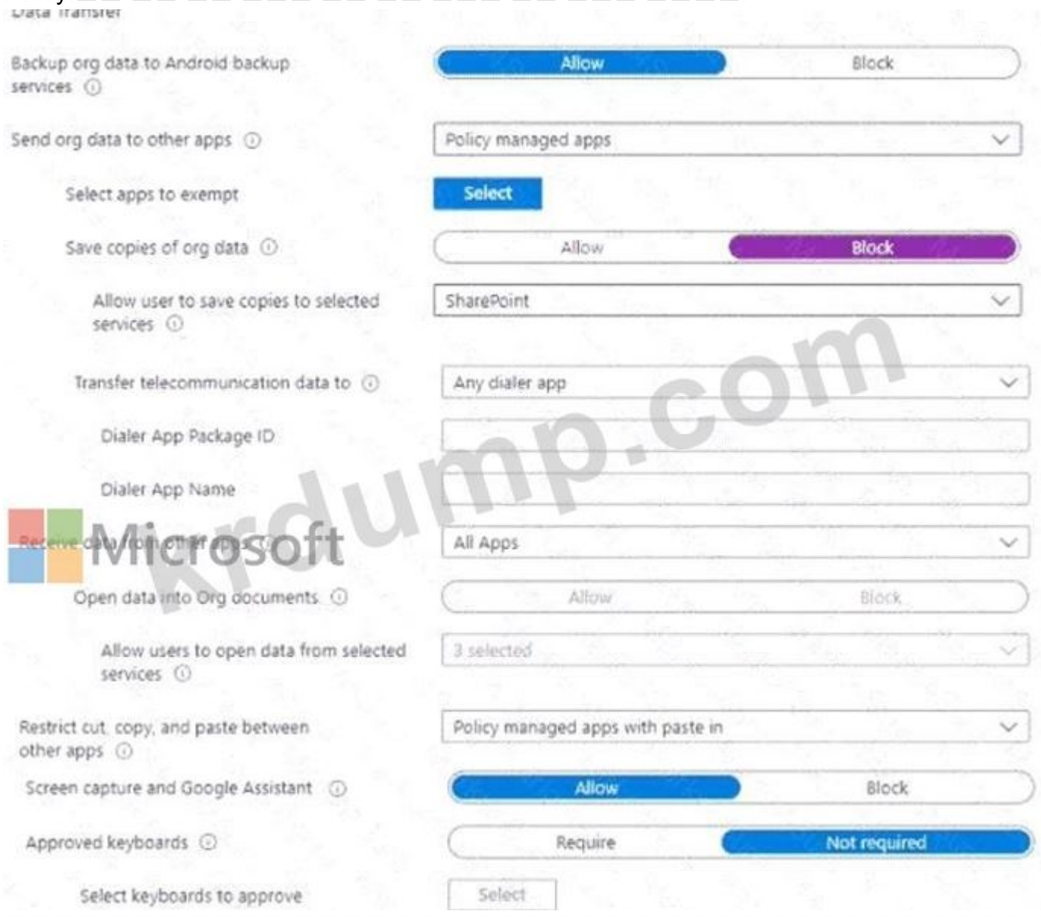
NEW QUESTION: 79

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

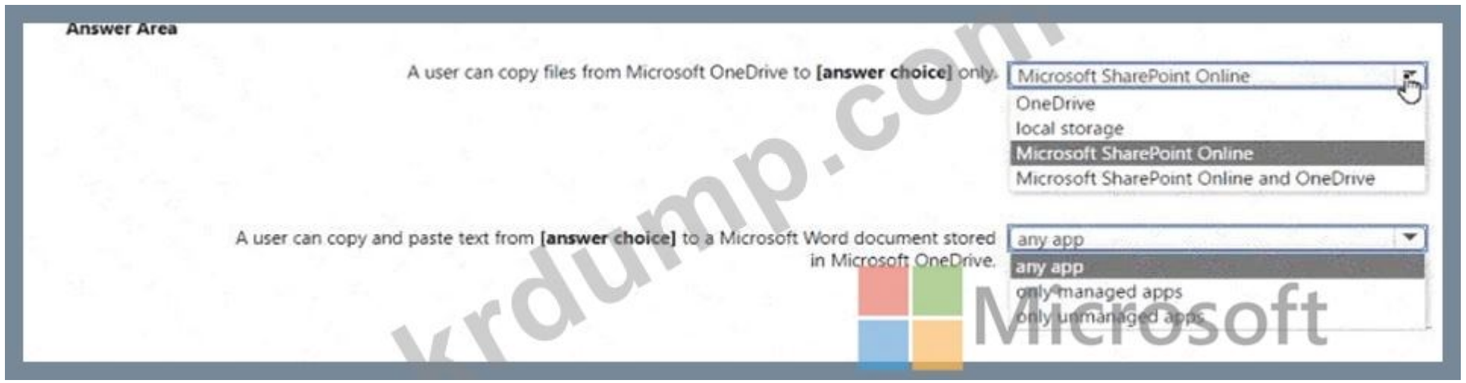
Name	Microsoft 365 admin role	Microsoft Exchange Online admin role
User1	Global Administrator	*None*
User2	Exchange Administrator	*None*
User3	Service Support Administrator	*None*
User4	*None*	Organization Management

DNS □□□□ □□□□ □□□□ □□ Exchange Online□ □□□□□ □□□.
□□□□ □□□ DNS □□□□ □□□□□.
DNS □□□□ □□□ '□□□ □□□□ □□□□□'□□□.
DNS □□□ □□□ □□□ □ □□ □□□□ □□□□ □□□. □□□□ □□ □□□ □□□ □□□□ □□□.
□□ □□□□ □□□□ □□□?
A. □□□3
B. □□□2
C. □□□1
D. □□□4
Answer: C (LEAVE A REPLY)

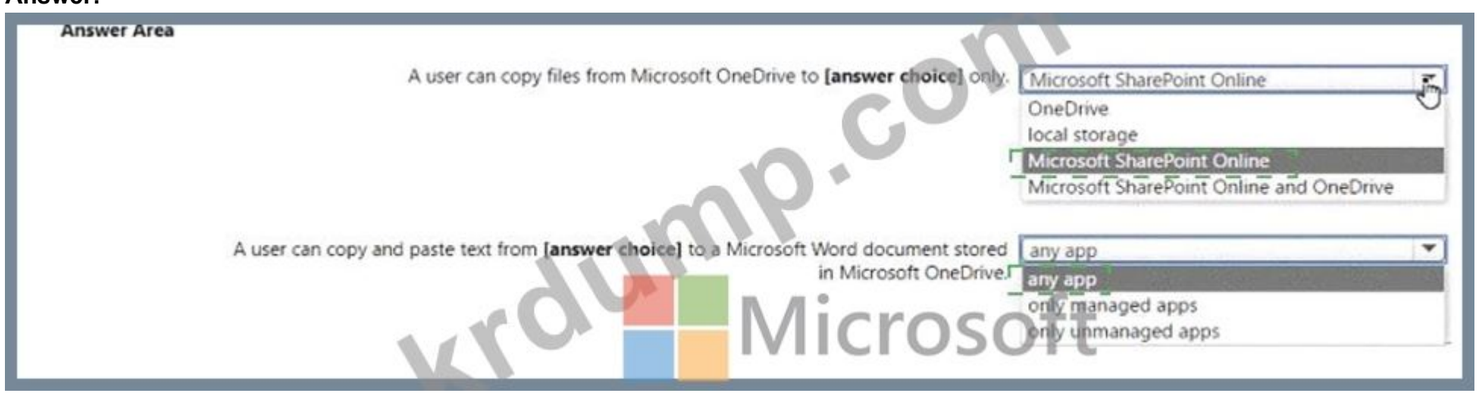
NEW QUESTION: 80
Microsoft Intune□ □□□ Android □□ 200□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□ Microsoft □□ □□□□ □□ □□ □□□□□ □□□□ Policy!□□ □□□ Android □ □□ □□□ □□□□.
Policy!□□ □□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□.



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



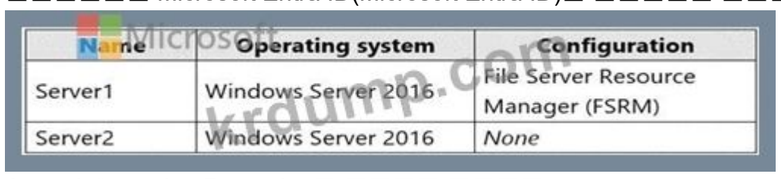
Answer:



Explanation:

NEW QUESTION: 81

□□□□□□ Microsoft Entra ID(Microsoft Entra ID)□ □□□□□ □□□□□ 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 □□□□ □□□ □ □□□ □□□□ □□□.

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

Actions

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

Answer Area

Answer:

Actions

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

Answer Area

1. Install the Microsoft Rights Management connector on Server2.
2. Authorize Server1.
3. Run `GenConnectorConfig.ps1` on Server1.

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: 82
□□□ Microsoft 365 E5 □□□ contoso.com□□□ □□□ Microsoft Entra □□□□ □□□□ □□□□.
□□ □□□□ Windows 11□ □□□ □□□□ □□□□ □□□, contoso.com□ □□□□ □□, BitLocker □□□□ □□□(BitLocker)□ □□□□ □□□□ □□□□.
□□□ □□□ □□ □□□ □□□ Admin1□□□ □□□ □□□□ □□□ □□□□□.
* BitLocker □□ □□ □□□□□.
* contoso.com□□ □□□□ □□ □□□ □□□□□□.
□□ □□□ □□□□□ Admin1□ □□□ □□□□ □□□. □ □□□□ □□ □□ □□□ □□□ □□□. □□ □ □□ □□□ □□□□ □□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Devices

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

Global

- [ ] Global Administrator

Identity

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

- [ ] Hybrid Identity Administrator
- [ ] License Administrator
- [ ] Password Administrator

Answer:

Answer Area

Devices

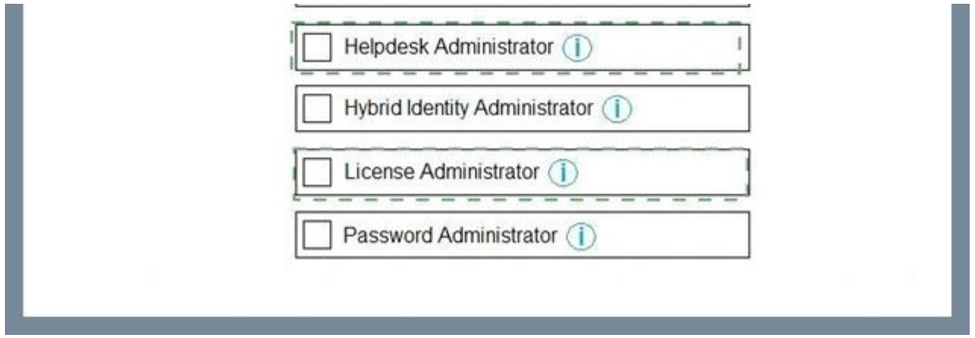
- [ ] Cloud Device Administrator
- [ ] Desktop Analytics Administrator
- [ ] Intune Administrator
- [ ] Printer Administrator
- [ ] Printer Technician
- [ ] Windows 365 Administrator

Global

- [ ] Global Administrator

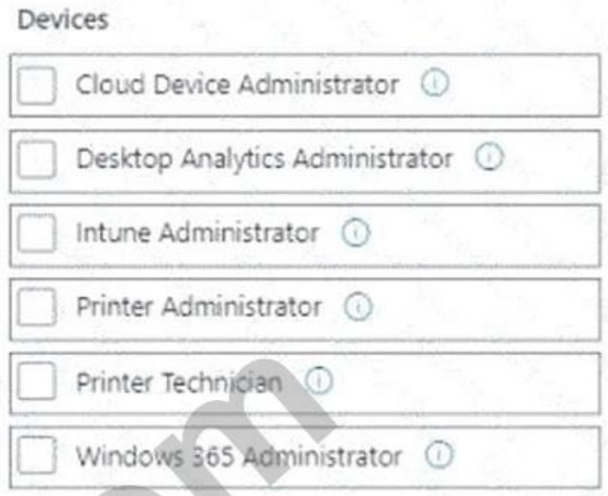
Identity

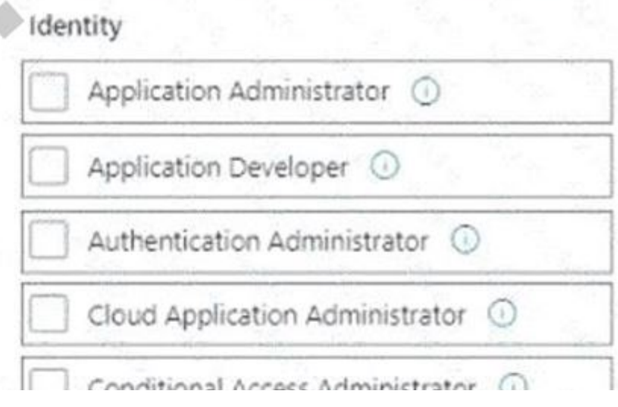
- [ ] Application Administrator
- [ ] Application Developer
- [ ] Authentication Administrator
- [ ] Cloud Application Administrator
- [ ] Conditional Access Administrator
- [ ] Domain Name Administrator
- [ ] External Identity Provider Administrator
- [ ] Guest Inviter

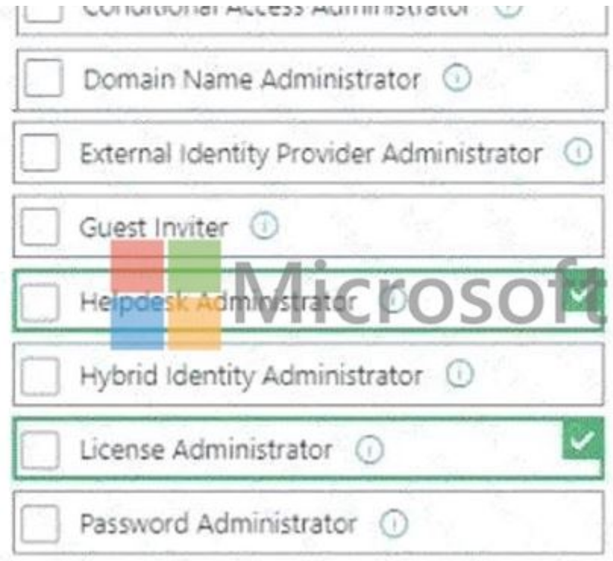


Explanation:

Answer Area







NEW QUESTION: 83
Microsoft 365 E5 □□□ □□□□.
□□ □□□□ Mac □□□□ □□□ □□□□. ATI □□□□ Microsoft Endpoint Manager□ □□□□ Microsoft Defender for Endpoint□ □□□□□□.
□□□□□ Endpoint□ Microsoft Defender□ □□□□ □□□.
Endpoint Management □□ □□□□ □□□ □□□□ □□□?
A. Microsoft Defender for Endpoint □□ □□□
B. □□ □□ □□□
C. iOS □□□□ □□
D. □□□ □□ □□(MDM) □□ □□ □□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
500□□ Windows 10 □□□□□ Microsoft Endpoint Manager □□□□ □□ □□□ □□□ Microsoft 365 □□□□ □□□□.
□□□ □□□□ □□□ □□□ □□□ Microsoft Office 365 □□ □□□□ □ □□□ □□ □□□.
□□ □□ □□□ □□□□ □□□?
A. □□□ □□
B. □□ □□
C. □□ □□ □□(ASR)
D. □□□□□ □□ □ □□
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

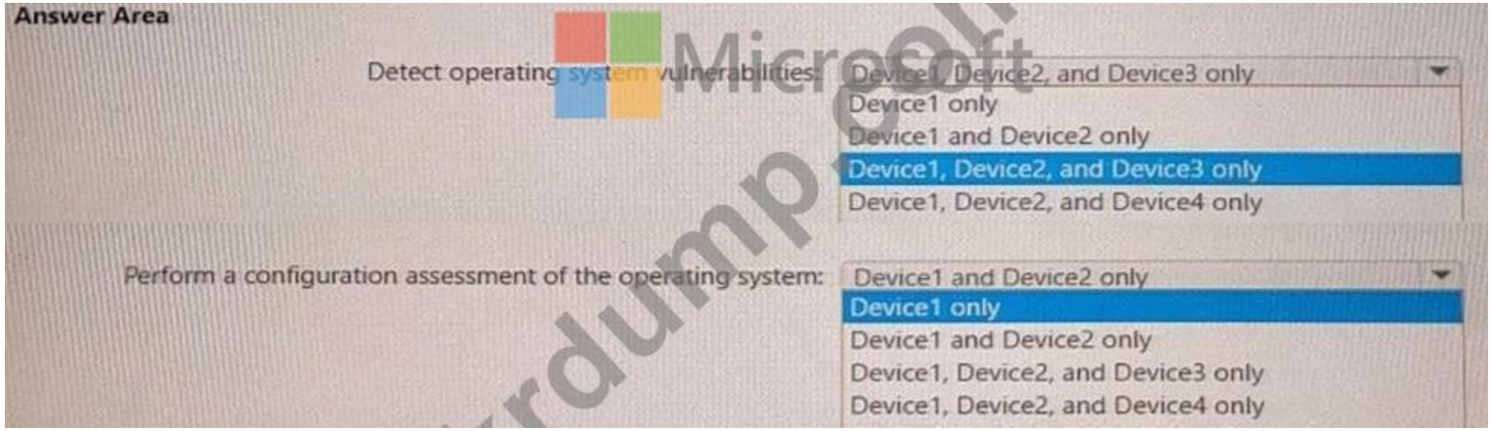
NEW QUESTION: 85

Microsoft 365 □□□ □□□□.
Microsoft Exchange Online □□□ □□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□. □□□ □□ □□□?
A. Microsoft 365 □□ □□□□ □□ □□□ □□□ □□□□□□□.
B. Microsoft Outlook □□□□□□□ □□ □□□ □□□ □□□□□.
C. Exchange □□ □□□□ □□□□ □□□□.
D. Microsoft 365 □□ □□□□ □□□ □□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

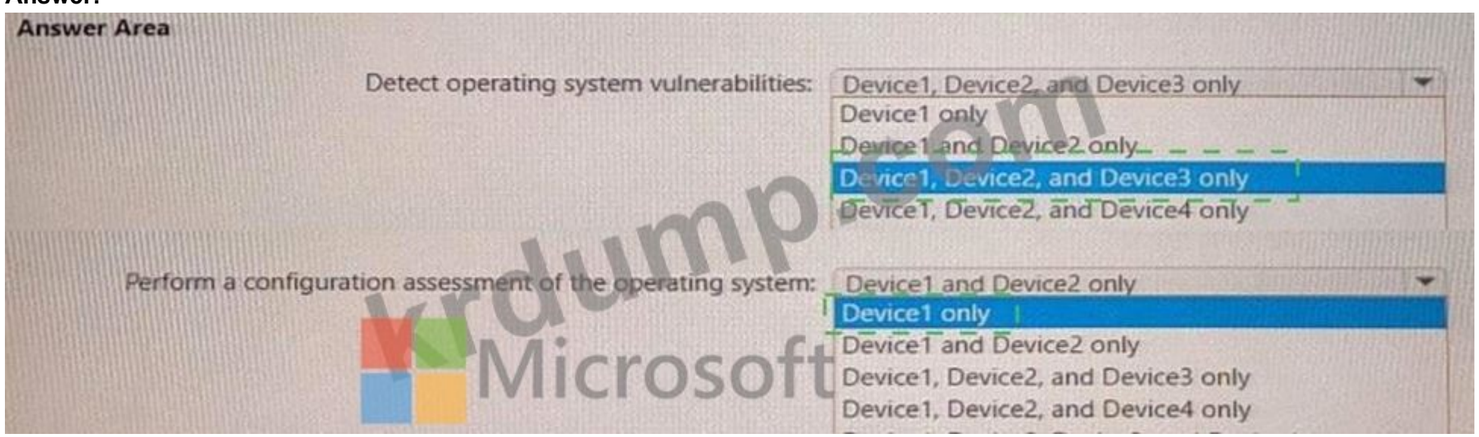
NEW QUESTION: 86
□□ □□ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

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



Answer:



Explanation:

NEW QUESTION: 87

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□□□□.

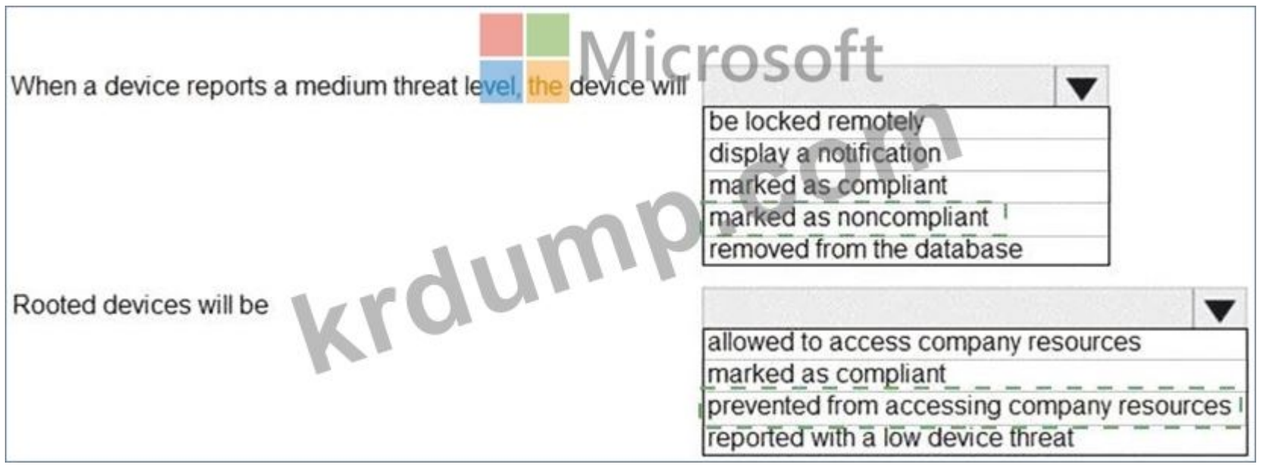
When a device reports a medium threat level, the device will

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

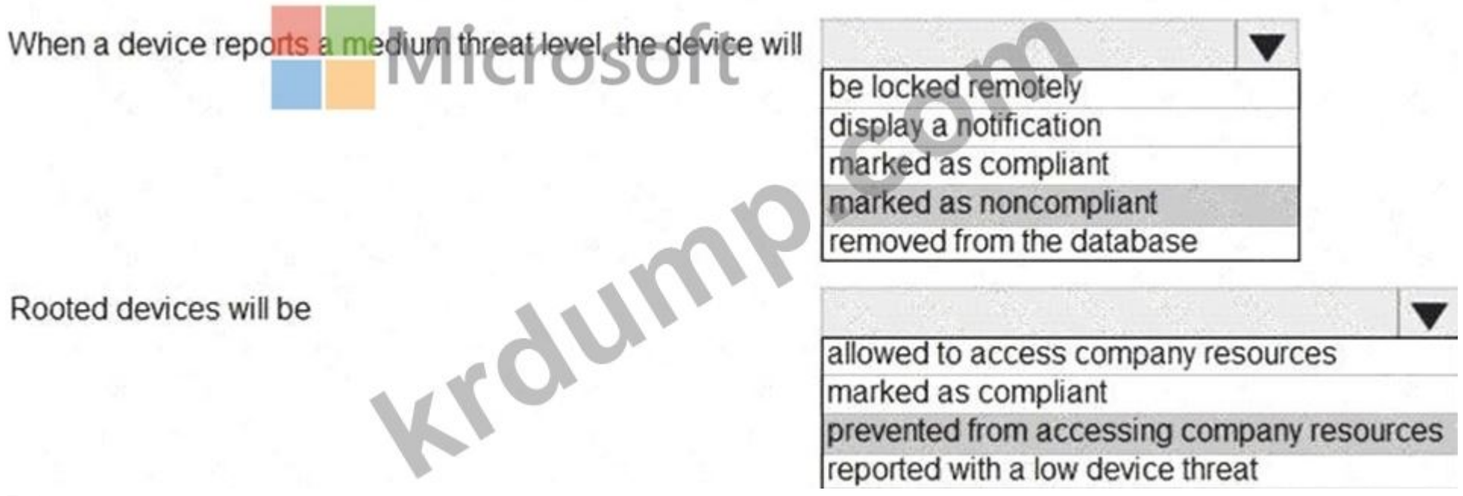
Rooted devices will be

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

Answer:

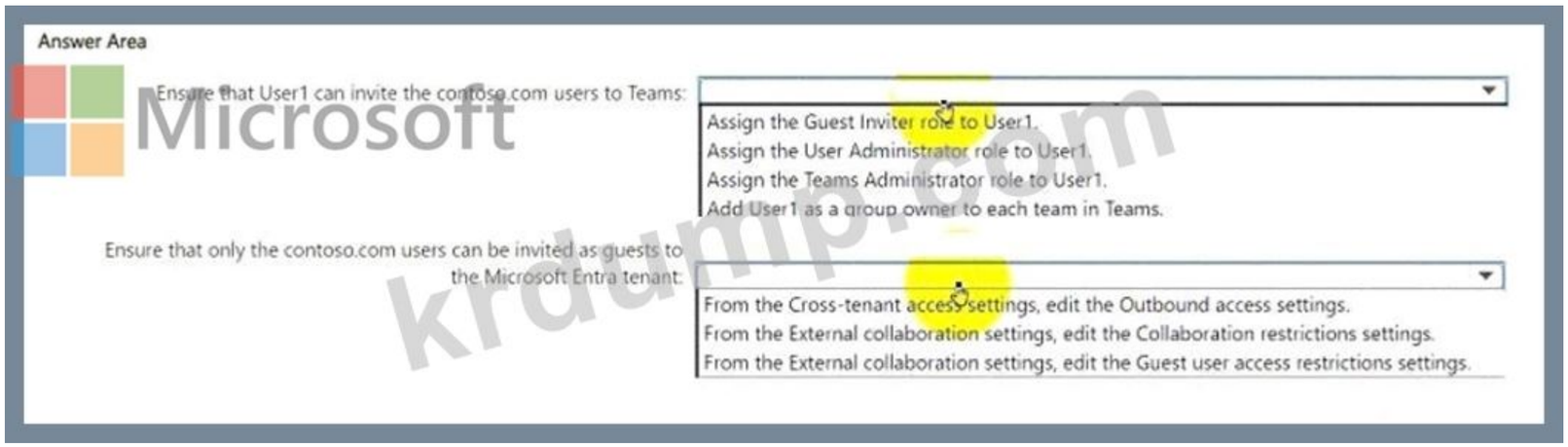


Explanation:

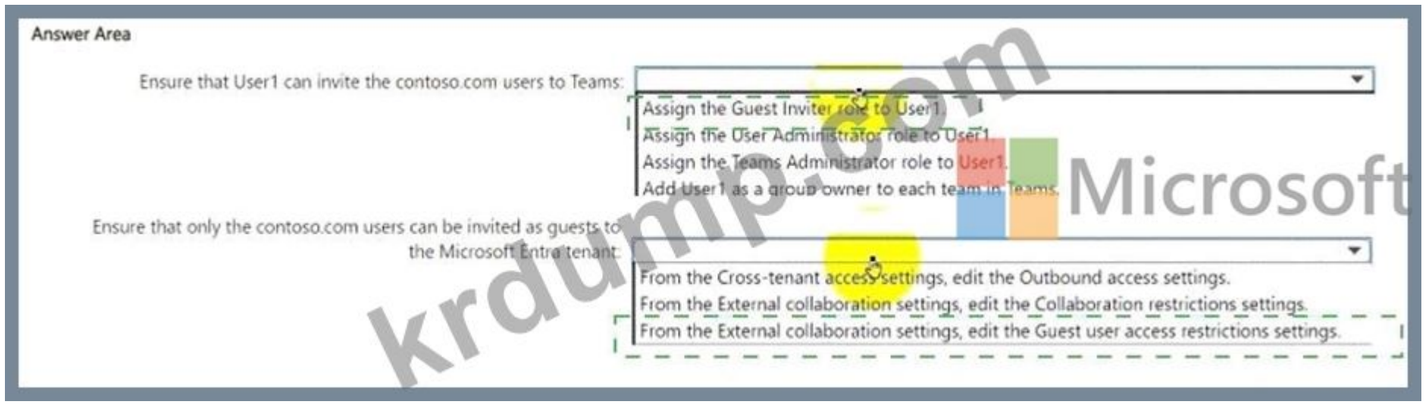


Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android

NEW QUESTION: 88
adatum.com□□□ □□□ □□□ □□□□ Microsoft 365 □□□ □□□□.
Microsoft Entra ID□□ □□□ □□ □□□ '□□ □□□ □□□ □□□ □□□□ □□□ □□□□ □□□ □ □□'□□ □□□□□.
used@adatum.corn□□□ □□□□ contoso.com□□□ □□□□ □□ □□□□ □ □□ Microsoft Teams□□ □□□□□ □□□ □ □□□ □□□□□.
□□ □□ □□□ □□□□□ Microsoft Entra ID □□□ □□□□ □□□.
* User1□ contoso.com □□□□ Teams□ □□□ □ □□□ □□□□□.
* contoso.com □□□□ Microsoft Entra □□□□ □□□□ □□□ □ □□□ □□□□□.
* □□ □□□ □□□ □□□□
□ □□ □□□ □□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.



Answer:



Explanation:

Ensure that User1 can invite the contoso.com users to Teams: Assign the Guest Inviter role to User1 Assigning the Guest Inviter role ensures that User1 has the necessary permissions to invite external users, such as those from contoso.com, to Microsoft Teams.

Ensure that only the contoso.com users can be invited as guests to the Microsoft Entra tenant: From the External collaboration settings, edit the Guest user access restrictions settings Modifying the Guest user access restrictions settings under External collaboration ensures that only users from specific domains, like contoso.com, can be invited as guests to the Microsoft Entra tenant.

NEW QUESTION: 89

(□□□ 1,000□□ Windows □□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.)

□□□ □□ □□□ □□□□ □□□.

□□ □□□ □□□□ □□□?

A. Microsoft Intune □□ □□

B. Microsoft Purview □□

C. □□□□□□□ □□□ □□

D. Microsoft 365 □□ □□

Answer: C (LEAVE A REPLY)

The correct answer is the Microsoft Defender portal .

Explanation:

* Exposure Score is a security metric provided by Microsoft Defender for Endpoint . It measures an organization's overall security posture by evaluating device configuration, vulnerabilities, and security controls across endpoints.

* Microsoft documentation defines Exposure Score as part of the Microsoft Defender Vulnerability Management experience, which is accessed through the Microsoft Defender portal .

* The Exposure Score helps administrators:

* Understand how vulnerable devices are across the organization

* Track improvements to security posture over time

* Prioritize remediation actions based on risk

* Microsoft explicitly states that Exposure Score is viewed and managed within the Microsoft Defender portal , which serves as the central dashboard for Defender for Endpoint, Defender for Office 365, and related security services.

Why the other options are incorrect

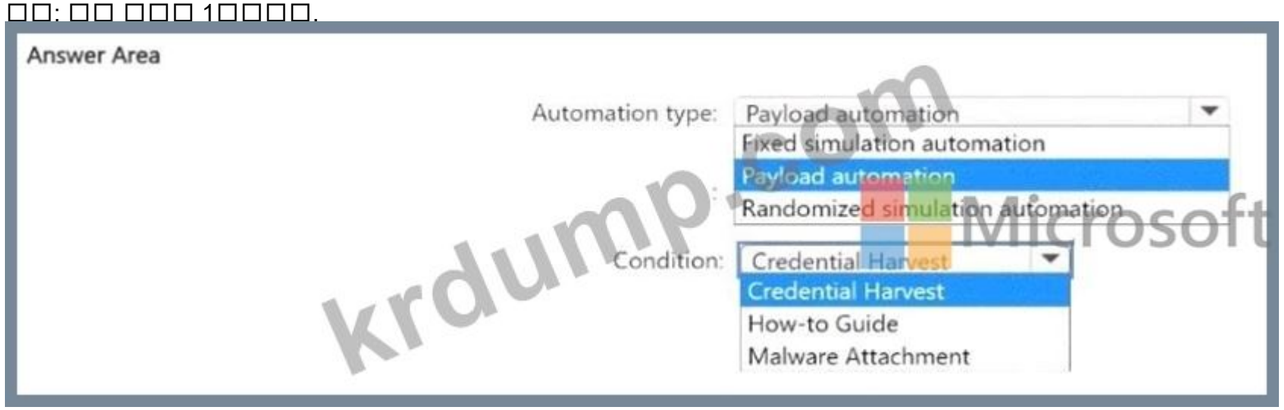
A). the Microsoft Intune admin center

Intune focuses on device management, compliance, and configuration profiles. While it provides device health and compliance reporting, it does not display the Defender Exposure Score.

B). the Microsoft Purview portal

Microsoft Purview is used for data governance, compliance, insider risk, and information protection. It has no functionality related to endpoint exposure scoring.
D). the Microsoft 365 admin center
The Microsoft 365 admin center is designed for tenant-wide administration such as users, licenses, and services. It does not provide detailed endpoint security metrics like Exposure Score.

NEW QUESTION: 90
Office 365□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□□ □□□□□ □□□□ □□□□ □□ □□ □□□□□ □□□ □□□□□ □□□.
□□ □□□ □□□□ □□□□ □□□? □□□ □□ □□□□□ □□□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:

NEW QUESTION: 91
Youi □□□□□□ Active Directory □□□□ □□□□ □□□□.
□□ □□□□ □□□□□ Microsoft Entra □□□□ □□□□.

Microsoft Entra Connect Sync□ □□□□ □□□□ □□ □□□□□□□□. □□ □□ □□□ □ □□□□ □□□ □□□□□□□□□.
□□□ □□ □□□ □□□□□ Microsoft Entra ID Protection□ □□□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Microsoft Entra □□ □□□□ □□ □□□ □□ □□□ □□□□□.
B. Microsoft Entra □□ □□□□ □□ □□□□ □□□□□□.
C. Microsoft Entra Connect□□ □□□□ □□□ □□□□□□.
D. Microsoft Entra Connect□□ □□□□ □□ □□□□ □□□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 92
□□□ Microsoft 365 □□□ □□□□ □□□□.
App1□□□ □□□ □□□ Microsoft Entra ID □□□□□□ □□□□□□□ □□□□□. App1□ □□□□□ □□□□□ □□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□ □□□ □□□□ App1□ □□□□□□ □□ □□□ □□□ □□□□ □□□?
A. □□□□ □□□ Microsoft 365 □□
B. □□ □□□ □□□□ □□ Microsoft 365 □□
C. □□□□ □□□ □□ □□
D. □□ □□□ □□□□ □□ □□ □□
Answer: (SHOW ANSWER)
To grant permissions to assignees to manage users and group access for a specific enterprise app, go to that app in Microsoft Entra ID 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 Microsoft Entra ID 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 Microsoft Entra ID, 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

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

□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□ □□□ □□□ □□□ □□□ □□□ □□□□.
* □□
o □□□
* □□ : Group1
* □□ : Group2, Group3
o □□ □□
* □□□□ □
*□1
* □□ □□
* □□□□
* □□ □□
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 94

□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

□□□□ □□ □□□□ □□□ □□ □□□□ □□□(VDI) □□□ □□□□ Microsoft 365□ □□□□ □ □□□□.

Microsoft Entra ID Protection□□ □□□ □□ □□□ □□□□ □ □□□□.

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

□□□ □□□□ □□□?

A. Microsoft Entra ID□ □□□ □□ □□

B. □□□ □ □□ □□

C. □□□ □□□ □□ □□

D. Microsoft 365 □□□□ □□ □□

Answer: (SHOW ANSWER)

There are two types of risk policies in Microsoft Entra ID (Microsoft Entra ID) Conditional Access you can set up to automate the response to risks and allow users to self-remediate when risk is detected:

Sign-in risk policy

User risk policy

Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.

Reference:

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

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

NEW QUESTION: 95
□□ □□□ 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: 96
Project1□ Project2□□ □□ □□ □□ □□□□ □□□□□ □□□ □ □□□ □□□□ □□□.
□□ □□□□□□ □□ □□ □□□ □□□□ □□□?
A. □□□□ □□
B. □□□□ □□ □ □□□ SSO
C. □□□□ □□ □□□ □ □□□ SSO
D. □□□□ □□ □□□
Answer: C (LEAVE A REPLY)
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
Fabrikam does NOT plan to implement identity federation.
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
Topic 5, Litware, IrkLitware, 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

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 Microsoft Entra ID Premium P2 licenses.
The subscription contains a verified DNS domain named litware.com.
Microsoft Entra Connect Sync 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 Microsoft Entra 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 Microsoft Entra Connect Sync 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: 97
□□□□□□ □ □□ Active Directory □□□□□ □□□□. □□□□ □□□ □□□□ □□□□ □□□ □□□□ □□□□.
Microsoft Entra □□□□ □□□□□.
□□□□□ Active Directory□ Microsoft Entra ID□ □□□□ □□□□□.

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

A. Microsoft Entra Connect Sync □□□ □□ 1□□ □□□□ □□□ Microsoft Entra Connect Sync □□□ □□ 1□
B. Microsoft Entra Connect Sync □□□ □□ 3□□ □□□□ □□□ □□ Microsoft Entra Connect Sync □□□ □□ 1□
C. Microsoft Entra Connect Sync □□□ □□ 6□□ □□□□ □□□ □□ Microsoft Entra Connect Sync □□□ □□ 3□
D. Microsoft Entra Connect Sync □□□ □□ 3□□ □□□□ □□□ □□ Microsoft Entra Connect Sync □□□ □□ 3□

Answer: A (LEAVE A REPLY)

Microsoft Entra Connect Sync can be active on only one server. You can install Microsoft Entra Connect Sync on another server for redundancy but the additional installation would need to be in Staging mode. An Microsoft Entra Connect Sync installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

NEW QUESTION: 98

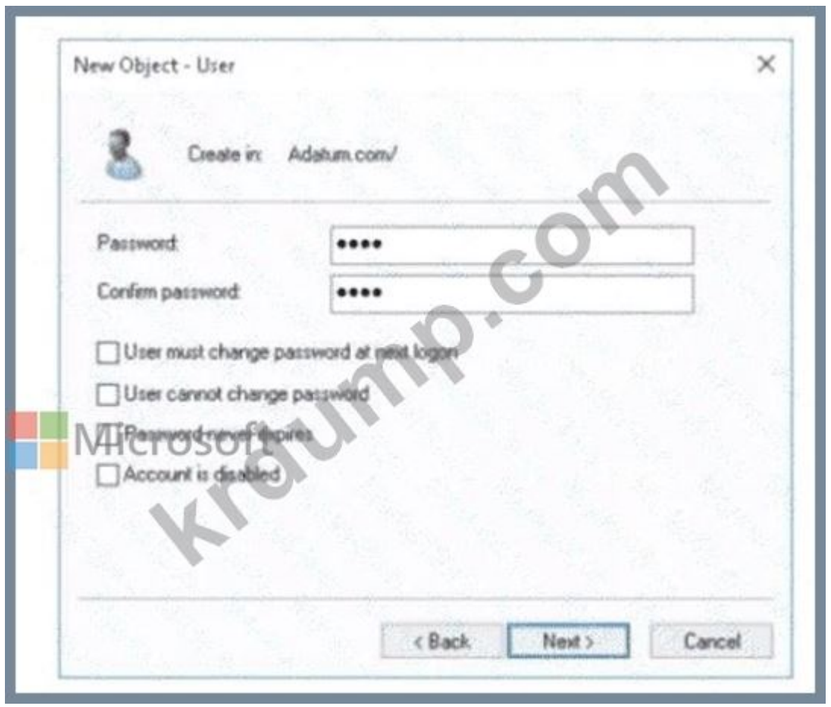
Endpoint Security□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□ □□□ □□ □□□ Endpoint Security Manager □□□ □□□□ □□□.
□□ □□□ □□□ □□□ □ □□□?

A. □□ □□ □□ □ □□ □□
B. □□ □□
C. Microsoft 365□ □□
D. □□ □□ □□, Microsoft 365 □ □□ □□
E. □□, □□ □□ □□, Microsoft 365 □ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 99

□□□□□□ Microsoft Entra Connect Sync Express □□□ □□□□ Microsoft Entra ID□ □□□□□ adatum.com□□□ □□□□□ Active Directory □□□□ □□□□. □□ □□ □□□ □□□□□□ □□□□.
User1□□□ □□□ □□□□ □□□□ □□ □□□ □□ □□ □□□ Pass□ □□□□□.



Microsoft Entra ID □□ □□□ □□ □□□ □□ □□□□□.
□□□□ □□
□□ □ □□ □□□□ □□ □□ □□□ □□□□□.
□□□□ □□ 90□ □
□□□□ 14□ □□ □□□ □□□□.
□□
□□□1□ Microsoft Entra ID□ □□□□□□□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Answer Area

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

Explanation:

NEW QUESTION: 100

□□ □□ □□□ □□□□ □□□ contoso.com□□□ Microsoft Entra □□□□ □□□□.

Name	Member of	Per-user multifactor authentication status
User1	Group1	Disabled
User2	Group1	Enforced

□□□□ □□ □□ □□□ 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

□□ □□□ □□ □□□ □□□ □□□ □□□□.

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

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 101

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

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

A. □□2□ □□3□

B. □□! □ □□2□

C. □□ 1, □□ 2, □□ 3□

D. □□2, □□3, □□4□

E. □□3□ □□4□

Answer: (SHOW ANSWER)

NEW QUESTION: 102

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

□□ □□□□ □□□ □□□ □□□ contoso.com□□□ Microsoft Entra □□□□ □□□□□□. (□□ □□ □□□□□□.)

User2□ user2@fabrikam.com□□ □□□□ □ Microsoft Entra ID □□□ □□□□□.
User2□ Microsoft Entra ID□ □□□□ □□□□ □ □□□ □□ □□□.
□□ □□: □□□□□ Active Directory □□□□□ User2□ UPN □□□□ @contoso.com□□ □□□□□.
User2□□ user2@contoso.com□□ □□□□□□ □□□□□.
□□□ □□□ □□□□□?

A. □
B. □□□

Answer: A (LEAVE A REPLY)

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: 103
□□□ □□ □□□ □□□□□ □□ □□ □□□ □□□□ □□□.
Microsoft Endpoint Manager □□ □□□□ □□□ □□ □□□?
A. □□ □□ □□□□ □□ □□□ □□□□□.
B. □□□□ □□□ □□□ □□ □ □□□ □□□□.
C. □□□ □□ □□□□ □□ □□ □□ □□ □□□□ □□□□□.
D. □□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION: 104
□□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□. □ □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

contoso.com□ Microsoft Entra ID□ □□□□□□ Microsoft Entra Connect Sync□ □□□□□.
□□ □□□ Microsoft Entra ID□ □□□□□□?
A. □□1□ □□
B. User1□ User2□ □□
C. □□1 □ □□□1□ □□
D. □□1, □□□1, □□□2
Answer: D (LEAVE A REPLY)
Disabled accounts
Disabled accounts are synchronized as well to Microsoft Entra ID. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Microsoft Entra ID.
The assumption is that if a disabled user account is found, then we won ' t find another active account later and the object is provisioned to Microsoft Entra ID with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts

NEW QUESTION: 105
□□ □□ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Platform
Device1	Windows 11
Device2	Linux
Device3	MacOS

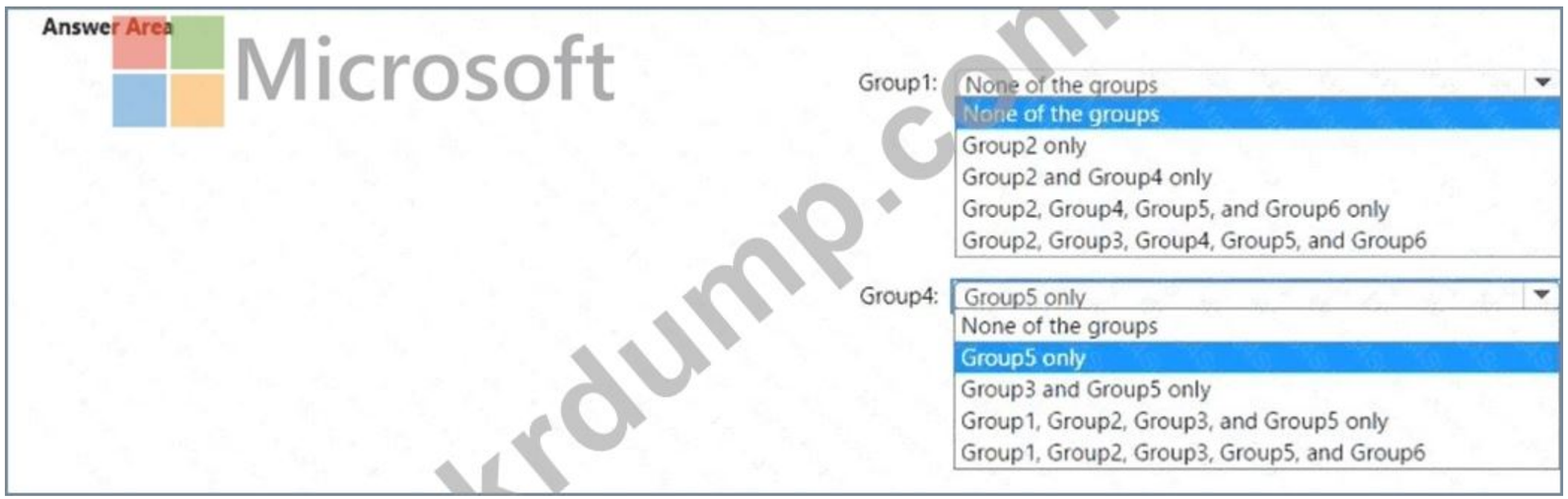
Defender Update □□□ □□□□ □□□□ Endpoint □□ □□□ □□ □□□□□. □□ □□□ □□□ □□□ □ □□□□?
A. Device1 □ Devke2□

B. Device1☐
C. Devke1 ☐ Device3☐
D. Devke1, Device2 ☐ Devke3
Answer: B (LEAVE A REPLY)

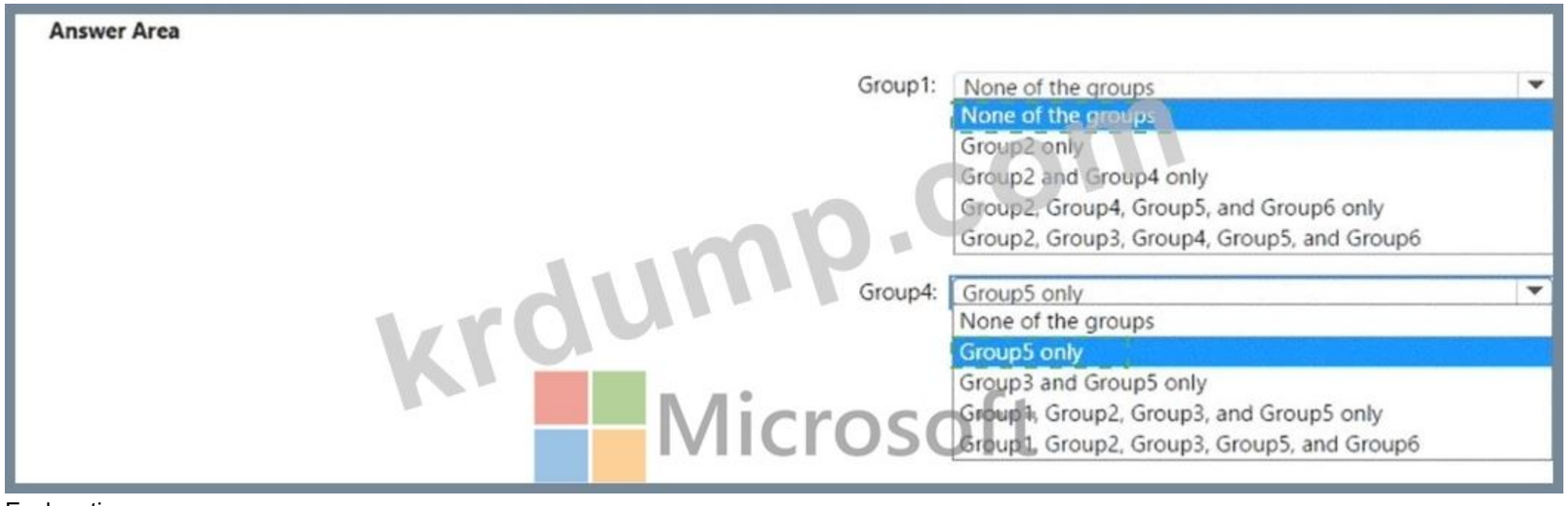
NEW QUESTION: 106
☐☐ ☐☐ ☐☐☐ ☐☐☐ ☐☐☐ Microsoft 365 E5 ☐☐☐ ☐☐☐☐.

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: 107

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

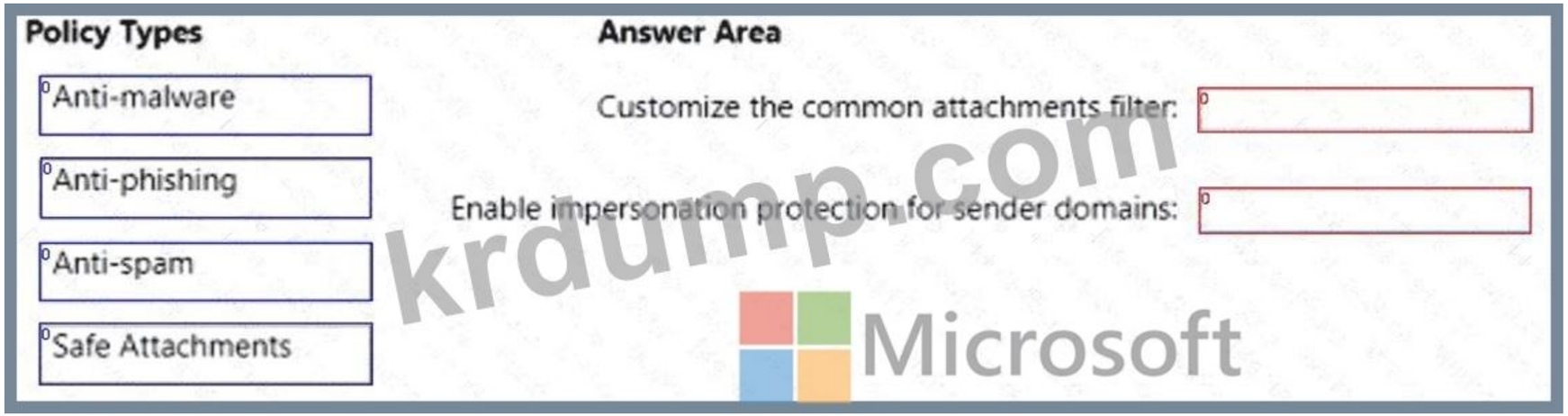
□□ □□ □□□ □□□□□ □□□ □□□□ □□□.

□□□□ □□ □□ □□□ □□□ □□□□□.

□□□ □□□□ □□ □□ □□□ □□□□□□.

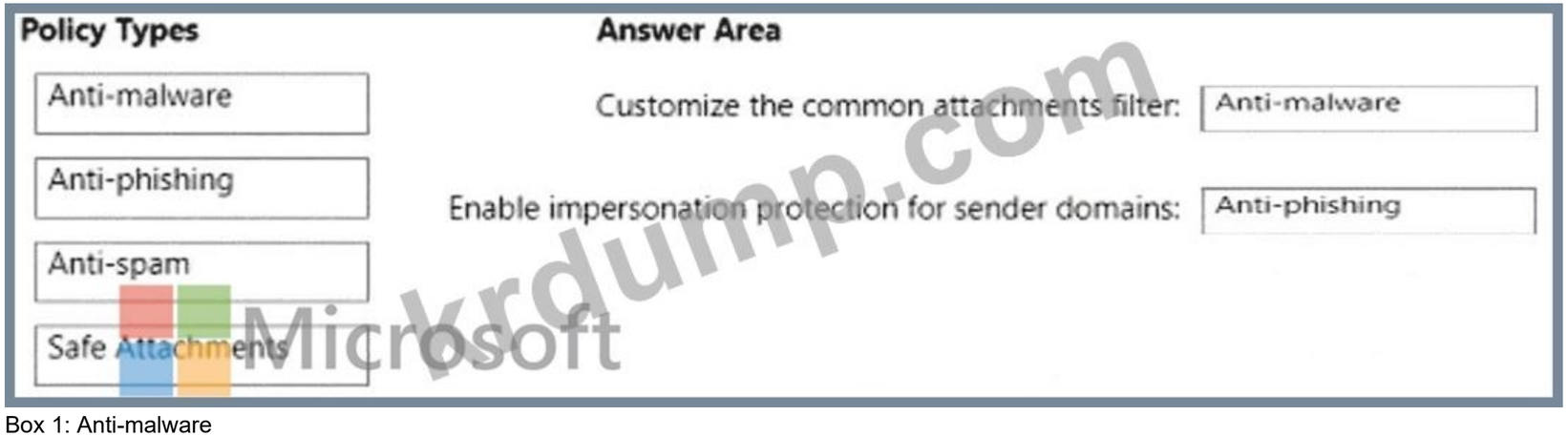
□ □□ □□□ □□ □□ □□□ □□□ □□□□ □□□? □□□□ □□□ □□ □□□ □□□ □□ □□□□ □□□ □□□□□. □ □□ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □□□ □□□ □□□ □□□□□ □□□□ □ □ □□□□.

□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:



Box 1: Anti-malware

Customize the common attachments filter.

See step 5 below.

1. Use the Microsoft Defender XDR portal to create anti-malware policies In the Microsoft Defender XDR portal at https://security.microsoft.com, go to Email & Collaboration > Policies & Rules > Threat policies > Anti-

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

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

Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-policies-configure
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about

NEW QUESTION: 108
Site1□□□ Microsoft SharePoint Online □□□□ □□□□ Microsoft 365 E5 □□□□ □□□□. Site1□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

Sensitivity1□□□ □□□ □□□ □□□□ □□ □□□ □□ □□ □□□ □□□ □□□□.

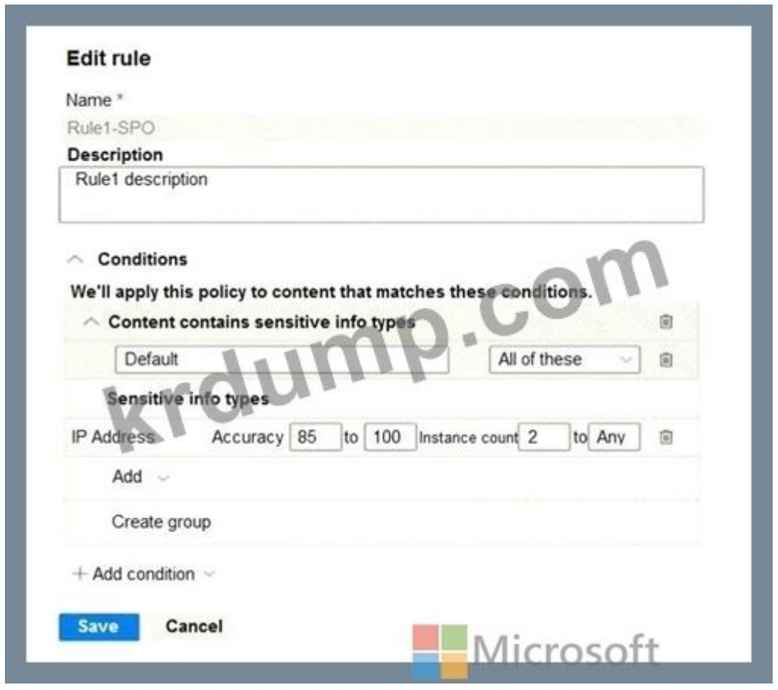
□□: AutoLabel1

□□ □□□ □□□: □□□1

SharePoint Online □□□□ □□ □□: Rule1-SPO

□□□ □□□ □□□ □□□□□: Site1

Rule1-SPO□ □□ □□□ □□ □□□□□.



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

□□□□: □□ □□□ 1□□□□.

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

Answer:

Explanation:

Reference:

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

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

NEW QUESTION: 109

□□□

Microsoft 365 □□□□ □□□□.

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

Label Policy □□□ □□□ □□ □□□ □□□ □□□□. (Label Policy □□ □□□□□.)

□□ □□□ □□ □□ □□ □□□□□.

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

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

Box 1: No

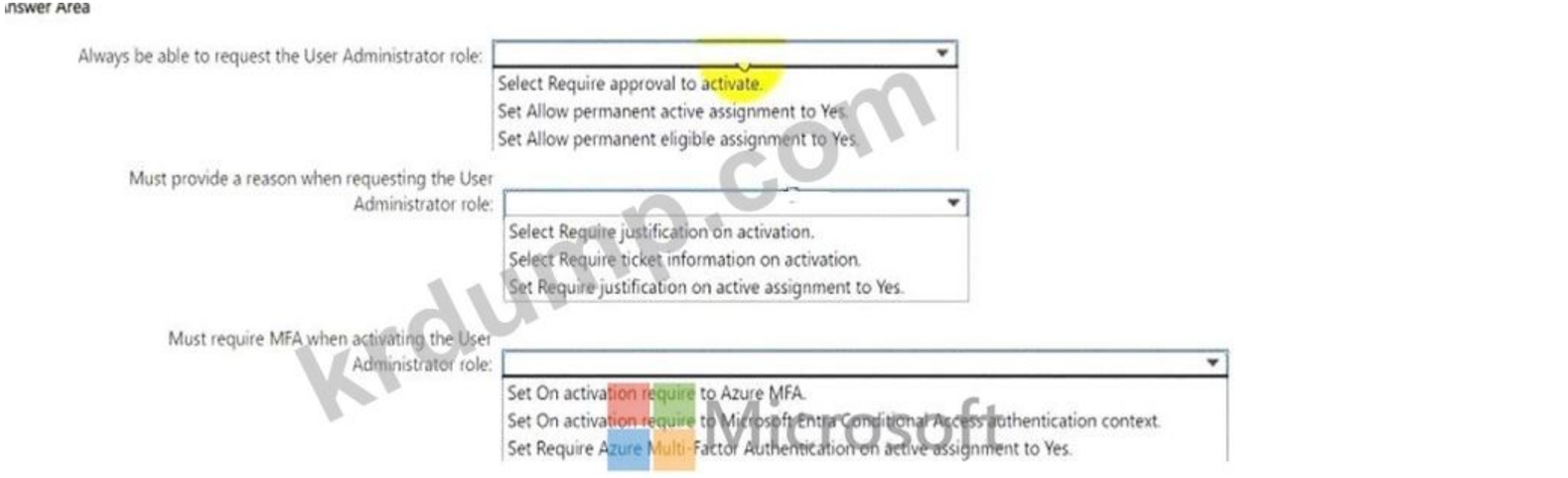
Box 2: Yes

Box 3: No

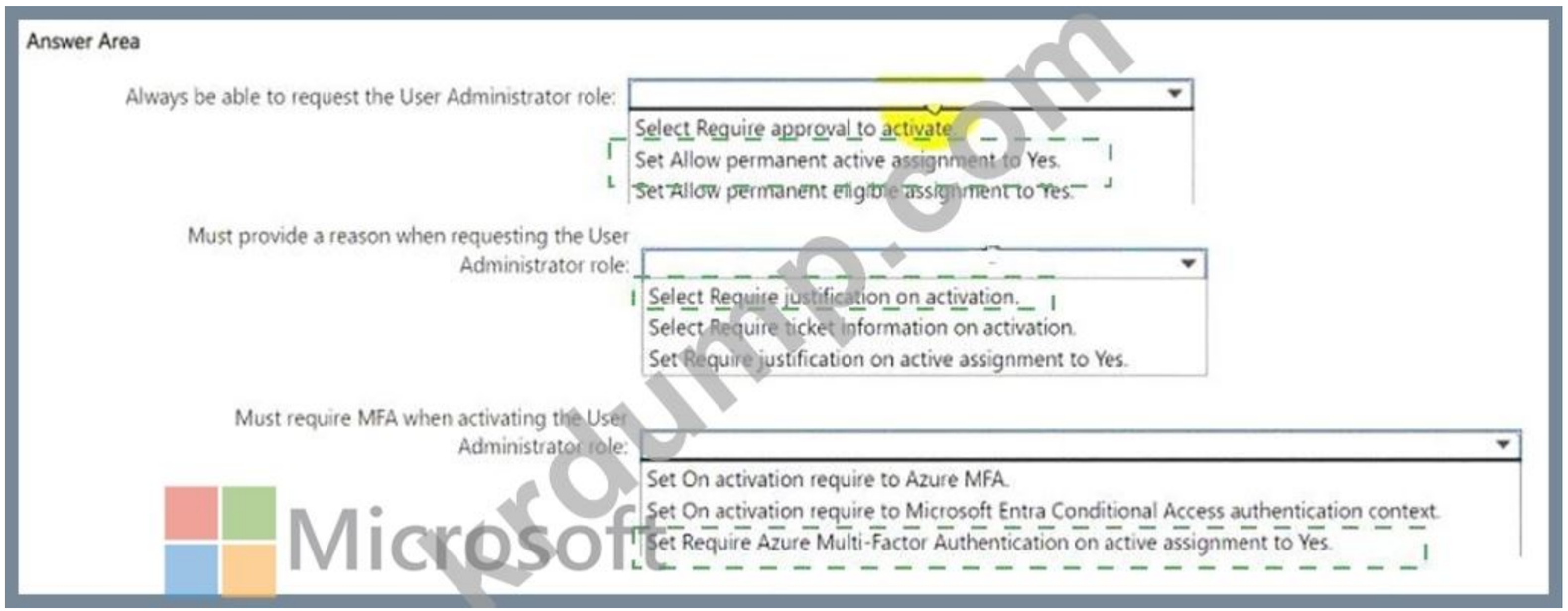
Reference:

https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

NEW QUESTION: 110
Microsoft 365 E5 □□□ □□□□.
Microsoft Entr a□□ □□□ □□□ □□□ □□ Privileged Identity Management(PIM)□ □□□□ □□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.
* □□ □□□ □□□ □□□ □□□ □ □□□□.
* □□□ □□□ □□□ □□□ □ □□□ □□□□ □□□.
* □□□ □□□ □□□ □□□□ □ □□ □□ □□(MFA)□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.



Answer:

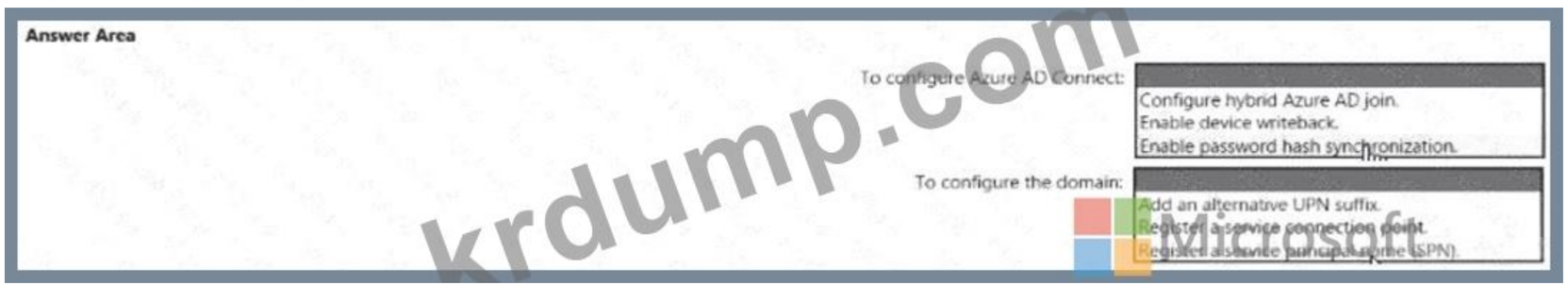


Explanation:
Always be able to request the User Administrator role: Setting " Allow permanent eligible assignment to Yes

" 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: 111
Microsoft 365 E5 □□□ □□ □□□□ □□ Microsoft Defender□ □□□□ □□□□.
Cloud Discovery□□ □□□ □□ □□ □□ □□ □□□ □□□ □□□□□.
□□ □□ □□□□□□ □□□□ □□□. □□□□ □□□ □ □□□ □□□□ □ □□□□□ □□□ □ □□□ □□□.
A. □ □□ □□□ □□ □ □□□ □□□□□.
B. Cloud Discovery □□□ □□□□ □□□□□.
C. □ □□□□□ □□□□□□.
D. □□□ □□□ □ □□□ □□□□□.
E. □ □□ □□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
□□□□□ □□□□□□ Active Directory □□□□ Microsoft Endpoint Configuration Manager □□□□ □□□□ □□□□.
□□□ Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Microsoft Entra Connect Sync□ □□□□ □□□ □□ □ □□ □□□ Azure □□□□(Microsoft Entra ID)□ □□□□□□. □□ □□ □□□□ □□□□□□ □□□□.
□□□ □□ □□□ □□□ □□□□□.
□□ □□□ □□□□□ Microsoft Entra Connect Sync□ □□□□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:

NEW QUESTION: 113

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

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

LinkedIn □□□□ □□□□ □□□ □□□ □ □□□?

A. Microsoft OneDrive for Business □□

B. Microsoft SharePoint Online □□ □□□□□

C. Microsoft 365 □□□

D. Azure □□

Answer: C (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 114

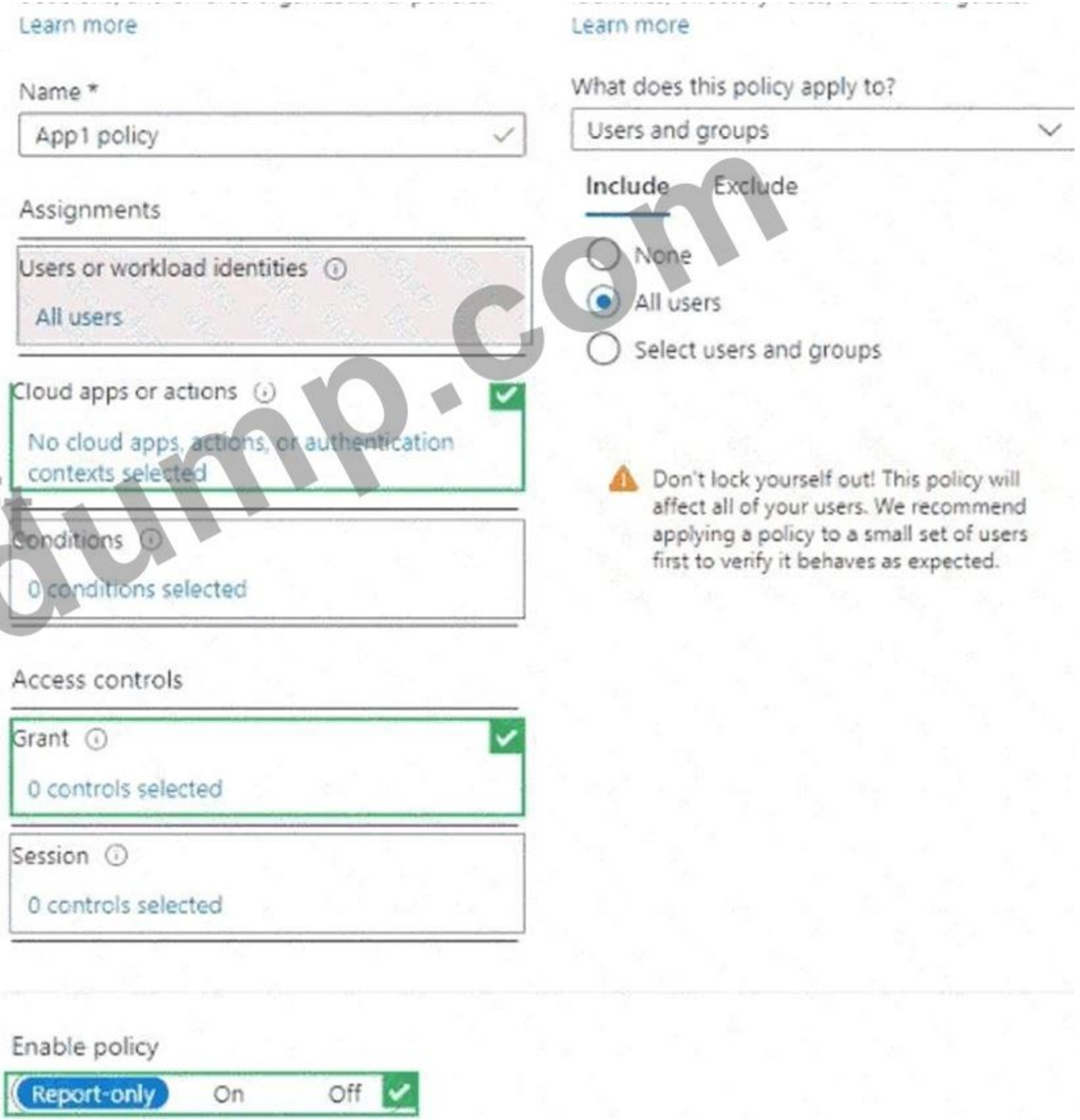
□□□ Microsoft 365 Enterprise E5 □□□ □□□□ □□□□.

Microsoft Entra ID □□□□□□ □□□□□□ □□□ App1□□□ □□□□ □□ □□ □□□□□.

App1□ □□□ □□□ □ □□ □□□ □□□ □□ 2□□ □□□ □□□□□ □□ □□□.

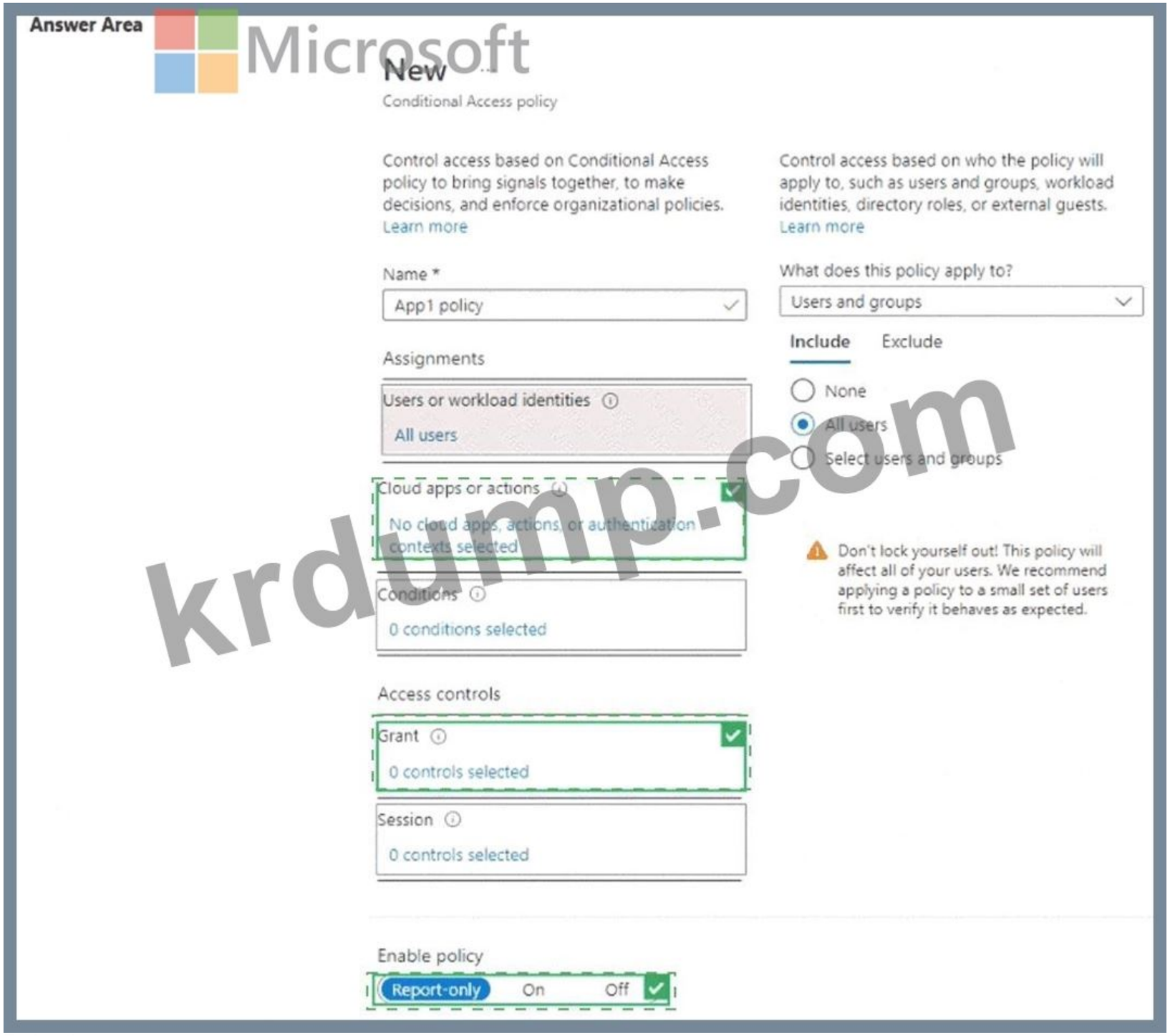
□□□□ □□ □ □□ □□□ □□□□ □□□? □□□ □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.



Answer:

Answer Area



Explanation:

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more

Name *

App1 policy

Assignments

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.
Learn more

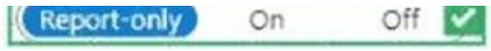
What does this policy apply to?

Users and groups

Include Exclude

- None
- All users
- Select users and groups

Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.



NEW QUESTION: 115

□□□ User1□ Microsoft SharePoint Online □□□ Site1□ □□□ Microsoft 365 □□□ □□□□. User1□ Site1□ □□□ □□□ □□□□□. Site1□ □□ □□ □□□ □□ □□ □□ □□□□ □□□□□.

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

Site1□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

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

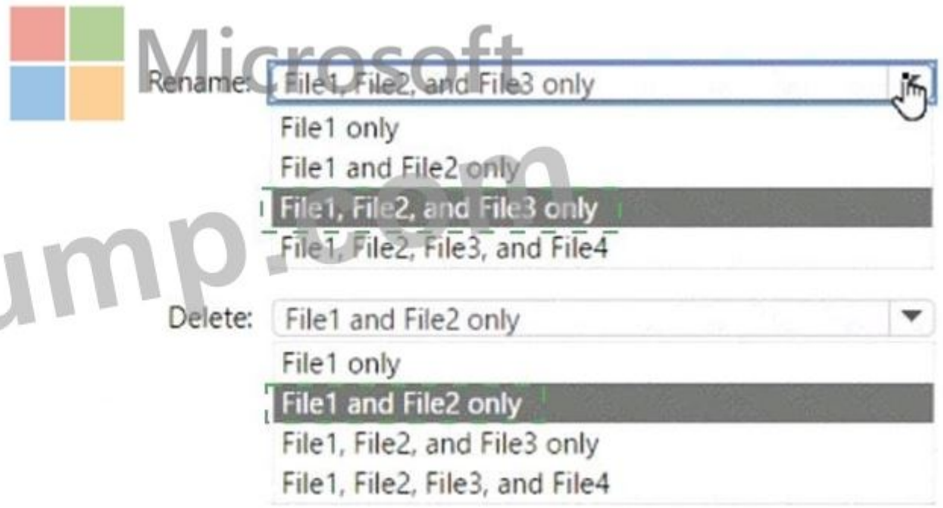
□□□□: □□ □□□ 1□□□□.

Answer Area

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

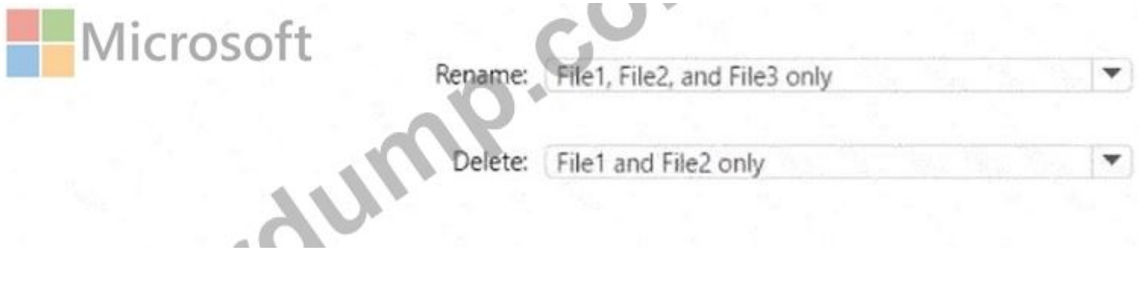
Delete: File1 and File2 only
- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

Answer Area



Explanation:

Answer Area



NEW QUESTION: 116

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

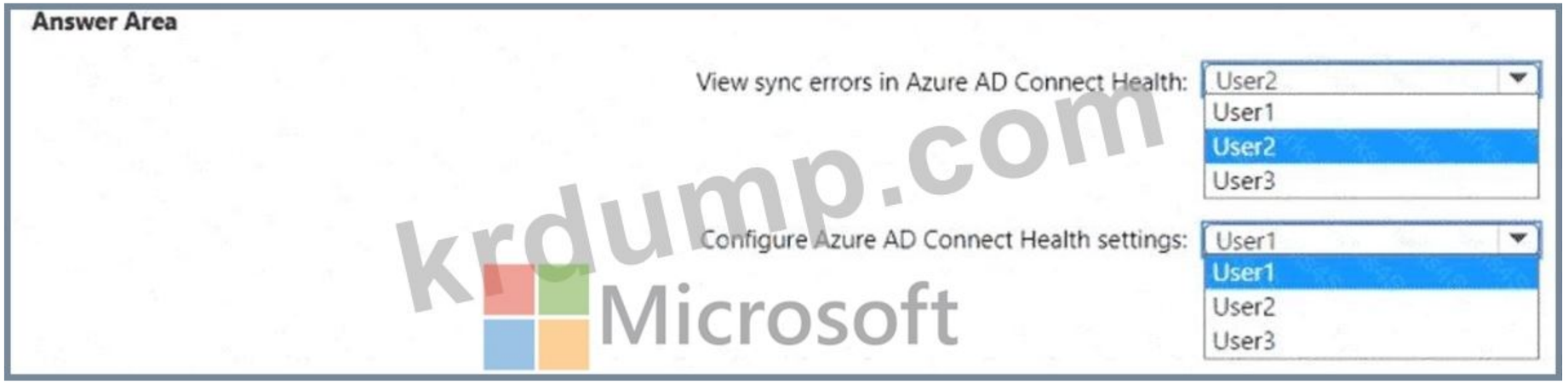
Name	Description
User1	Azure AD Connect sync account
User2	Contributor for Azure AD Connect Health
User3	Application administrator in Azure AD

□□ □□□ □□□ □ □□ □□□□ □□□□ □□□.

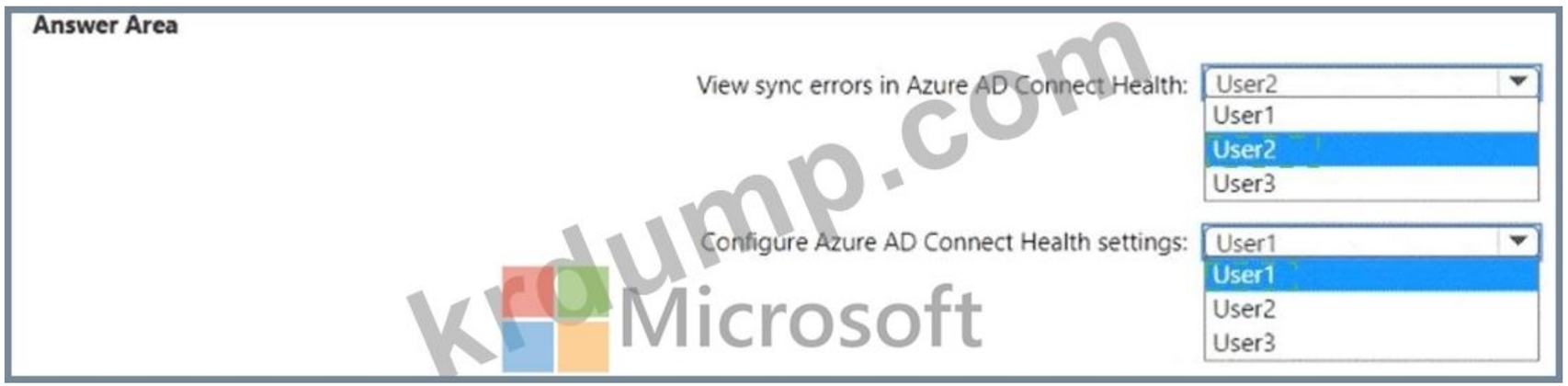
* Microsoft Entra Connect Health□□ □□□ □□□ □□□□□.
* Microsoft Entra Connect □□ □□□ □□□□□.

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

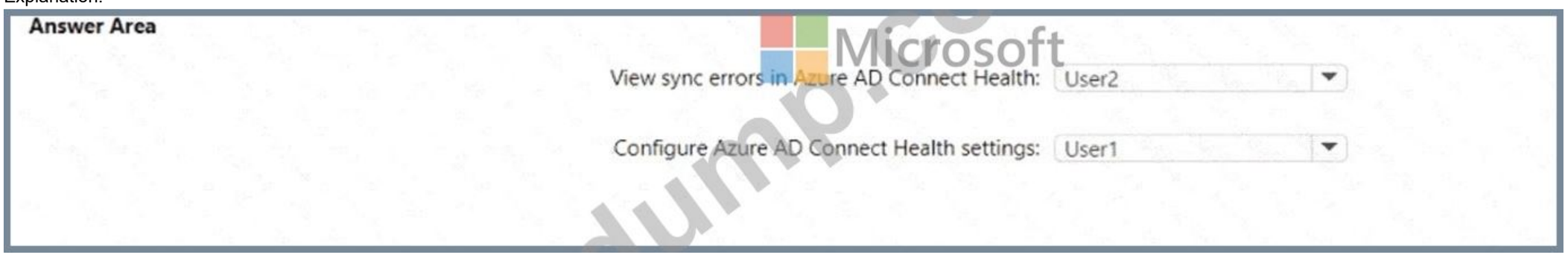
□□: □□ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 117

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

□□ □□□□ □□□ □□□ □□□ contoso.com□□□ Microsoft Entra □□□□ □□□□□□. (□□ □□ □□□□□□.)

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

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

USER SIGN-IN

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

User2□ user2@fabrikam.com□□ □□□□ □ Microsoft Entra ID □□□ □□□□□.
User2□ Microsoft Entra ID□ □□□□ □□□□ □ □□□ □□ □□□.
□□ □□: Microsoft Entra □□ □□□□ fabrikam.com□ □□□ □□ □□□□□ □□□□□. □□ □□ User2□□ user2@fabrikam.com□□ □□□□□□ □□□□□.
□□□ □□□ □□□□□?

A. □

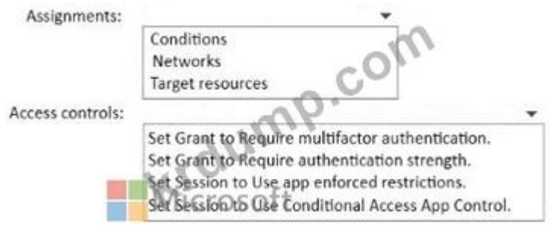
B. □□□

Answer: (SHOW ANSWER)

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

NEW QUESTION: 118

□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□□□ Microsoft Entra □□□□ □□□ □□□□□ □□□□□ □ □ □□ □□ □□□ □□(MFA) □□□ □□□□ Policy1□□□ □□□ □□□ □□□ □□□□ □□□.
Policy1□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:

Assignments

Target resources

Access controls

Set Grant to Require authentication strength

The correct assignment area is Target resources because the policy must apply when users attempt to register or join devices. In Conditional Access, device registration and device join are handled as a user action under target resources, not as a network condition. Microsoft's Conditional Access deployment guidance explicitly lists the scenario "Require multifactor authentication for device join and device registration using user action," which confirms that the assignment must target the device-registration/join user action.

The correct access control is Set Grant to Require authentication strength. Plain "Require multifactor authentication" only requires any MFA method that satisfies the MFA claim, such as push notification, SMS, voice, or OATH. That does not guarantee phishing resistance. Microsoft documents that the Require authentication strength grant control lets administrators require a specific authentication strength in Conditional Access. Microsoft's built-in Phishing-resistant MFA strength includes methods such as FIDO2 security keys, Windows Hello for Business/platform credentials, and multifactor certificate-based authentication.

Therefore, the policy must target the device registration/join user action under Target resources and grant access only when the user satisfies the Phishing-resistant MFA authentication strength.

NEW QUESTION: 119

□□□ □□ 3□□ □□ 1□□ □□□□ □□□□. □□□ □□ □□□□ □□□□□.

□□ □□□ □□□□□□□ 365 □□□□ □□□□ □□□ □□□ □□□ □□□□□.

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

□□ □□□ □□□ □□□□ □□□?

A. Microsoft Intune □□ □□ □□□

B. Microsoft Entra □□□ □□□

C. Microsoft Intune □□ □□ □□ □□

D. Microsoft Entra ID □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 120

□□ □□□ □□ □□ □□ □□□ □□ □□□□.

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: 121

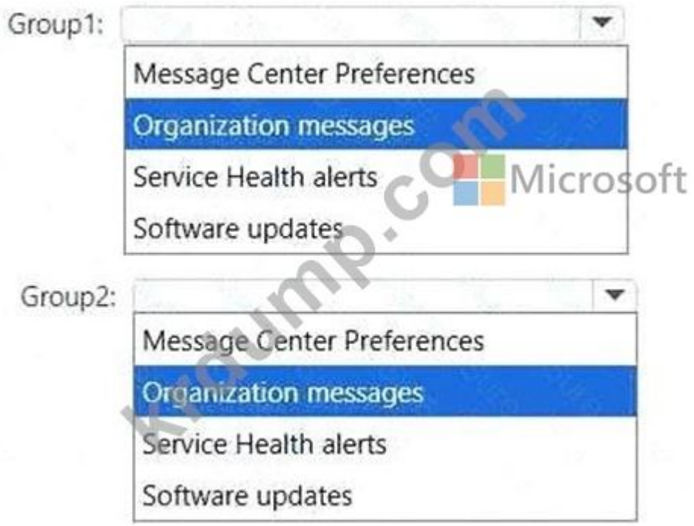
Group1□ Group2□□ □ □□ □□□ □□□ Microsoft 365 □□□ □□□□.

□□ □□ □□□ □□□□□ □□□ □□□ □□□□ □□□.

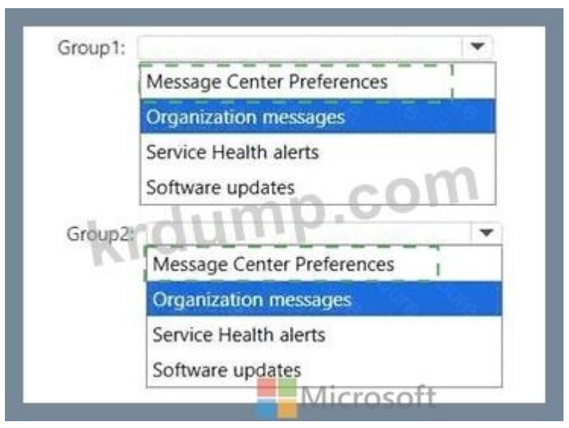
* □□1: □□ □□□ □□□□□ □□□ □ □□□ □□□ □□□□.

* □□2: Microsoft 365 □□ □□ □□□□ □□□ □ □□□ □□□ □□□□.

□ □□□ □□ □□ □□□ □□□ □□□□ □□□?



Answer:



Explanation:

Group

Notification type

Group1

Message Center Preferences

Group2

Message Center Preferences

The correct answer for both groups is Message Center Preferences. Do not select Organization messages; that option is for sending adoption, onboarding, or product-use messages to users inside Microsoft 365 experiences, not for administrator service-update or maintenance notifications.

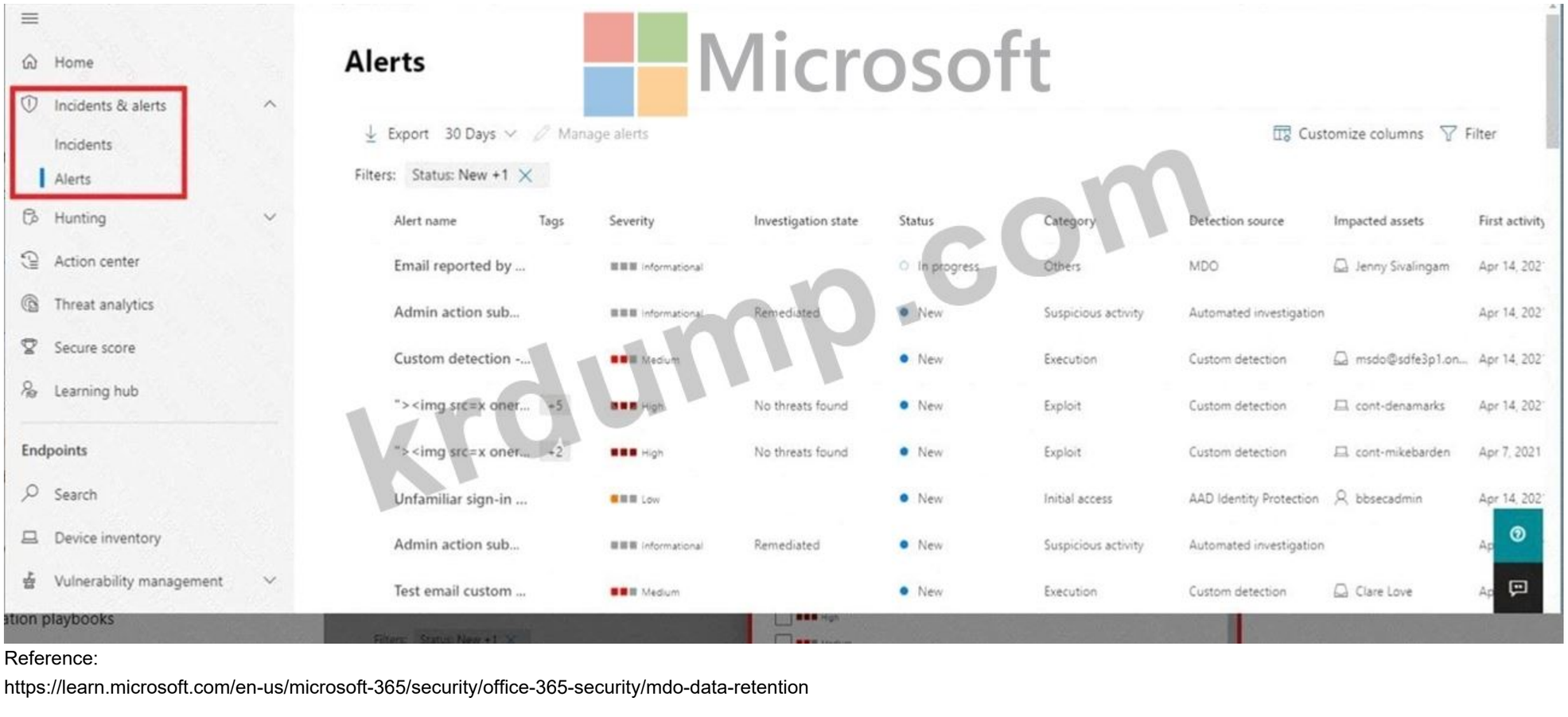
For Group1, major service updates are delivered through the Microsoft 365 Message center. Microsoft states that Message center helps admins track upcoming changes, feature updates, and required actions across Microsoft 365 services. Message center preferences can be configured so admins receive email for major updates only.

For Group2, Microsoft 365 planned maintenance events are also handled through Message center, not Service Health alerts. Microsoft's service health documentation is explicit that planned maintenance events are not shown in Service health and should be tracked by staying current with Message center. Microsoft's service continuity documentation also states that customers are notified of planned maintenance through Message center in the Microsoft 365 admin center.

Therefore, select Message Center Preferences for both Group1 and Group2.

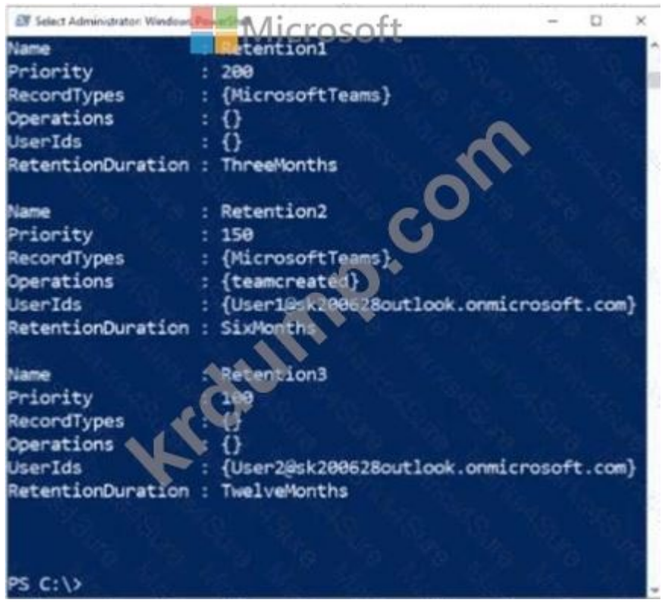
NEW QUESTION: 122
□□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft 365 □□□ □□□□.
□□□□ □□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□□□□ Active Directory □□ □□□ □□□ □□□□ □□□.
* □□□□ Microsoft Entra Self-Service Password Reset(SSPR)□ □□□ □ □□□ □□□.
□□□ □□□□ □□□?
A. Microsoft Entra Seamless Single Sign-On(Microsoft Entra Seamless SSO)
B. □□□□ □□
C. □□□□ □□ □□□
D. Microsoft Entra ID □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 123
Microsoft Defender XDR □□□□ □□□ □□□□ □□□□.
□□□ □□□ □□□ □□ □□□□□?
A. 30□
B. 60□
C. 3□□
D. 6□□
E. 12□□
Answer: (SHOW ANSWER)
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 Defender XDR 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.



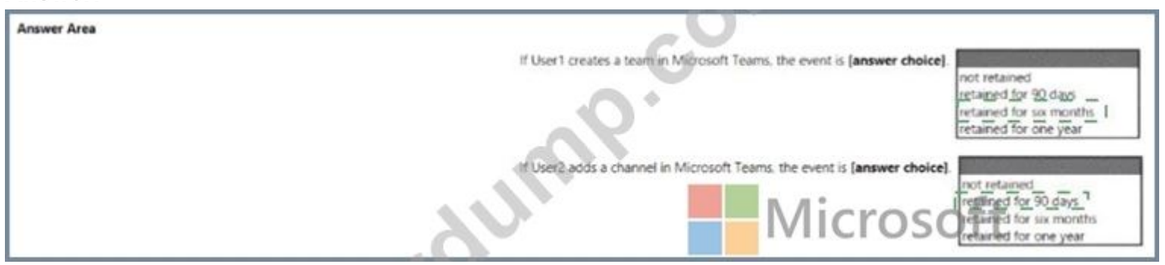
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention

NEW QUESTION: 124
□□ □□ □□□ □□□ 3□□ □□ □□ □□□ □□ Microsoft 365 ES □□□ □□□□.



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

Answer:

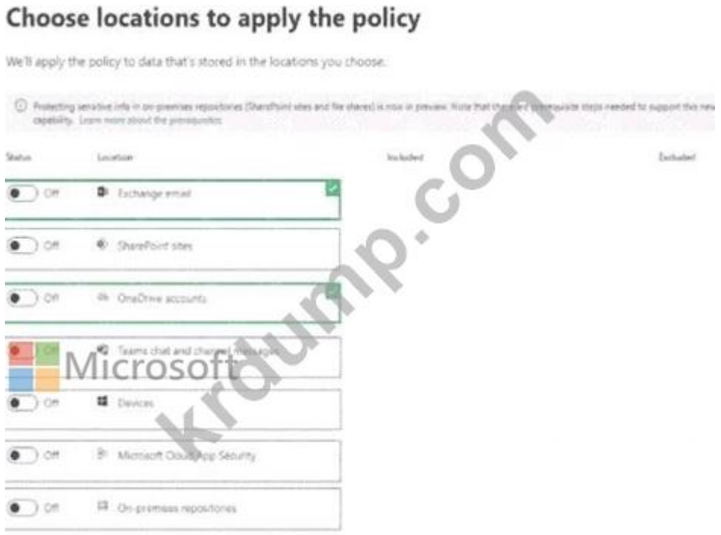


Explanation:

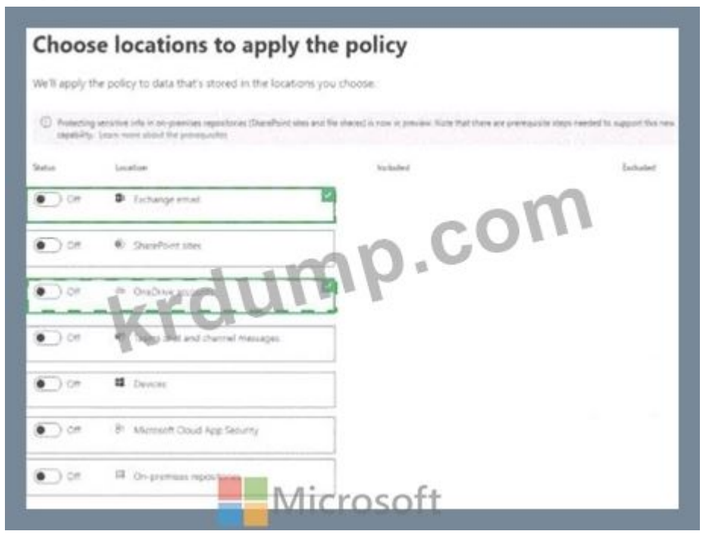
NEW QUESTION: 125
□□□ □□ 3□□ □□ 1□□ □□□ □□□□. □□□ □□□ □□□□□.
□ □□□ Microsoft 365 □□□□ □□□□ □□ □□ □□□ □□□ □□□□□.
□□ □□□□ □□□□□□ □□ □□ □□□ □□□□□ □□ Microsoft 365 □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. Microsoft Entra □□□ □□□
B. Microsoft Intune □□ □□ □□□
C. Microsoft Entra □□ □□
D. Microsoft Intune □□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 126
□□□ □□□□ □□□ □□□ □ □□□□□□□ □□□□.
Microsoft Defender Advanced Threat Protection(Microsoft Defender ATP)□ □□□ □□□ □□ □□□□□ □□□ □□□ □□□□ □□ □□□□ □□□ □□ □□□.
Microsoft Defender □□ □□□□ □□□ □□□□ □□□?
A. □□□ □□ □□ □□
B. □□/□□ □□ □□
C. □□ □□ □□
D. □□□
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage- indicators

NEW QUESTION: 127
Microsoft 365 E5 □□□□ □□□□.
□□□□ Microsoft Teams□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□□□□ □□□ □□ □□(DLP) □□□ □□□□.
□□□ □□□□ □□ □ □□□ □□□□□? □□□□ □□ □□□□ □□□ □□□ □□□□□.



Answer:



NEW QUESTION: 128

□□□□□□ □□□□□ Active Directory Domain Services(AD DS) □□□□ □□□□ □□□□.

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

Name	Source location	Authentication method
User1	On-premises	Password hash
User2	On-premises	Password hash
User3	On-premises	Password hash
User4	On-premises	Password hash
User5	Cloud	Cloud-only
User6	Cloud	Cloud-only

□□ □□□□ Microsoft 365 □□□ □□□□ □□□ □□□ □ □□□ □□ □□□. □□ □□□□ □□□ □□□□□ □□□.
Microsoft Entra ID Free □ Microsoft Entra ID P1 □□□□□ □□ □□ □□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:
From the table in the question:
User1-User4 are On-premises (synced) with Password hash authentication.
User5-User6 are Cloud users (cloud-only).
Microsoft's licensing guidance for Self-Service Password Reset (SSPR) scenarios (which includes password change) states:
Cloud-only user password change (user knows their password and wants to change it) is available in Microsoft Entra ID Free.
Exact extract: "Cloud-only user password change ... Microsoft Entra ID Free" Hybrid user password change or reset with on-prem writeback (synced from on-prem using Entra Connect and writing the password back) requires Microsoft Entra ID P1 or P2 (or Microsoft 365 Business Premium).
Exact extract: "Hybrid user password change or reset with on-prem writeback ... Microsoft Entra ID P1 or P2" Because User1-User4 are synced (hybrid) users and must change passwords using a Microsoft 365 portal and keep passwords consistent with on-premises AD DS, they require password writeback, which requires P1 for those users.
Because User5-User6 are cloud-only users, they can change passwords with Entra ID Free.
Minimum licenses (cost-optimized)
Microsoft Entra ID P1 licenses: 4 (User1-User4)
Microsoft Entra ID Free licenses: 2 (User5-User6)

NEW QUESTION: 129
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Microsoft Defender for Cloud Apps□ □□□□ Microsoft 365□ Defender for Cloud Apps□ □□□ □□□□□.
□ □□□□ □□□ □ □□ Microsoft 365 □□ □□□ □□□□ □ □□□ □□□□ □□□.
□□□ □□ □□ □□□?
A. □□□□ □□□ □□□□□.
B. □□□□ □□ Defender□ □□ □□ □□□□□ □□□□□□.
C. □□□□ □□ Defender□ API □□□ □□□□□.

D. □□□ □□□ □ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

The correct answer is B. Enable file monitoring for Defender for Cloud Apps. Microsoft's Microsoft 365 connector guidance states that when connecting Microsoft 365 to Defender for Cloud Apps, admins select the Microsoft 365 components to protect, and for maximum protection Microsoft recommends selecting all components. However, Microsoft explicitly notes that to enable protection for Microsoft 365 files, you must first enable Defender for Cloud Apps file monitoring under Settings > Cloud Apps > Files > Enable file monitoring. This makes option B the prerequisite action.

Do not select Add an API token. API tokens are commonly used for certain third-party app connectors, but Microsoft 365 connects through the built-in app connector flow and Microsoft 365 audit/API integration. Cloud Discovery is for discovering cloud app usage from network logs, not enabling Microsoft 365 connector components. Conditional Access app control is for real-time session control and is not required before selecting Microsoft 365 connector components. Microsoft also states that Defender for Cloud Apps integrates directly with Microsoft 365 audit logs and that Microsoft 365 components are selected during the app connector setup.

=====

NEW QUESTION: 130

Admin4□ SSPR□ □□□ □ □□□ □□□□ □□□.

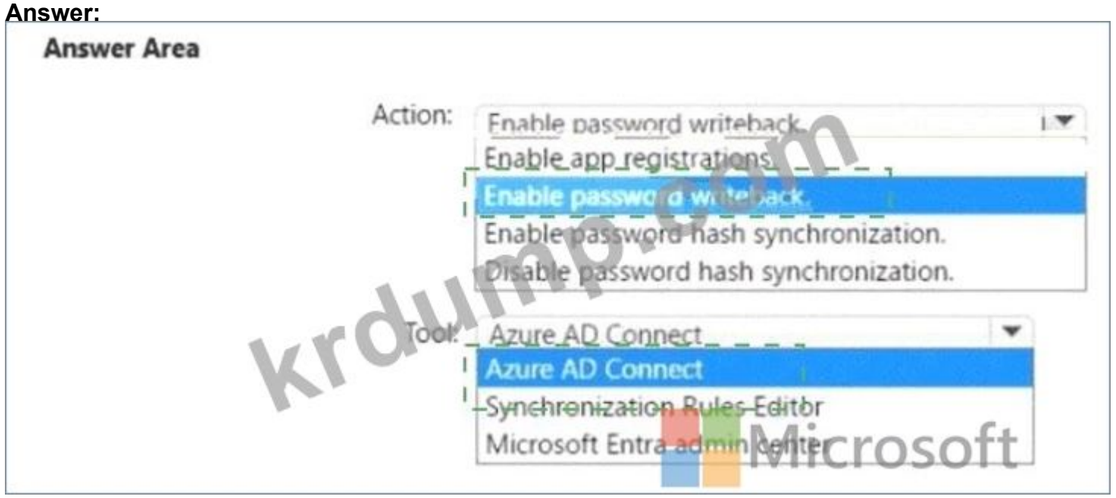
□□ □□□ □□□□ □□□? □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

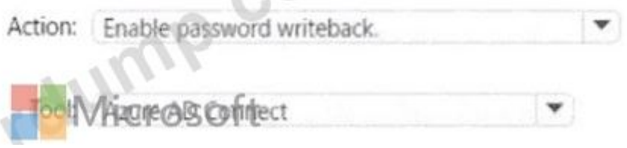
Answer:

Answer Area



Explanation:

Answer Area



NEW QUESTION: 131
Microsoft 365 E5 □□□ □□□□.
□□□□ Android □□ iOS □□□ □□□ □□□, Windows 11 □□ MacOS□ □□□□ □□□□□ Microsoft 365 □□□□ □□□□□□.
□□□□ □□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□?
A. FID02 □□ □□ □
B. Microsoft Authenticator □
C. □□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 132
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.
□□□ □□ □□□ □□□ □□□□□.
User1□ □□ □□□ □□□ □ □□□ □□□□ □□□.
□□□ □□□□□.
□□□ □□□□□.
□□□□ □□□□ □□□□.
□□□ □□□□ □□□□ □□□ □□□□ □□□□□.
□□□□ □□ □□□ □□□ □□□□ □□□.
□□ □□ □□□ User1□ □□□□ □□□?
A. □□□ □□ □□
B. □□ □□ □□ □□□
C. □□ □□ □□ □□□
D. □□ □□ □□ □□□
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365- worldwide

NEW QUESTION: 133
□□□ Contoso.com□□□ □□□ Microsoft Entra ID(Microsoft Entra ID) □□□□ □□□□ □□□□.
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

□□ □□□ □□ □□□□ □□□ □□□□ □□□.
□□ □□: User4□□ ID □□ □□□ □□ Defender□ □□□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 134
□□□□ contoso.com□□□ Microsoft Entra □□□□ Microsoft 365 □□□ □□□□. □□ □□□□ Windows 10 □□□ □□□□ Microsoft 365 □□ □□□□□□. □□ □□□ □□ □□□ □□□□.
contoso.com□ □□□□ □□ □□□□□ □□□ □□□□□ □□□.
□□□ □□□ □□ □□□□ □□ □□ □□□ □□□□ □□□. □□ □□□□ □□□ □□□□ □□□?
A. Microsoft Authenticate □□ □□□□□.
B. Microsoft Entra Connect □□□□□ □□□□□ □□□□□.
C. □□ □□□ contoso.com□ □□□□□.
D. Microsoft Entra □□□□□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 135
Microsoft 365 E5 □□□ □□ Microsoft Defender for Endpoint□ □□□□□. □□□□ Windows 11 □□□ □□□□ □□□□.
□□□ Windows Defender □□ □□□□ □□□□ □□ □□ □□□ □□ □□ □□□ □□□□□ □□ □□□□ □□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□, □□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
Answer Area

Answer:

Answer Area

Explanation:

NEW QUESTION: 136

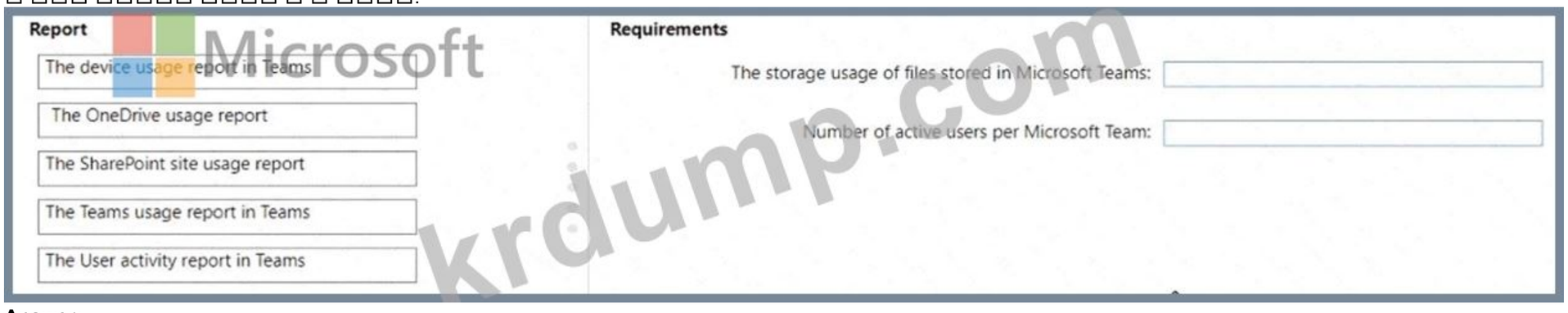
Microsoft 365 □□□ □□□□.

□□ □□□ □□□□□ □□□□ □□□□ □□□.

* Microsoft Teams□ □□□ □□□ □□□ □□□

* □□ □□ □□□ □

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



Answer:

Report

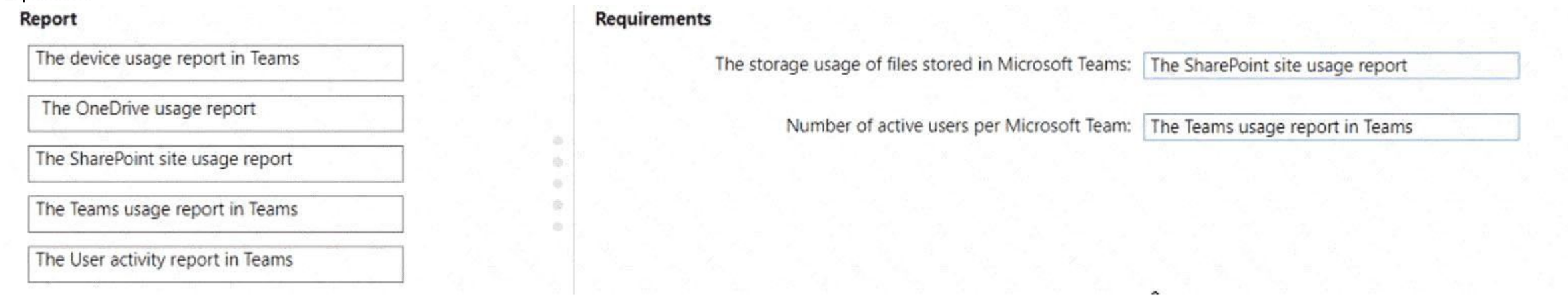
- The device usage report in Teams
- The OneDrive usage report
- The SharePoint site usage report
- The Teams usage report in Teams
- The User activity report in Teams

Requirements

The storage usage of files stored in Microsoft Teams: The SharePoint site usage report

Number of active users per Microsoft Team: The Teams usage report in Teams

Explanation:



NEW QUESTION: 137

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

□ □ □, □□ □□□ Microsoft Entra Connect Health □□□□□ □□□□□□□.

□□ □□□ □□□ □□□□□ □□□□□.

□□□ Server1□□□ □□□ □□□ □□□□□ □□□□□, □□ □□□ Microsoft Entra Connect □□□ □□ □□□ □□□□ □□ □□ □□□□□□.

□□ □□□□ Server1□ □□□□ □□□□ □□□□ □□□ □□□□□□□.

Server1□ □□□ □□□ □ □□□ □□□□ □□□.

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

□□: □□ □□□ 1□□□□.

A. Server1□□ Microsoft Entra Connect Health Services □□ □□□ □□(□□ □□)□□ □□□□□.

B. Server1□□ Microsoft Entra Connect Health □□□□□ □□ □□□□□□.

C. Server1□□ Microsoft Entra Connect Health Services □□ □□□ □□□□ □□□□□.
D. Windows PowerShell□□ Rejister-ArureADConnectHealthsyncAgent cmdlet□ □□□□□.
E. Azure □□□□ □□□ Connect-Microsoft Entra ID cmdlet□ □□□□□.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 138
□□□ □□□□□□ □ □□ Active Directory □□□□□ □□□□. □□□□ □□□ □□□□ □□ □□□ □□□□.
Microsoft Entra □□□□ □□□□.
□-Ł□□□□ Active Directory□ Microsoft Entra □□□□ □□□□□□ □□□.
□□□ □□□□ □□□□ □□□. □□□□ □□ □□□ □□□□□□ □□□□ □□□ □ □□ □□□ □ □□ □□□ □ □□□ □□ □□□.
□□□□□ □□□ □□□□ □□□?
A. □□□□ □□□ □ □□ Microsoft Entra Connect □□□ □□□ □□□ Microsoft Entra Connect □□□ □□
B. □□□□ □□□ 6□ Microsoft Entra Connect □□□ □□□ 3□ Microsoft Entra Connect □□□ □□
C. □□□ Microsoft Entra Connect □□□ □□□ □□□□ □□□ □□□ Microsoft Entra Connect □□□ □□
D. 3□□ Microsoft Entra Connect □□□ □□□ □□□□ □□□ 3□□ Microsoft Entra Connect □□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 139
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
□□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft Entra □□□□ □□□□□.
□□ □□□□ □□□□ Microsoft Entra □□□□ □□□□□□ □□□□□.
□□ □□(OU)□ 10□ □□□ □□□ Microsoft Entra □□□□ □□□□□ □□ □□ □□□□□□. □□ □□ □□□ □□□ □□□□□ □□□□□□□□.
Microsoft Entra Connect Health□ □□□ □□ □□ □□□ □□ □□□□ □□□□□ □□□□□□ □ □ □□□□.
10□□ □□□ □□□ Microsoft Entra □□□□ □□□□□□□ □□□□ □□□.
□□ □□: Microsoft Entra Connect□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 140
□□ □□ □□□ □□□ □□□ Microsoft 365 □□□ □□□□.

Name	Operating system	Microsoft Intune
Device1	Windows 11 Enterprise	Enrolled
Device2	iOS	Enrolled
Device3	Android	Not enrolled

□□ □□□ Microsoft Word□ □□□□□.
□□ □□ □□□ □□□□□ □□□ □□□ □□□□□.
* Windows □□□ □□□□ □□ Word □□□ □□□□ □□□□□□ □□□.
* Android □□□ □□□□ Word□□ □□ □□□□ □□ □□□ □□□□ □□□.
* iOS □□□ □□ □□□□ □□ □□ □□ □□ □□□□□□ □□□□ Microsoft 365□ □□□□ □□□□ □□□□ □□□.
□ □□□ □□ □□□ □□□/□ □□□□ □□□? □□□□ □□□ □□ □□□ □□□ □□□ □□□□□□. □ □□ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □□□ □□□□□□ □□□□□ □□□□ □ □ □□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 141

Microsoft 365 E5 □□□ □□□□.
□□ □□□□ Mac □□□□ □□□ □□□□. □□ □□□□ Microsoft Endpoint Manager□ □□□□ □□□ Microsoft Defender Advanced Threat Protection(Microsoft Defender ATP)□ □□□□□ □□□□.
□□□□□ Microsoft Defender ATP□ □□□□ □□□.
Endpoint Management □□ □□□□ □□□ □□□□ □□□?
A. □□ □□ □□□
B. iOS □□□□ □□
C. Microsoft Defender ATP □□ □□□
D. □□□ □□ □□(MDM) □□ □□ □□□
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

NEW QUESTION: 142
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □ □, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Windows 10□ □□□□ □□□□ □□□□.
□□□ Windows 10 □□□ □□□□ □□□.
□□ □□: □□ □□□ □□□□ □ □□□ □□□□ □□□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 143
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□ □□□□.

Name	Assigned role
Admin1	Security Administrator
Admin2	Security Operator
Admin3	Security Reader

Microsoft Entra ID Protection□ □□□ □□□□□.
□□□ □□ □□□ □□ □□ □□□ □□□□ □□□□ □□□□ □□□□□?
A. Admin1 □ Admin3□
B. Admin1□
C. Admin2□
D. Admin1 □ Admin2□
E. □□□1, □□□2, □□□3
Answer: A (LEAVE A REPLY)

NEW QUESTION: 144
contoso.com□□□ Microsoft Entra □□□□ □□□ 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□ □□ □□ □□(PI)□ □□□ □□□ □□ □□ □□□□□ □□□□ □□□□ □□ □□□□□ □□□□□.
User!□ PII□ □□□ □□□ □□ □□□□□ □□ □ □□□□?

A. □□□2□ □□□3□ □□

B. □□□2, □□□3, □□□4, □□□5

C. User2only

D. User2, User3, User4□ □□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 145

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

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

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

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:

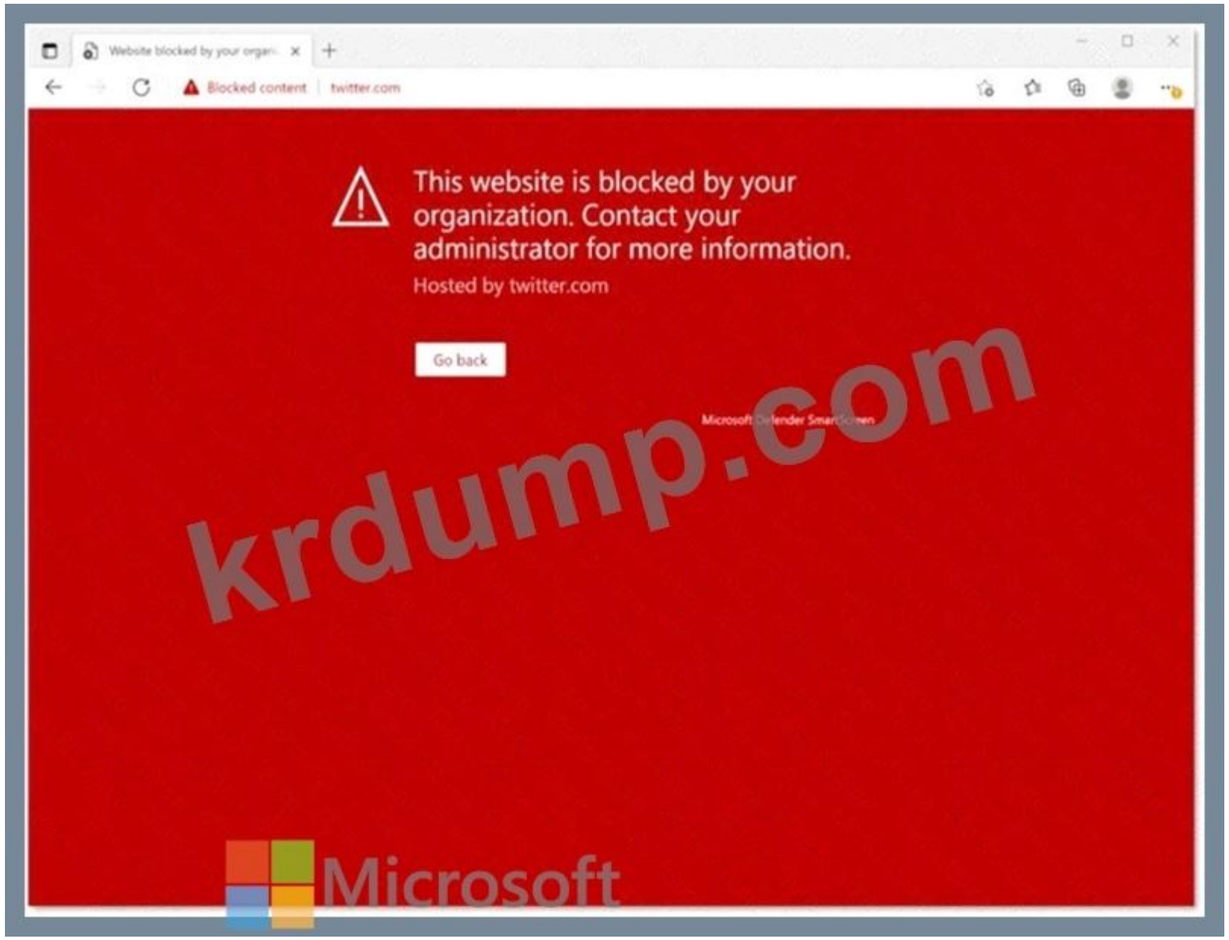
Answer Area

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:

NEW QUESTION: 146
Microsoft Defender for Endpoint□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□□ □□□ □□□ □□□ □□□□□ □□ □□ □□□ □□ □□□□ □□□□□.

□□□ □□ □□□ □□ □□□ □□□□ □□□□□ □□□.
□□ Microsoft Defender for Endpoint □□□ □□□□ □□□?
A. □□ □□
B. □□ □□
C. □□□ □□ □□
D. □□□□
E. □□
Answer: E (LEAVE A REPLY)



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: 147

□□: □ □□□□ □□□ □□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.
□ □□□ □□□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□ □□□□ □□□.
□□□ □□ □ □ □□□ □□□□ □□□ □□□ □ □□□□.
□□□ □□ □□□ □ □□ □□ □□□ □□□□ □□ □□ □□□□.
□ □□□ □□□ □□ □□□ □□□ □ □□□□.
□□□□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Microsoft 365 E5 □□□ □□ Office 365□ Microsoft Defender□ □□□□ □□□□.
□□, □□, □□□□□□ □□□□ □□ □□ □□ □□ □□ □□□□ □□□□ □□ □□□ □□□□ □□□.
□□□: □□□ □□ □□□ □□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

NEW QUESTION: 148
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□(MFA)□ □□□□□ □□□.
□□□□ □□ □□ □□□ □□□□ □□□. □□□□ □□□□□ MFA□ □□□□ □□□□ □□□ □□□ MFA□ □□□ □□□□□□ □□□ □□□□□ □□ □□□.
□□□ □□□□ □□?
A. Microsoft □□□
B. □□
C. FID02 □□ □
D. □□□□
E. □□□ OTP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 149
□□: □ □□□□ □□□ □□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□ □□□□ □□□.
□□□ □□ □ □ □□□ □□□□ □□□ □□□ □ □□□□. □□□ □□ □□□ □ □□ □□ □□□ □□□□ □□ □□ □□□□.
□ □□□ □□□ □□ □□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Microsoft 365 E5 □□□ □□ Office 365□ Microsoft Defender□ □□□□ □□□□.
□□, □□, □□□□□□ □□□□ □□ □□ □□ □□ □□ □□□□ □□□□ □□ □□□ □□□□ □□□.
□□□: □□□ □□ □□ □□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 150
□□□ □□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Name	Email	Role
Admin1	Admin1@contoso.com	Password Administrator
Admin2	Admin2@contoso.com	Security Reader
Admin3	Admin3@contoso.com	User Administrator
User1	User1@contoso.com	*None*

Microsoft Entra ID Protection□ □□□□ □□□□.
'□□□ □□ □□□ □□ □□' □□□□ □□ □□□ □□□□□.
* □□□: Admin1
* □□□ □□ □□□ '□□' □□□ □□ □□ □□

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

Time	Detected risk level
1:00 PM	Low
2:00 PM	Medium
3:00 PM	Medium
4:00 PM	High

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

Answer:

Explanation:

Statement

Answer

By the end of the day, Admin1 has received two email alerts.

No

By the end of the day, Admin2 has received three email alerts.

Yes

By the end of the day, Admin3 has received three email alerts.

No

Microsoft Entra ID Protection sends Users at risk detected email alerts when a user's risk level reaches the configured threshold. Here, the threshold is Medium or above, so the 1:00 PM Low risk event does not generate an alert. The 2:00 PM Medium event generates one alert, the 3:00 PM Medium event generates another because Microsoft states that later risk detections can trigger additional emails even if the recalculated risk remains at the configured level, and the 4:00 PM High event generates a third alert because it is still above the configured threshold. Microsoft also states that extra emails are suppressed only within a five- second period; these events are one hour apart, so that suppression rule does not reduce the count.

Admin1 receives the alerts because Admin1 is explicitly configured as a recipient, but the statement says two alerts; the correct count is three, so it is No. Admin2 receives three alerts because Security Reader users are automatically included by default for ID Protection notifications when they have a valid email or alternate email. Admin3 does not receive the alerts because User Administrator is not one of the automatically included roles and is not configured as a recipient.

NEW QUESTION: 151
Microsoft Store for Business□ □□□□ □□□. □□ □□□□ □□□□ □□ □ □□□?
A. □□□2
B. □□□3
C. □□□4
D. □□□5
Answer: C (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

NEW QUESTION: 152
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□□ □□□.
□□ □□□□ □□ □□□□ □□□□ □□□□ □ □□□ □□(MFA)□ □□□□ □□□.
□□□□ □□□ □□□□ □□□□ □□□□□ □□□□ □□ □□□□ □□□□ □□□□ □ □□□ □□□.
□□□ □□□ □□ □□□□ □□□□ □□ □□□□ □□□□ □□□□□ □□□.
□□□□ □□ □□□ □□□□□ □ iOS □□□□ □□□□□ □□□□ □□□□ □□□.
□□ □□ □□□□ App1□□□ Microsoft Entra ID □□□□□□ □□□□□□□ □□□□ □ □□□ □□□. □□ □□ □□□□ App1□ □□□□ □ □□□ □□□□ □□□.
□□□ □□□ □□□ □□ □ □ □□ □□□□ □□□?
A. 3
B. 4
C. 5
D. 6
E. 7
F. 8
Answer: B (LEAVE A REPLY)
* Only users in the finance department must be able to sign in to an Microsoft Entra ID enterprise application named App1. All other users must be blocked from signing in to App1.
One Policy.
* Only users in the R & D department must be blocked from signing in from both Android and iOS devices.
One Policy.
* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.
All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.
One policy
* All users must be blocked from signing in from outside the United States and Canada.
Only users in the R & D department must be blocked from signing in from both Android One Policy Reference:

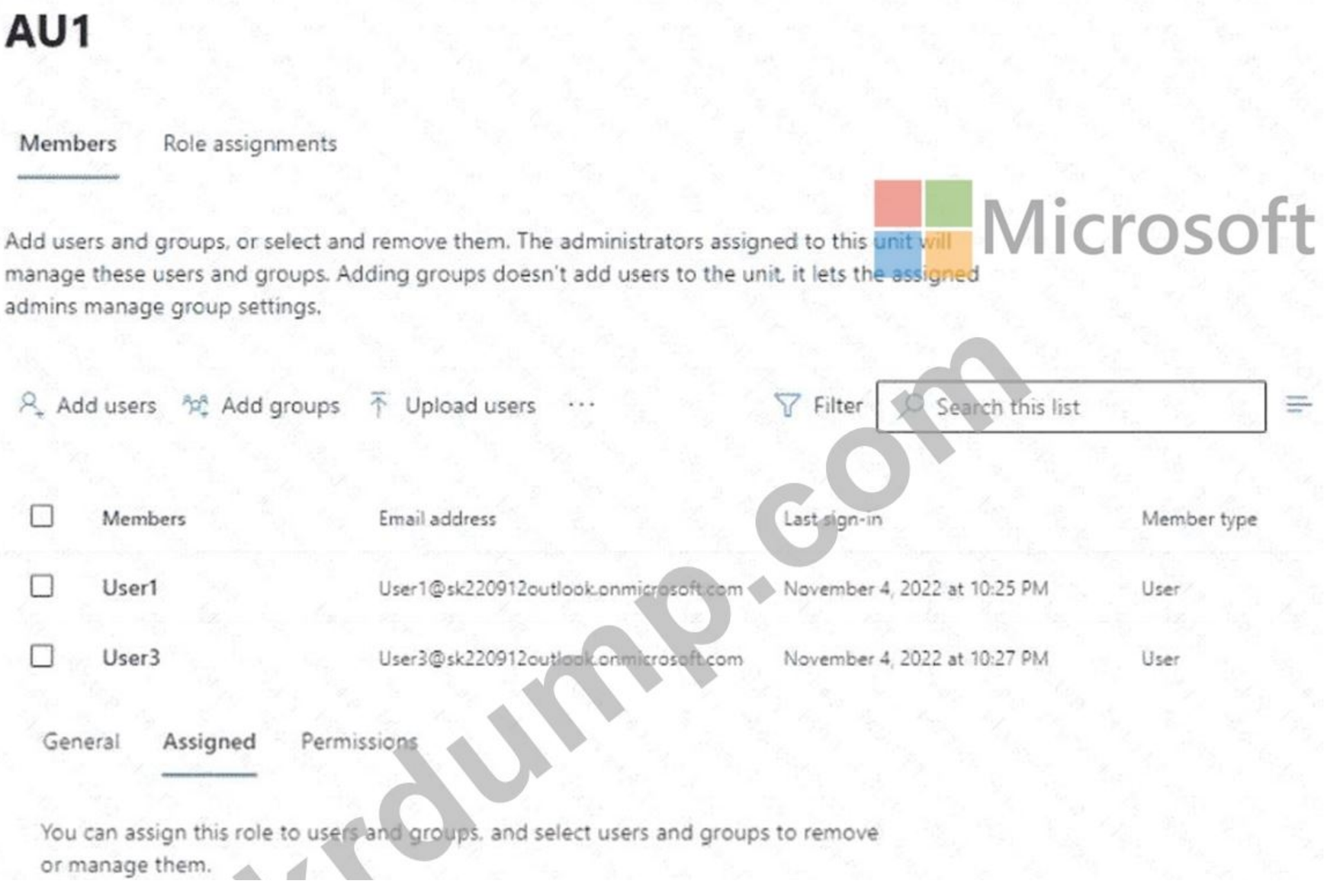
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

NEW QUESTION: 153

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

Name	Member of
User1	Group1
User2	Group2
User3	None

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



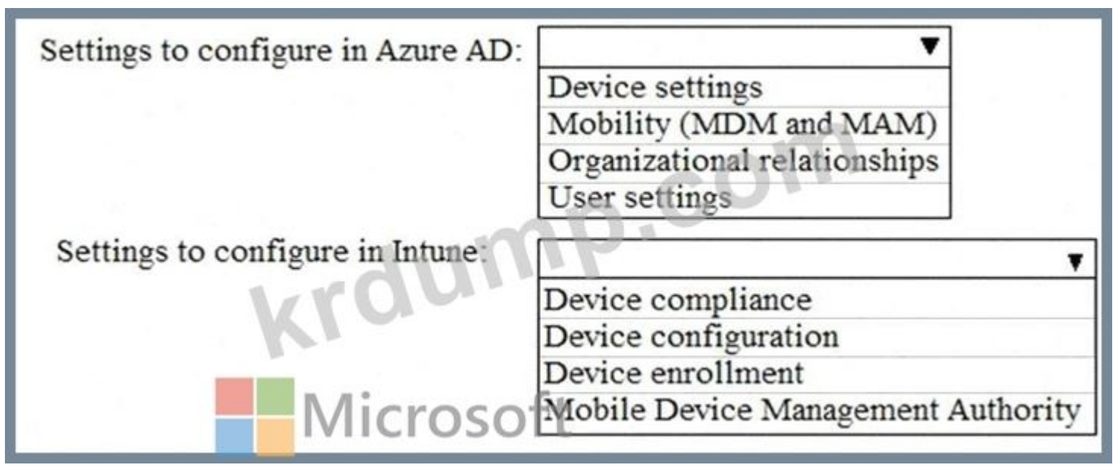
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

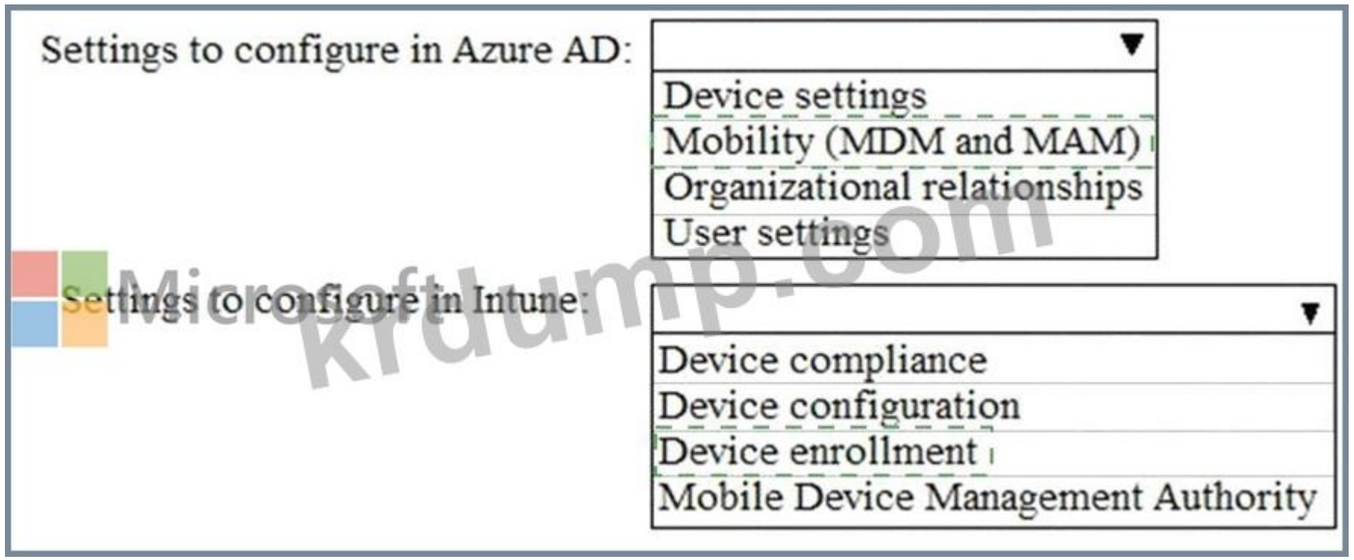
Explanation:

NEW QUESTION: 154
Microsoft Defender XDR□ □□□□ Microsoft 365 □□□ □□□□.
Microsoft Defender □□□ □□ □□□□ □□□ □□□ ' □=□□□ □□ □□□ □□ □□ □□'□ □□□□□.
□□□ □□ □□□ □□□□□□ □□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□ □□□ □□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. \program files (X86) \" □□□□ □□□ □□□□ □□□ □□□□ □□□□□.
B. □□ □□□ □□ □□□ □□□ □□□□□.
C. \windows\ □□□□ □□□ □□□□ □□□ □□□□ □□□□□.
D. \users\"\downloads\" □□□□ □□□ □□□□ □□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)

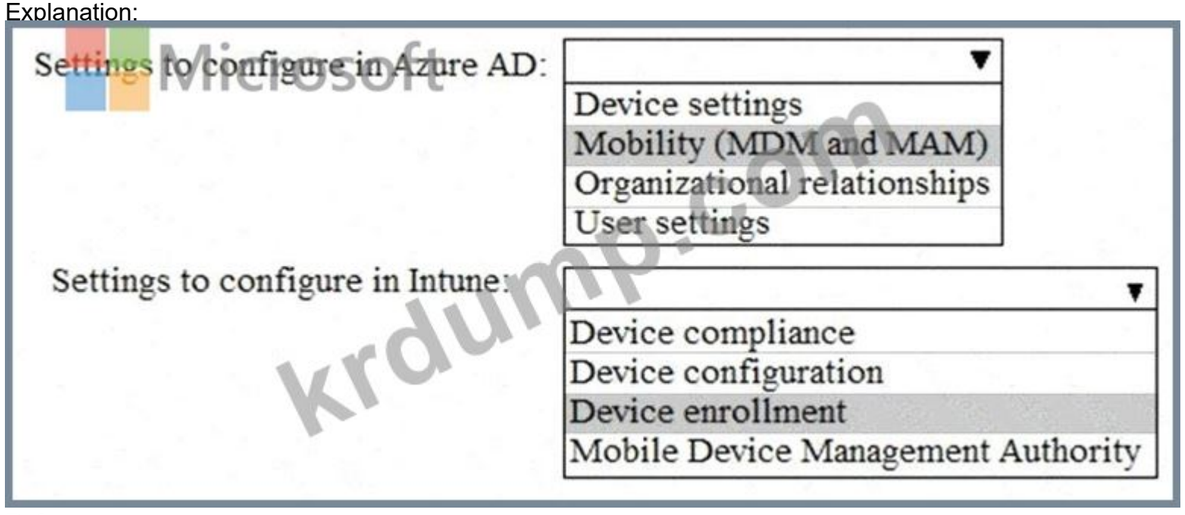
NEW QUESTION: 155
Windows 10 □□□ □□ Intune □□ □□□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



References:

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

NEW QUESTION: 156

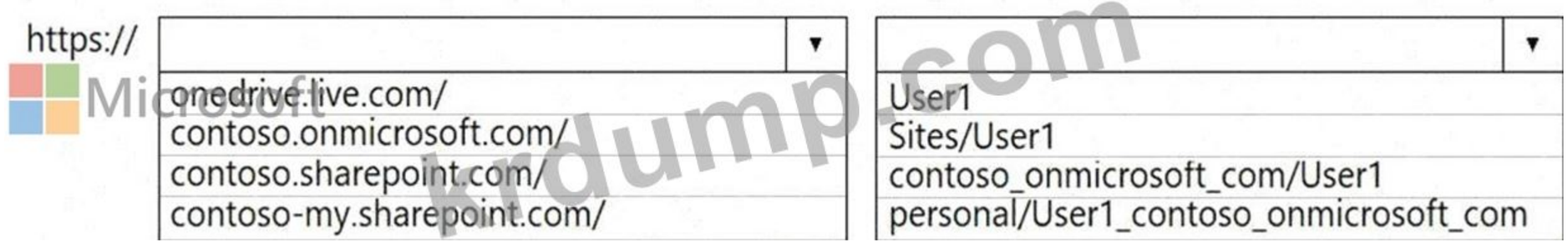
contoso.onmicrosoft.com□□□ Microsoft Entra ID □□□□ □□□ Microsoft 365 □□□ □□□□.

User1□□□ □□□□ Microsoft OneDrive□ □□□ □□□□□.

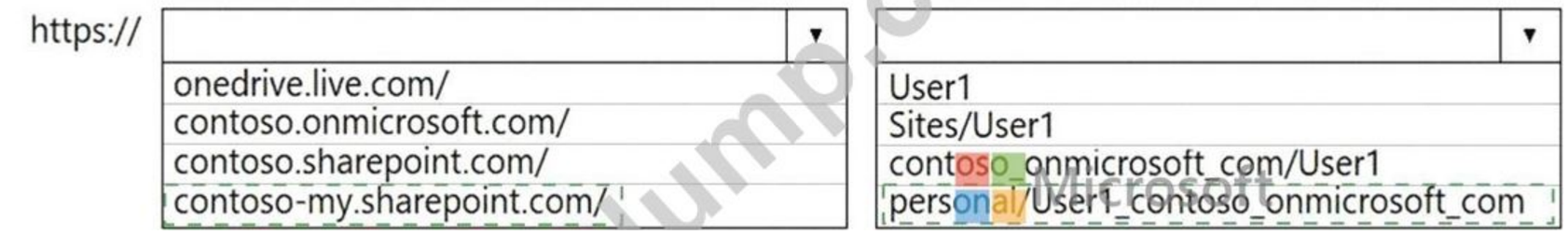
User1□ OneDrive □□ □□□□ eDiscovery □□ □□□□ □□□□ □□□.

eDiscovery □□□ □□ □□ URL□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds

NEW QUESTION: 157

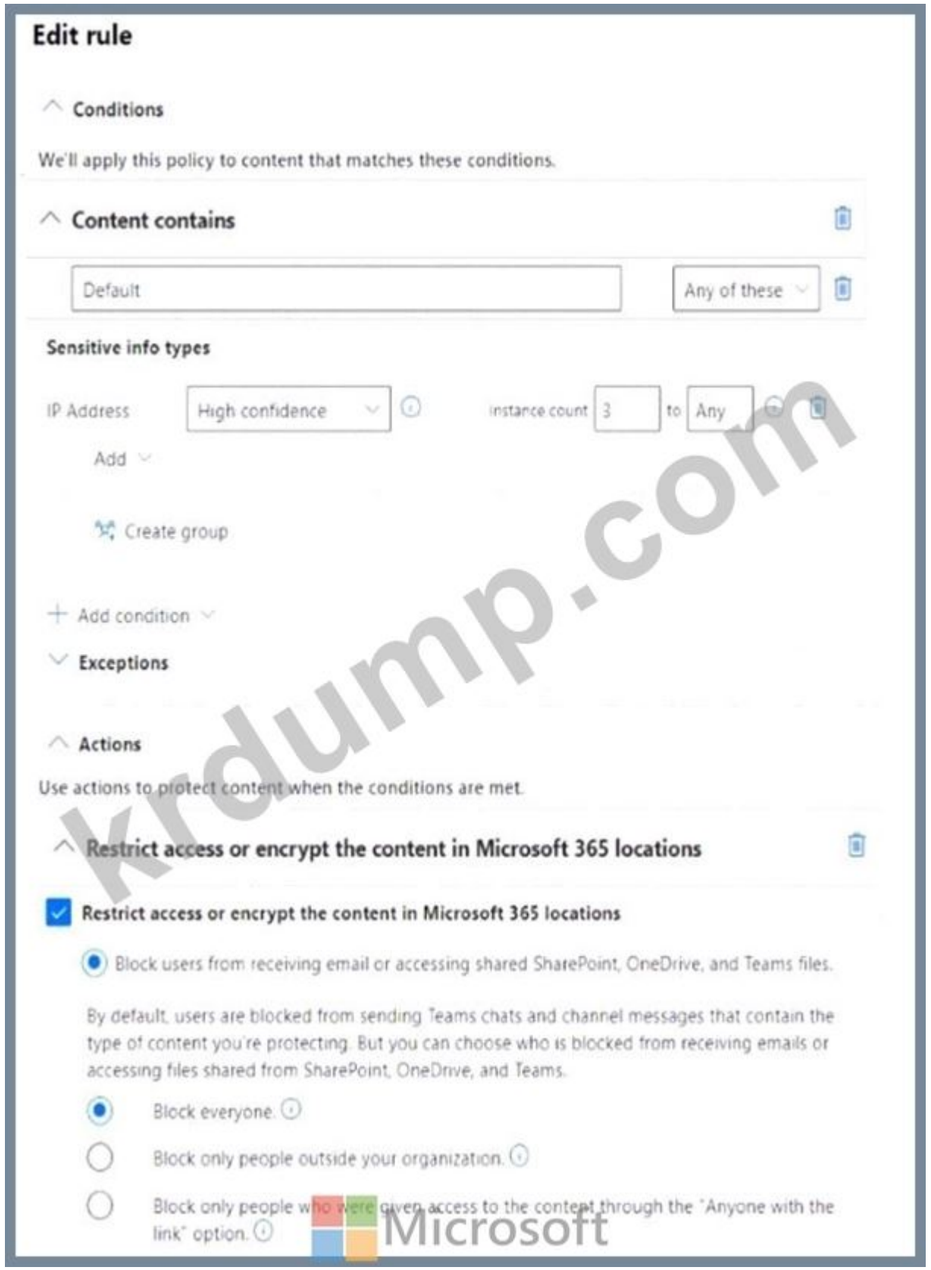
Site1□□□ SharePoint □□□□ □□□ Microsoft 365 E5 □□□ □□□□. Site1□□ □□ □□ □□□ □□□ □□□□ □□□□.

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: No

User2 can open File1: Yes

Admin1 can open File2: Yes

User1 can open File2: No

The 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: Yes

File1 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: Yes

Admin1 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: 158

□□□□□□ □□□□□ Active Directory Domain Services(AD DS) □□□□ □□□□ □□□□.

□□□□ □□□□□ Microsoft 365 □□□ □□□□. □ □□□□ Microsoft Exchange Online□ □□□□ □□□□ □□ □□□ 500□□ □□□□ □□□□.

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

* □□□□ □□ □□□□ SSPR□ □□□ □ □□□ □□□.

* □□□□□ □□□□ □□□□ □□□ □□□□ SSPR □□□ □□□ □ □□□ □□□.

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

□ □□ □□□ □□ □□□□□ □□□□ □□□?

Answer:

Explanation:

The cloud-only users must be able to use SSPR.

Microsoft 365 Business Standard

The hybrid users must be able to use SSPR with password writeback to the domain.

Microsoft Entra ID P1

For cloud-only users, the lowest suitable option in the list is Microsoft 365 Business Standard. Microsoft states that basic SSPR capabilities are available in Microsoft 365 Business Standard or higher, and the licensing comparison shows cloud-only user password reset is supported by Microsoft 365 Business Standard, Business Premium, and Microsoft Entra ID P1 or P2. Since the requirement is only for cloud-only SSPR, assigning a higher Entra ID P1 or P2 license would increase cost unnecessarily.

For hybrid users who must reset passwords with password writeback to the on-premises AD DS domain, the correct minimum license is Microsoft Entra ID P1. Microsoft's licensing table identifies hybrid user password change or reset with on-premises writeback as supported by Microsoft 365 Business Premium and Microsoft Entra ID P1 or P2, and Microsoft explicitly warns that standalone Microsoft 365 Basic and Standard plans do not support SSPR with on-premises writeback.

Therefore, Business Standard is enough for cloud-only users, while Entra ID P1 is the least-cost dedicated license for hybrid SSPR with writeback. Microsoft Entra ID P2 is unnecessary because risk-based identity

protection features are not required.

NEW QUESTION: 159
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: 160
Microsoft 365 E5 □□□ □□□□.
Endpoint□ Microsoft Defender □□□□ □□□□ □□□.
□□ □□□ □□□□ □□□?
A. Microsoft Purview □□
B. Microsoft Defender □□
C. Microsoft Intune □□ □□
D. Microsoft 365 □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 161
□□□ □□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Name	Role
User1	Security Administrator
User2	Directory Writers
User3	Reports Reader

□□ □□□□ □□ □□ □□□ □□ □□□(SSPR)□ □□□□□ □□ □□□ □□□□ SSPR □□ □□□ □□□□□.
* □□□□ □□□ □□ □: 1
* □□□□ □□□ □ □□ □□: □□ □□
* □□□ □□□ □□ □: 3□
* □□□□ □□□ □□ □: 3□
□□ □□ □□□ □□□□□□.
* □□ □□□□ □□□ □□□□□?
* □ □□□ □□ □□□□ □□□□□?
* □□□ □ □□□□ □□□ □□□□□□?
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

Answer:

Explanation:

Statement

Answer

User1 must correctly answer "In which city was your first job?" to reset their password.

No

User2 must correctly answer "What is your favorite food?" to reset their password.

No

User3 must correctly answer "What was the name of your first pet?" to reset their password.

Yes

Microsoft Entra SSPR applies a different reset policy to accounts assigned Azure/Microsoft Entra administrator roles. Microsoft states that administrator accounts use a strong default two-gate password reset policy, that this policy cannot be changed, and that the policy prohibits security questions. Microsoft's affected administrator-role list explicitly includes Security Administrator and Directory Writers, so User1 and User2 cannot reset their passwords by answering security questions. Therefore, the statements for User1 and User2 are No, even though security questions are enabled for regular users.

User3 has the Reports Reader role, which is not listed in Microsoft's affected administrator-role list for the two-gate administrator SSPR policy. User3 therefore follows the configured user SSPR policy. The tenant requires one authentication method, the only available method is security questions, and the configuration requires three questions to reset. Since exactly three security questions are enabled, User3 must answer all three enabled questions, including "What was the name of your first pet?" Microsoft confirms that SSPR checks whether the user has the required authentication methods according to the administrator-configured policy before allowing password reset.

NEW QUESTION: 162

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

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

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

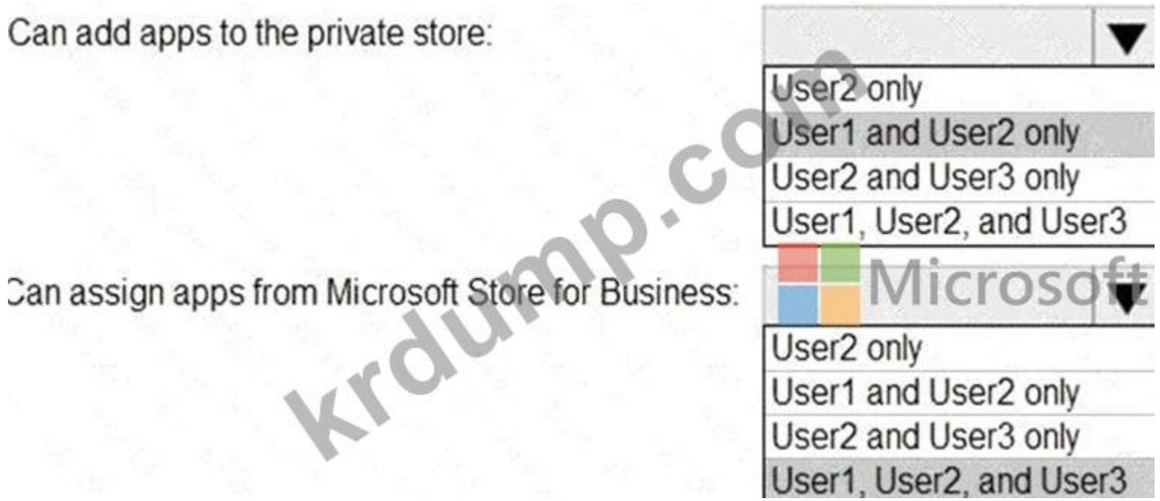
□□ □□ □□□ □□ Microsoft Store for Business □□□ □□□□□ □□□□□.

Name	Role
User1	None
User2	Purchaser
User3	Basic Purchaser

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

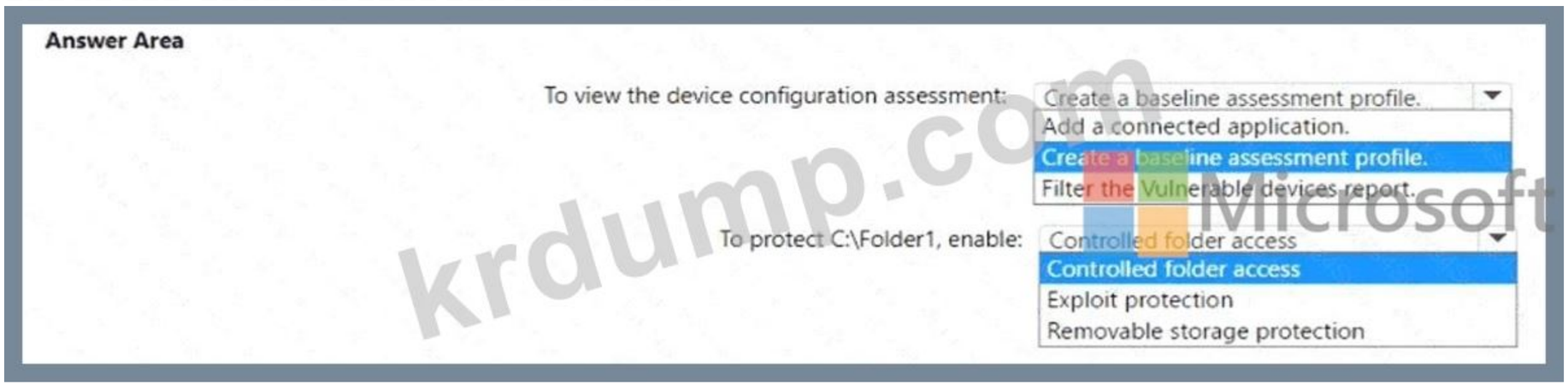
Answer:

Explanation:

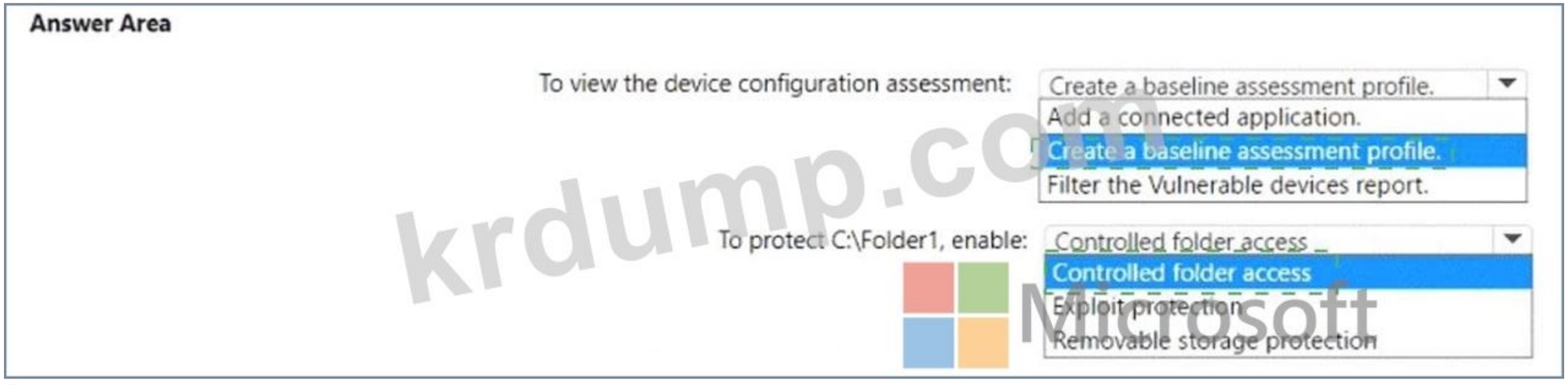


Reference:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business
https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-role

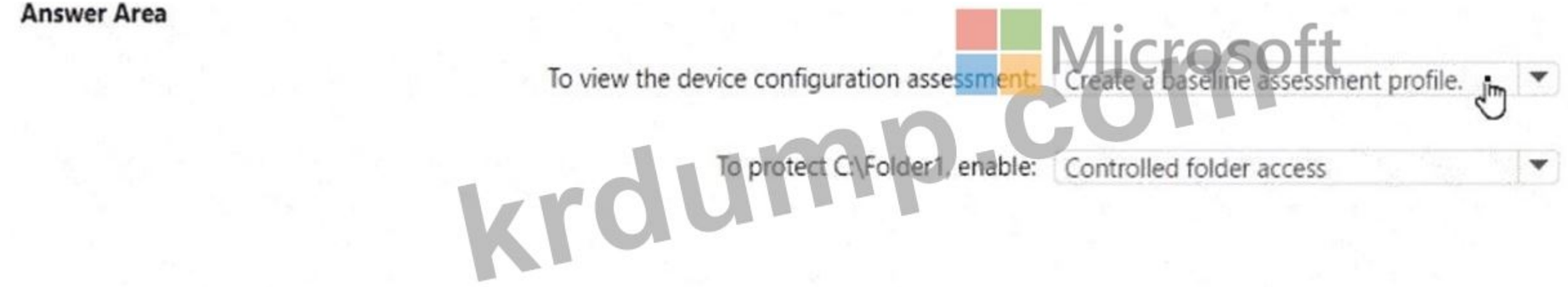
NEW QUESTION: 163
Microsoft 365 E5 □□□ □□□□.
□□ □□□ Windows 11 □□□ Microsoft Intune□ □□□□ □□□□ Microsoft Defender for Endpoint□ □□□□□.
□□ □□ □□□ □□□□ □□□.
* Center for Internet Security(CIS) vl.0.0 □□□□□ □□ □□ □□ □□□ □□□□□.
* □□□□ □□□ □ □□ □□□□□□□ C:\Folder1□□□ □□□ □□□□ □□ □□□□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.



Answer:



Explanation:



NEW QUESTION: 164
Microsoft 365 E5 □□□ □□□□.
□□ □□□ Endpoint□ Microsoft Defender□ □□□□□□.
www.contoso.com□ □□ □□□□□ □□ □□□□ □□□□□ Defender for Endpoint□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□□□: □□□ □□ 1□□□□.
A. □□□□ □□□□□.
B. □□ □□□ □□□□□.
C. □□ □□□ □□□□□□.
D. □ □□□ □□□ □□□ □□□□.
E. □□□ □□ □□□□ □□□□ □□□□□□.
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 165
1,000□□ Windows 10 □□□□□ □□□□ Microsoft 365 □□□□ □□□□. □□□□□ Microsoft Intune□ □□□□ □□□□.
□□ □□□ □□ □□□ □□□ □□ □□□ □□□ □□□.

* □□□ □□□□□ □□□□□.
* □□□ □□□ □□ □□□ □□□□ □□□□□.
* Microsoft Defender Antivirus □□□ □□ □□□ □□□□□□.
□□ □□□ □□□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □ □□ □□
B. □□ □□
C □□ □□ □□□
D □□□ □□□ □□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION: 166
Microsoft 365 E5 □□□ □□□□.
□□□□ □□ Microsoft Defender□ □□□□ □□□□.
□□□ □□□ □ □□□ □□□□ □ □□ □□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. □□ □□
B. □□ □□
C. □ □□ □□
D. □□ □□
E. □□ □□
F. OAuth □ □□
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 167
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: 168
contoso.com□□□ □□□□ □□□ Microsoft 365 ES □□□ □□ □□, user1@contoso.com□□□ □□□□ □□ □□□ □□ □□□ □□□□ Policy1□□□ □ Microsoft Defender(□□ Office 365 □□ □□ □□)□ □□□□□.
Policy1□ usei1@fabunkam.com□□□ □□ □□□□□ □□ □□□ □□□□ □□□□□ □□ □□ □□□□□.
□□□□ □□□□□ □□□□□□ □□□□ □□□.
Policy1□ □□ □□□ □□ □□□?
A. □□□ □□□ □□□□□□ □□□□□.
B. □□□ □□□□ □□□□□.
C. □□□ □□□□□ □□□□ □□□□□
D. □□ □□□ □□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 169
Microsoft 365 □□□□ □□□□.
Microsoft 365 □□ □□□ □□□□ □□□□ □□□□□ □□□ □□□□□.
Microsoft 365 □□ □□□ □□□□ □□□□□ □□ Microsoft □□□ □□□ □□□□□?
A. □□□□□ Microsoft Defender□ □□□□□.
B. Microsoft Purview
C. Azure Arc
D. ID□ □□ Microsoft Defender
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

NEW QUESTION: 170
Microsoft 365 E5 □□□□ □□□□.
ISO 27001:2013 □□□□ □□□□ □□□ □□□□□□ □□□ □□ □□□□ □□ □□□□□.
□□ □□□□ □□□□ □□□.
□□□ □□□□ □□ □□ □□□ □□□□ □□□?
A. CSV
B. XLSX
C. JSON
D. XML
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365- worldwide#export-a-template

NEW QUESTION: 171
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

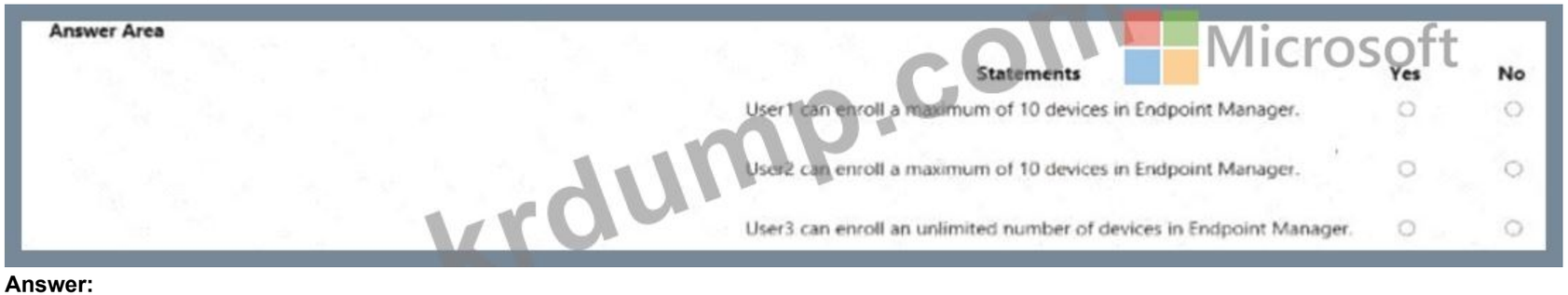
NEW QUESTION: 172
Microsoft Endpoint Manager□ □□ □□□ □□□□ □□□□.
□□□ □□ □□ □□□ □□□□ □□□ Microsoft Entra ID(Microsoft Entra ID) □□□□ □□□□ □□□□.

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

□□□□□ □□□□ □□ □□ □□□ □□ □□ □□ □□□□□.

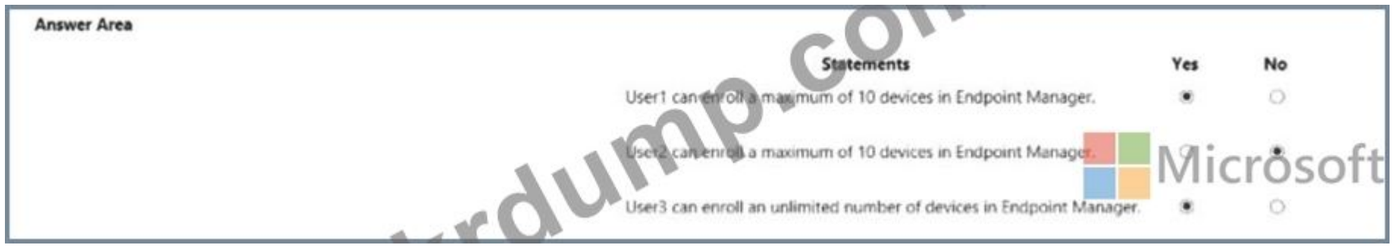
Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All users

□□□□□ □□□□□ □□□□ □□ □□ □□□□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.



Answer:

Explanation:



NEW QUESTION: 173
□□□ 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: 174
Microsoft 365 E5 □□□ □□□□.
Microsoft Teams □□□□ □□□□ □□ □□□□ □□□□ □□ □□□□ DLP1□□□ □ □□□ □□ □□(DLP) □□□ □□□□. □□ □□ □□□□□ DLP1□ □□□□□.
□□□ □□□ User1□ □□ □□□ □□□ Teams □□□□ □□ □□□□ □□□ □ □□□ □□□□□.
User1□ Teams□ □□□□ 1:1 □□□□ □□ □□□□ □□□ □□□□ □□□ □□, □□□□ □□□□ □□□□□.
□□ □□□ □□□ Teams □□□□ User1□ □□ □□□□ □□□□ □□□□ □□ □□□.
□□□ □□ □□□?
A. DLP1□ □□ □□□ □□□□□.
B. DLP1□ □□ □□□ □□□□□.
C. User1□ □□□ □□□□□ □□□□□.
D. □□□ □□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 175
Project1□ □□□ □□□□□ □□□□ □□□□.
□□□□□ □□□ □□□ □□□□ □□ □□ DNS □□□□ □□□□ □□□ □□□□ □□□.
□□ DNS □□□□ □□□□ □□□?
A. □□□(A)
B. □□□ □□
C. □□□(TXT)
D. □□(CNAME)

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

NEW QUESTION: 176
□□□□ □□□□□ □□□ □□□□ □□ □□□□□□□ □□□□ □□□□ 10,000□ □□□□.
Microsoft 365 □□□ □□□□ □□□□ □□□□□ □□□□□□□ □□□□□.
□□□□ □□□□ □□□ □□□□□□.
□□□ □□ □□□ Microsoft Entra ID□ □□□□□ □□□□□□ □□□.
□□ □□□ □□□ Microsoft Entra ID□ □□□□□ □□ □□ □□□□□□.
□ □□□ □□□ □□ □□□□ □□□.
□□□ □□ □□□?
A. Active Directory □□ □□□□ □□ □□□□ □□□ □□ □□□ □□□ □□□ □□□□□.
B. idfix.exe□ □□□ □□ □□□ □□□□□.
C. Windows PowerShell□□ start-AdSyncSyncCycle -PolicyType Delta □□□ □□□□□.
D. idfix.exe□ □□□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Microsoft Entra ID. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Microsoft Entra ID.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for-synch-with-idfix

NEW QUESTION: 177
□□□□□□ Active Directory □□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□□□□ □□□ □□□□□ □□□ □□□ □□□ □□□□ □□□□□.
□□□□ □□□□ □□□□□ □□□ □□□□□□.
□□□□ □□ □□□ □□□□□.
* □□□□□□□□□□

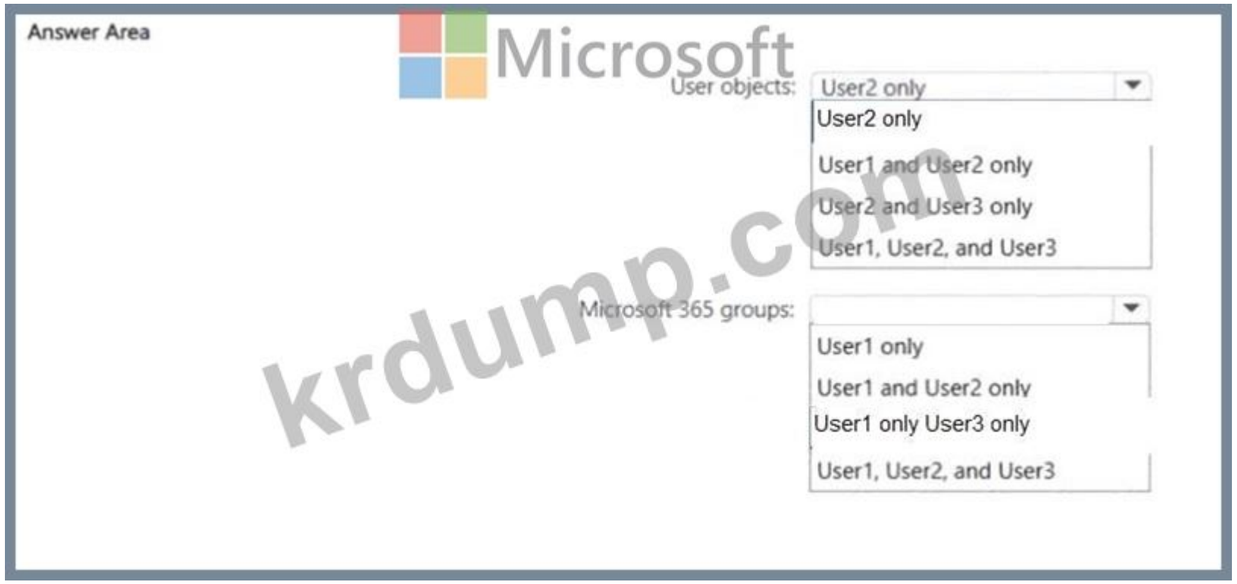
* □□□□□
□□□□ □□□□ □□□□□ □□□□□□ □□□□ □□□.
□□□ □□□□ □□ □□ □□ □□ □□□ □□□□?
A. □□□□□ Azure □□□ □□□ IP □□ □□□ □□□□□ □□□ □□□□□.
B. □□□□□ □□□□ □□□□□ □□□ □□□ □□□□□.
C. Microsoft Entra Connect□□ □□□ □□ □□□ □□ □□□ □□□□□.
D. □□□□ □□□□ Microsoft Entra Connect Sync □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 178
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

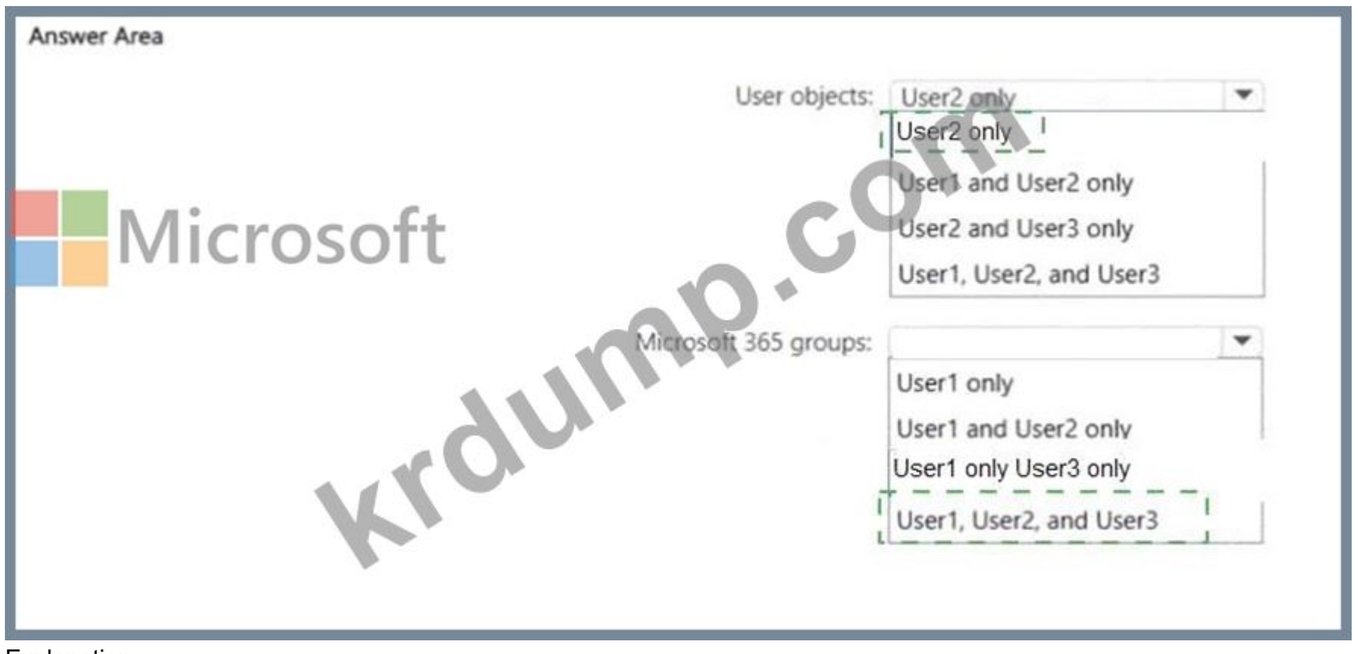
NEW QUESTION: 179
□□□ □□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Name	Assigned role
User1	Groups Administrator
User2	User Administrator
User3	Teams Administrator

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



Answer:



Explanation:

NEW QUESTION: 180
Microsoft Intune□ □□□□ Microsoft 365 E5 □□□□ □□□□.
□□□□ Intune□ □□□ □□□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□ □□ □□□
C. □□ □□□□
D. □□ □□ □□
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

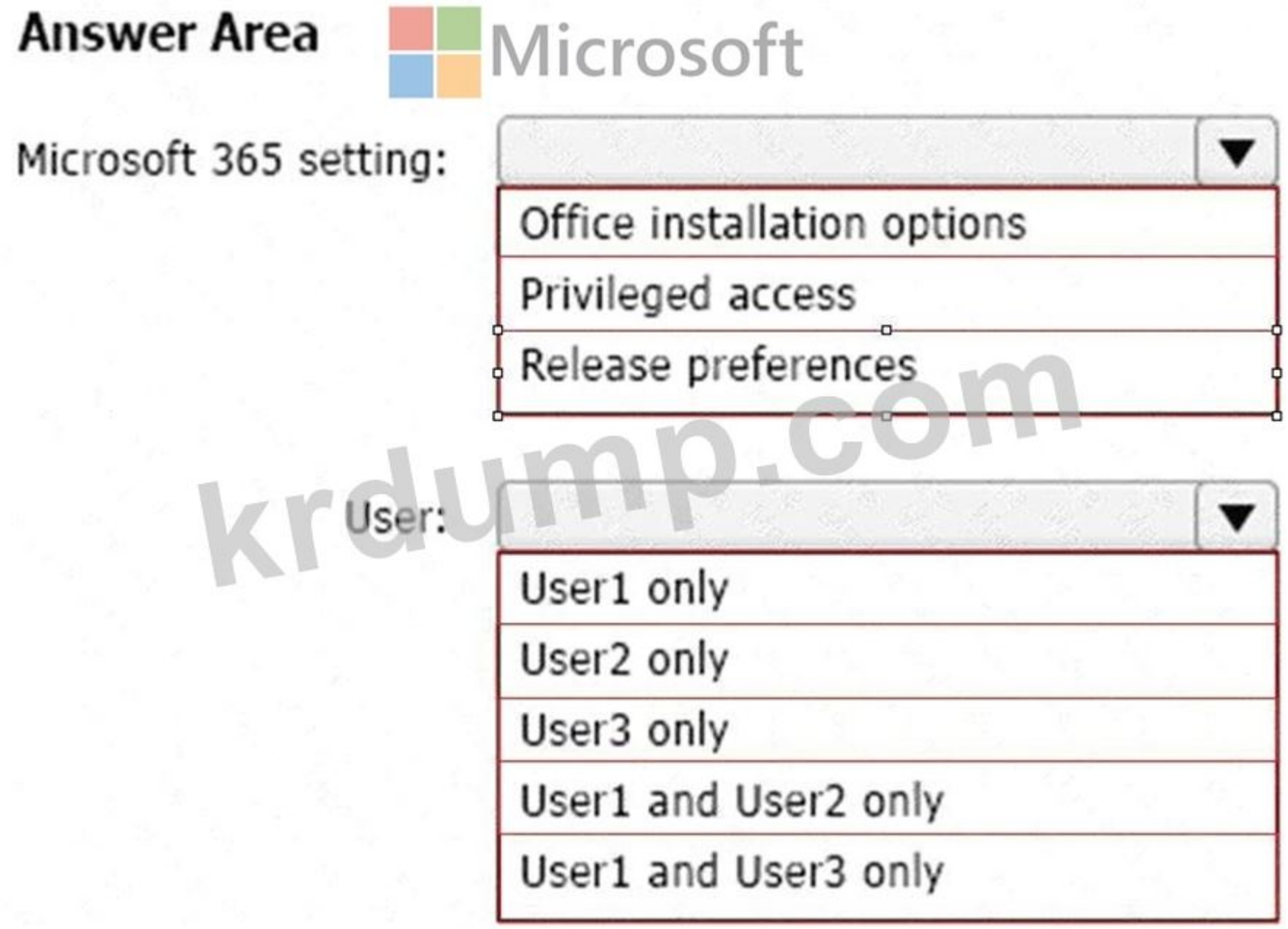
NEW QUESTION: 181
Microsoft 365 □□□ □□□□.
Microsoft Purview Privileged Access Management□ □□□□□ □□□.
□□ Microsoft Office 365 □□□□□ □□ □□ □□□□ □□□□□?
A. Microsoft Exchange Online□ □□
B. Microsoft Teams□ □□
C. Microsoft Exchange Online □ SharePoint Online□ □□
D. Microsoft Teams □ SharePoint Online□ □□
E. Microsoft Teams, Exchange Online □ SharePoint Online
Answer: A (LEAVE A REPLY)
Privileged access management
Having standing access by some users to sensitive information or critical network configuration settings in Microsoft Exchange Online is a potential pathway for compromised accounts or internal threat activities. Microsoft Purview Privileged Access Management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. Instead of administrators having constant access, just-in-time access rules are implemented for tasks that need elevated permissions. Enabling privileged access management for Exchange Online in Microsoft
365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.
Note: When will privileged access support Office 365 workloads beyond Exchange?
Privileged access management will be available in other Office 365 workloads soon.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management-solution-overview
https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management

NEW QUESTION: 182
□□□

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

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

User4□□ Microsoft 365 □□ □ □□□ □□□□□ □□ □□ □□□ □□□ □□□ □□□□□.
□□ Microsoft 365 □□□ □□□□ □□□, □□□ □□ □□□□ □□□ □□□ □ □□□ □□□□ □□□.
□□□□ □□ □□□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□



Answer:

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

Explanation:

Answer Area

Microsoft 365 setting:

- Office installation options
- Privileged access
- Release preferences

User:

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

NEW QUESTION: 183

□□□

Microsoft 365 E5 □□□ □□□□.

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

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

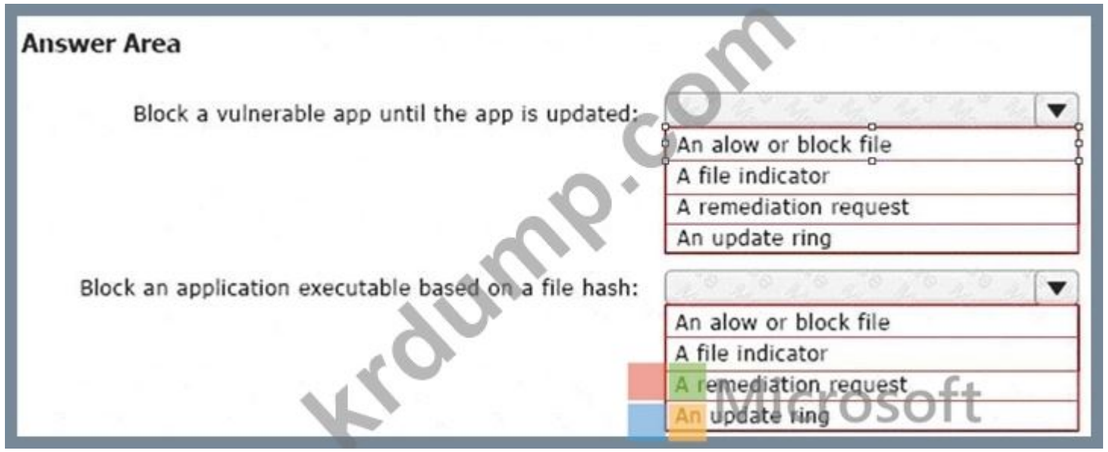
* □□ □□□□□ □□□ □□□ □□ □□□□□.

* □□ □□□ □□□□ □□□□□□ □□ □□□ □□□□□.

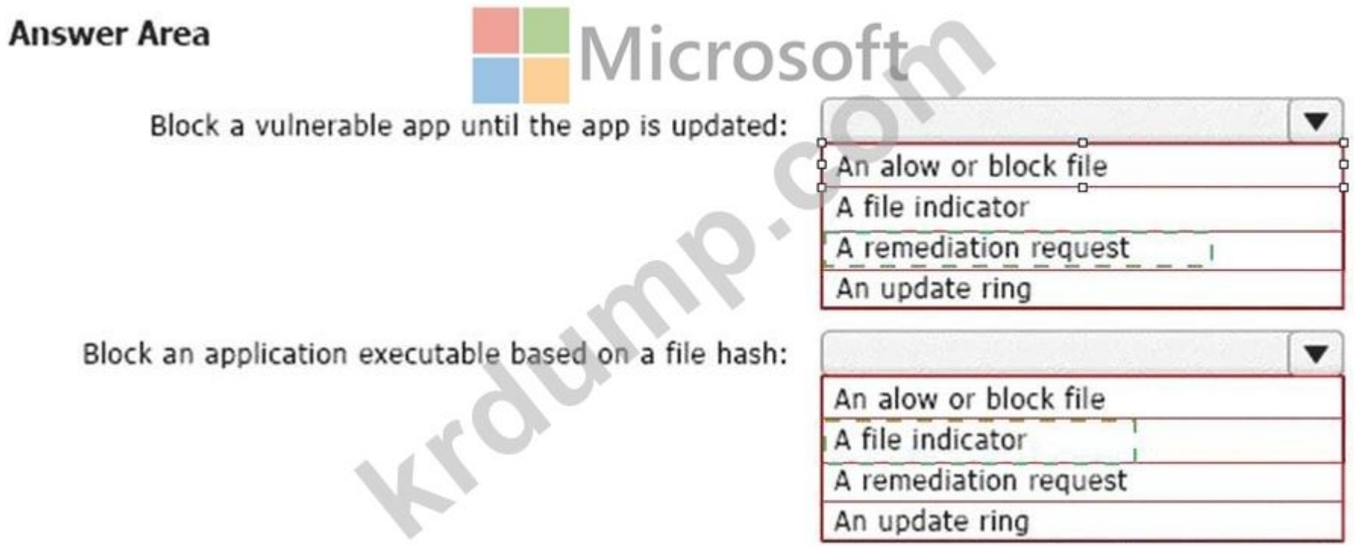
□□□□ □□□ □□□ □□□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.

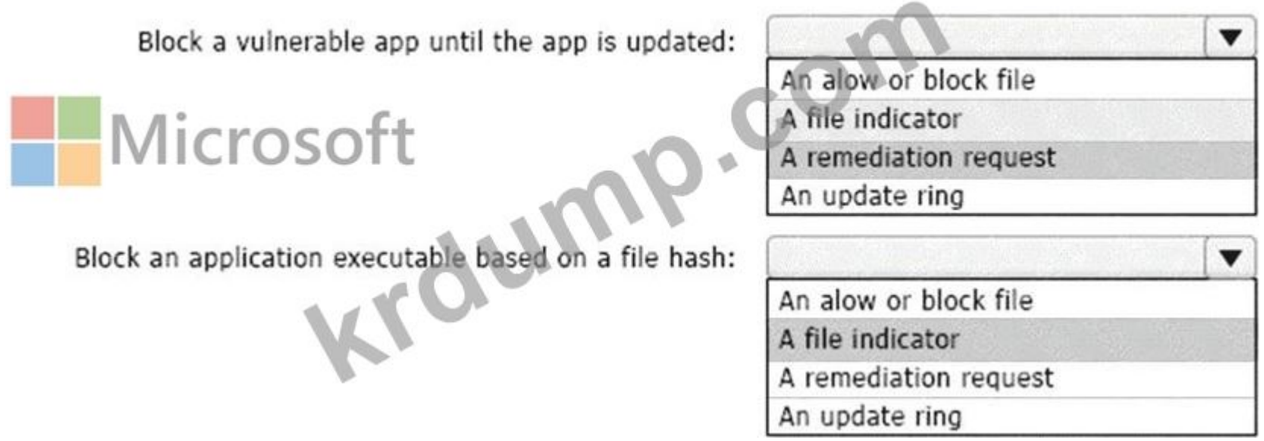


Answer:



Explanation:

Answer Area



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 Defender XDR 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: 184

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

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

□□ cmdlet□ □□□□ □□□?

A. □□□□ □□

B. Execute-AzureAdLebelSync

C. □□□ □□ □□

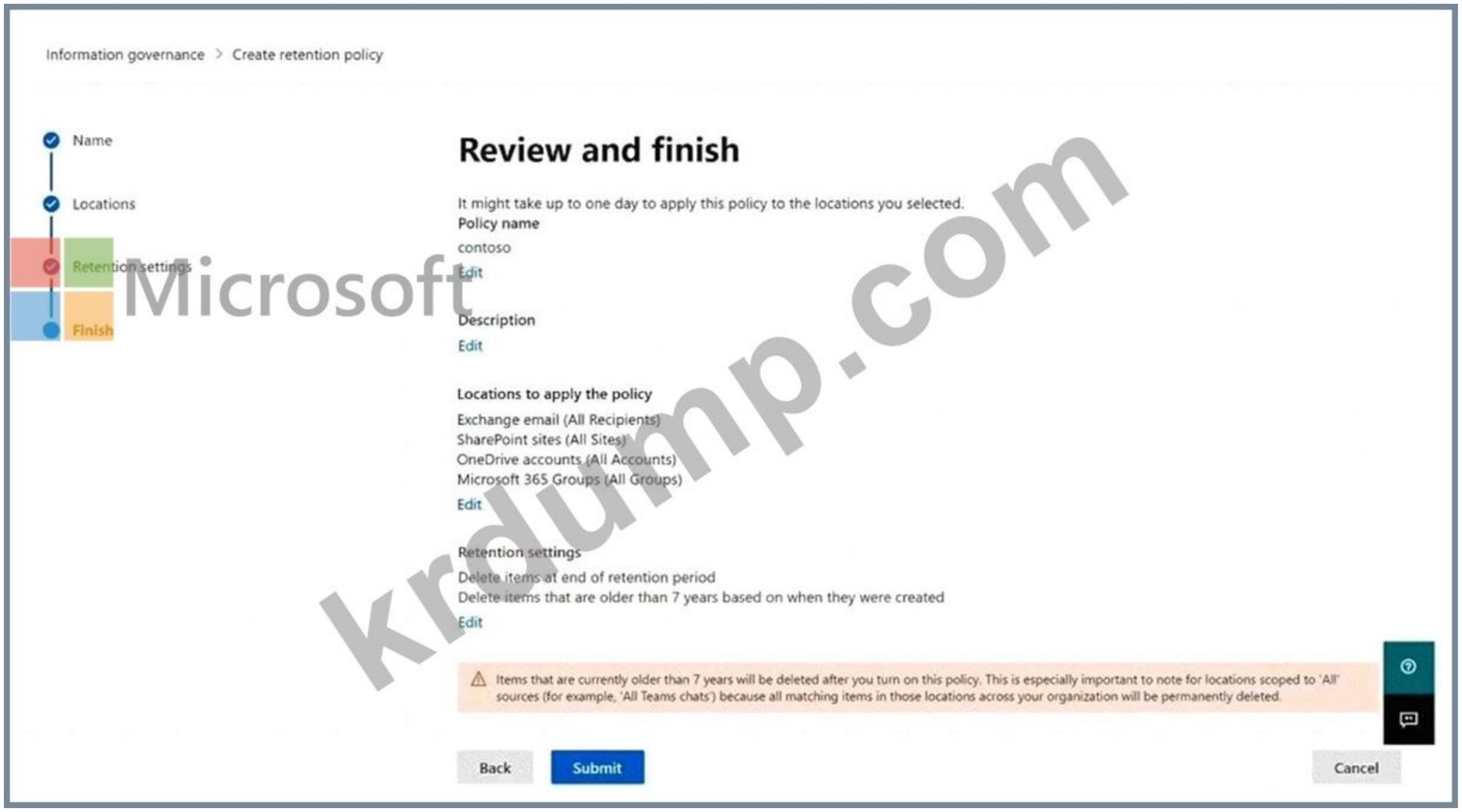
D. □□□□□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 185
Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□□ □□□□ □□, □□ □□ □□□ □□□ □□ □□□□ □□□.
□□ □□□ □□□□ □□, □□□□ □□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□ □□: □□□ □□□ □□□ 1□□□□.

Answer:

Explanation:

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


Information governance > Create retention policy
Name
Locations
Retention settings
Finish
Review and finish
It might take up to one day to apply this policy to the locations you selected.
Policy name
contoso
Edit
Description
Edit
Locations to apply the policy
Exchange email (All Recipients)
SharePoint sites (All Sites)
OneDrive accounts (All Accounts)
Microsoft 365 Groups (All Groups)
Edit
Retention settings
Delete items at end of retention period
Delete items that are older than 7 years based on when they were created
Edit
Items that are currently older than 7 years will be deleted after you turn on this policy. This is especially important to note for locations scoped to 'All' sources (for example, 'All Teams chats') because all matching items in those locations across your organization will be permanently deleted.
Back
Submit
Cancel

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

Answer Area

Microsoft SharePoint files that are affected by the policy will be **[answer choice]**.

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, **[answer choice]**.

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

Answer:

Answer Area

Microsoft SharePoint files that are affected by the policy will be **[answer choice]**.

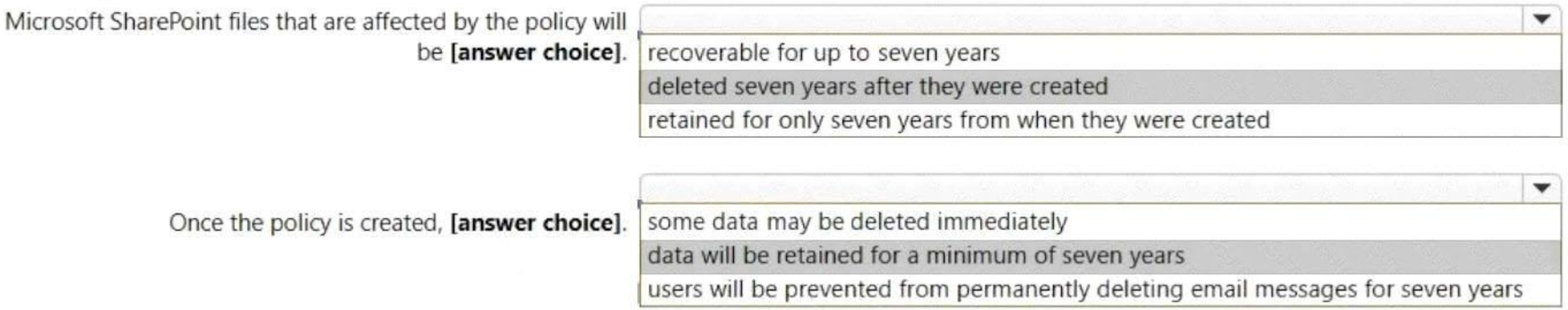
- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, **[answer choice]**.

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

Explanation:

Answer Area



Box 1: Deleted seven years after they were created.
From the exhibit:
The retention policy applies to SharePoint sites.
Delete items that are older than 7 years based on when they were created.
Box 2: data will retained for a minimum of seven years
The longest retention period wins. If content is subject to multiple retention settings that retain content for different periods of time, the content will be retained until the end of the longest retention period for the item.
Note: Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email).
For example, if all documents in a SharePoint site should be retained for 5 years, it ' s more efficient to do this with a retention policy than apply the same retention label to all documents in that site. However, if some documents in that site should be retained for 5 years and others retained for 10 years, a retention policy wouldn ' t be able to do this. When you need to specify retention settings at the item level, use retention labels.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

NEW QUESTION: 187
□□□ □□ □□□ □□□□□ □□ □□□(Just-in-Time Access)□ □□□□ □□□.
□□□ □□□□ □□□?
A. Microsoft Entra ID □□
B. Microsoft Entra □□ □□ ID □□(PIM)
C. □□ □□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 188
□□□ Microsoft Defender XDR□ □□□□ Microsoft 365 □□□ □□□□ □□□□.
□□ □□ □□□ Microsoft□ □□ □□□ □□□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□

B. □□ □□
C. □□□□□□□ □□ □□
D. □□□□ □□
E. □□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 189
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: 190
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Microsoft Defender □□□□ □□□ □□□□ □□□□□ □□□ □□□□ □□□□ □□□□.
□□□ □□□ □□□ □□□□ □□ □□□□ □□□□□□□□ □□□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:

1. Analysis 2. Take Action

NEW QUESTION: 191

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

□□ □□□□ Windows 11□ □□□□ □□□ □□□ □□□□.

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

□□ □□□ □□□□ □□ □□□ □□□ □□□.

□□□ □□ □□□?

A. Office □□□□□□ □□ □□□ □□□ □□□□□.

B. □□ □□ □□(ASR) □□□ □□□□.

C. □□□□□ □□ □ □□(EDR) □□□ □□□□□.

D. Office □□ □□□□□ □□ □□□ □□□□.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 192

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

Name	Platform
Device1	Windows 11
Device2	Android
Device3	Linux

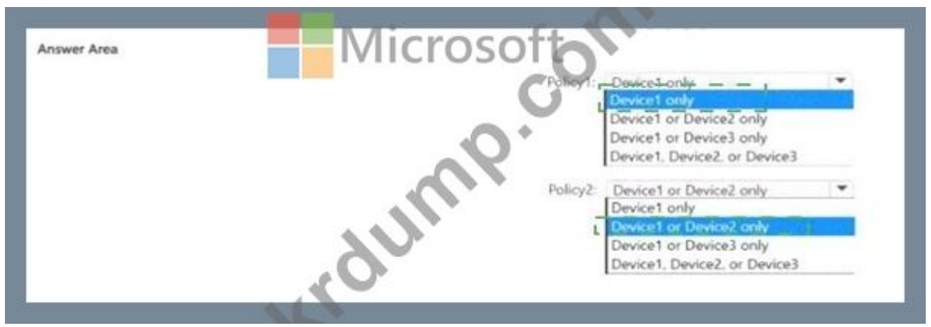
□□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□.

Name	Template
Policy1	Microsoft Defender Antivirus
Policy2	Device Control

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

Answer Area

Answer:



Explanation:

Answer Area

NEW QUESTION: 193

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

□□□ Branch□□ □□□ □□□ □□□ □□□□□□!

Admin1□□ Branch1 □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

* Admin1□ □□□ □□□ Branch1□ □□□ □□□□ □□□ □ □□□ □□□.

* Admin1□ Branch1□ □□□□ □□□□ □□□□ □□□, □□□ □□□□ □□, □□□ □□ □□□ □□□□ □□□.

Branch1 □□□□ □□□ □□□□ □□, Admin1□□□ □□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area

Explanation:

NEW QUESTION: 194

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

□□□ □□ □□ □□ □□ □□ □□ □□□ □□□□□.

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

□□□□: □□ □□□ 1□□□□.

A. □□ □□

B. □□□ □□ □□

C. □□□ □□

D. □□□ □□

E. □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 195

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □□ □□□ □□□□.
□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □ □□□□ □□ □□□ □□□□ □□□□.
□□□□□□ Microsoft Entra ID(Microsoft Entra ID)□ □□□□ contoso.com□□□ Active Directory □□□□ □□□□.
Windows 10 □□□ Microsoft System Center Configuration Manager(□□ □□)□ □□□□ □□□ □ □□□□.
□□ □□□ □□ □□□ □□□□□ □□□□□.
□□□□ Device1□□□ □ □□□ □□□□□. Device1□ Configuration Manager □□□□□□ □□□□□.
Microsoft Intune □ Configuration Manager□ □□□□ Device1□ □□□ □ □□□ □□□□ □□□.
□□ □□: □□ □□ □□ □□□□ □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 196

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

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

Compliance1□□□ □□□ □□ □□□ □□ □□□□□.
□□ □□ □□□ □□□□ □□□ □□□□ □□□.
* □□□ □□ □□□□ Compliance1□ □□□ □ □□□□.
* Compliance1□ □□ □□
□□□□□ □□ □□□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

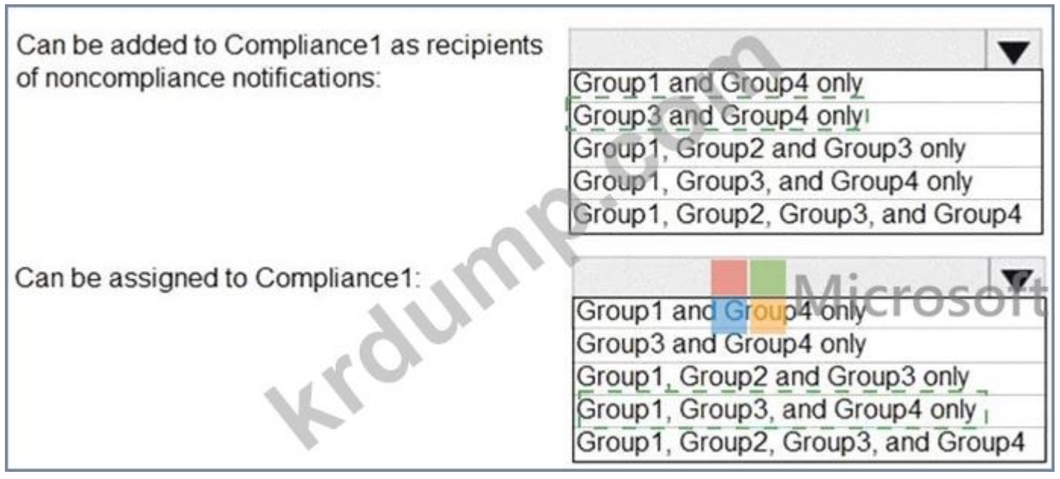
Can be added to Compliance1 as recipients of noncompliance notifications:

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

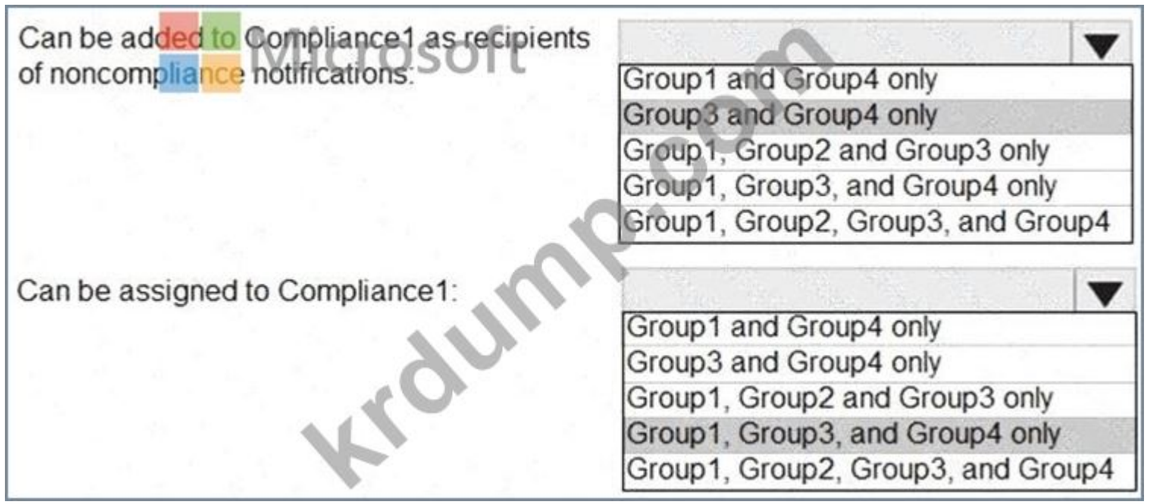
Can be assigned to Compliance1:

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

Answer:

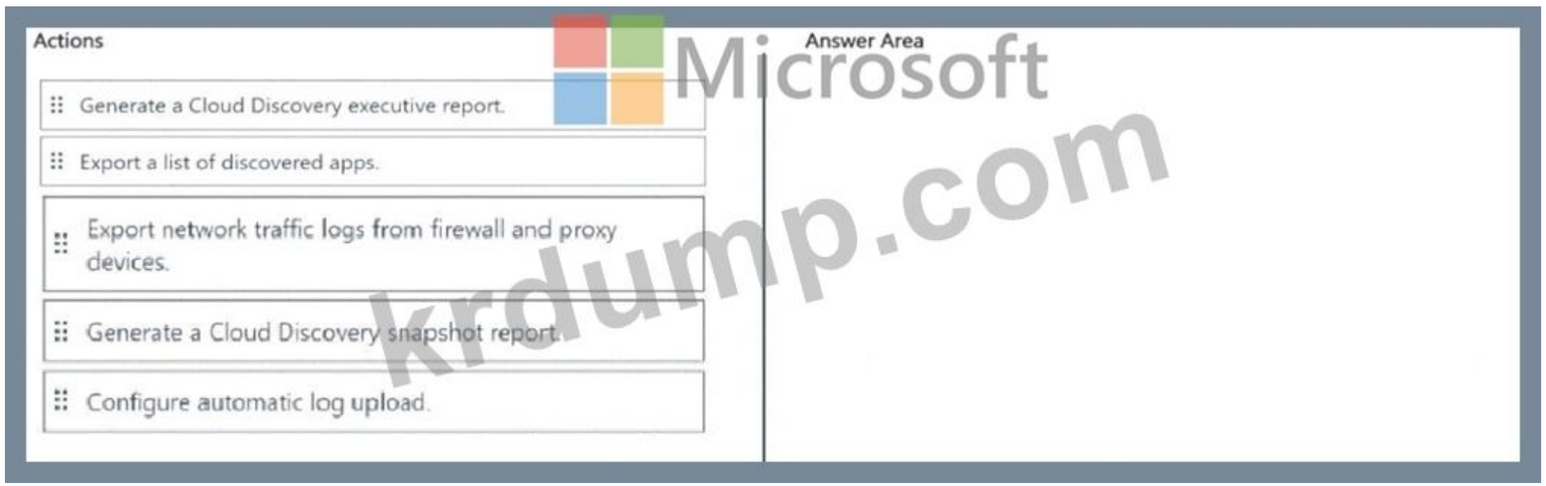


Explanation:

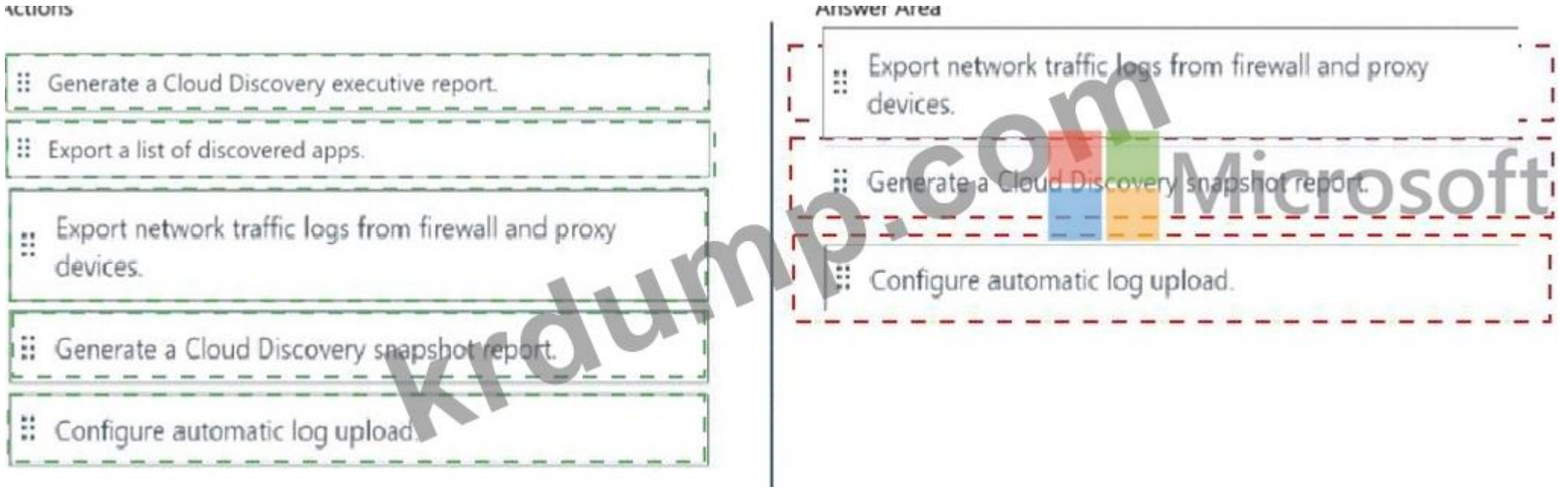


Reference:
https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manager-intune/

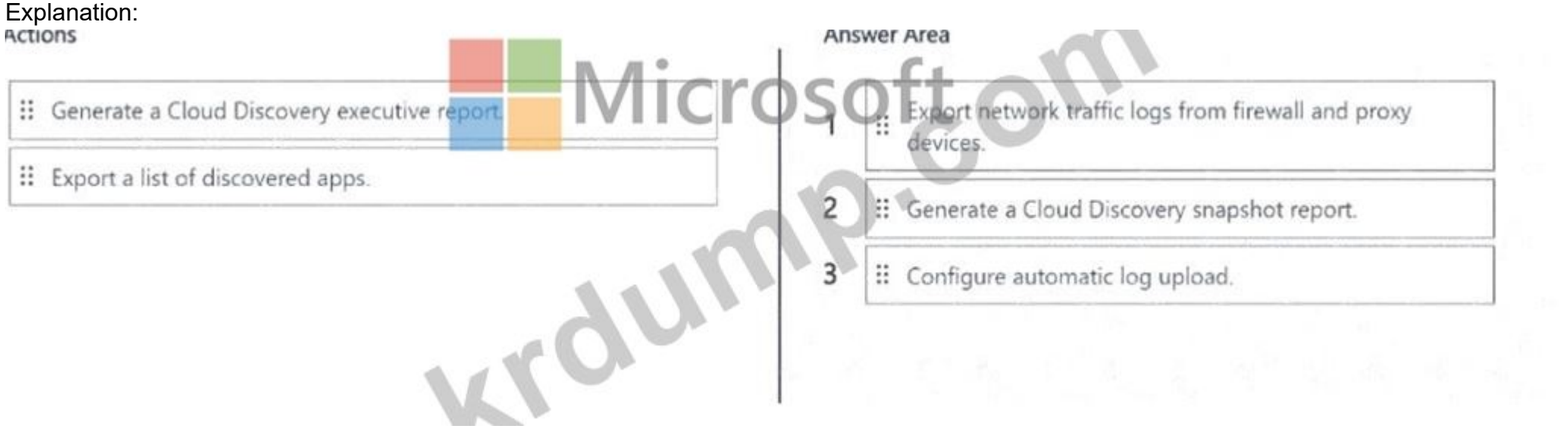
NEW QUESTION: 197
Microsoft 365 E5 □□□ □□ □□□□ □□ Microsoft Defender□ □□□□ □□□□.
□□□ □□□ □□□□ □□□ □□□□ □□□□ □□ □□□□□ □□□□ □□□□ □□□□□ Cloud Discovery□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:



NEW QUESTION: 198
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: 199
□□□ □□□□ Microsoft 365 □□□□ □□□□.
Engineering□□□ □□□ □□□□ □□□□ □□□ □□ □□(MDM)□ □□□ □□□ □□□□□ □□□□□ □□□. □□ □□ □□□ □□ □□ □□ □□□□□.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

□□ □□ □□□ □□ □□ □□ □□□□□.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

Answer:

Explanation:

https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restriction-priority

NEW QUESTION: 200
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□ □□□ □□□□ □□□ □□ □□(DLP) □□□ □□□ □□□□.

□□ □□□ DIP □□□□ □□ □□□ □□□ □ □□□?

A. □□□ □□□

B. □□□ □□ □□

C. □□□ □□ □□

D. □□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 201

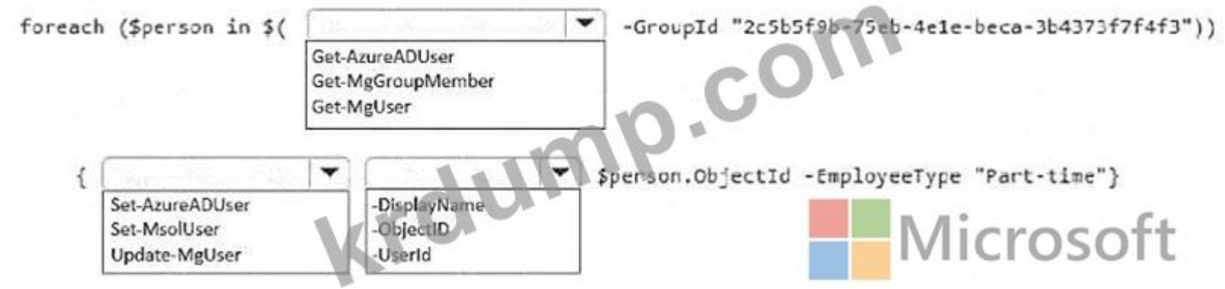
□□□ Microsoft 365 □□□ □□□□ □□□□.

Contractors□□ □□□ □□ □□ □□□□ EmployeeType □□□ □□□□□□□ □□□. Contractors □□□ GroupId □□ □□□□□.

Microsoft Graph PowerShell□ □□□□ Contractors □□□ □□ □□□□ □□□□ EmployeeType □□□ Part-time□□ □□□□ □□□.

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

□□: □□ □□□ 1□□□□.



Answer:

Explanation:
foreach ($person in $(Get-MgGroupMember -GroupId " 2c5bf9b-75eb-4e1e-beca-3b43737f74f3 "))
{
Update-MgUser -UserId $person.ObjectId -EmployeeType " Part-time "
}
Correct selections:
Get-MgGroupMember
Update-MgUser
-UserId
The correct first cmdlet is Get-MgGroupMember because the task requires retrieving all members of an existing Microsoft Entra group by using the group's GroupId. Microsoft documents Get-MgGroupMember - GroupId as the Microsoft Graph PowerShell cmdlet used to get members of a specified group.
The correct update cmdlet is Update-MgUser, not Set-AzureADUser or Set-MsolUser, because the question explicitly requires Microsoft Graph PowerShell. Microsoft documents Update-MgUser as the cmdlet that updates properties of a user object, and its syntax includes -UserId as the identity parameter and - EmployeeType as an updateable user property.
The third dropdown must be -UserId because Update-MgUser identifies the target user through the -UserId parameter. The value passed is the user object identifier returned from the group membership query. -ObjectId belongs to older Microsoft Entra ID PowerShell patterns, and -DisplayName cannot uniquely identify or update the user object. References/topics: Microsoft Graph PowerShell, Microsoft Entra group membership, Get-MgGroupMember, Update-MgUser, user attribute management.

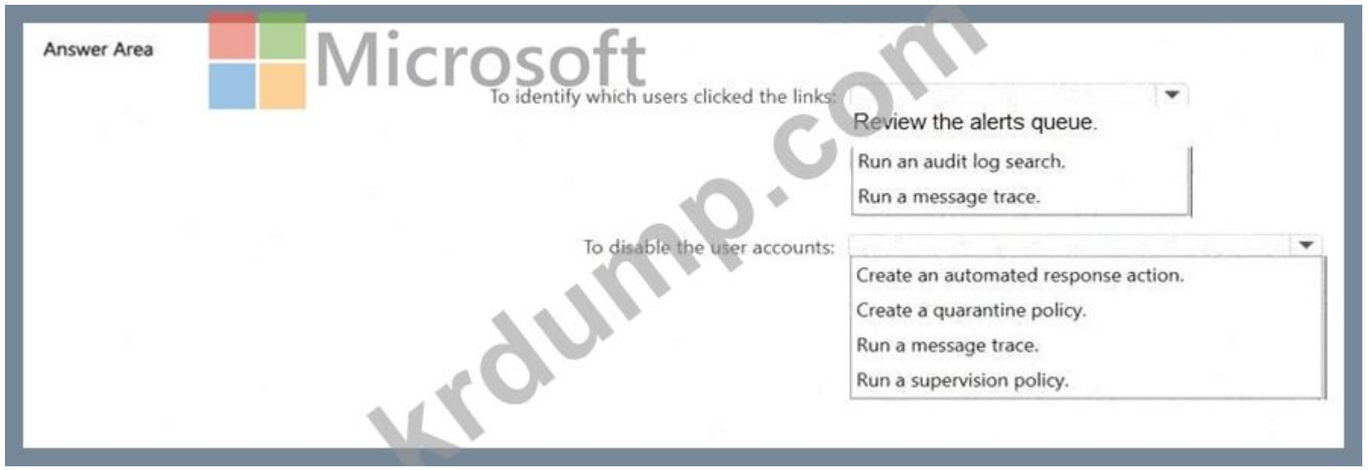
NEW QUESTION: 202
□□□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□□□ □□□ □□□□ □□□□□.
□□ □□ □□□□ □□□ □□□□ □□□ □□□ □□□□□□ □□□□ □□□□□ □□□□ □□ □□□□□ □□□□□ □□ □□□□ □□□. □□ □□□ □□□□ □□□□□□ □ □□□.
□□□ □□ □□□?
A. □□□□ □□□ □□□ □□ □□□ □□ □□(DLP) □□□ □□□□.
B. □□□ □□ □□ □□□ □□□ □□□□□.
C. □□□□ □□□□ □□ □□□ □□ □□□ □□ □□(DLP) □□□ □□□□.
D. □□□ □□□ □□ □□□ □□□□.
Answer: D (LEAVE A REPLY)
Use the Microsoft Defender XDR portal to create Safe Links policies
In the Microsoft Defender XDR 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: 203
Microsoft 365 E5 □□□ □□□□.
Microsoft Defender for Endpoint□ Microsoft Intune□ □□□□□.
Intune□ □□□ □ □□□ Defender for Endpoint□ □□□□ □□□□□□ □□ □□□.
□□□: □□ □□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: (SHOW ANSWER)

NEW QUESTION: 204
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□□(FID02)□ □□□ □□ □□□□ □□□□ □□ □□□ □□□ □□□□□. □□ □□□□ □ □□□(FID02)□ FIDO Alliance □□□□□ □□□□ □□ □□□□□ □□ □□□. □□ □□□ □□□□□ □□□?
A. □□ □ □□
B. □□ □□□ □□ □□
C. □□ □□
D. □ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 205
Microsoft 365 E5 □□□□ □□□□ □□□□.
□□□□□ □□ □□□ □□□ □□□ □□□□ □□□□ □□□□□□.
□□□ □□□ □□□□ □□□□ □□ □□ □□□□ □□□ □□□□□□ □□□. □ □□□□ □□ □□□ □□□□□ □□□.
Microsoft Defender □□□□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:

NEW QUESTION: 206

Office 365□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□ □□□□. □□ □□ □□□ □□□ □□□□.

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

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

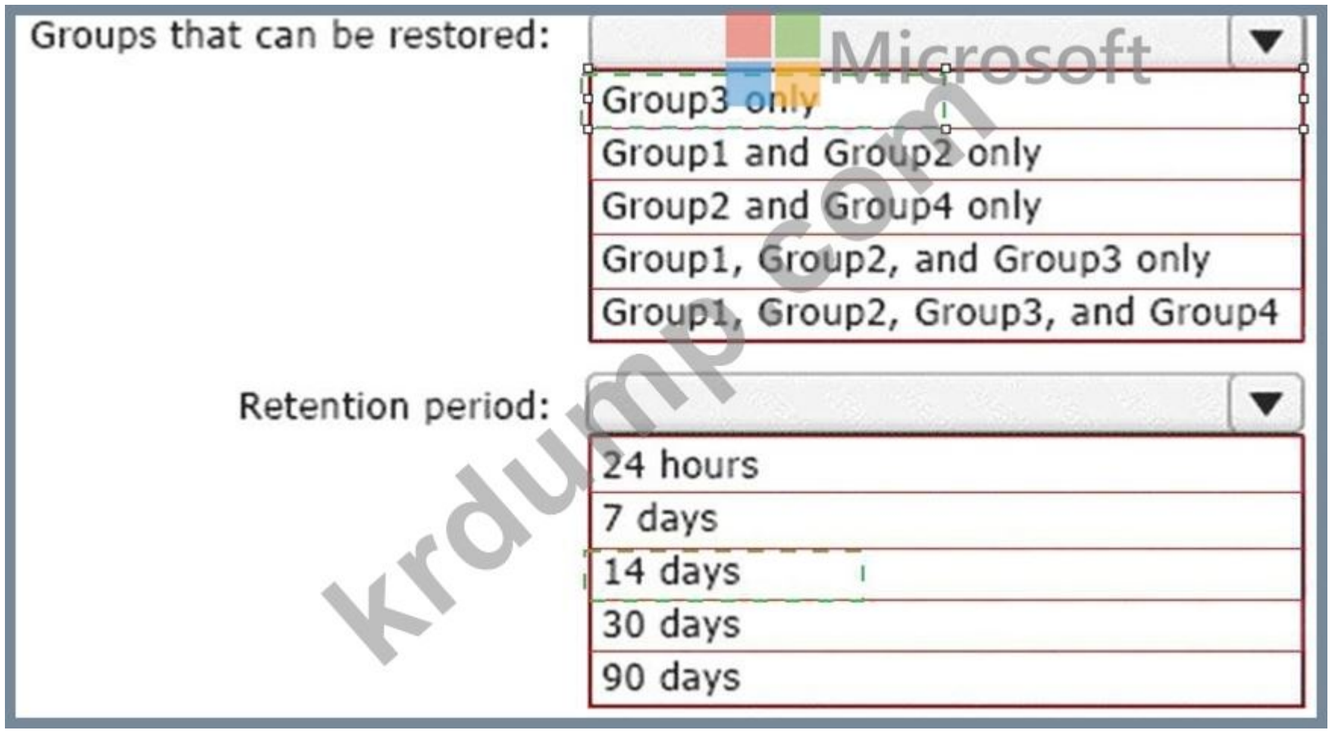
A. Policy3 □ Policy4□
B. □□1 □ □□3□
C. Policy2 □ Policy4□
D. Policy1□ Policy2□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 207
□□□
□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

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

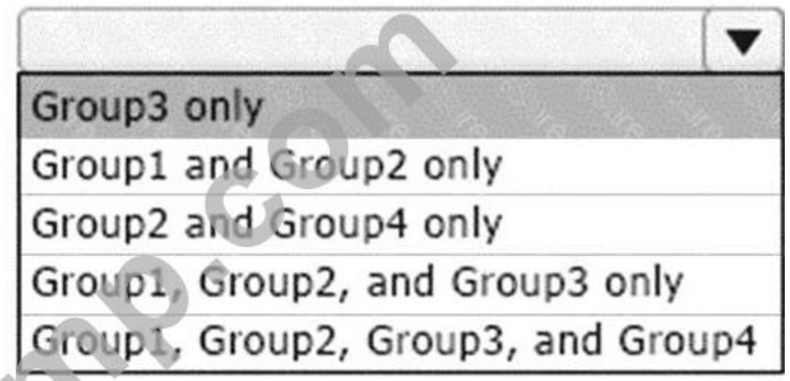
Answer:



Explanation:

Answer Area

Groups that can be restored:



Retention period:

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: 208

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

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

□□ □□□ □□ □□ □□ □□□ □□□□ □□□□□.

□□ □□□ Group1□ □□□□□.

□□ □□ □□□ □□□ □□□□□.

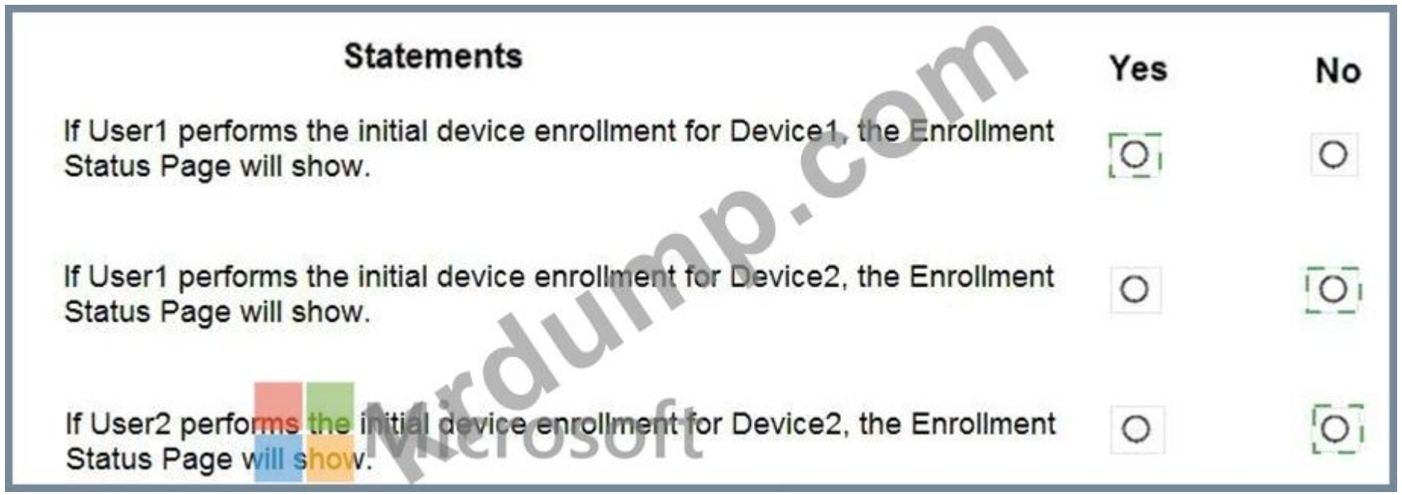
Name	Platform
Device1	Windows 10
Device2	Android

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

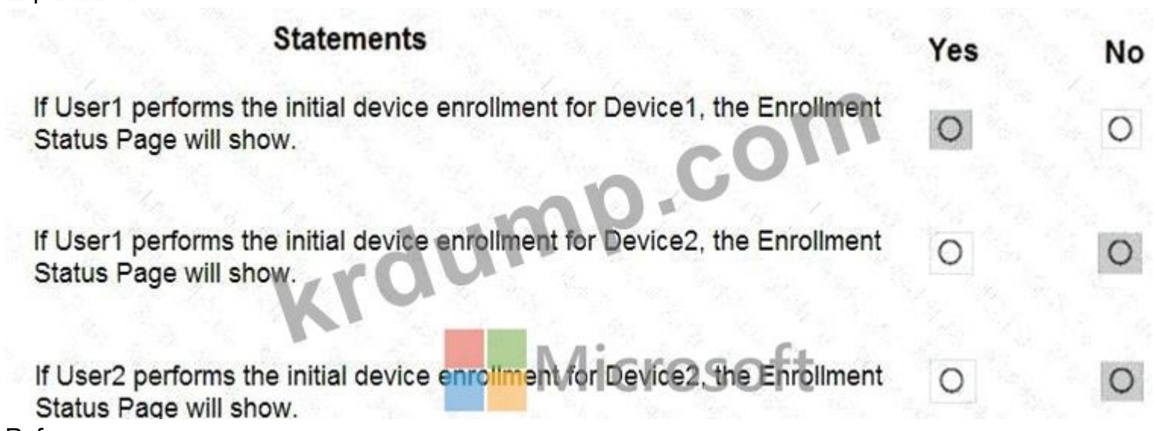
□□□□: □□ □□□ 1□□□□.

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

Answer:



Explanation:



Reference:

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

NEW QUESTION: 209

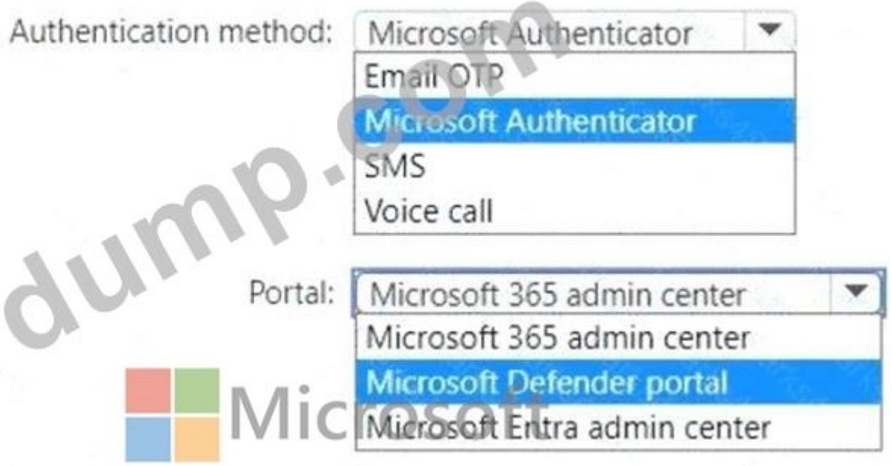
Microsoft 365 E5 □□□ □□□□.

□□ □□□□ □□ □□□□ □□ □□□ □□□□□ □□□.

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

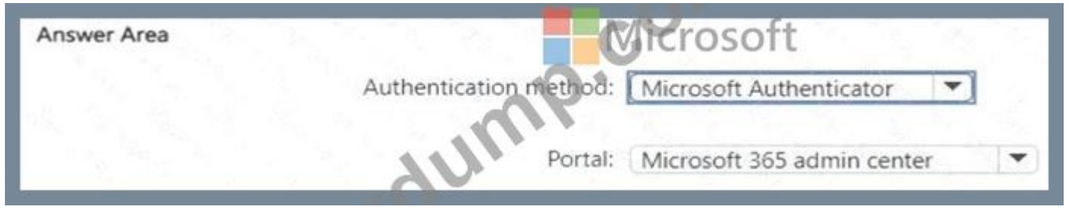
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

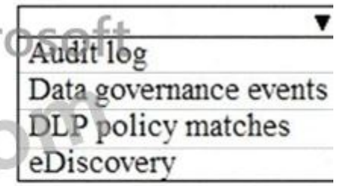
Explanation:



NEW QUESTION: 210

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

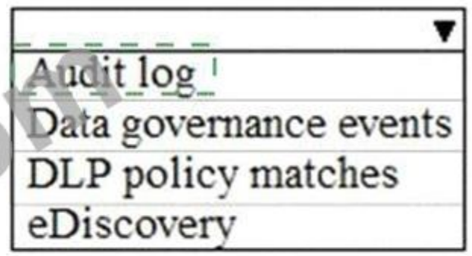
From the Security & Compliance admin center, perform a search by using:



Filter by:

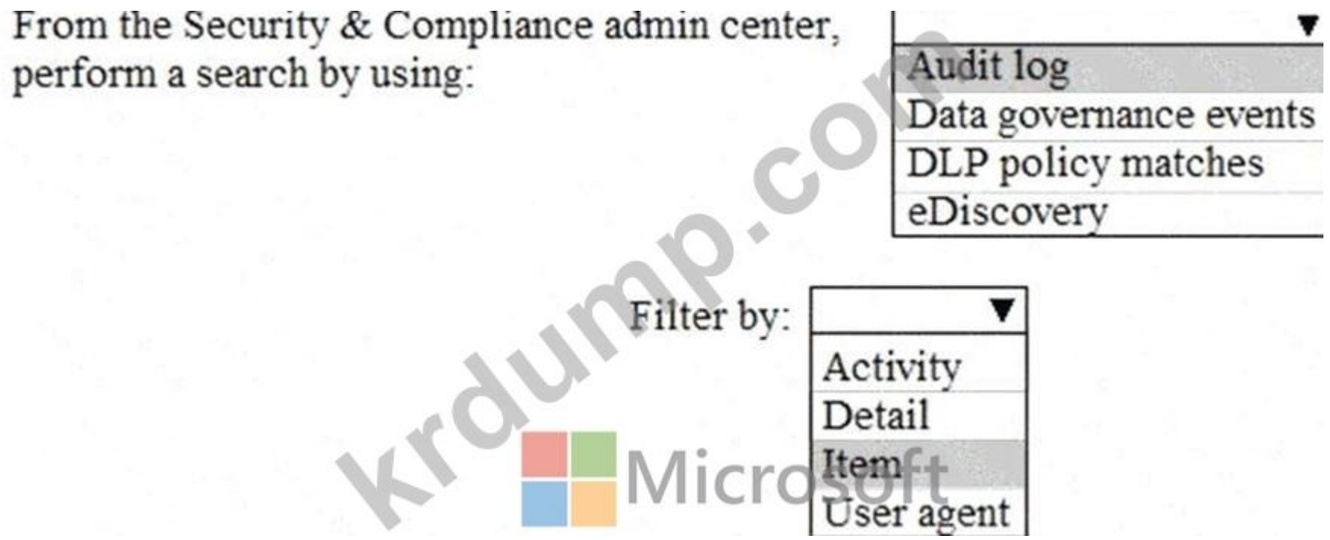
Answer:

From the Security & Compliance admin center, perform a search by using:



Filter by:

Explanation:



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

NEW QUESTION: 211
□□□
□□ □□ □□ □□ □□□□ □□□ 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

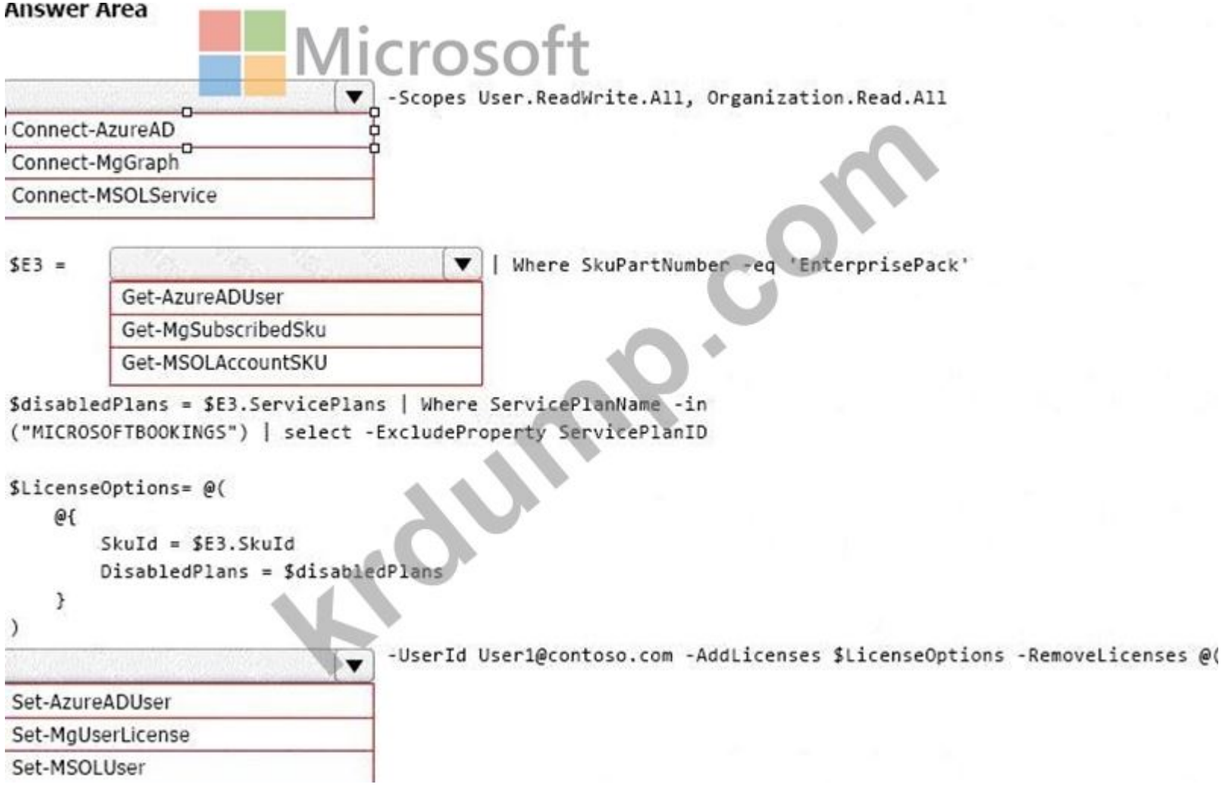
July 15, 2023 is with the assignment period.

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

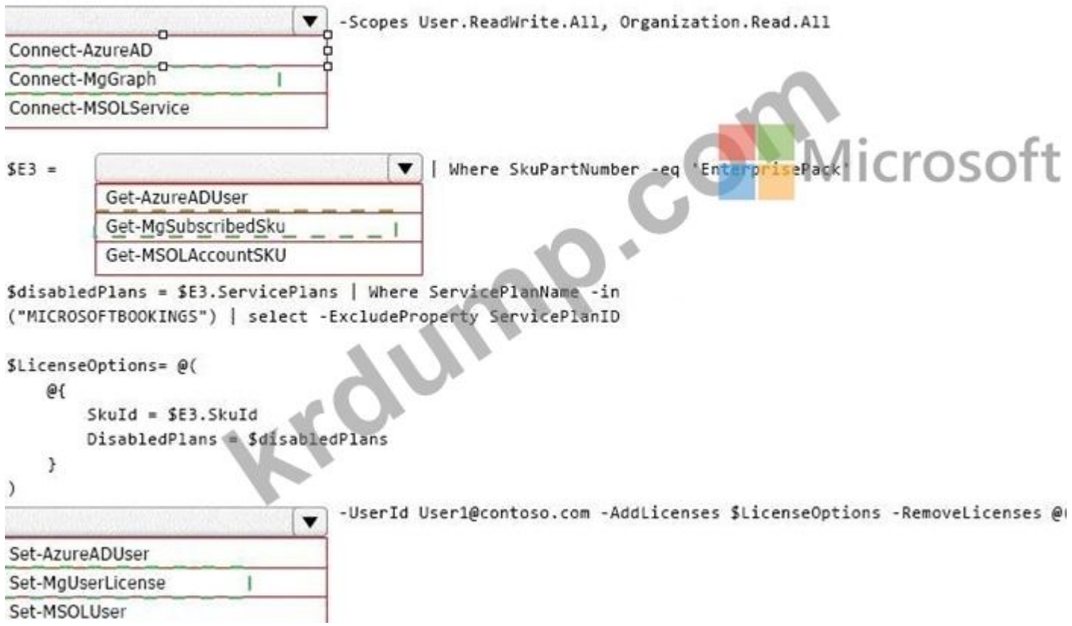
NEW QUESTION: 212
□□□
Microsoft 365 □□□ □□□□.
user1@contoso.com□□□ □□□□ □□ □□□□□□□□□□.
PowerShell□ □□□□ User1□ Microsoft Office 365 E3 □□□□□ □□□□ □□□. Microsoft Bookings□ □□□□□□□ □ □□□.
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

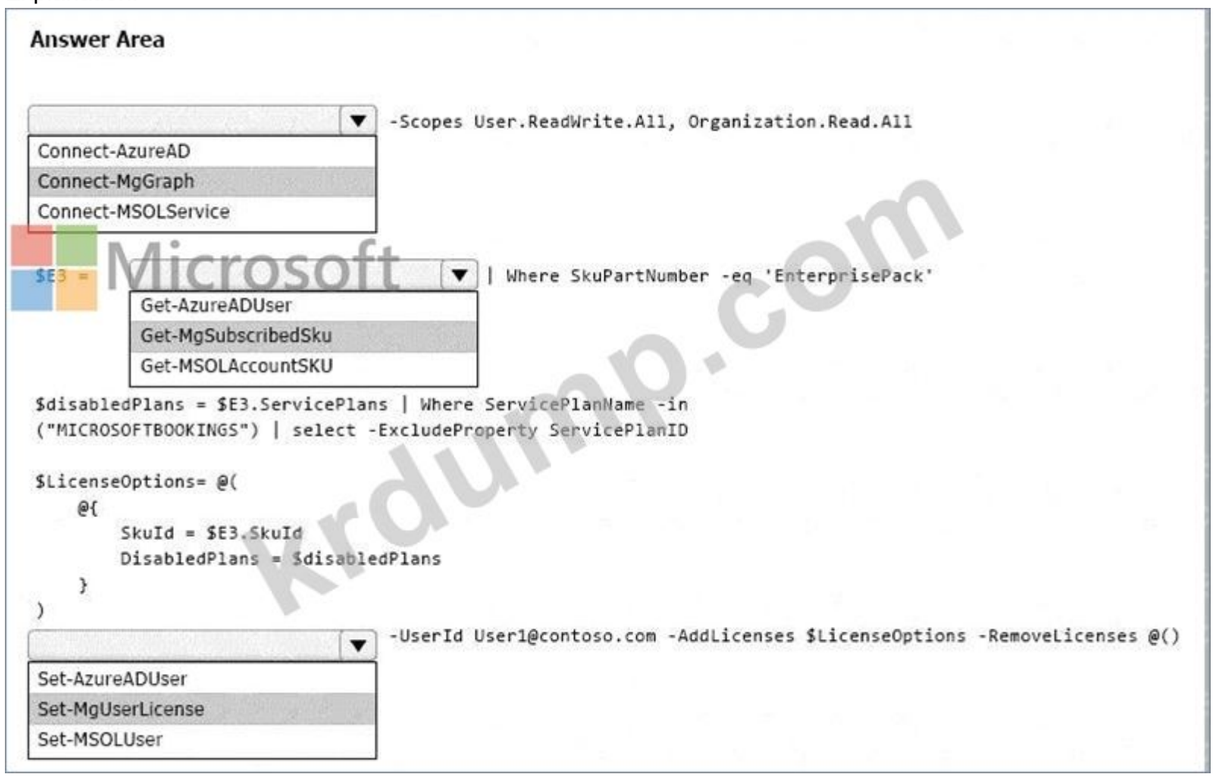


Answer:

Answer Area



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:

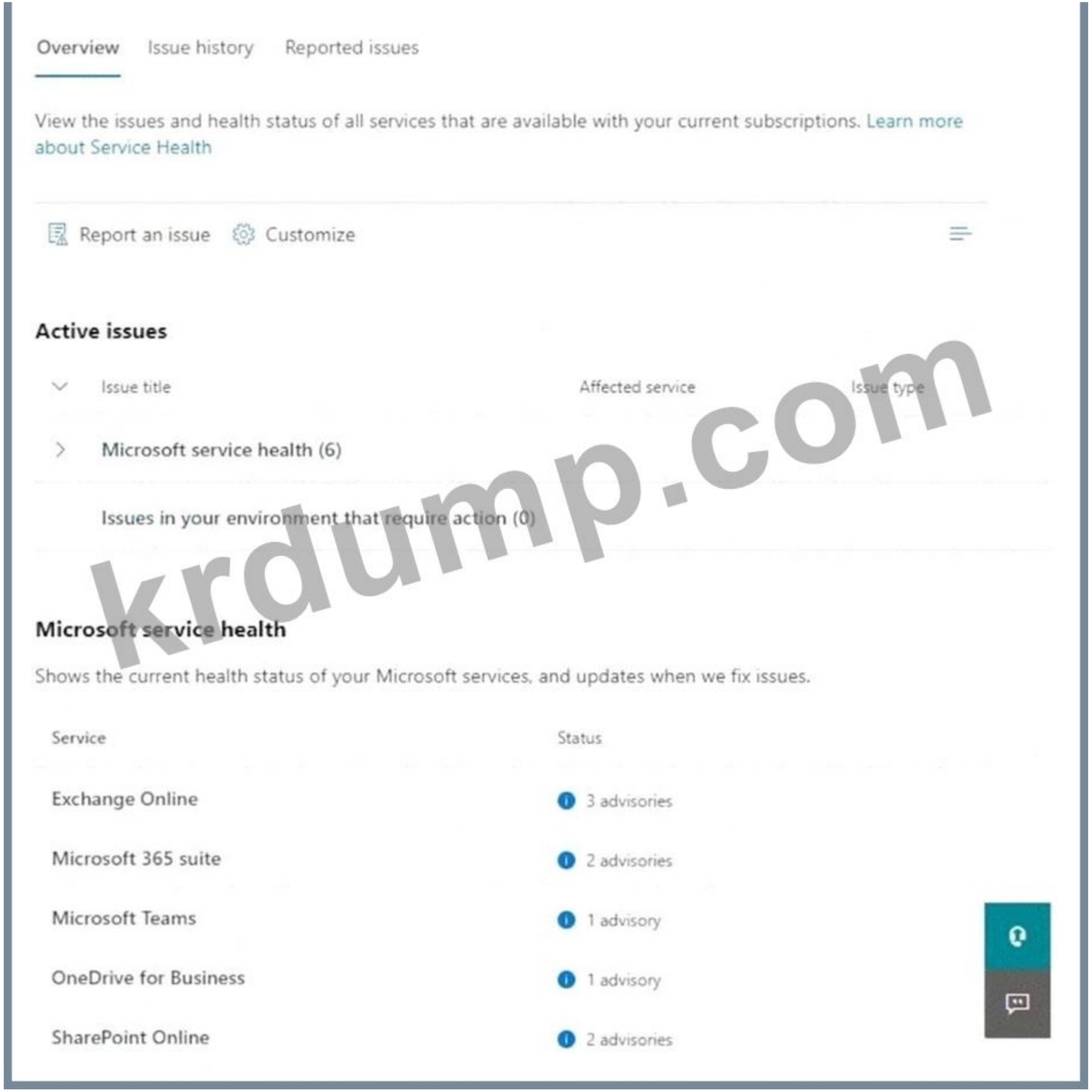
https://learn.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell

NEW QUESTION: 213

Microsoft 365 E5 □□□□ □□□□.
□□□□□ 1,000□□ □□□ iOS □□□ □□□ □□□□□. □□□ □□□□□□ □□□□□ □□ □□□□□.
□□ □□ □□□ □□□□ Microsoft Intune □□ □□□ □□□□ □□□.
* □□□ □□□□□ □□□□□□
* □□□ □□□ □□□□□□
* □□□ □□ □□□□ □□□□□.
□□□ □□□□ □□□?
A. □□ □□ □□(ADE)
B. BYOD(Bring Your Own Device) □□□ □ □□ □□
C. Apple Configurator □□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll

NEW QUESTION: 214
□□□□□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□. □ □□□□□ 500□□ Windows 11 □□□ □□□□.
Sub1□□□ □□□ Microsoft 365 □□□ □□□□.
Sub1□ □□□ Microsoft Entra □□□□ □□□□ □□□□□ □□ Microsoft Entra Connect Sync□ □□□ □□□□□.
□□□□ □□ □□ □□ □□□□ Sub1□ □□□ □ □□□ □□ □□□.
□□□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□□?
A. □□□□ □□ □□□□ □□□□□.
B. □□□□ □□□ □□□□□.
C. □□□□□ □□□□ □□□ □□□□□.
D. □□□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)
The correct answer is Hybrid join the devices. The devices already belong to an on-premises AD DS domain and run Windows 11, so the lowest-impact approach is to configure Microsoft Entra hybrid join. A Microsoft Entra hybrid joined device remains joined to the on-premises AD DS domain while also being registered in Microsoft Entra ID, which is the correct identity state for existing domain-joined Windows devices that need cloud access with single sign-on behavior. Microsoft's hybrid join guidance shows that Microsoft Entra Connect can be used to configure Microsoft Entra hybrid join through Configure device options, minimizing manual device-by-device work.
Password hash synchronization and pass-through authentication are user sign-in methods; they do not by themselves join or register the Windows 11 devices to Microsoft Entra ID. They address how credentials are validated, not whether the device has a cloud device identity for seamless access. Joining the devices directly to the tenant would mean Microsoft Entra joining them, which is more disruptive for existing AD DS domain-joined devices. Microsoft Entra joined devices are joined only to Microsoft Entra ID, while hybrid joined devices are intended for organizations that still use on-premises AD DS.
Therefore, select C. Hybrid join the devices.

NEW QUESTION: 215
Microsoft 365 □□□ □□□□.
□□ □□□ □□ □□□ □□ □□□ □ □ □□□□.



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

User1□□ □□ □□□ □□□□ □□□?

A. □□□ □□ □□
B. □□ □□□
C. □□□ □□ □□□
D. □□ □□ □□□
Answer: B (LEAVE A REPLY)
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 Microsoft Entra ID 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 Microsoft Entra ID
- 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: 216
□□ □□ □□□ □□□ □□ □□ □□□ □□□□□.

olicy setting	Policy name	Managers	
	Description		
	Applied to	If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.onmicrosoft.com	Edit
	Safety tips > User impersonation	Off	Edit
	Safety tips > Domain impersonation	Off	
	Safety tips > Unusual characters	Off	
	Mailbox intelligence	Off	
Spoof	Enable antispoofing protection	On	
	Action	Quarantine the message	Edit
Advanced settings	Advanced phishing thresholds	3 - More Aggressive	Edit

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

Answer Area

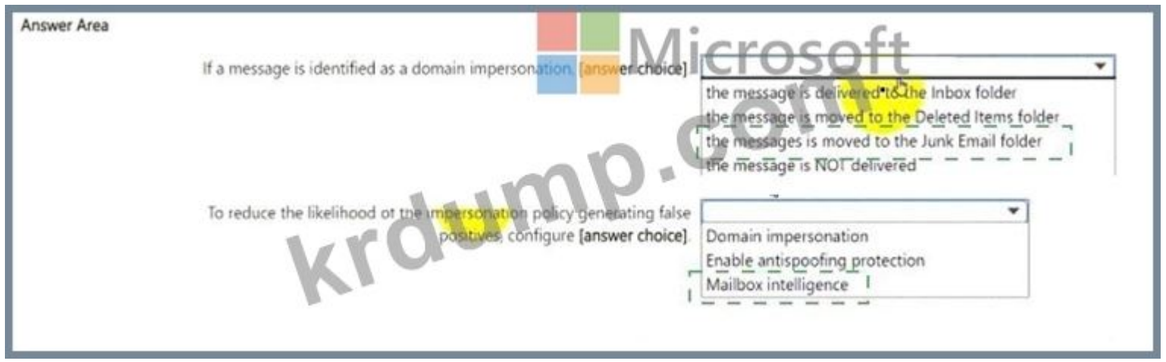
If a message is identified as a domain impersonation, [answer choice].

- the message is delivered to the Inbox folder
- the message is moved to the Deleted Items folder
- the messages is moved to the Junk Email folder
- the message is NOT delivered

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].

- Domain impersonation
- Enable antispoofing protection
- Mailbox intelligence

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: 217

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

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

□□□ □□□□□□ □□□□□ 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: B (LEAVE A REPLY)

NEW QUESTION: 218

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

A. Microsoft Entra ID □□ □□□□ User1□□ □□□□ □□ □□□ □□□ □□□□□.

B. Microsoft Entra ID □□ □□□□ □□□□ □□ □□ □ □□□ □□□□□.

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

D. Intune □□ □□□□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

References:

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

Topic 2, A. DatumCase Study:

Overview
Existing Environment
This is a case study Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.
Current Infrastructure
A). Datum recently purchased a Microsoft 365 subscription.
All user files are migrated to Microsoft 365.
All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.
Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.
A). Datum uses and processes Personally Identifiable Information (PII).
Problem Statements
Requirements
A). Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.
Business Goals
A). Datum warns to be fully compliant with all the relevant data privacy laws in the regions where it operates.
A). Datum wants to minimize the cost of hardware and software whenever possible.
Technical Requirements
A). Datum identifies the following technical requirements:
Centrally perform log analysis for all offices.
Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
Provide the users in the finance department with access to Service assurance information in Microsoft Office
365.
Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user ' s user account.
A security administrator requires a report that shows which Microsoft 36S users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive US. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

NEW QUESTION: 219
Microsoft 365 □□□ □□□□. User1□□□ □□□□ □□□□.
Used□ □□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. Microsoft Entra ID □□ □□□ □□ □□ □□□ IDE□□□.

B. Microsoft 365 □□ □□ □□□ eDiscovery Manager □□□.
C. Exchange □□ □□□ □□ □□ □□ □□□□□.
D. Microsoft 365 □□ □□□ □□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 220
□□□ □□ □□ □□□ ID□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Name	Type	Member of
User1	User	Group1
User2	User	Group2
User3	User	None
Group1	Group	None
Group2	Group	Group1

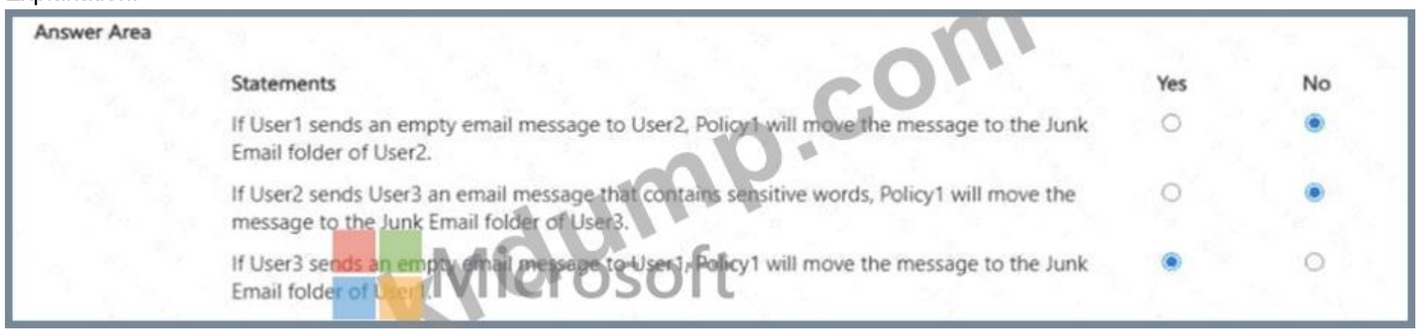
Microsoft Defender □□□□ Policy1□□□ □□□ □□ □□ □□ □□□ □□□ □□□ □□ □□□ □□□□□.
* □□ □□□, □□ □ □□□□ □□□□□
o □□□: User3 o □□: Group1
* □□ □□□, □□ □ □□□□ □□□□□.
o □□□: User1
Policy1□□ □□□ □□ □□ □□□ □□□ □ □□ □□ □□□ □□□□.
* □□□□ □□□□
o □ □□□: □□ o HTML□ □□ □□: □□ o □□□ □□: □□ o □□□: □□ Policy1□□ □□□ □□ □□ □□□ □□□□.
* □□□ □□
□□: □□ □□□□ □□ □□ □□□ □□
□□□□ □□□ □□□□ □□ □□: □□ □□□□ □□ □□ □□□ □□
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
If User1 sends an empty email message to User2, Policy1 will move the message to the Junk Email folder of User2.	○	○
If User2 sends User3 an email message that contains sensitive words, Policy1 will move the message to the Junk Email folder of User3.	○	○
If User3 sends an empty email message to User1, Policy1 will move the message to the Junk Email folder of User1.	○	○

Answer:

Explanation:



NEW QUESTION: 221

□□□

Microsoft 365 □□□ □□□, □□□□ Group1□□□ Microsoft 365 □□□ □□□□ □□□□. Group1□ □□ □□□ □□□ □□ □□□□ □□□□.

User1□□□ □□ □□□□ □□□ □□□ user1@outlook.com□□□.

User1□ Group1□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.

Answer Area

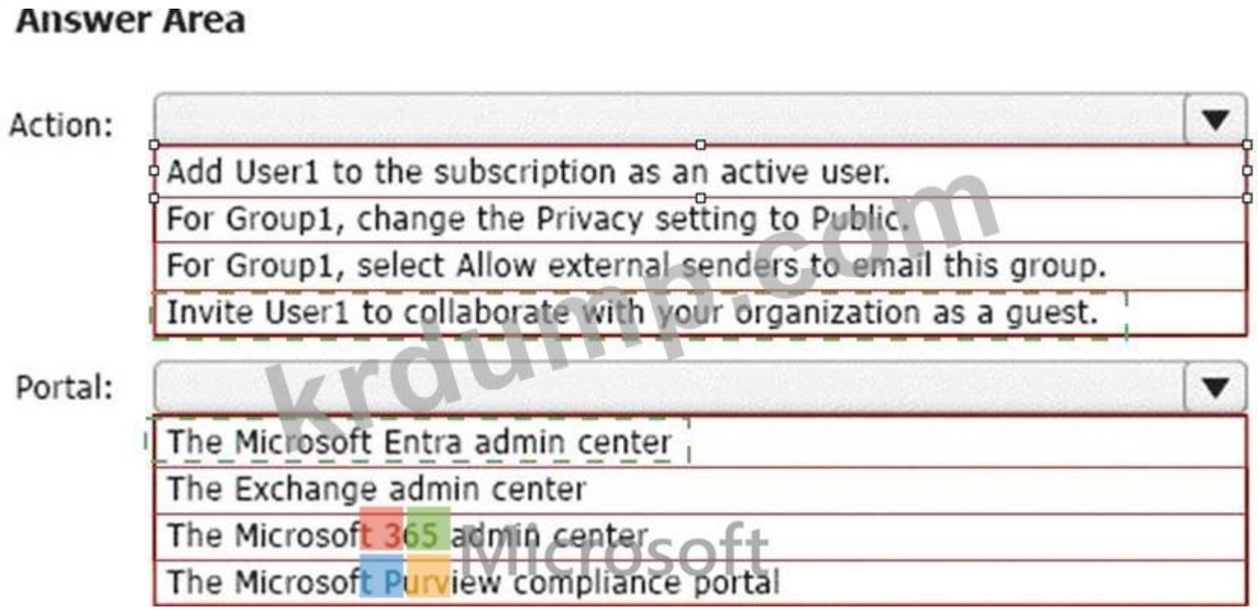
Action:

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

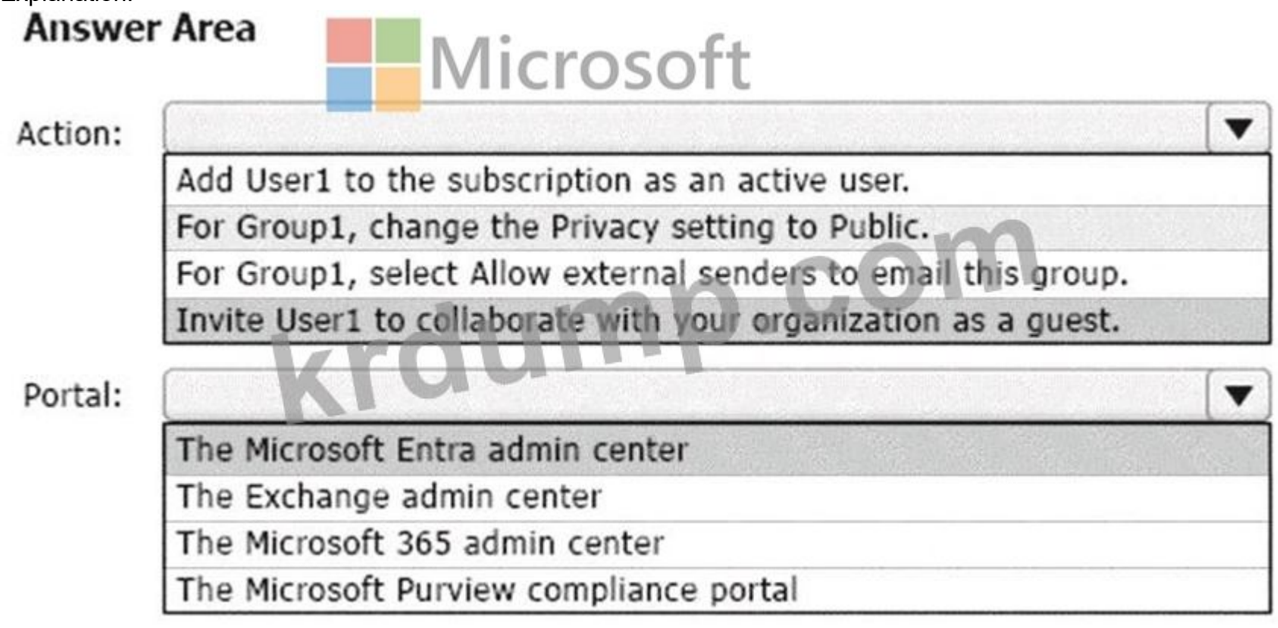
Portal:

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

Answer:



Explanation:



Box 1: Invite User1 to collaborate with your organization as a guest.

To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.

Navigate with your Web browser to https://admin.microsoft.com.

On the left pane, click on "Users", then click "Guest Users".

On the "Guest Users" page, to create a new guest user, click on either the "Add a guest user" link on the top of the page or click on "Go to Microsoft Entra ID to add guest users" link at the bottom of the page. Both of these links will take you to the Microsoft Entra ID portal, which is located at https://aad.portal.azure.com.

On the "New user" page in the Microsoft Azure portal, you must choose to either "Create user" or "Invite user". If you choose the "Create user" option, this will create a new user in your organization, which will have a login address with format username@tenantdomain,dot,com. If you choose the "Invite user" option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the "Invite user" option.
Box 2: The Microsoft Entra admin center
Microsoft Entra admin center unites Microsoft Entra ID with family of identity and access products Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Microsoft Entra ID (Microsoft Entra ID) and Microsoft Entra Permissions Management, formerly known as CloudKnox.
Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Microsoft Entra admin center (aad.portal.azure.com).
Reference:
https://stefanos.cloud/kb/how-to-manage-microsoft-365-guest-users
https://m365admin.handsontek.net/microsoft-entra-admin-center-unites-azure-ad-with-family-of-identity-and-access-products

NEW QUESTION: 222
□□□ Contoso, Ltd.□□ □□□□ □□□□.
Contoso□ □□ □□ □□□ DNS □□□□ □□□□□ □□□ Microsoft 365 □□□ □□□□ □□□□.
Contoso□ Fabrikam, Inc.□□ □□□ □□□□□.
Contoso□ □□ □□□□ Microsoft 365 □□□ □□□ □□□□□.
* □□□□□□
* □□□.□□□□□□
* □□□.□□□.com
□□ □□□ □□□□ □ □□□□ □□□ □□□ □ □□□ □□□□ □□□.
□ □□ □□□□ □□□□ □□, □□□□ □□ □□ □□□□□□ □□ DNS □□□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Answer Area

Explanation:

NEW QUESTION: 223

site1□□□ Microsoft SharePoint □□□□ □□□ Microsoft 365 E5 □□□ □□□□. site1□ □□ □□ □□□ □□□□□ □□□□ □□□.

* □□ □□□□ 10□□ □□□□□.

* □□ □□□□ □□□ □□□ □□□□□.

site1□ □□ □ □□□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□. □□: □ □□□ 1□□□□.

A. □□□ □□□

B. □□ □□ □□

C. □□□ □□ □□

D. □□□ □□ □□(DLP) □□

E. □□ □□

F. □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 224

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

□□□□ □□□ □□ □□ □□ □ □□ □□□ □□□ □□□□□.

Device1□□□ □□□ □□□□ □□□□ □□□□ □□□□□.

□ □□□□ □□□ □□ □□□?

A. □□□ □□□□ □□□□□□ □□□□□.
B. □□ □□□ □□□□□.
C. Microsoft □□ □□□ - □□□ □□ □□□ □□□□□.
D. Defender for Endpoint□ Microsoft Intune□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 225
□□□ Microsoft Defender for Endpoint□ □□□□□. Microsoft Defender for Endpoint□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

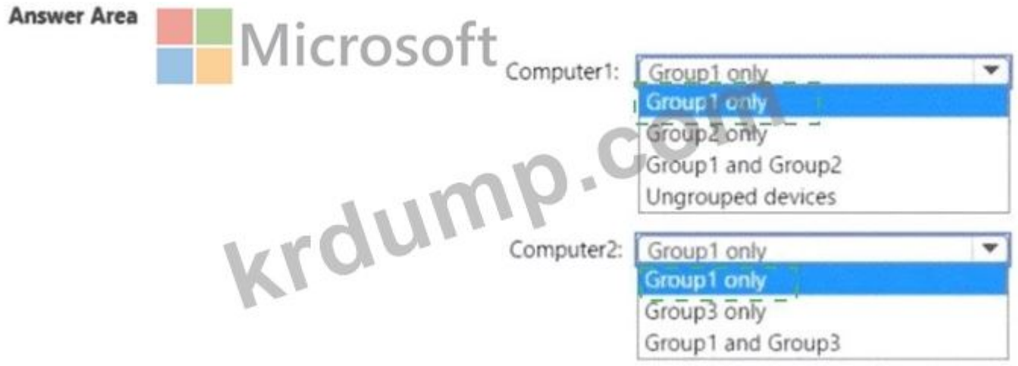
Rank	Device group	Member
1	Group1	Name starts with Comp
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped devices (default)	Not applicable

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

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

□□ □□□ Computer!□ Computed □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
Answer Area

Answer:



Explanation:

NEW QUESTION: 226

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

Platform	Count
Windows 10	50
Android	50
Linux	50

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

□□□ □□ □□ □□□?

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

B. Microsoft Defender XDR □□□□ □□ □□□ □□□□.

C. Microsoft Endpoint Manager □□ □□□□ □□ □□□ □□□□□.

D. Microsoft Entra ID □□ □□□□ □□ □□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

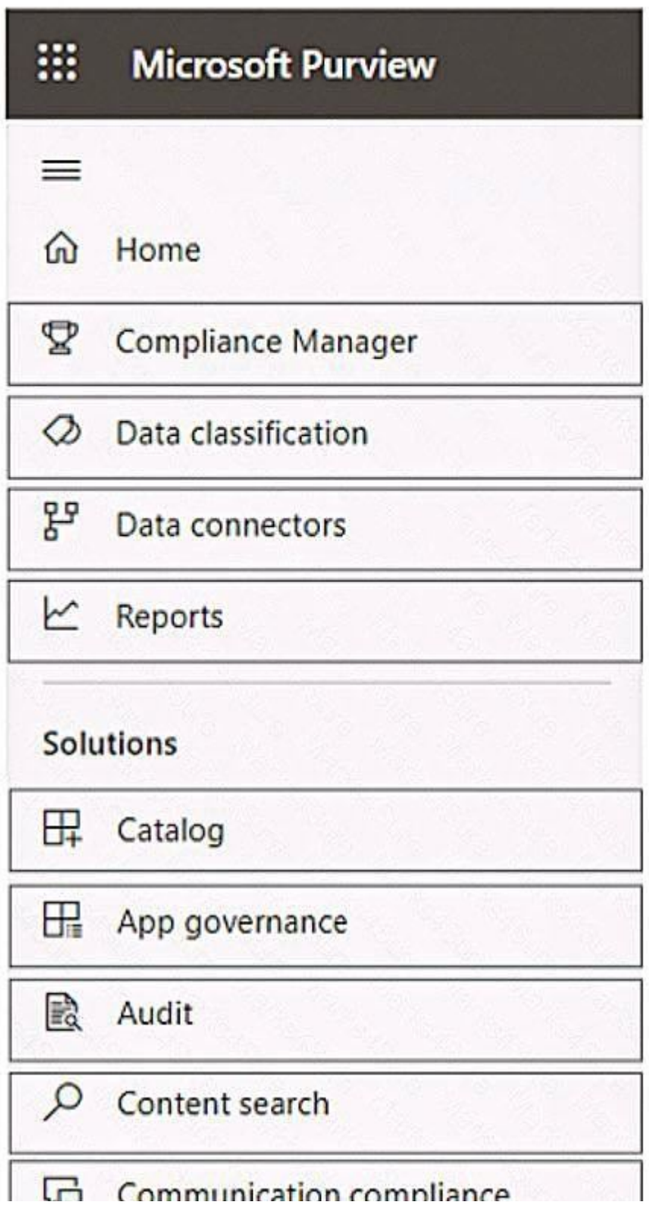
Reference:

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

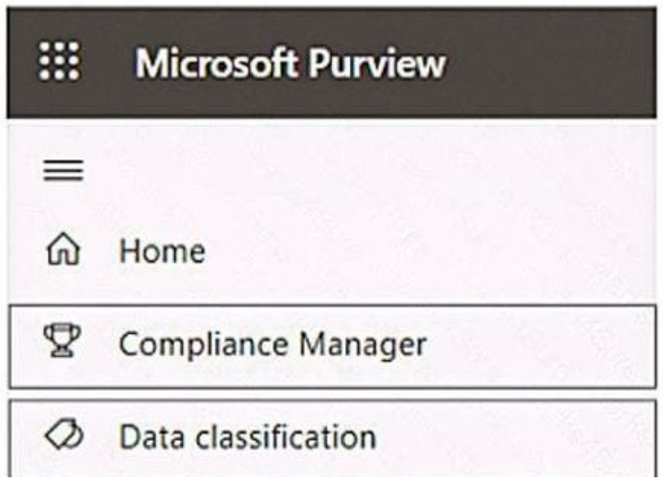
NEW QUESTION: 227
Sitel□□□ Microsoft SharePoint □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □□ □□□ □□□□ □□□.
* □□ □□□□ □□□□ SIT1□□□ □□□ □□□ □□ □□□ □□□□.
* SIT1□ □□□□ □□ □ □□□ □□□□□ □□□□□.
Microsoft Purview □□ □□ □□□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□

Answer Area

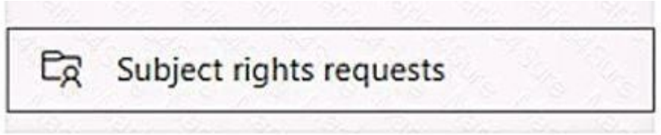


Answer:

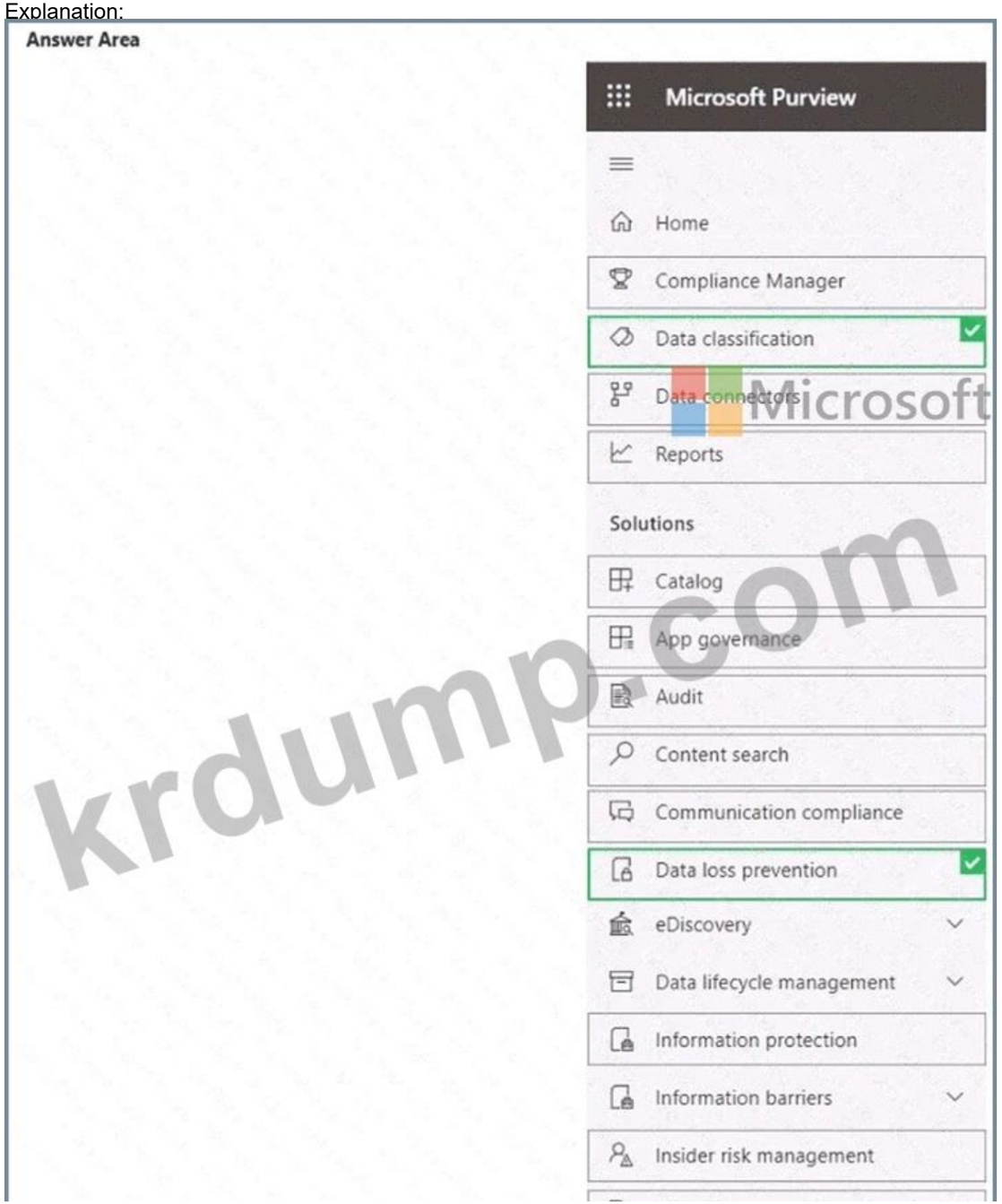
Answer Area




Data connectors
Reports
Solutions
Catalog
App governance
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management



Explanation:



NEW QUESTION: 228

□□□ Group1□ Group2□□ □ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□. □□ □□ □□□ □□□□ □□□ □□ □□(DLP) □□□ □□□ □□□□□.

* □□1 □□□□□ □□□□ □□□ □□□ □□□ □□□□ □□□□ □□ □□□.
* □□2□ □□□□ Microsoft Purview □□ □□□□ □□□□□ □□□ □□□ □□□□ □□□□ □□ □□□.
* □□□□ □□ □□□ □□□□□ □□□.

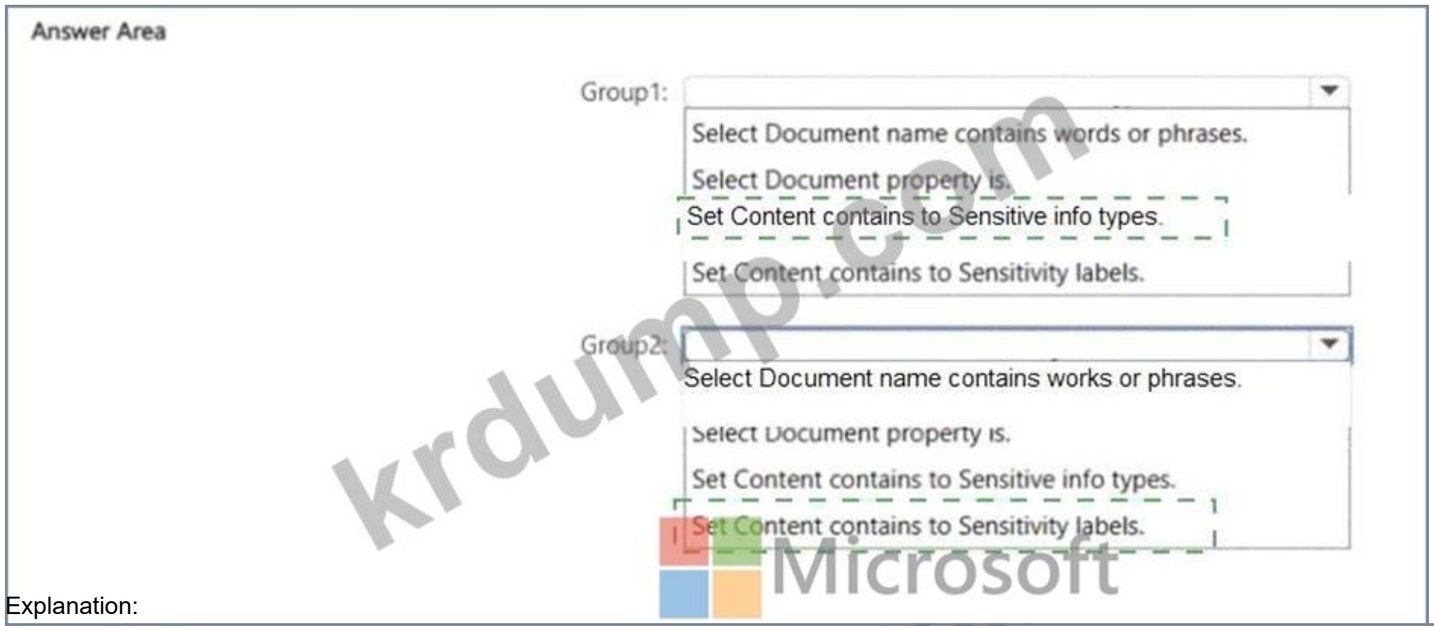
□ □□□□ DLP □□□ □□□□ □□□.

□ □□□ □□ DLP □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Answer:



Explanation:

NEW QUESTION: 229
Windows 10 □□□ □□ □□ □□ □□ □□□ □□□□ □□□.
Intune □□ □□□□ □□□ □□□□ □□□?
A. □ □□ □□
B. □□ □□□□ □□
C. □□ □□ □□□
D. □□ □□ □□
Answer: B (LEAVE A REPLY)

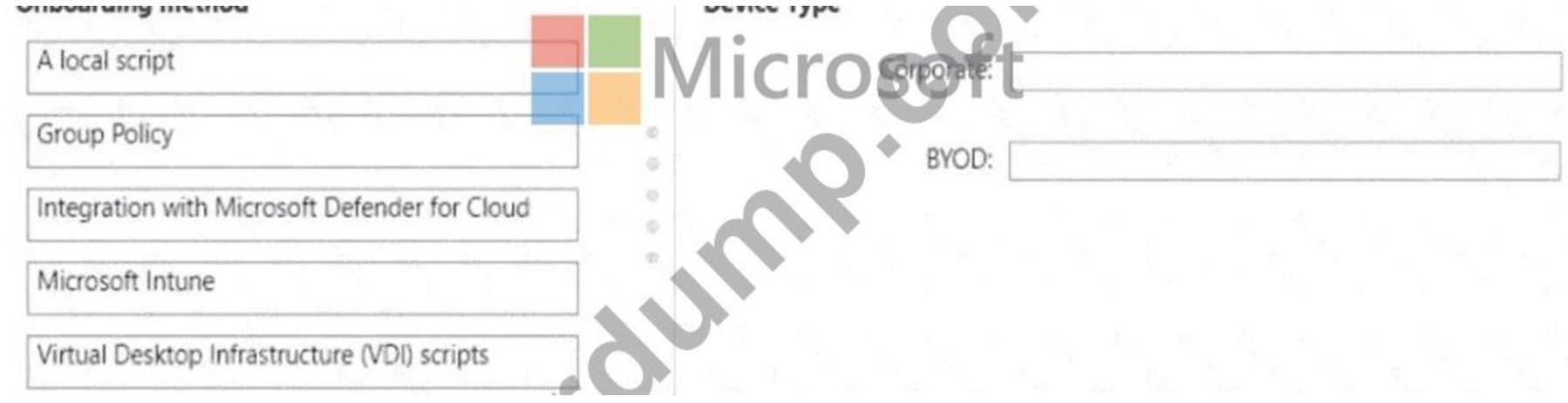
NEW QUESTION: 230
Microsoft 365 □□□ □□□□.
contoso.com□□□ □□□□ □□□□□.
□□□□ □□□□□ □□ admin@contoso.com□□ □□ □□□□ □□□□ □□□□ □□□□□.
□□□ □□□ □□□□ □□□ □□□ □□□□ □□□.
□□□ □□ □□□?
A. Microsoft 365 □□ □□□□ Microsoft 365 □□□ □□□ □□□□ □□□□□.
B. □□□ □□□□□□ □□□□ □□□ □□□ □□□□□.

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

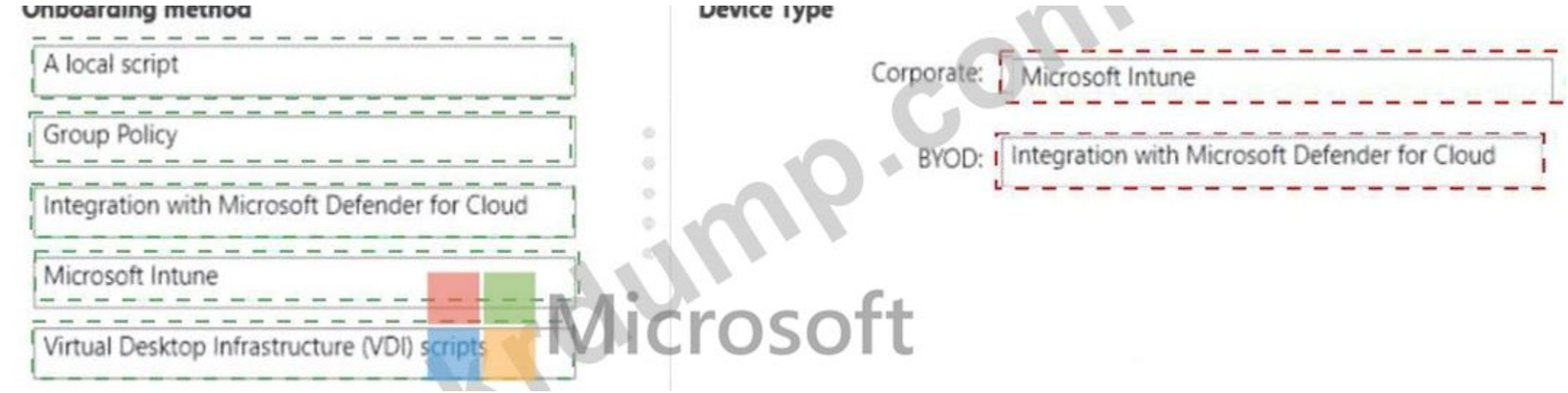
NEW QUESTION: 231
□□ □□ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

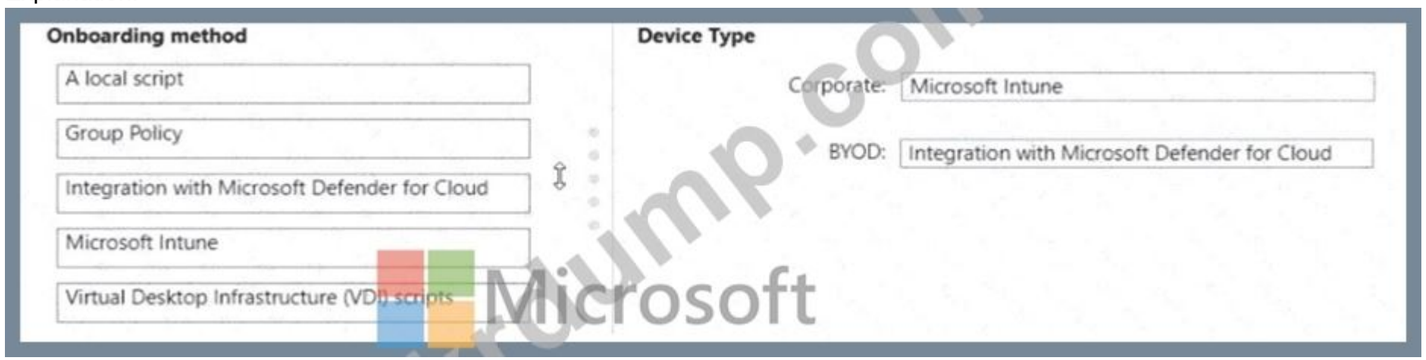
Microsoft Defender for Endpoint□ □□□ □□□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□ □□□ □□□ □□□□□ □ □□□ □□□□ □□□? □□□□□ □□□ □□□ □□□ □□□ □□ □□□□ □□□□□□. □ □□□ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □□□ □□□□□□ □□□□□ □□□□ □□□□ □ □□ □□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 232
□□□ □□□□ □□□□ □□ □□□□. □□□ □□□□□ □□□ □□□ 100□□ □□□ □□□□, □□ □□□□ □□ □□□ □□□□ □□□□□. □□□ □□□ □□□□ □□ □□□□ Group1□□□ □□ □□□ □□□□ □□□.

Answer:

See the solution below:

Explanation:

Create a dynamic user security group that evaluates the city attribute. Users will be added automatically whenever their city value equals Seattle.

Step-by-Step Solution with Explanation:

* Sign in to the Microsoft Entra admin center .
* Navigate to:

Entra ID # Groups # All groups

* Select New group .
* Configure the basic group settings:

Setting

Value

Group type

Security

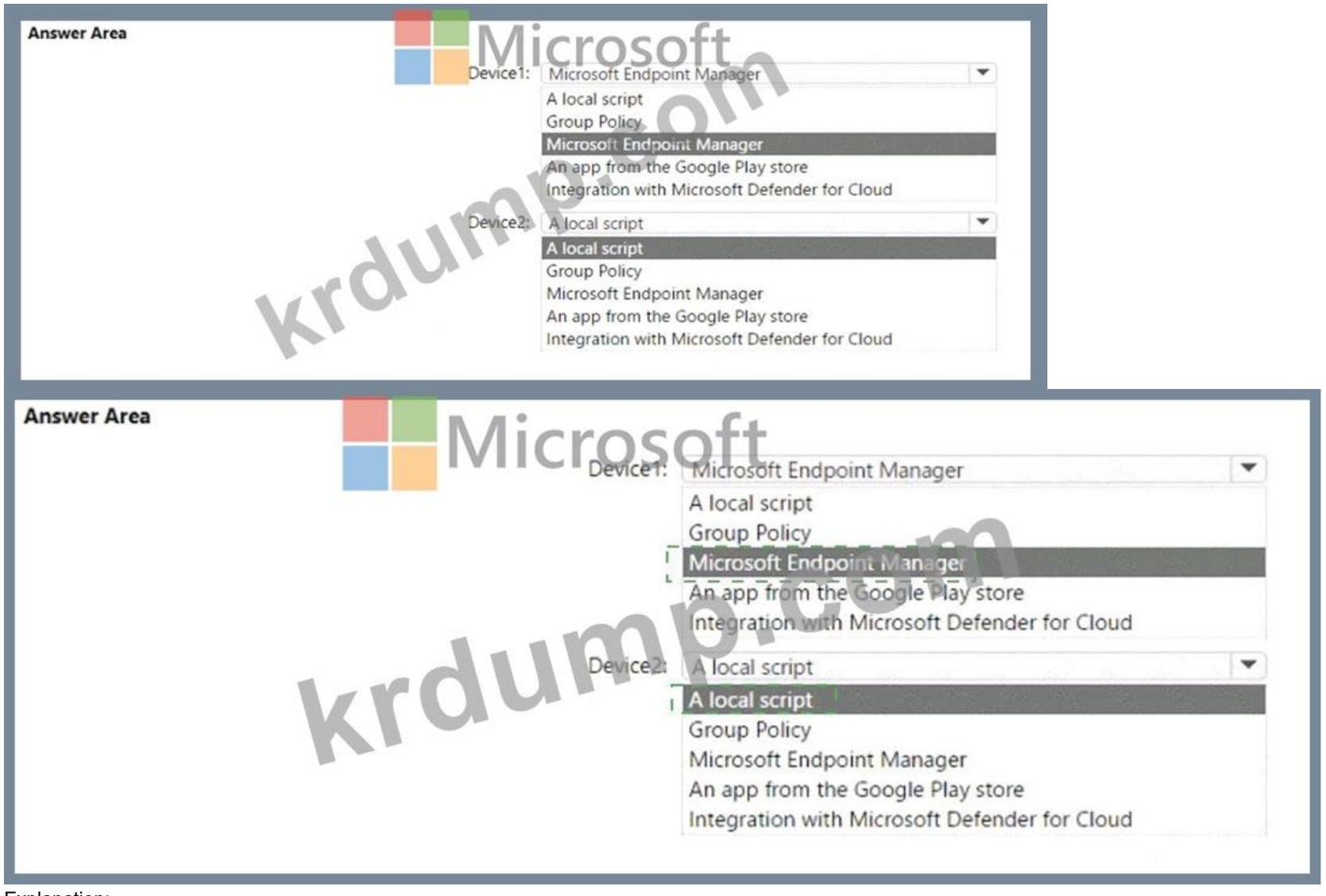
Group name

Group1
Microsoft Entra roles can be assigned to the group
No
Membership type
Dynamic User
* Under Dynamic user members , select Add dynamic query .
* In the rule builder, configure:
Rule component
Value
Property
city
Operator
Equals
Value
Seattle
* Select Add expression if the portal requires the expression to be added to the rule.
* Confirm that the complete rule syntax is:
(user.city -eq " Seattle ")
* Select Save to save the dynamic membership rule.
* Select Create to create Group1.
* Open Group1 # Dynamic membership rules and verify that the rule was saved correctly.
* After the users are created with City = Seattle , allow Microsoft Entra time to evaluate their attributes and populate the group. Dynamic membership processing is not always immediate.
Do not manually add the 100 users. The dynamic rule ensures that new Seattle users are added and users whose city changes from Seattle are removed automatically. Microsoft lists city as a supported dynamic membership property with the syntax user.city -eq " value " . Microsoft: Dynamic membership rules

NEW QUESTION: 233
Microsoft Intune□ □□□□ □□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

Device1□ Device2□ Microsoft Defender for Endpoint□ □□□□□ □□□.
□ □□□ □□□□□ □ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Explanation:

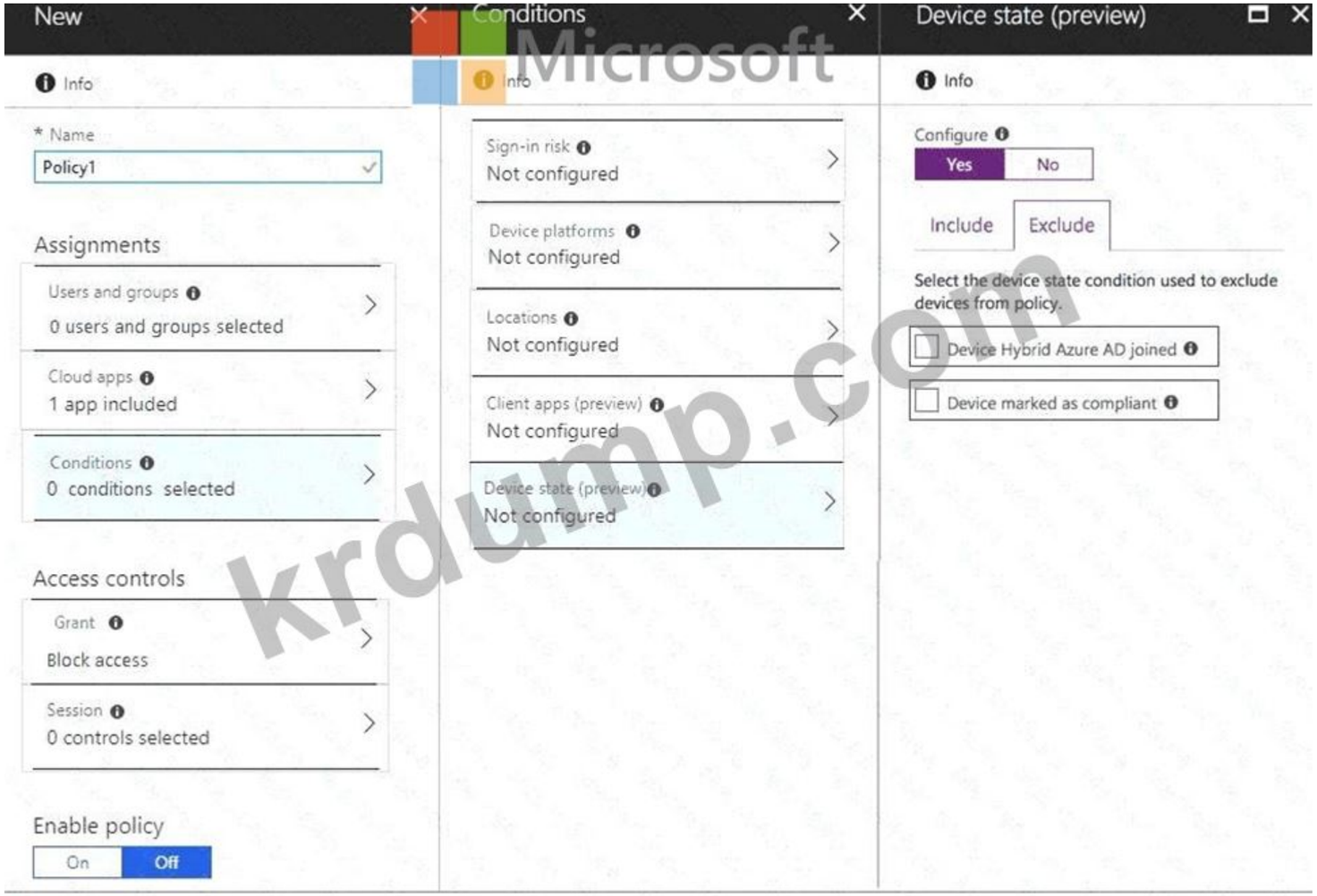
NEW QUESTION: 234

Microsoft Entra ID □□ □□ □□(Azure ATP)□ □□□□□.
□□ □□□ □□ Azure ATP □□□ □□□□ □□□□.

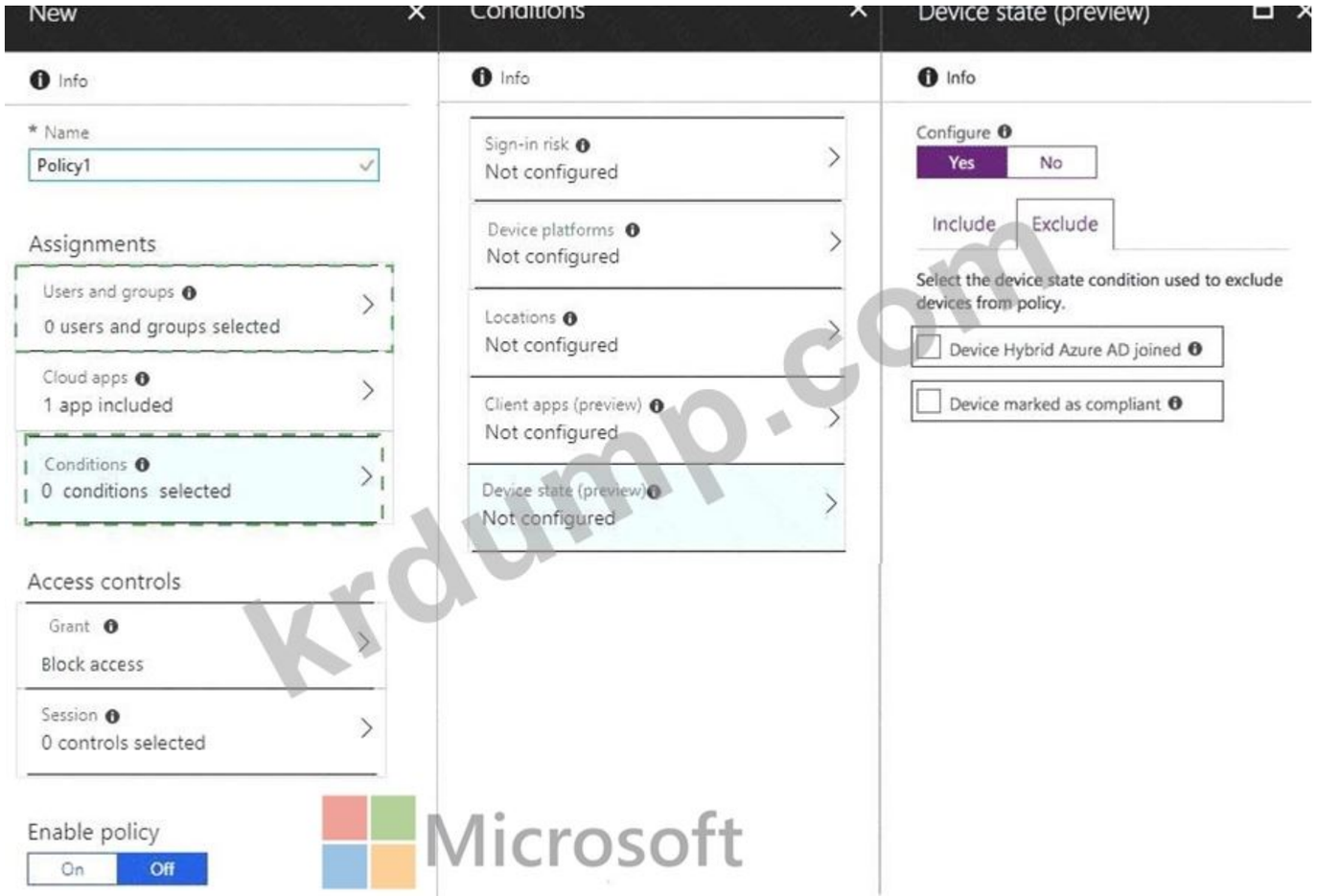
Azure ATP □□□□ □□□□ □□□□□ □ □□□ □□□□□□ □ □□□ □□□□?
A. 7□□
B. 48□□
C. 20□□
D. 12□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 235
□□□□ □□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□ □□□□.
60□ □□ □ □□□□ 50□□ □□ □□□ □□□□□□ □□ □□□ □□□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□ □□
C. □□ □□ □□
D. □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 236
□□ □□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□□ □□□.
Exchange Online□ □□□□ □□□ □□□□□.
Policy1□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

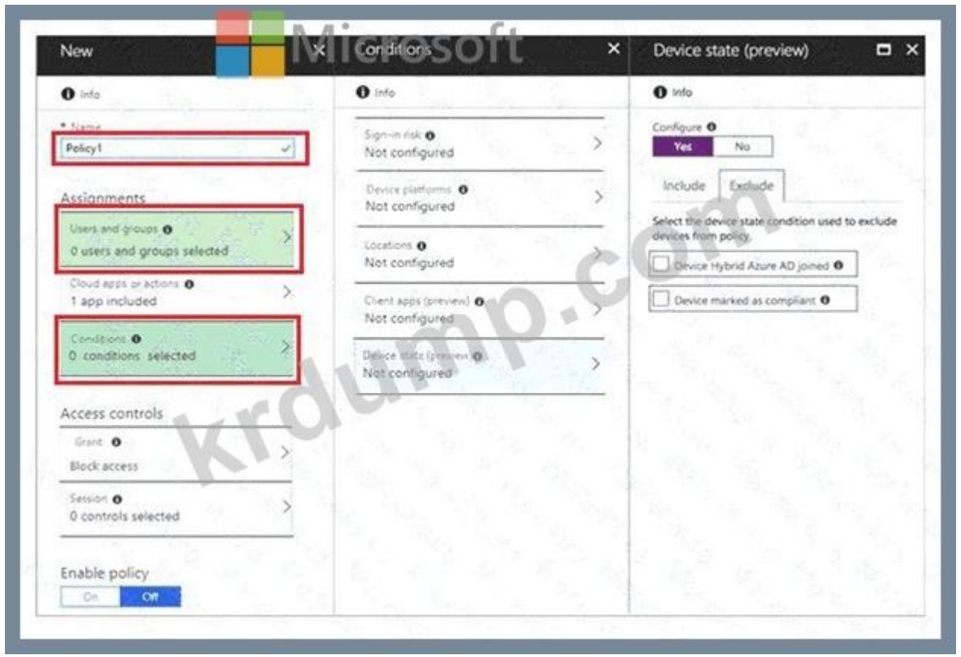


Answer:



Explanation:

Suggested answer:



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

NEW QUESTION: 237

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: 238

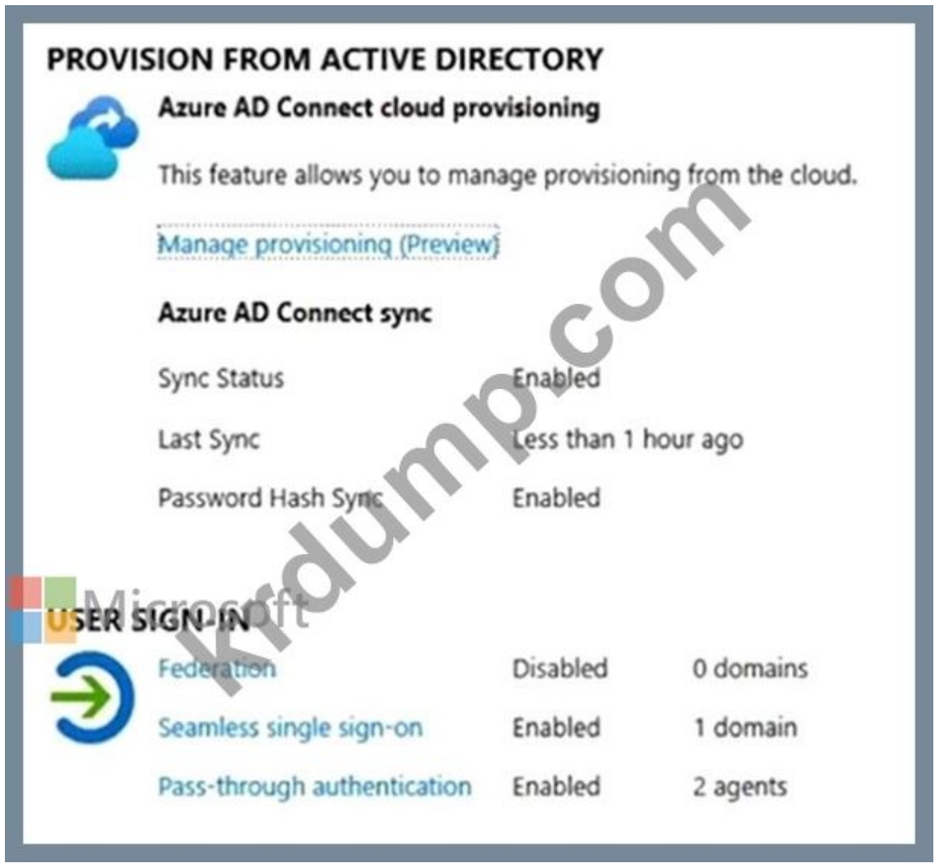
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □□ □□□ □□□□.

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

□□ □□□□ □□□ □□□ □□□ contoso.com□□□ Microsoft Entra □□□□ □□□□□□. (□□ □□ □□□□□□.)



User2□ user2@fabrikam.com□□ □□□□ □ Microsoft Entra ID □□□ □□□□□.

User2□ Microsoft Entra ID□ □□□□ □□□□ □ □□□ □□ □□□.

□□ □□: Microsoft Entra □□ □□□□ User2□□ □□ □□ □□□ □□□ □□□□□. User2□□ user2@contoso.com□□ □□□□□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

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

NEW QUESTION: 239
Microsoft 365 □□□ □□□□.
□□□ □□□□□ □□□ □□□□ □□□□ □□ □□□□ □□□ □□ □□(DLP) □□□ □□□□.
□□□ □□□□ □□□ □□□ □□□□ □□ □ □□ □□□□□ □□ □□□ □□, □□ □□□□ □□ □□□□□□ □□□□ □□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□ □□
B. DLP □□ □□
C. □□ □□ □□
D. □□ □□ □□
Answer: (SHOW ANSWER)