Microsoft.MS-102-KR.v2026-03-13.q214

□□□□:	MS-102-KR
□□□□:	Microsoft 365 Administrator (MS-102 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	214
□□:	v2026-03-13
# □□ □:	265
# □□ □□□:	2140
https://www.krdump.com/Microsoft.MS-102-KR.v2026-03-13.q214.html	

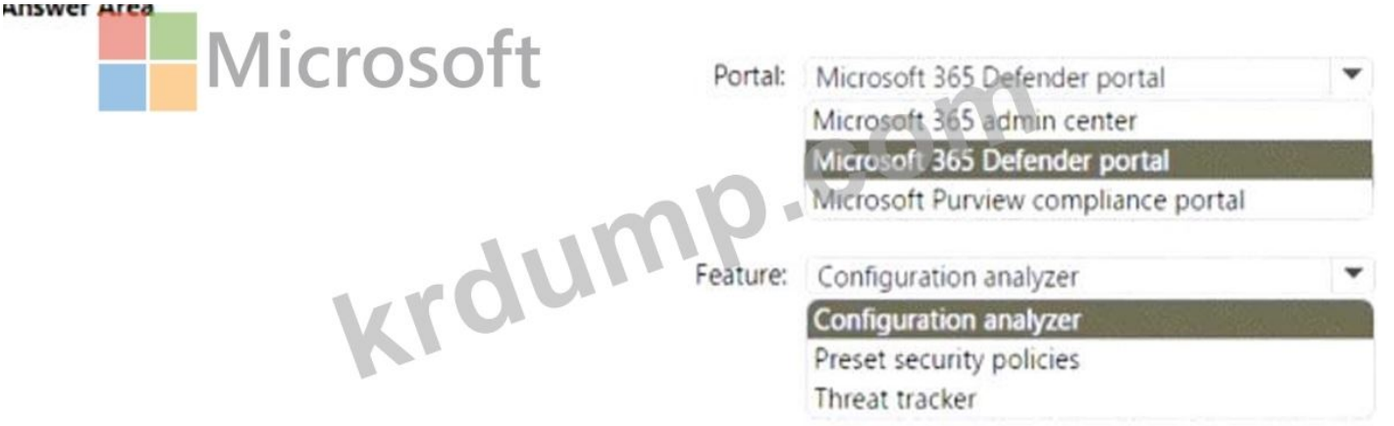
NEW QUESTION: 1

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

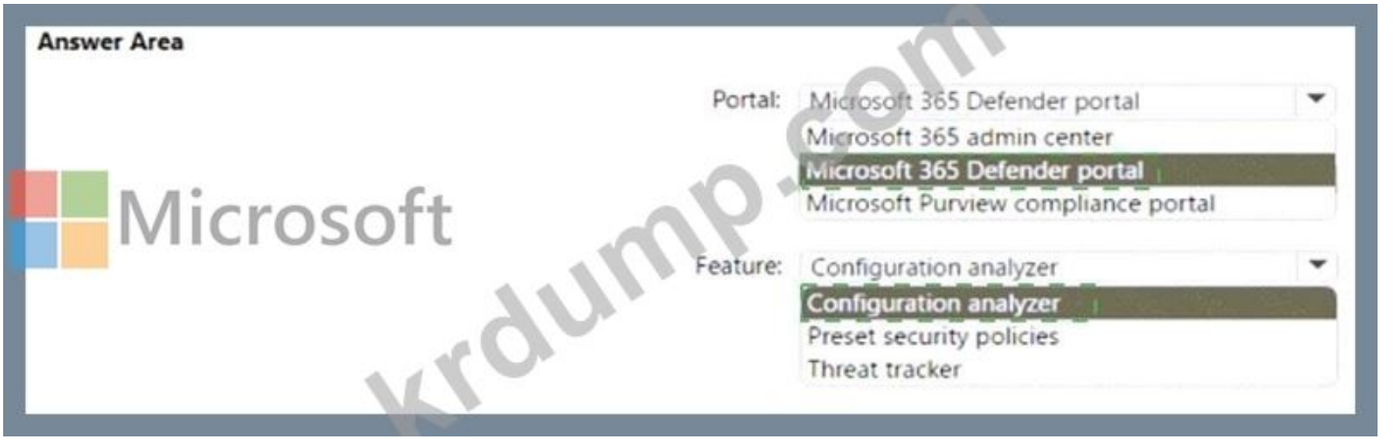
□□ □□□ □□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.



Answer:



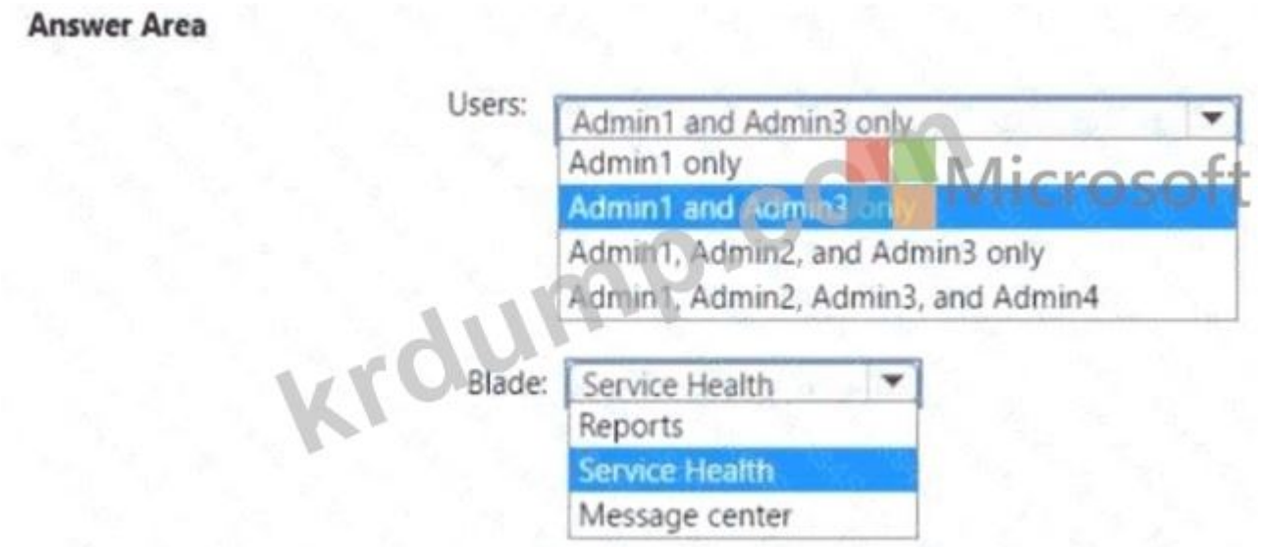
Explanation:

NEW QUESTION: 2

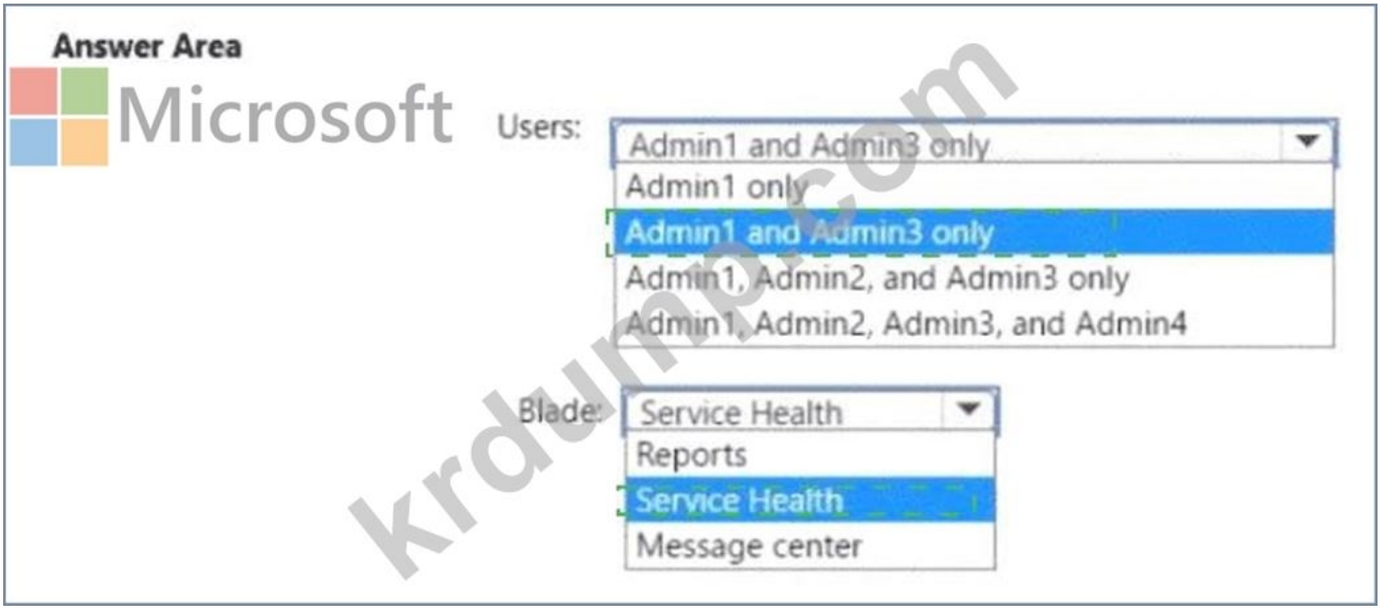
Microsoft 365 □□□□ □ □□ □□□ □□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.

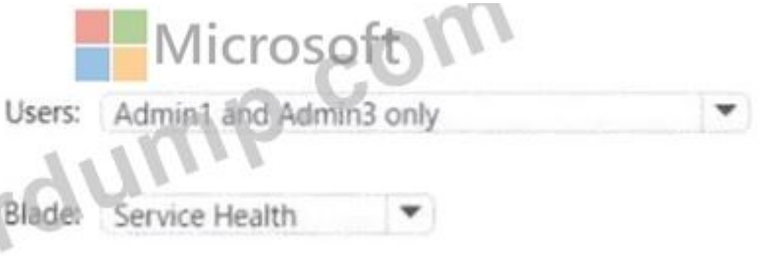


Answer:



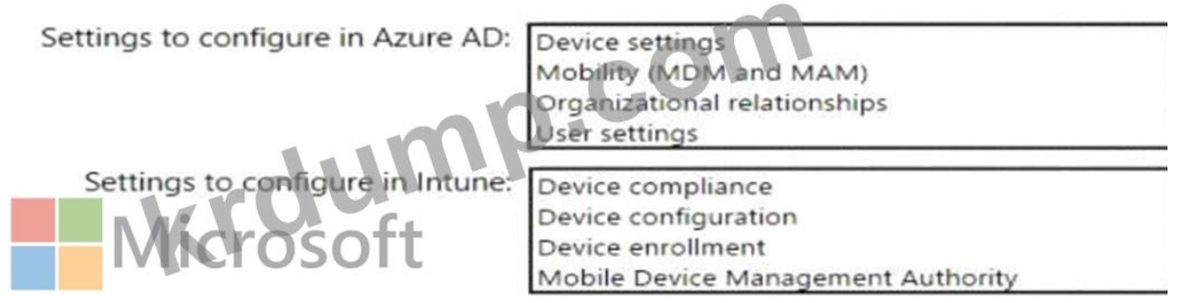
Explanation:

Answer Area



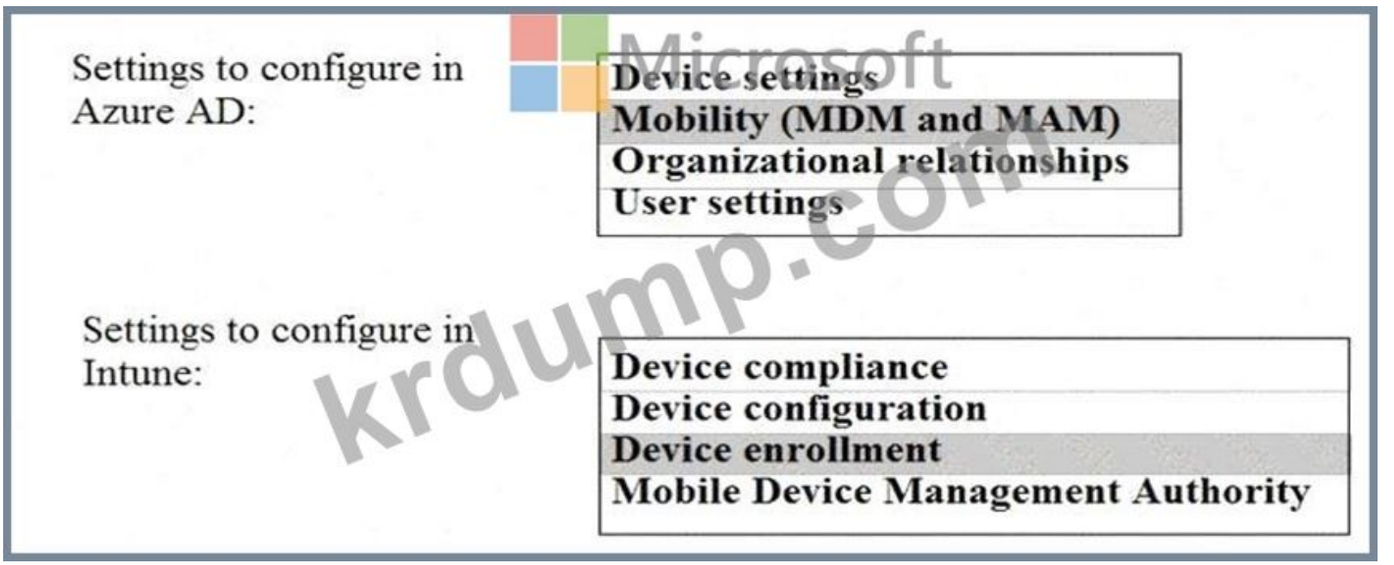
NEW QUESTION: 3
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□(MFA)□ □□□□□ □□□.
□□□□ □□ □□ □□□ □□□□ □□□. □□□□ □□□□□ MFA□ □□□□ □□□□ □ □□ □□□ MFA□ □□□ □□□□□□ □□□ □□□□□ □□ □□□.
□□□ □□□□ □□?
A. □□□□
B. FID02 □□ □
C. □□□ OTP
D. □□
E. Microsoft □□□
Answer: E (LEAVE A REPLY)

NEW QUESTION: 4
Intune□ □□ □□□ □□ □□□ □□□ □□ □□□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
Answer Area



Answer:
Answer Area

Explanation:



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

NEW QUESTION: 5
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows Server 2019□ □□□□ □□□ □□□□□ □□□□. □□□□□ □□□□ □□ □□□ Windows Server 2012 R2□□□.
□ □□□□□ Windows 10□ □□□□ 100□□ □□□□ Windows Server 2012 R2□ □□□□ Server1□□□ □□ □□□ □□□□ □□□□.
Server1□ □□□□ □□□□ □□□□ Windows 10 □□ □□ □□□ □□□ □□□□□.
Server1□ □□ □□ □□ □□(GPMC)□ □□□□□.
Server1□□ □□□□□ Windows □□□□ □□ □□ □□□ □□□□ □□□.
□□□: Server1□ Windows Server 2019□ □□□□□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 6
□□□ 5□ □□□ □□□□ □□ □□□□.
□□ □□□□ Microsoft 365 □□□□ □□□□.
□ □□□□ □□ □□□□ □□□□□.
Microsoft Intune□ □□□ □□□□□.
□□ □□ □□□ □□□□ Intune□ □□□□ □□□□ □□□□ □□□□ □□□.

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

A. □□ □□□□

B. □□ □□

C. □□ □□□

D. □□□ □□□ □□

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 7

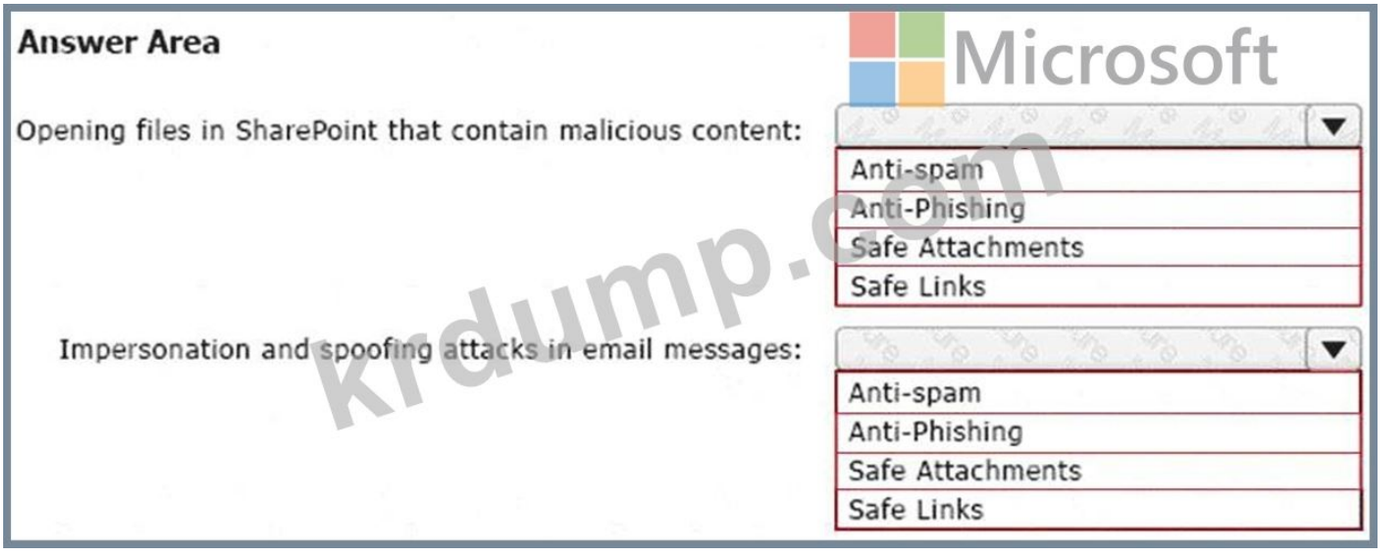
□□□

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

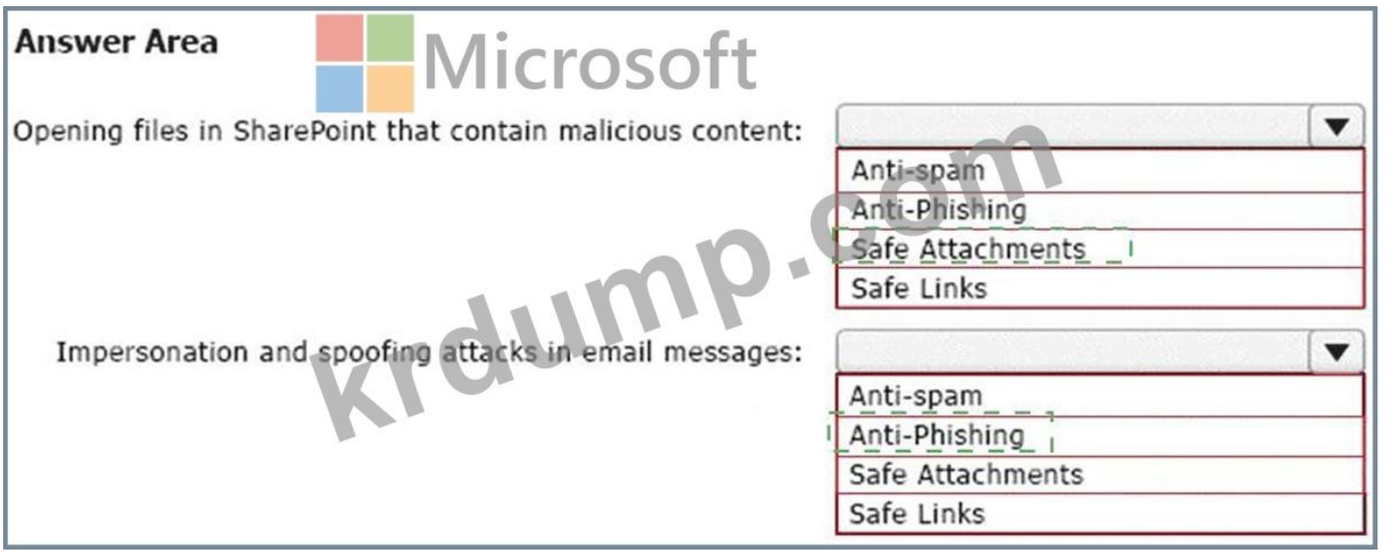
* □□ □□□□ □□□ Microsoft SharePoint□ □□ □□
* □□□ □□□□□□ □□ □ □□□ □□

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

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 8

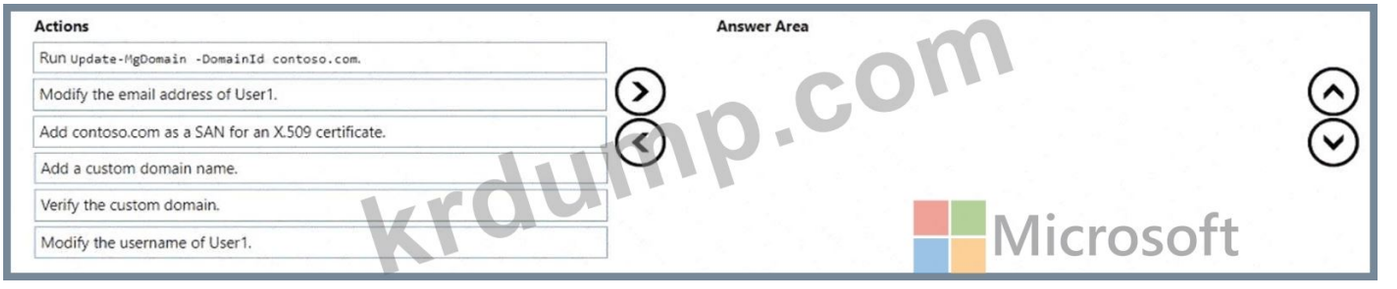
□□□ □□□□ contoso.onmicrosoft.com□□□ Azure AD □□□□ □□□□.

□□ □□□□ contoso.com□□□ □□□□ □□□□ □□□ □□ DNS □□□□ □□□□□.

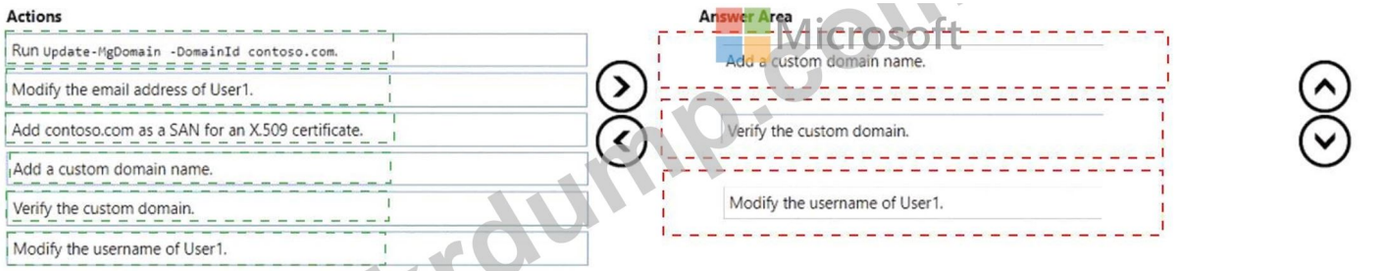
User1□□□ □□□ □□□ □□□□. User1□ userl@contoso.onmicrosoft.com□□ □□□□□ □ □□□□□.

User1□ user1@contoso.com□□ □□□□□□ □□□□ □□□.

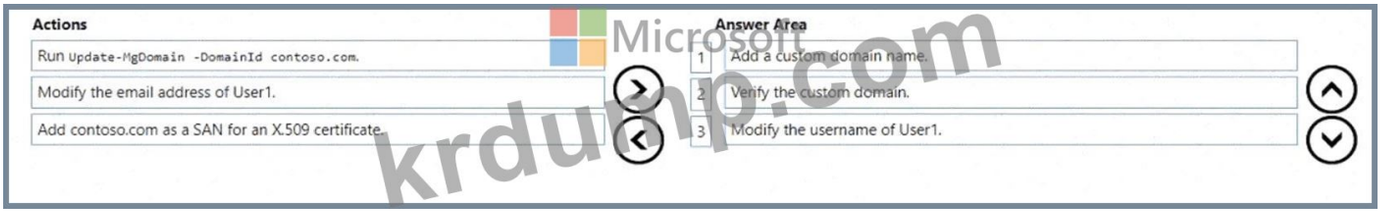
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □ □□□ □□□ □□□ □□□ □□□□□.



Answer:



Explanation:

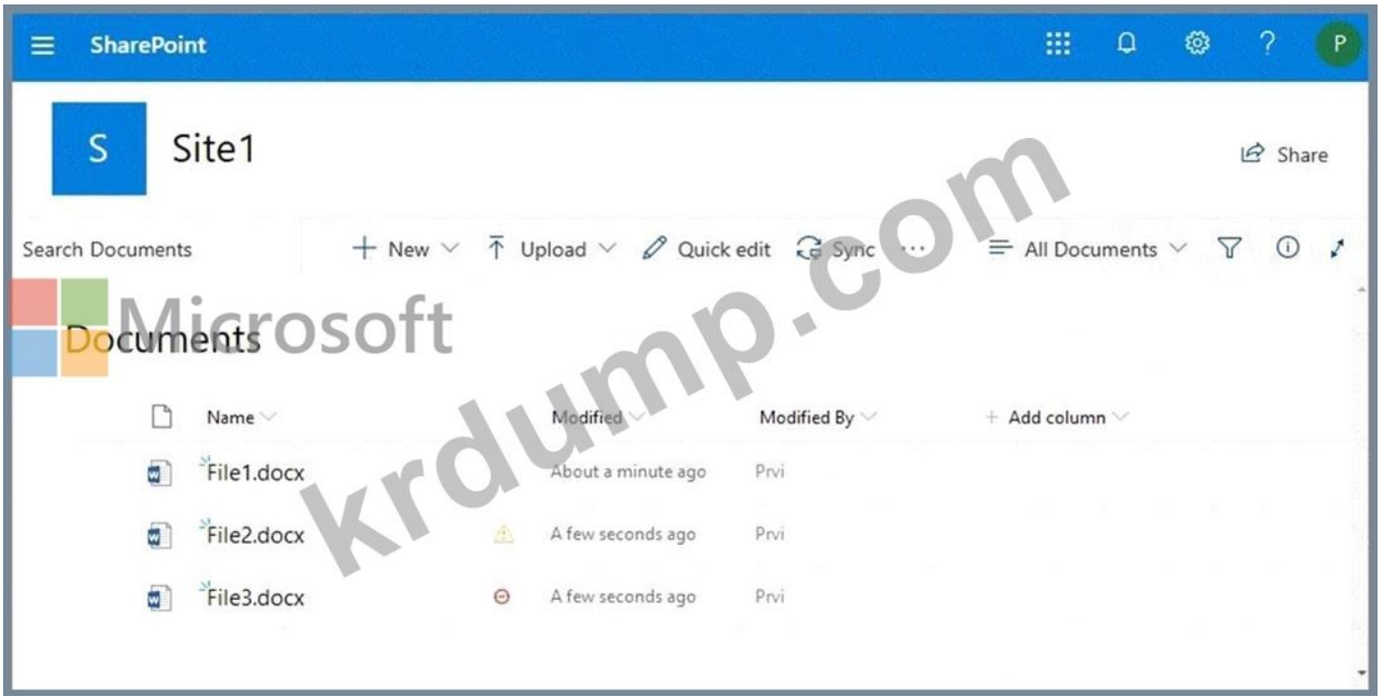


NEW QUESTION: 9

Microsoft 365 □□ □□ □□□□ Site1□□□ Microsoft SharePoint Online □□□□ □□ □□□ □□ □□(DLP) □□□ □□□□□. Site1□□ □□ □□ □□□ □□□ □□□□ □□□□.

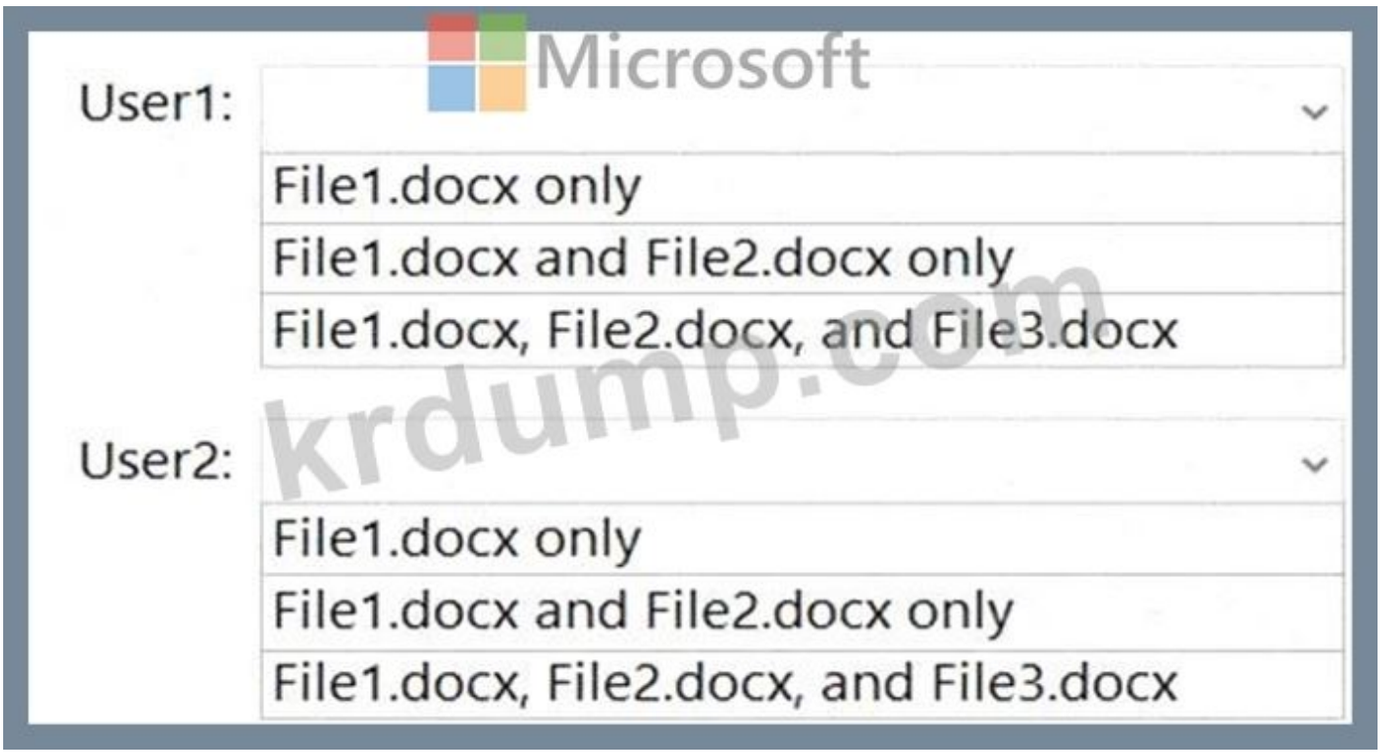
Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

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



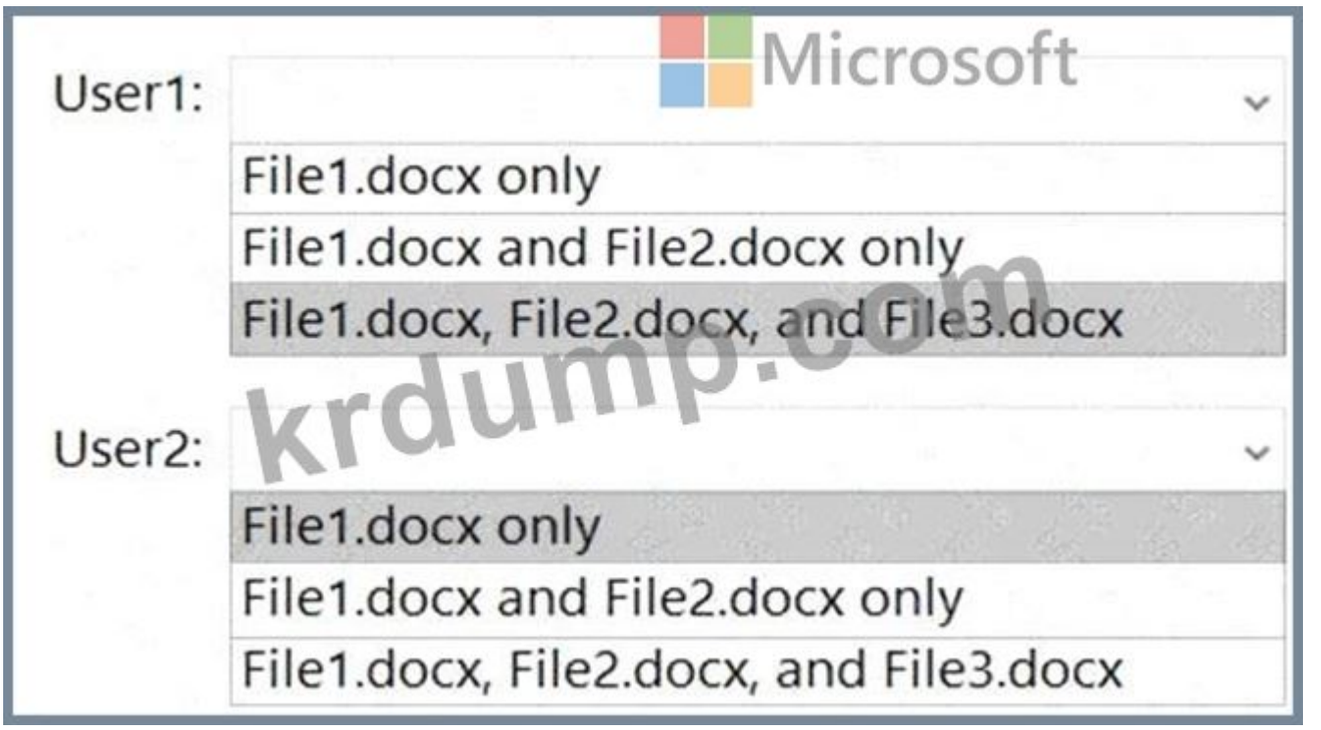
User1□ User2□ □□ □□□ □ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□ □.

□□□□: □□ □□□ 1□□□□.



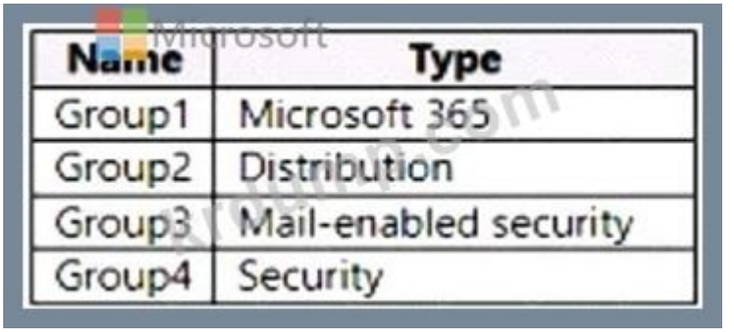
Answer:

Explanation:



Reference:
https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/
https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/

NEW QUESTION: 10
□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.



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

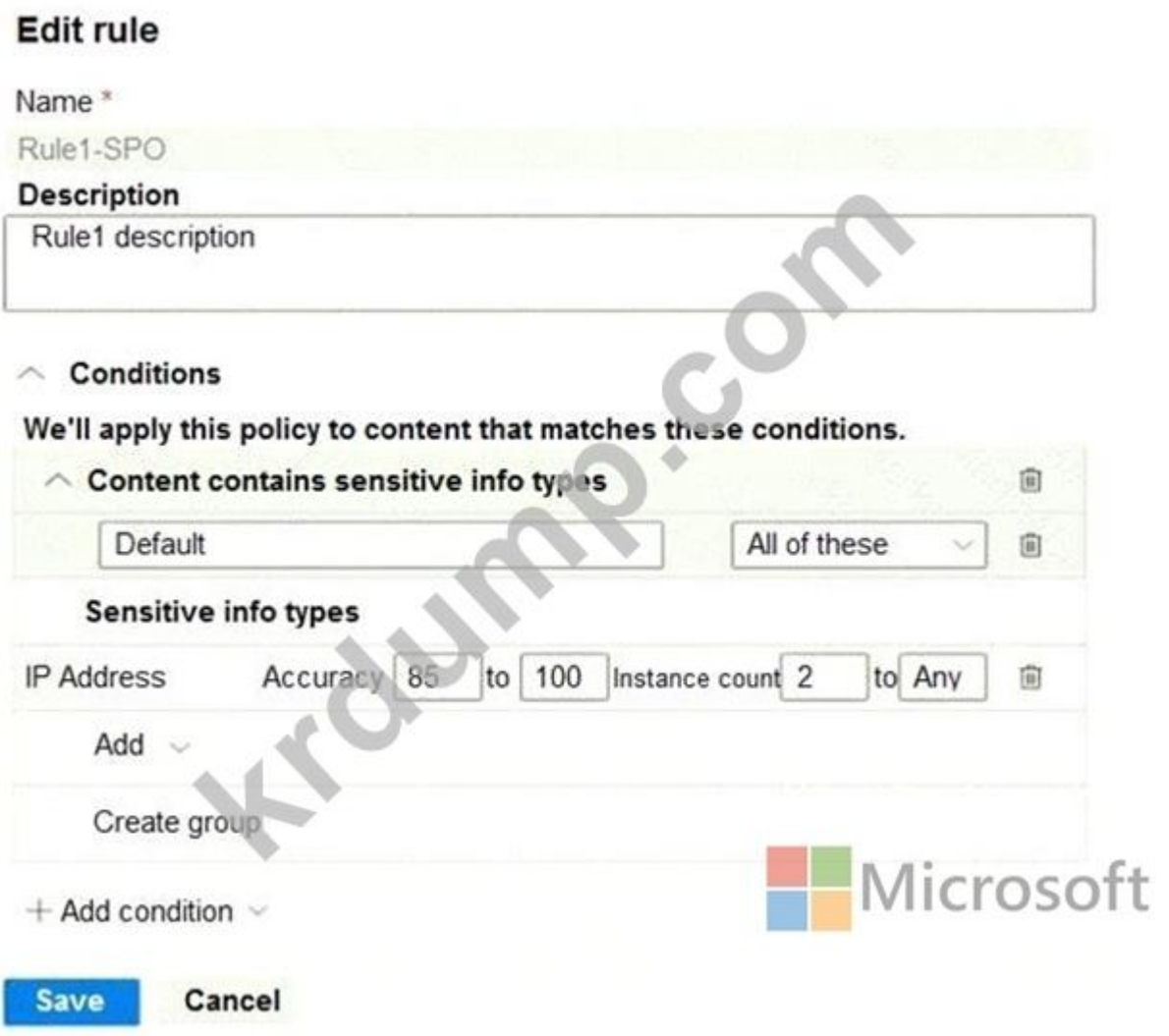
Label1□□□ □□□ □□□ □□□□ □□□ □□□□□.
□□ □□□ Label1□ □□□ □ □□□?
A. □□1□
B. □□1□ □□2□
C. □□1□ □□4□
D. Group1, Group2, Group3□
E. □□1 □□2, □□3, □□4
Answer: A (LEAVE A REPLY)
In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the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

NEW QUESTION: 11
Microsoft 365 □□□ □□□□.
□□ □□□□ □□□□ Microsoft Exchange Online□ □□□□□.
User1□□□ □□□□ □□□□□ ProjectX□□ □□□ □□□ □□ □□□ □□□□ □□□ □□ □□ □□□.
□□ □□ □□□ □□ □□□?
A. □□□□ □□ Microsoft Defender□□ □□ □□□ □□□□.
B. Microsoft Purview □□ □□ □□□□ □□□□ □□□ □□□ □□□□.
C. Microsoft 365 Defender□□ □□□ □□□ □□□□□.
D. Exchange □□ □□□□ □□ □□ □□□ □□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
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□ □□ □□□ □□ □□□□□.

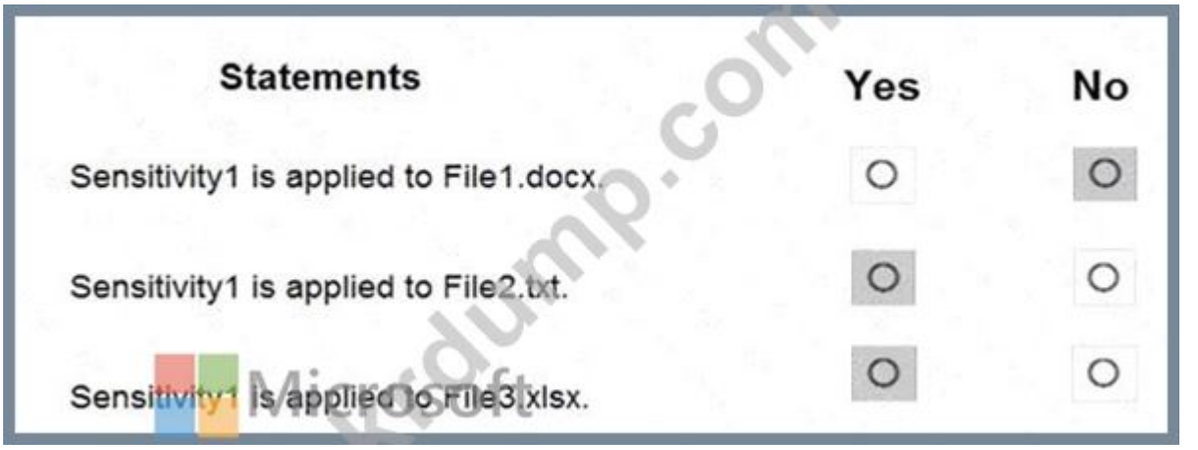


□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

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: 13
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

□□1□ □□ □□ □□□ □□□□ □□□(SSPR)□ □□□□□□. SSPR□ □□ □□□ □□ □ □□□ □□ □□□ □□□□□.
□□ □□□□ SSPR□ □□□ □ □□, □□ □□□□ □□□□□ □□□□□ □□ □□ □□□ □□□ □□□? □□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 14

□□□

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

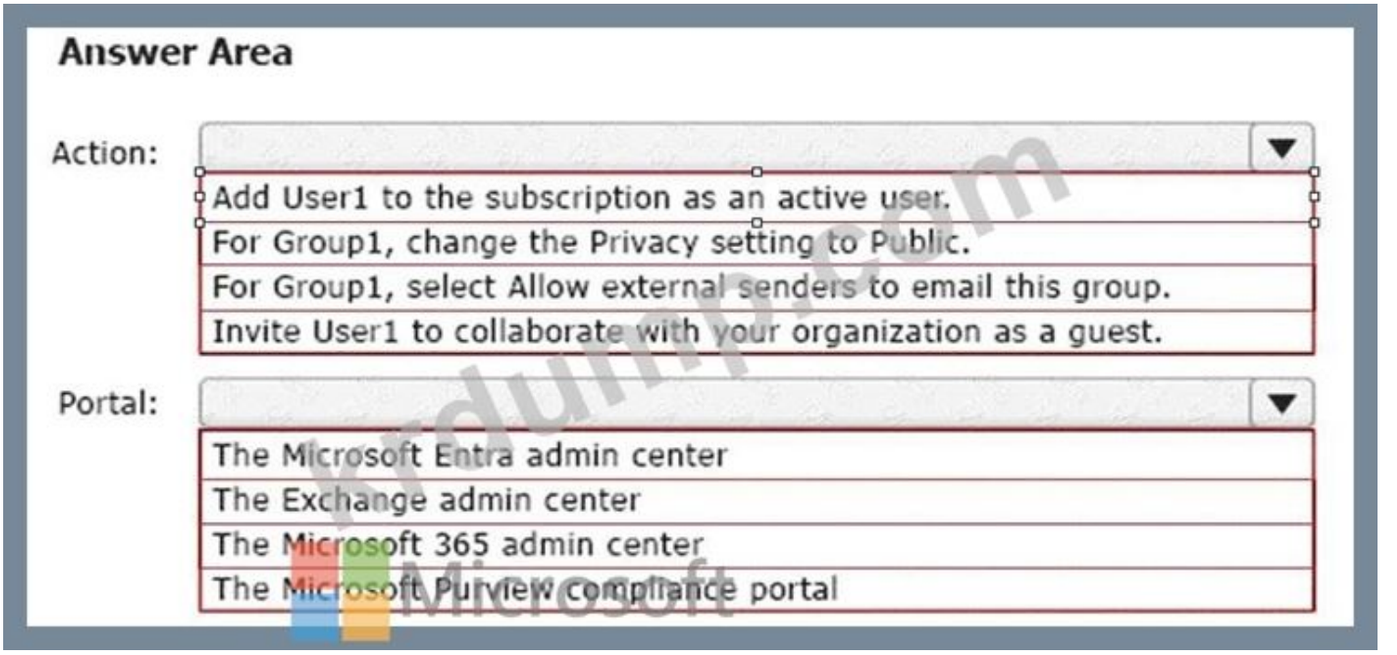
Group1□ □□ □□□ □□□ □□ □□□□ □□□□.

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

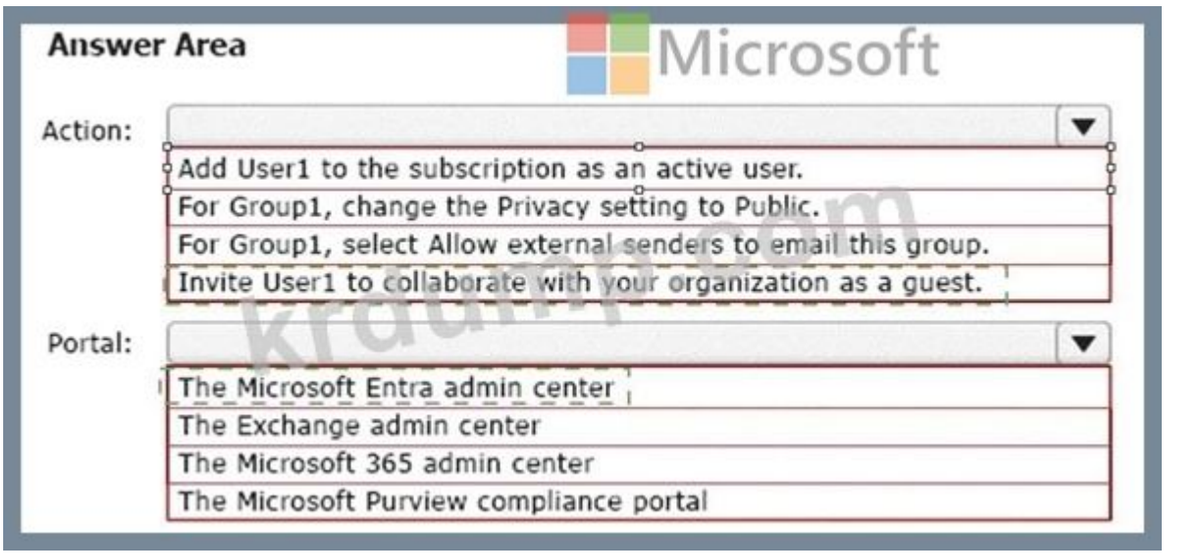
User1□ Group1□ □□□□ □□□.

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

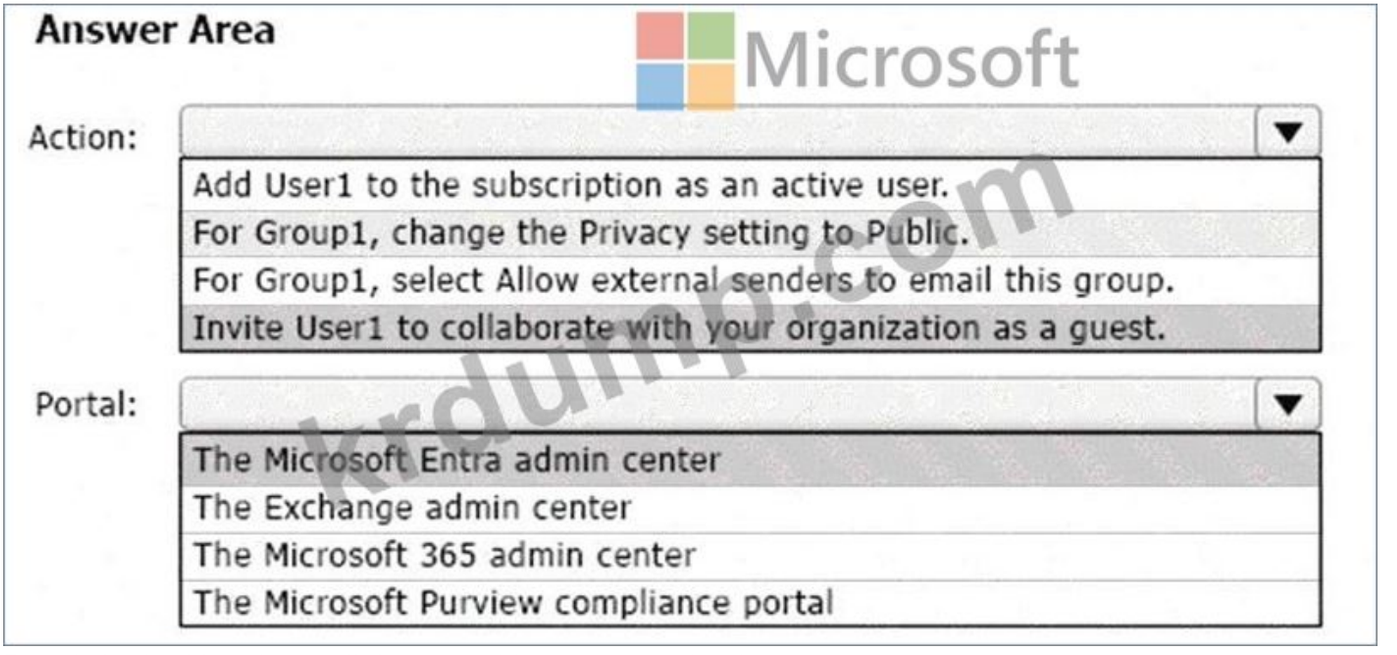
□□□□: □□ □□□ 1□□□□.



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 Azure Active Directory to add guest users" link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at https://aad.portal.azure.

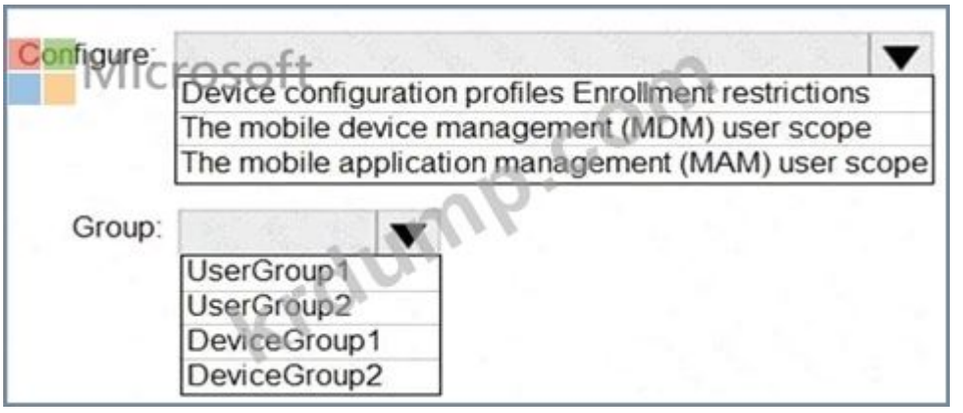
com.

On the "New user" page in the Microsoft Azure portal, you must choose to either "Create user" or "Invite user". If you choose the "Create user" option, this will create a new user in your organization, which will have a login address with format username@tenantdomain,dot,com. If you choose the "Invite user" option, this will invite a new guest user to collaborate with your

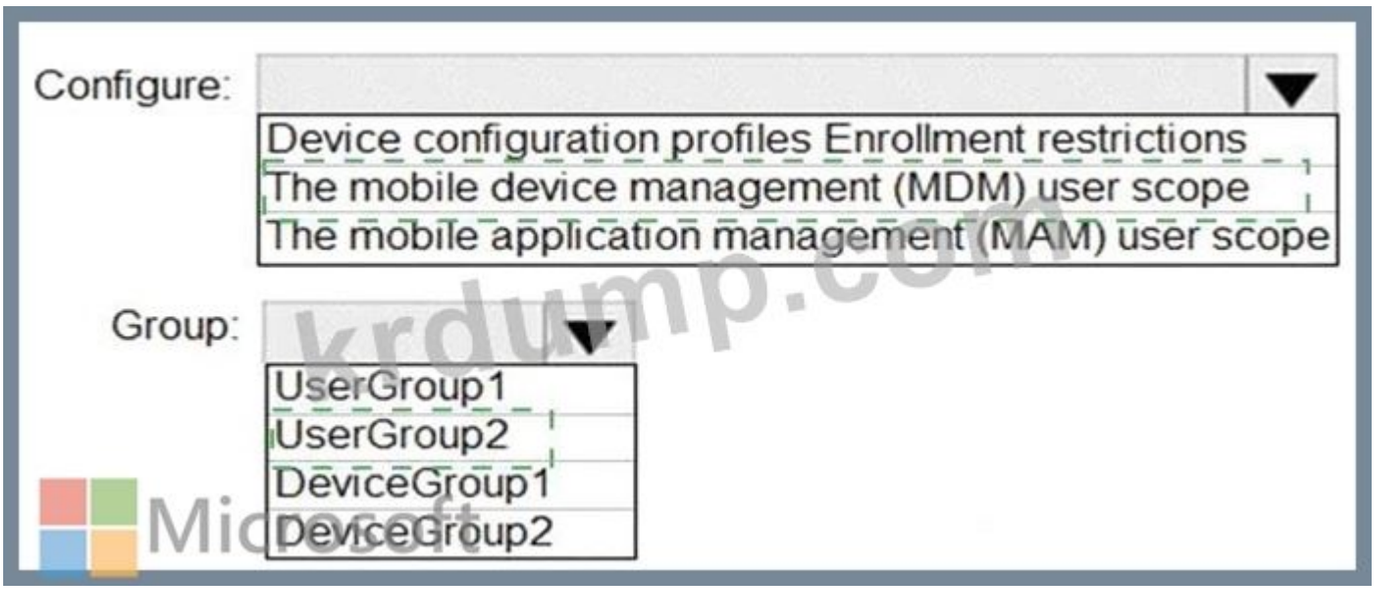
organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the "Invite user" option.
Box 2: The Microsoft Entra admin center
Microsoft Entra admin center unites Azure AD with family of identity and access products
Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.
Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).
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: 15
Microsoft 365 E5 □□□ □□□□.
□□□ □□□ □□□ □□□□□□□ Microsoft Defender for Cloud Apps□ □□□□ □□□. □ □□ □□ □□□?
A. □□ □□□ □□□□.
B. □□□ □□ □□□ □□□□□□.
C. □□□ □□□ □□□□.
D. Microsoft 365□ □ □□□□ □□□□.
Answer: (SHOW ANSWER)

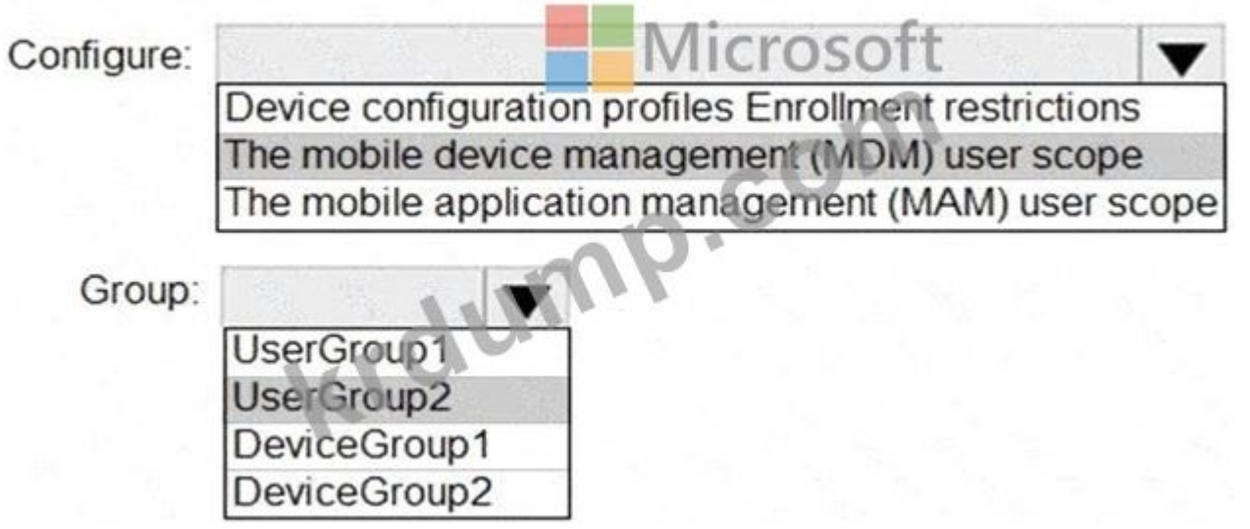
NEW QUESTION: 16
Intune□□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□, □□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □ □□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

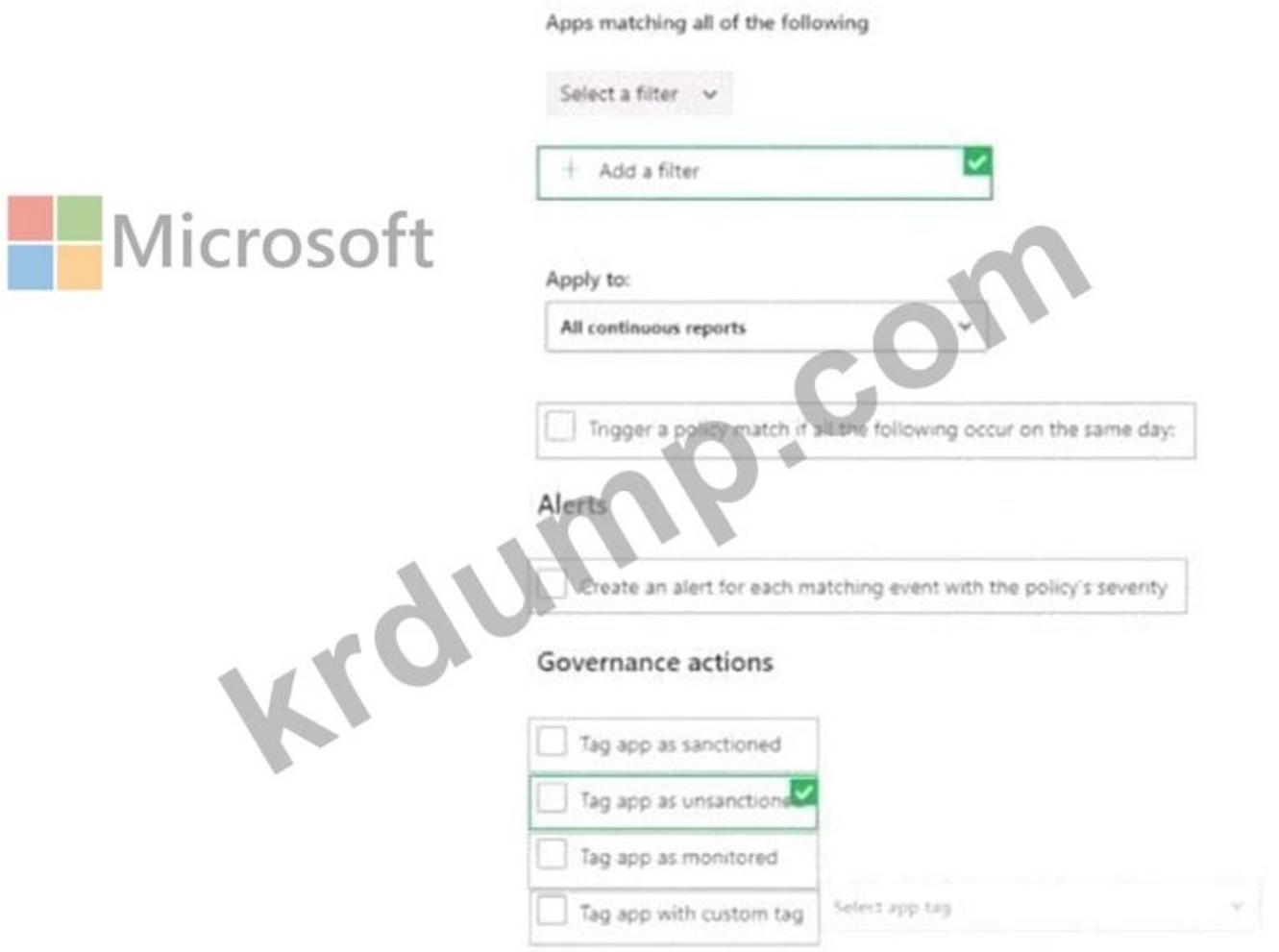


Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

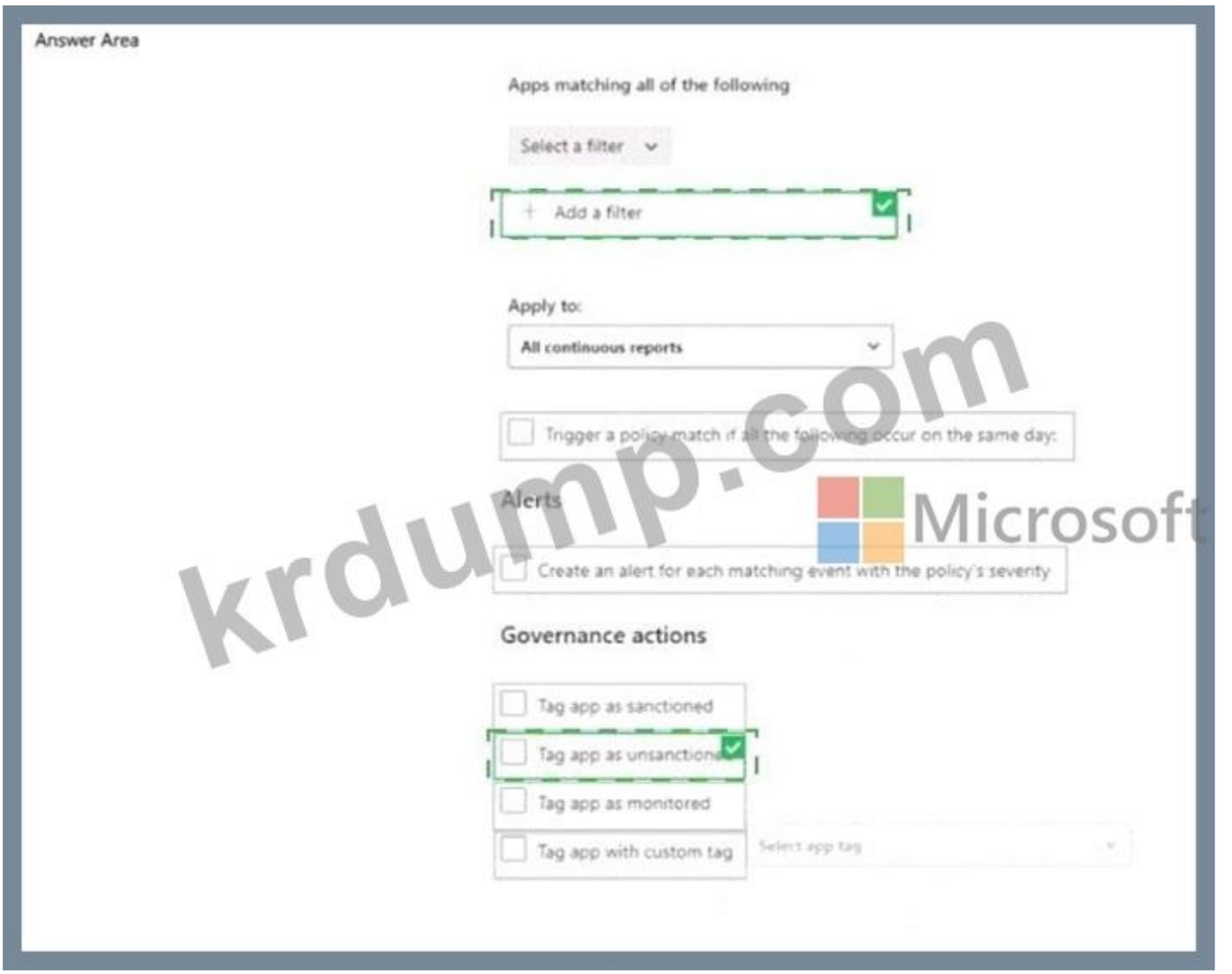
NEW QUESTION: 17
Microsoft 365 □□□ □□□□.
□□□□ □□ Microsoft Defender□ □□□□□□ Microsoft Defender□ □□□□□.
□□ □□□ 4□ □□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

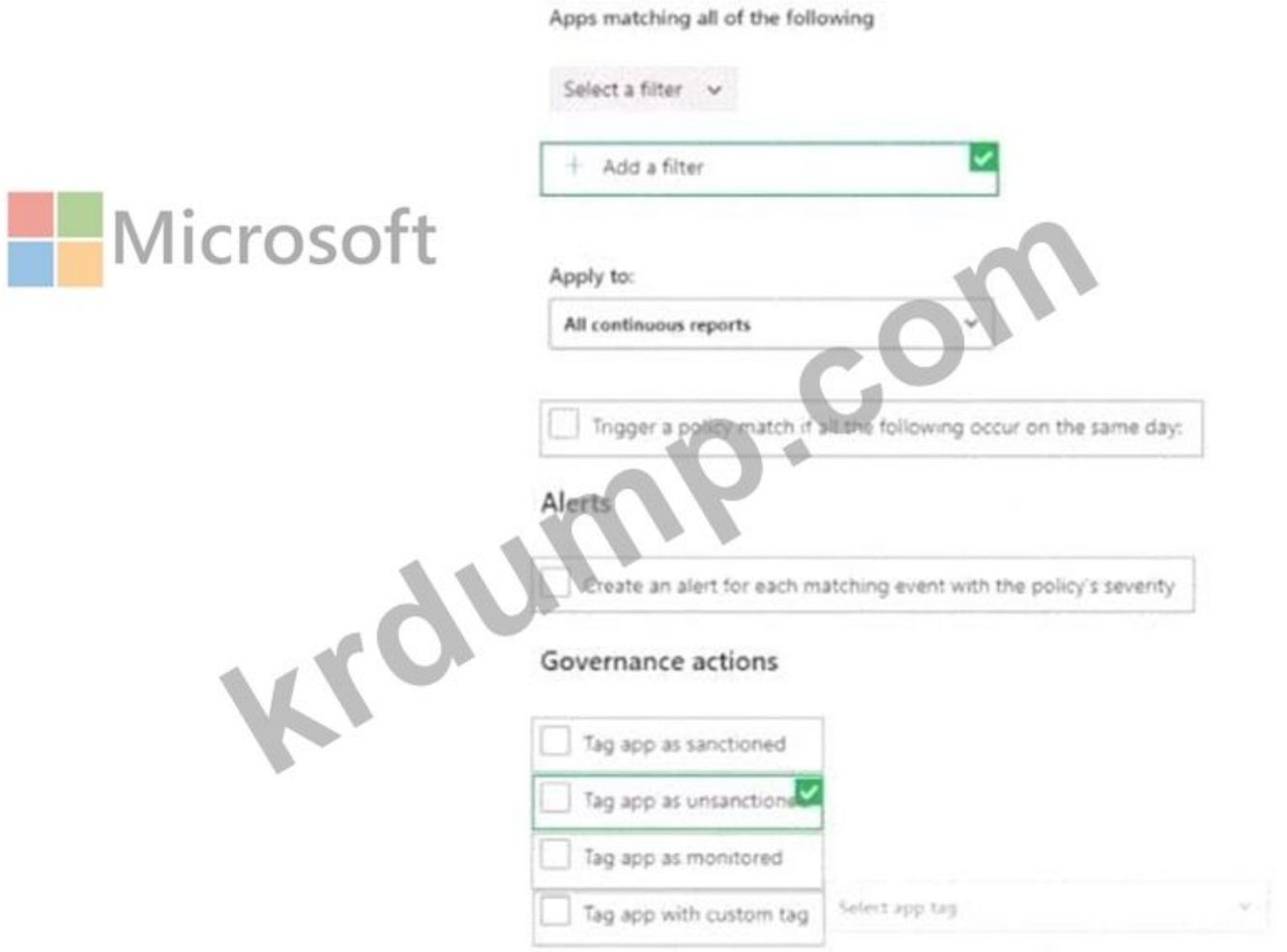


Answer:



Explanation:

Answer Area



NEW QUESTION: 18

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

NEW QUESTION: 19

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

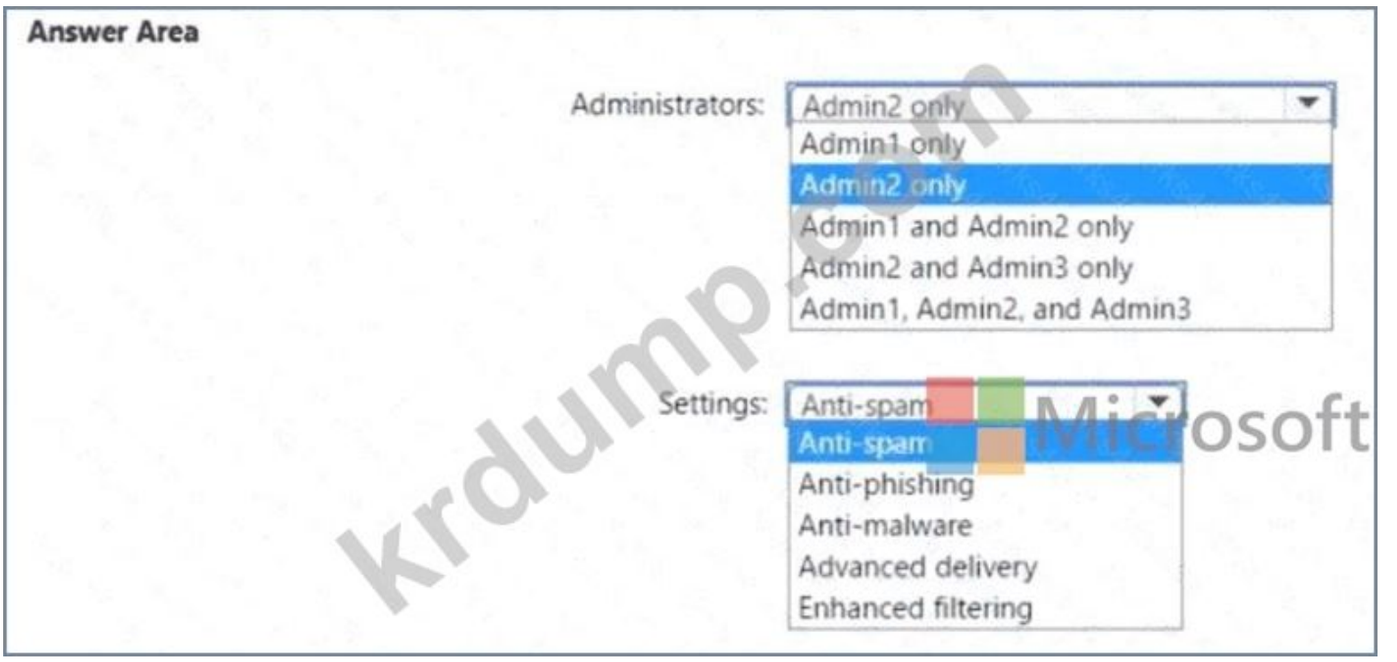
A. □□□

B. □

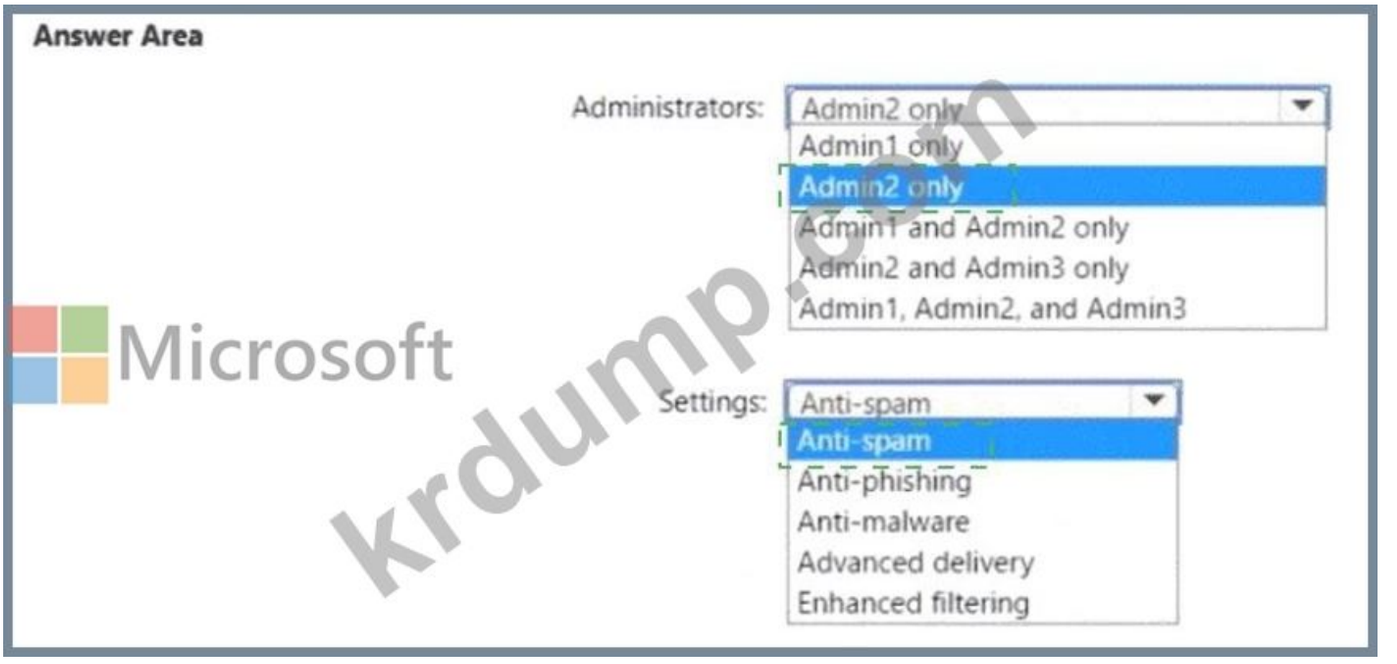
Answer: (SHOW ANSWER)

NEW QUESTION: 20

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



Answer:



Explanation:

NEW QUESTION: 21

Microsoft 365 □□□ □□□□.

□□ □□□ □□ □□ □□□ □□□□.

Policy1

Edit policy | Delete policy

Status On

Name your alert

Description
Add a description

Severity
Low

Category
Threat management

Policy contains tags
-

Create alert settings

Conditions
Activity is FileMalwareDetected

Aggregation
Aggregated

Scope
All users

Threshold
20

Window
2 hours

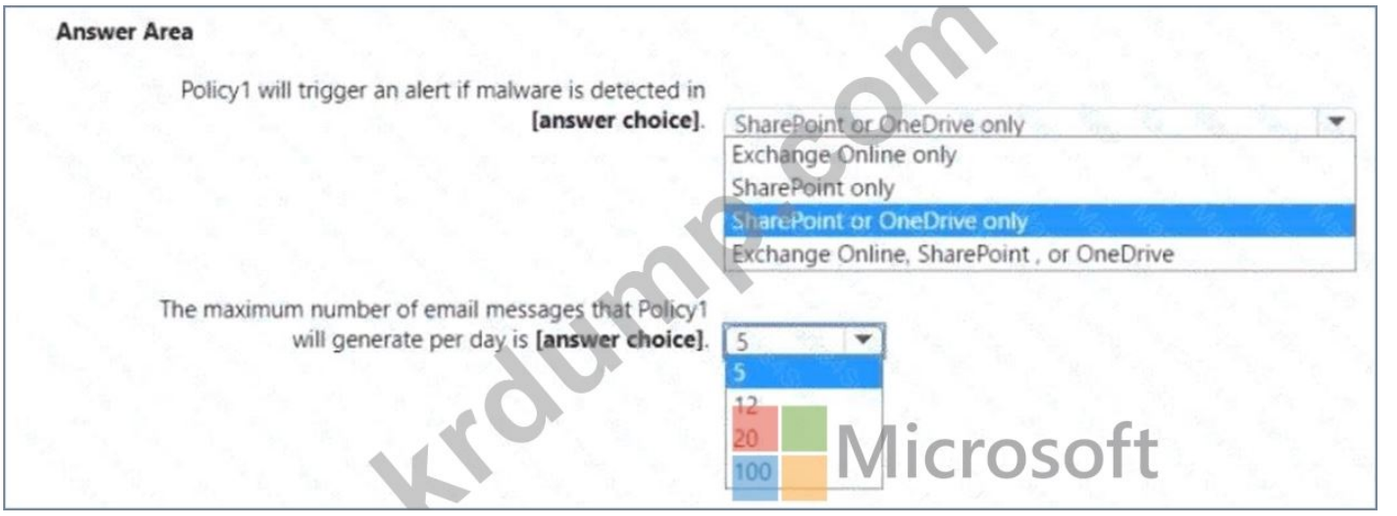
Severity
Low

Set your recipients

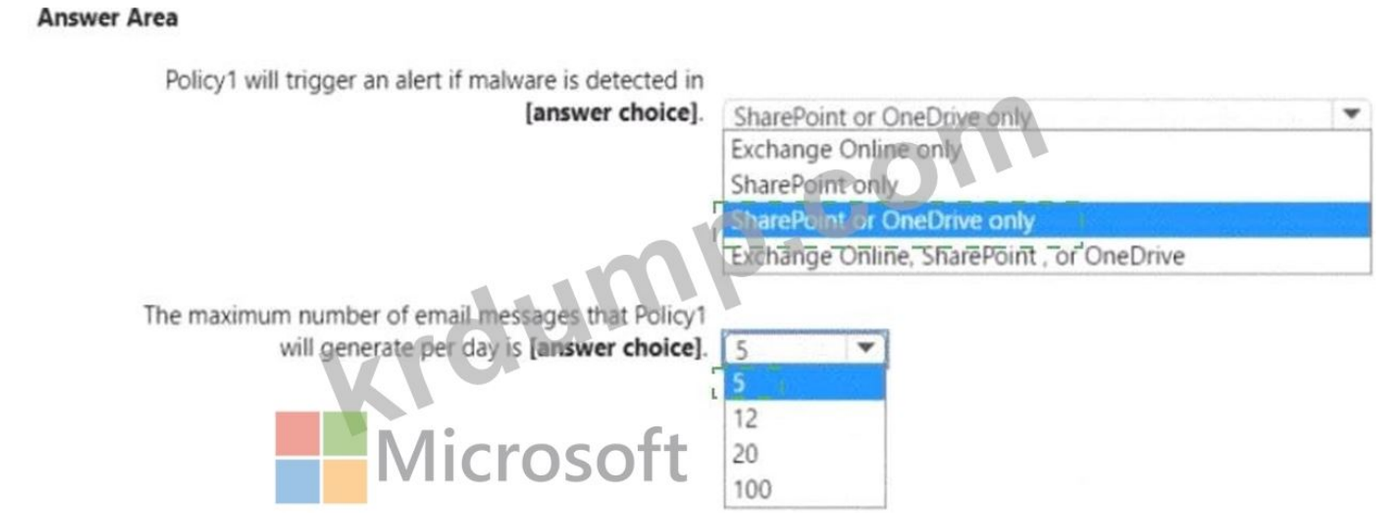
Recipients
User1@sk220912outlook.onmicrosoft.com

Daily notification limit
100

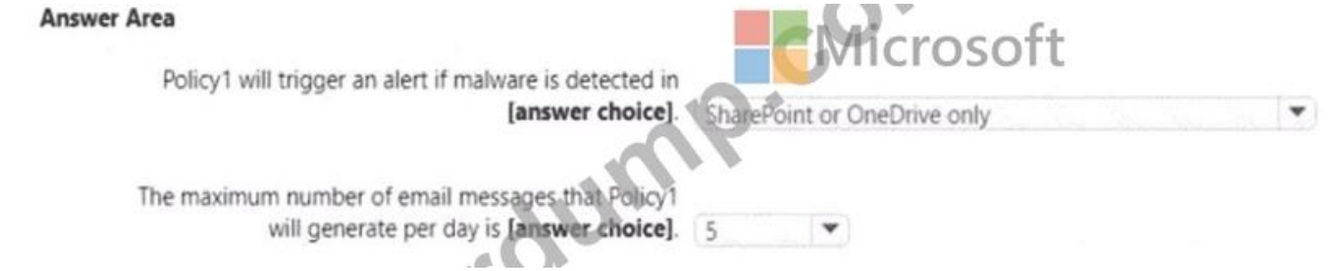
□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□ □□□ □□□□ □□□□□. □□: □□□ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 22

Microsoft 365 E5 □□□□ □□□□.

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

□□ □□□ □□□□ □□□?

A. □□ □□

B. □□ □□ □□

C. □□ □□□ □□

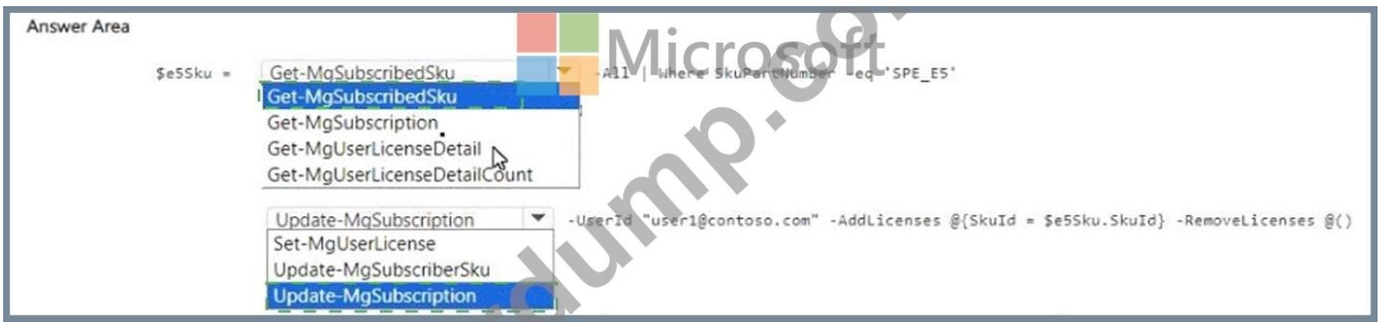
D. □□□ □□ □□

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

NEW QUESTION: 23
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Compliance Manager □□□ □□□□□ User1□ □□□□□ □□□.
□□ □□: Microsoft 365 □□ □□□□ User1□□ □□ □□ □□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

NEW QUESTION: 24
Microsoft 365 E5 □□□ □□□□.
user1□□□ □ □□□□□ Microsoft 365 E5 □□□□□ □□□□□ Microsoft Graph PowerShell □ □□□□ □□□.
@contoso.com.
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:



Explanation:

NEW QUESTION: 25

Microsoft Endpoint Manager□ □□ □□□ □□□□ Microsoft 365 □□□□ □□□□. □□ □□ □□ □□ □□□□ □□□□□ □□□□ □□□. □□□ □□ □□□?

A. Microsoft Endpoint Manager □□ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□ □□.

B. Microsoft Endpoint Manager □□ □□□□ □ □□ □□□ □□□□.

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

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

Answer: (SHOW ANSWER)

Reference:

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

Q

NEW QUESTION: 26

□□ □□□ □□□□ □□ □□□□ □□□□ □□□?

A. DLP □□□ □□□□□.

B. DLP □□□ □ □□□

C. DLP □□

D. □□ □□□ □ □□□

Answer: (SHOW ANSWER)

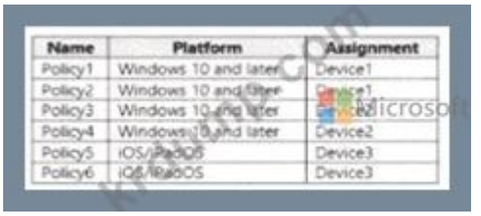
References:

https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific

rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

NEW QUESTION: 27

□□ □□□ □□ □□ □□ □□□ □□ □□□□.



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: 28

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

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

Microsoft 365 E5 □□□ □□□□.

SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.
SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Office 365 Advanced Threat Protection(ATP) □□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Microsoft 365 □□ □□□□ SecAdmin1□□ SharePoint □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
You need to assign the Security Administrator role.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

NEW QUESTION: 29
Microsoft 365 E5 □□□ □□□□.
Microsoft 365 Defender□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□□ □□ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
Azure AD □□□□ □□□□.
Windows 10 Pro□ □□□□ Azure AD□ □□□ □□□□ 1,000□ □□□□.
Microsoft 365 E3 □□□ □□□□□.
□□□□ Windows 10 Enterprise□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□□?
A. Azure Active Directory □□ □□□□ □□ □□ □□□□ □□ □□ □□□ □□□□. □□□ □□□□□ □□□□ □□□□□ □□□□ □□□□□□ □□□□□.
B. Microsoft Intune□ □□□□ □□□□□. Edition □□□□□ □ □□ □□ □□□□ □□□□ □□ □□□□ □□□□. Microsoft Endpoint Manager □□ □□□□ □□ □□□□ □□□□ □ □□□ □□□□□ □□□□ □□ □□□□□ □□□□□.
C. Microsoft Endpoinf Manager □□ □□□□ Windows Autopilot □□ □□□□ □□□□. □□ □□□□ □□□□ □□□□□. □□□□□ □□□□ □□ □□□□ □□□□□ □□ □□□□□ □□□□□.
D. Windows □□ □□□□□□ EditionUpgrade □□□ □□ □□□□□ □□□□ □□□ □□□ □ Microsoft SharePoint Online □□□□ □□□□□□. □□□□□ SharePoint Online□□ □□ □□□ □□□□ □□□□□ □□□□□.

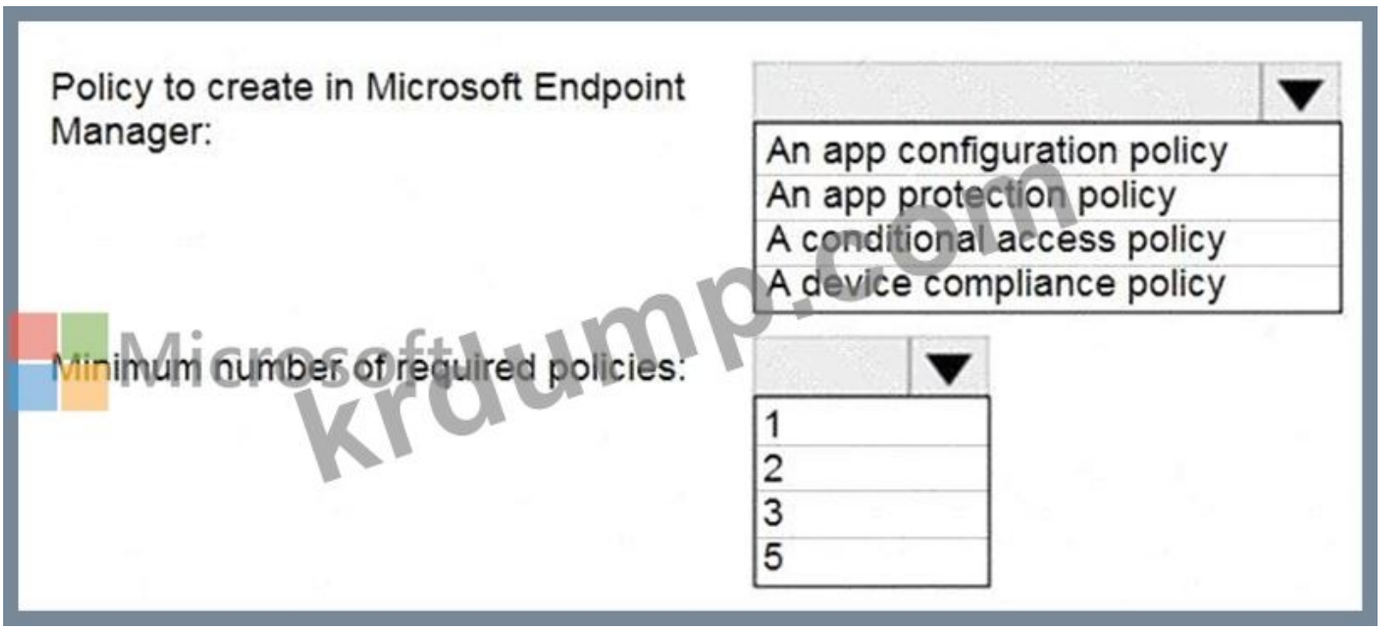
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
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

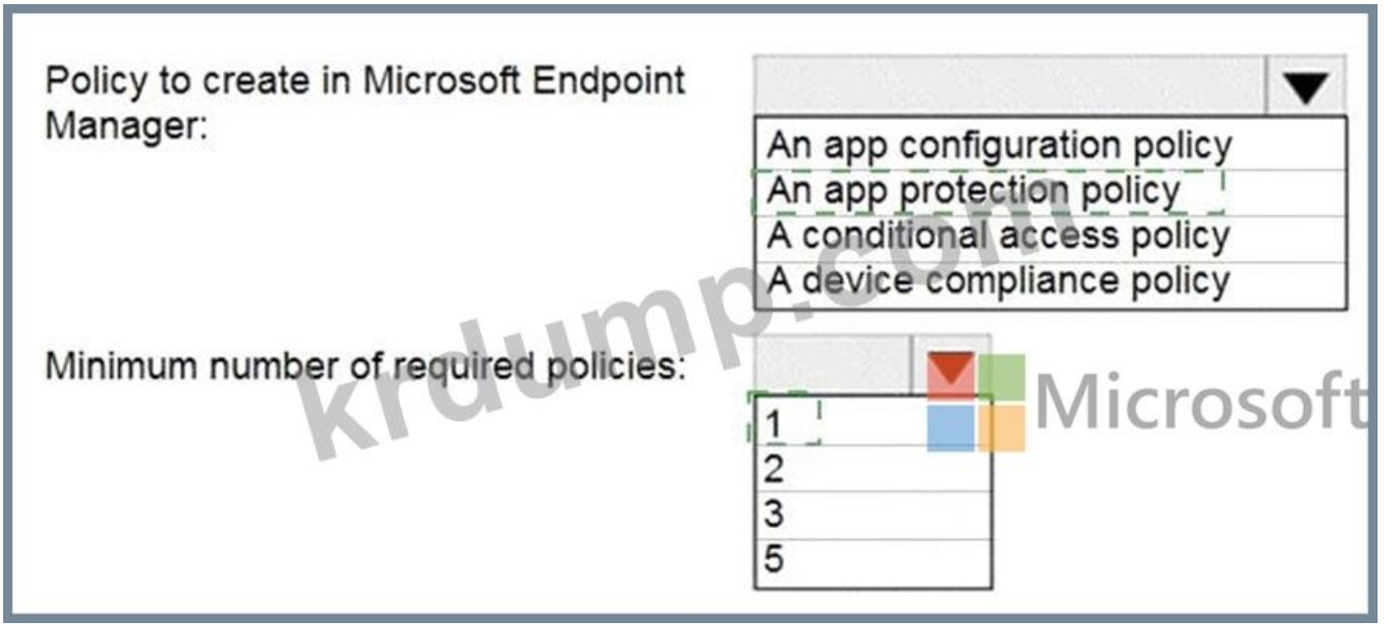
NEW QUESTION: 32
□□ □□ □□□ □□ Microsoft Intune□ □□□ 5□□ □□□ □□ Microsoft 365 E5 □□□□ □ □□□.

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

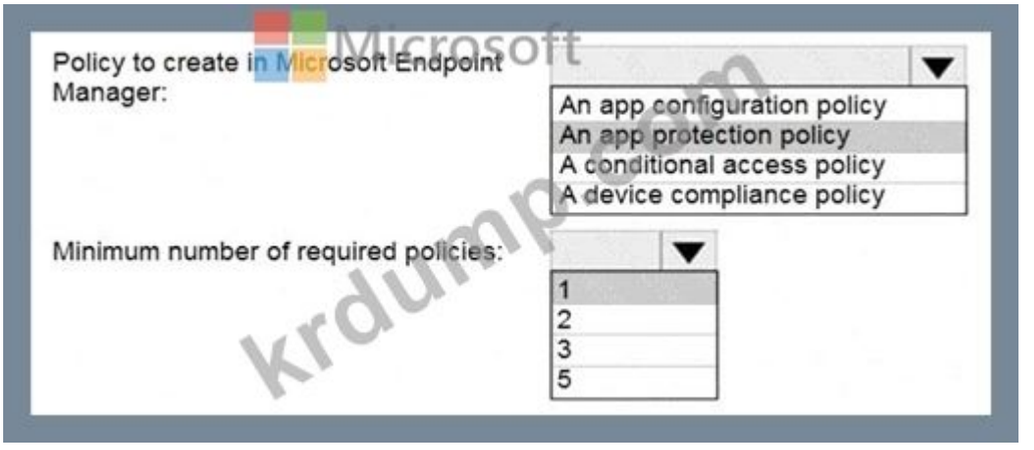
□□ □□□□ App1□□□ □□ □□□□ □□□□.
□□□□ App1□□ □□□□ □□□□ □□ □□ □□□□ □□ □□□□ □□□.
Microsoft Endpoint Manager□□ □□ □□□ □□□□ □□, □□□ □□□ □□ □□ □□□□ □? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



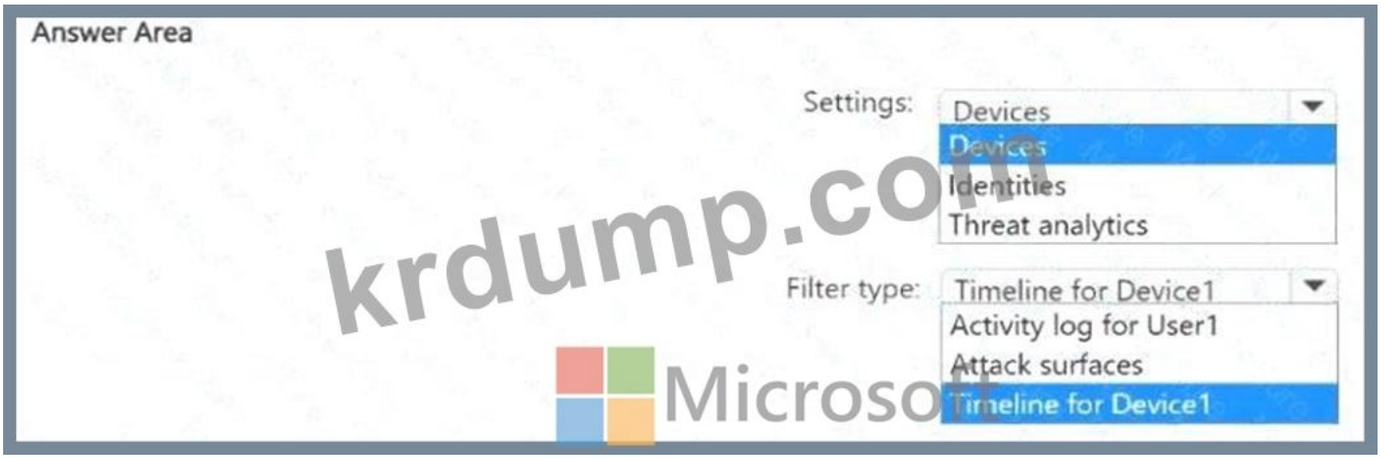
Reference:

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

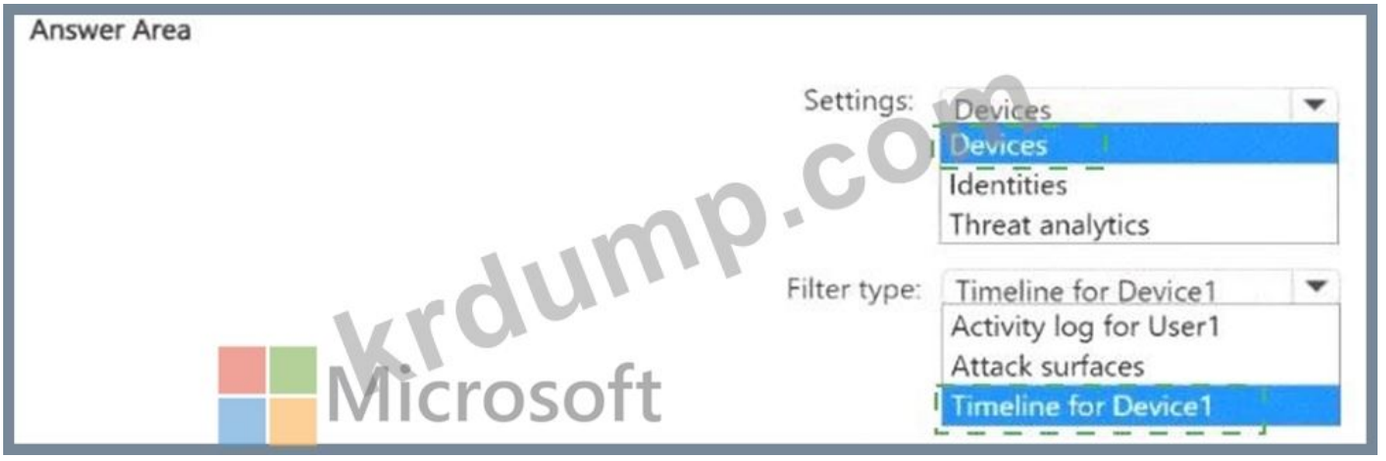
NEW QUESTION: 33
□□□ □□□□□□ contoso.local□□□ □□□□□ Active Directory □□□□ □□□□. □□□ □□ 5□□ □□□ □□□□□ □□□□.
□□□□ Microsoft 365□ □□□□ contoso.onmicrosoft.com□□□ Azure AD □□□□ □□□ □.
□□ □□□ Azure AD Connect□ □□□□ □□ □□□ □□□ □□□□□.
□□□□ □□□ □□□□□ □□□□ □□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. □□□ □□□□□□ □□ □□□□□ □□□□□.
B. Microsoft Entra □□ □□□□ □□ □□□ □□□□□.
C. Active Director□□ □□□ □ □□□□□ UPN □□□□ □□□□□.
D. □ □□□ □□□ □□ □□□ □□ □□□ □□□□□.
E. Microsoft Entra □□ □□□□ □□□ □□ □□□ □□□ □□□□□.
F. □ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
Answer: A,B,E (LEAVE A REPLY)
Deploy Azure AD Pass-through Authentication
Step 1: Check the prerequisites
Ensure that the following prerequisites are in place.
In the Entra admin center
1. Create a cloud-only Hybrid Identity Administrator account or a Hybrid Identity administrator account on your Azure AD tenant. This way, you can manage the configuration of your tenant should your on-premises services fail or become unavailable.
(E) 2. Add one or more custom domain names to your Azure AD tenant. Your users can sign in with one of these domain names.
(A) In your on-premises environment
1. Identify a server running Windows Server 2016 or later to run Azure AD Connect. If not enabled already, enable TLS 1.2 on the server. Add the server to the same Active Directory forest as the users whose passwords you need to validate. It should be noted that installation of Pass-Through Authentication agent on Windows Server Core versions is not supported.
2. Install the latest version of Azure AD Connect on the server identified in the preceding step. If you already have Azure AD Connect running, ensure that the version is supported.
3. Identify one or more additional servers (running Windows Server 2016 or later, with TLS 1.2 enabled) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.
4. Etc.
(B) Step 2: Enable the feature
Enable Pass-through Authentication through Azure AD Connect.
If you're installing Azure AD Connect for the first time, choose the custom installation path. At the User sign-in page, choose Pass-through Authentication as the Sign On method. On successful

completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect. In addition, the Pass-through Authentication feature is enabled on your tenant.
Incorrect:
Not C: From Active Directory Domains and Trusts, add a UPN suffix
Not D. Modify the email address attribute for each user account.
Not F. Modify the User logon name for each user account.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start

NEW QUESTION: 34
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□. User1□ Microsoft Defender for Endpoint□ □□□□ Device1□□□ Windows 11 □□□ □□□ □□□□.
User1□ Device1□□ □□□ □□□ □□□□□□ □□□□□.
□□□ □□□ □□□□ □□□□□ □□□ □□□□ □□□.
Microsoft Defender □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□? □
□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Answer Area

NEW QUESTION: 35

Microsoft 365 E5 □□□ □□□□.

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

Azure AD Identity Protection□□ □□□ □□ □□□ □□□□□ □□□□□.

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

□□□ □□□□ □□□?

A. Azure AD□ □□□ □□ □□

B. □□□ □ □□ □□

C. □□□ □□□ □□ □□

D. Microsoft 365 □□□□ □□ □□

Answer: B (LEAVE A REPLY)

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

Sign-in risk policy

User risk policy

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

Reference:

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

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

NEW QUESTION: 36

Microsoft 365 E5 □□□ □□□□.

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

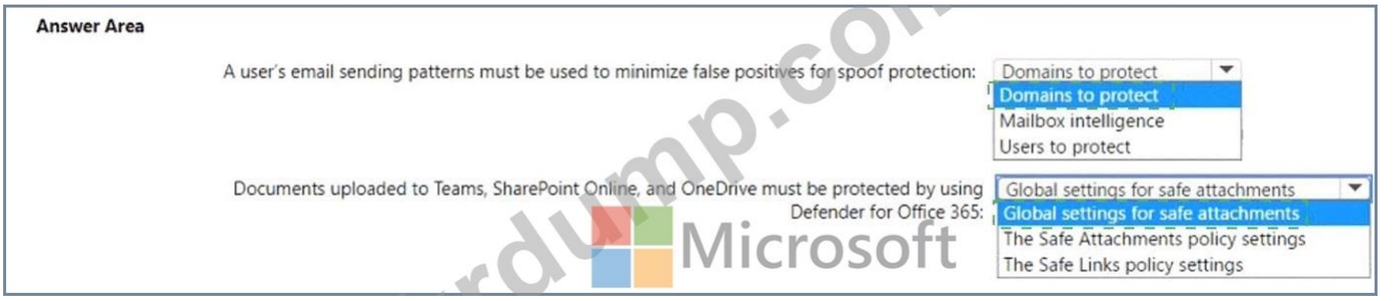
* □□□□ □□□ □□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□□ □□□.

* Microsoft Teams, SharePoint Online □ OneDrive□ □□□□ □□□ Defender for Office 365□ □□□□ □□□□ □□□.

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

□□: □ □□□ □□□ 1□□□□.

Answer:



Explanation:

NEW QUESTION: 37

Microsoft 365 E5 □□□ □□□□.

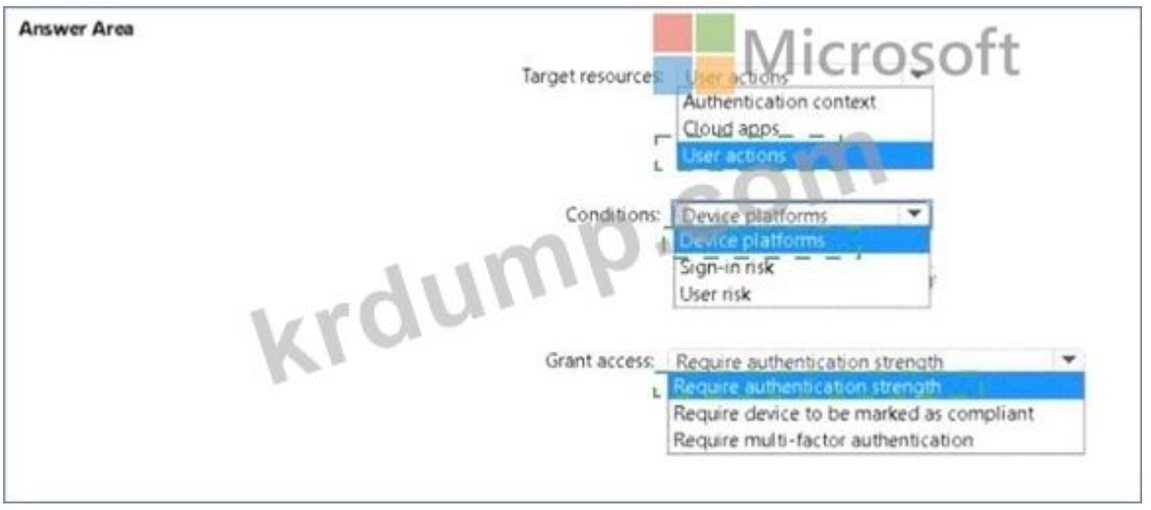
□□□□ Windows □□□ Microsoft Entra ID□ □□□ □□ FID02 □□ □□ □□□□□ □□□ □ □□□ □□□ □□□ □□□□ □□□.

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

□□ □□: □□□ □□□ □□□ 1□□□□.

Answer Area

Answer:



Explanation:

NEW QUESTION: 38

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

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

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

Microsoft System Center Configuration Manager(□□ □□)□ □□□□ Windows 10 □□□ □□ □□□.

□□ □□□ □□ □□□□ □□□□□.

□□□□ Device1□□□ □ □□□ □□□□□. Device1□ Configuration Manager □□□□□□ □□□□□.

Microsoft Intune □ Configuration Manager□ □□□□ Device1□ □□□ □ □□□ □□□□ □ □□.

□□□: Configuration Manager □□ □□□□ □□□ □□□□□ □□□□□. □□□□ Device1 □ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

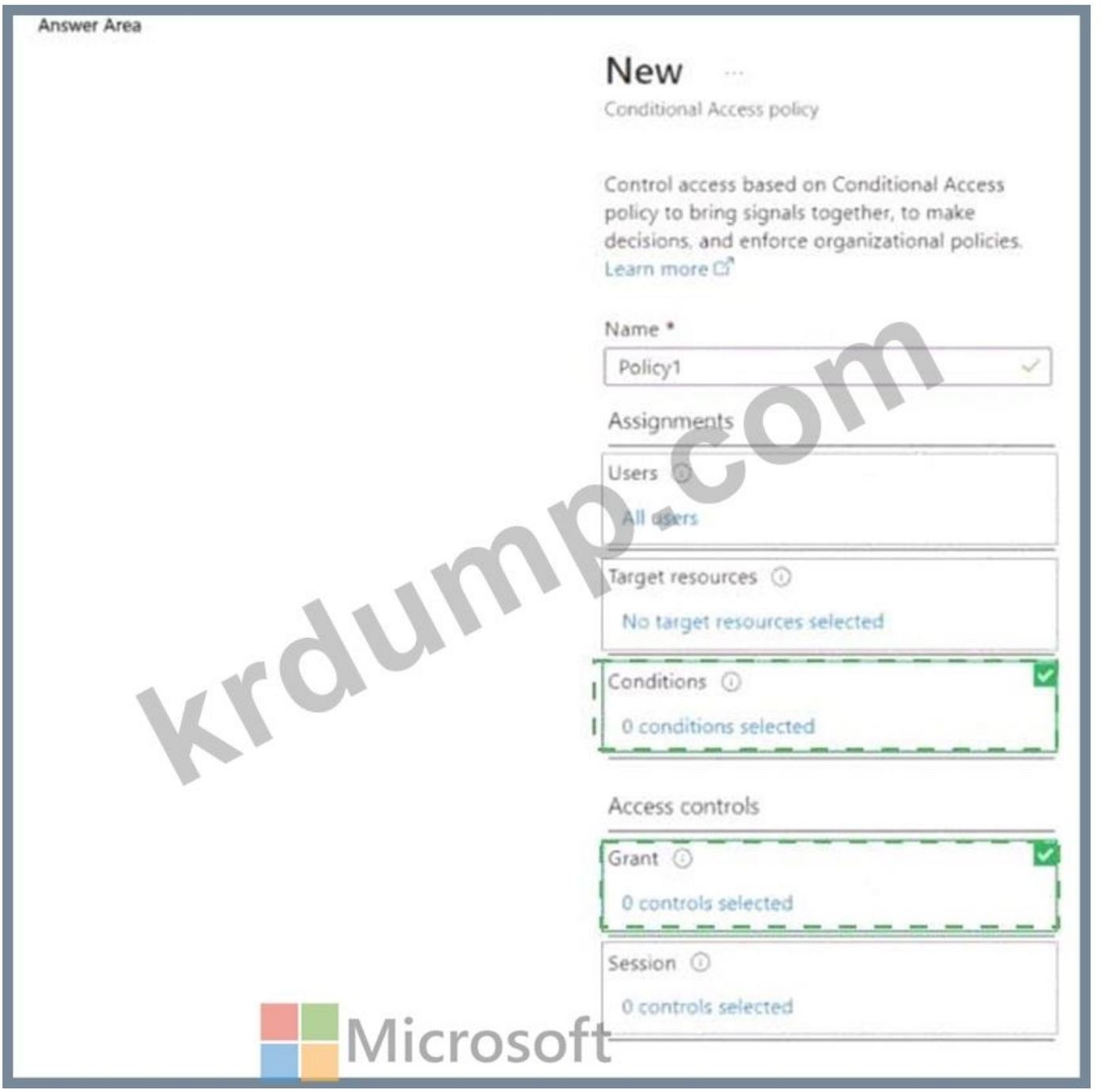
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection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

NEW QUESTION: 39
□□□ □□□□□□ Contoso□□ Active Directory □□□□□ □□□□ □□□□. □□.
Microsoft 365 □□□ □□□□.
□□□□ □□ □□□□ □□□□ □□□□ □□□ □□□□ □□□□□ □□□.
Microsoft 365 □□ □□□□ contoso.com □□□ □□□ □□□□□ □□□□□□.
□□□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. contoso.com□ □□ DNS □□□□ □□□ □□ □□□(MX) □□□□ □□□□□.
B. Active Directory □□□ □ □□□□□ □□ □□□□ UPN □□□□ □□□□□.
C. Microsoft 365 □□ □□□□ Contoso.Local □□□ □□□ □□□□□.
D. Active Directory □□□ □ □□□□□□ contoso.com□ UPN □□□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□ Policy□□ □□□ □□□ □□□ □□□□ □□□.
* □□□ □□□□□ □□□□□.
* □□ □□(MFA)□ □□□□□.
□□ □ □□ □□□ □□□□ □□□? □□□□ □□□ □□□ □□□ □□□□□□. a. □□: □ □□□ 1□□□□.

Answer:

Answer Area



Explanation:

NEW QUESTION: 41

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

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

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

Compliance Manager □□□ □□□□□ User1□ □□□□□ □□□.

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

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

Reference:

https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

NEW QUESTION: 42

□□□

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

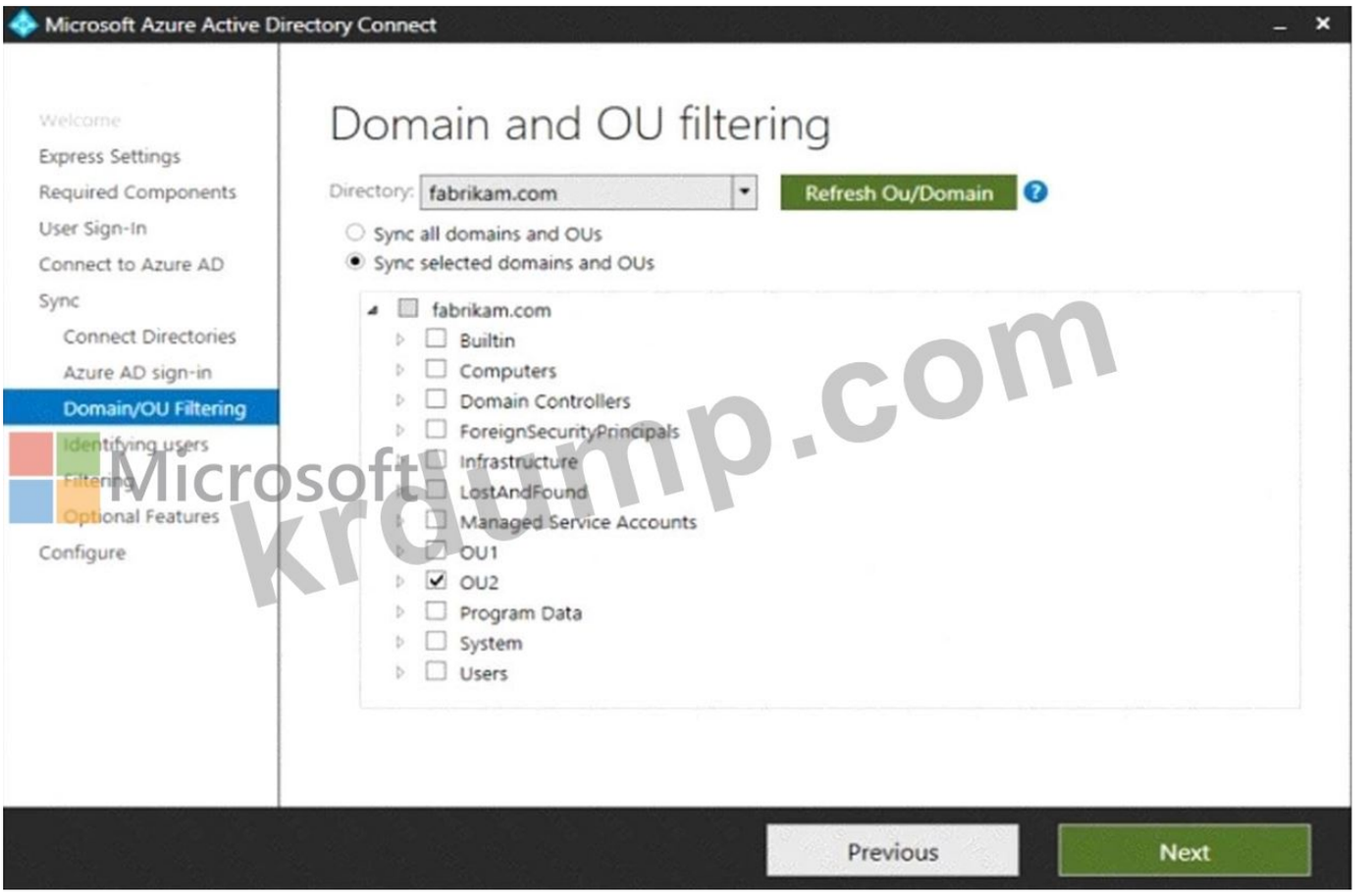
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

□□□ □□□□ □□ □□ □□ □□□□.

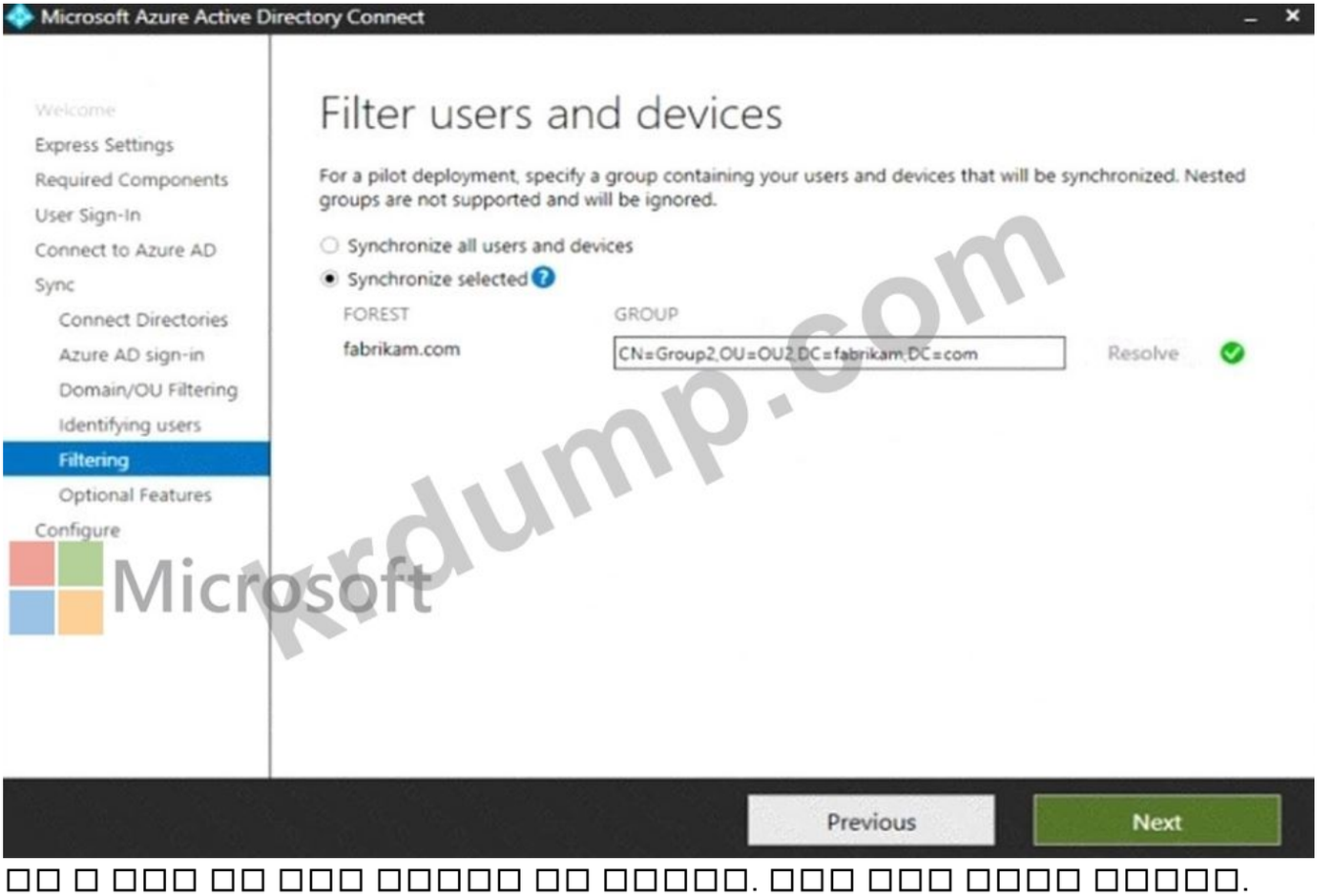
Group	Members
Group1	User1
Group2	User2, User3, Group1

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

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

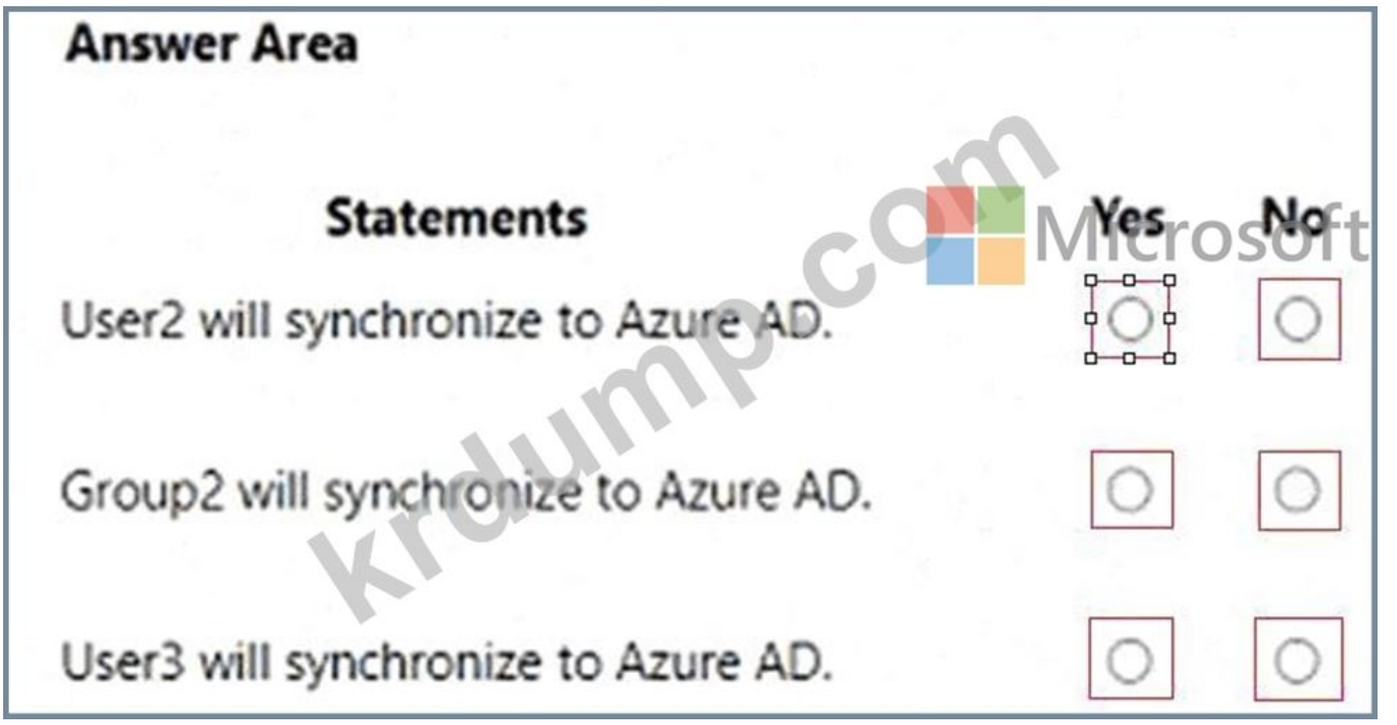


Azure AD Connect□□ □□□ □□□ □□□ □□□ □□□ □□ □□□□□. (□□□ □□ □□ □□□.)

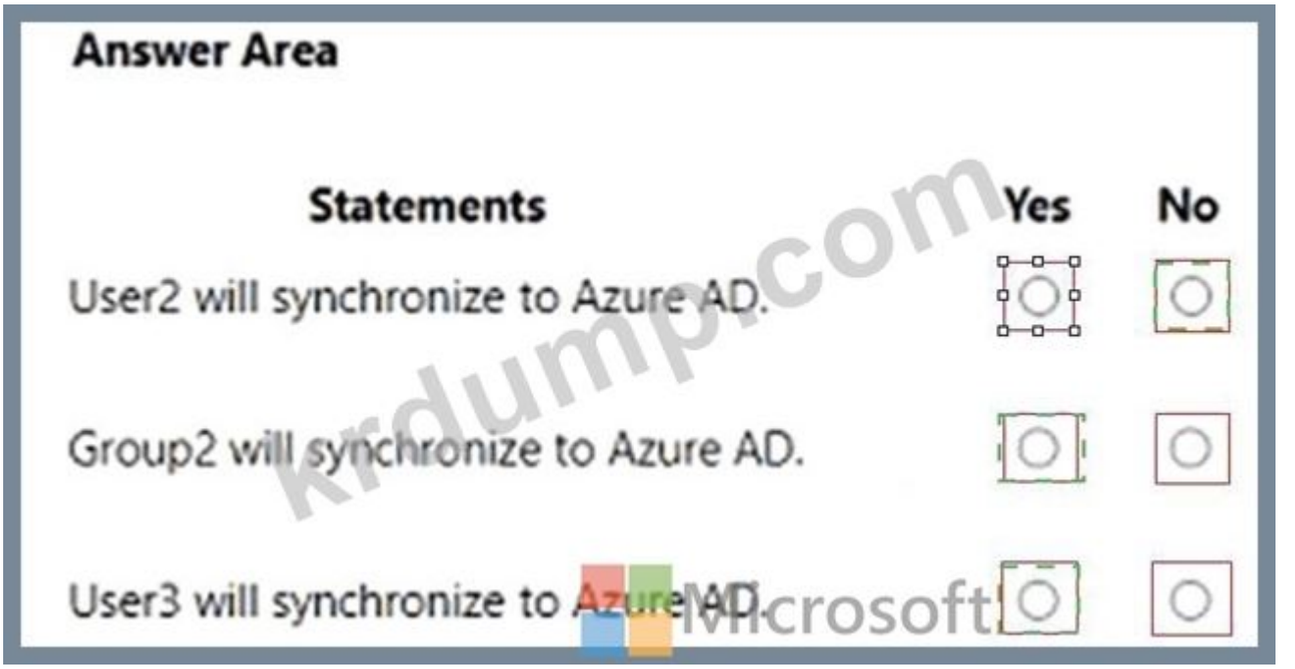


□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

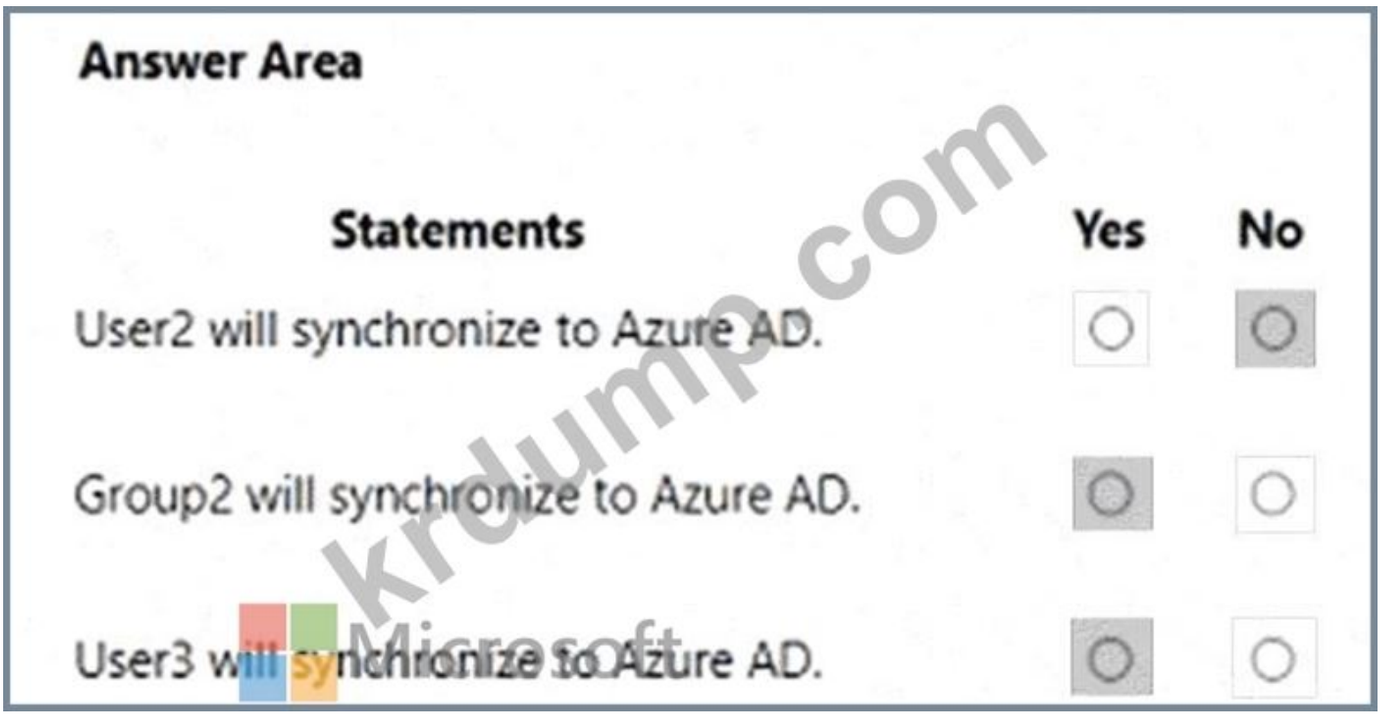
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Box 1: No

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

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

Box 2: Yes

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

Box 3: Yes

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

Reference:

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

NEW QUESTION: 43

Microsoft 365 E5 □□□ □□□□. Microsoft Entra ID Protection□ □□□ □□□□□.

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

A. □□□ □□ □□

B. □□ □□□ □□□□ □□□(SSPR)

C. □□□ □□ □□

D. □□ □□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 44

□□□ □□□□ Microsoft 365 E5 □□□□ □□□□.

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

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

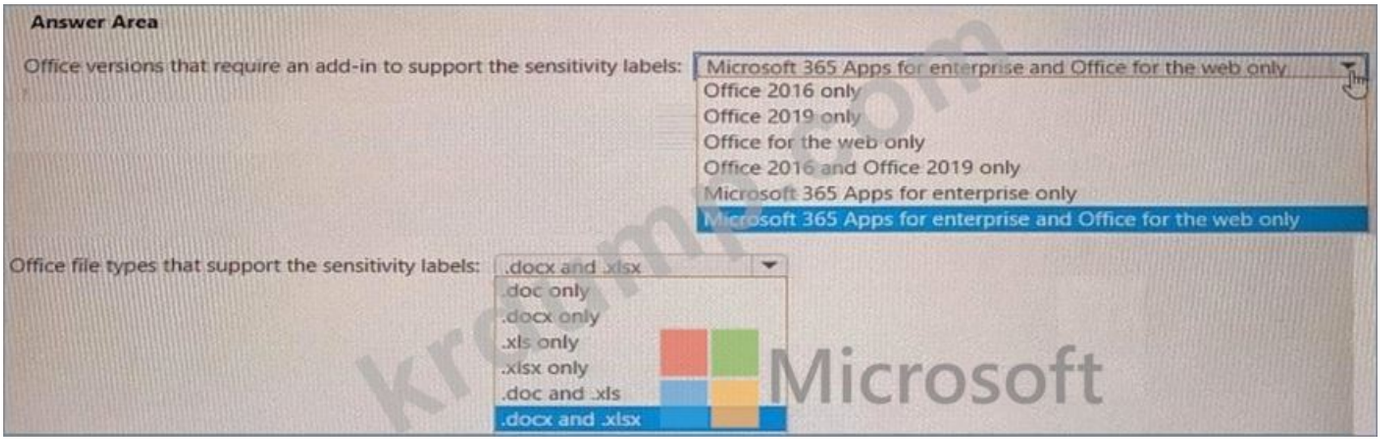
□□ □□□□□ □□□ □□ Office □□ □□□ □□□□□.

* .docx
* .xlsx
* .□□
* □□

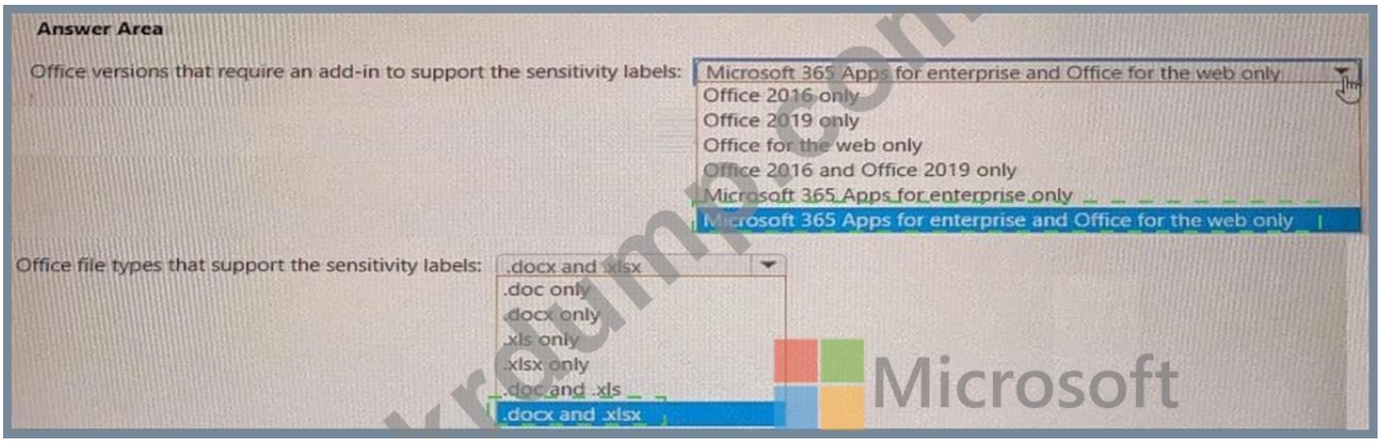
□□□ □□□□ □□□ □□□□□. □□□ □□□□ □□□.

* □□□ □□□□ □□□□ □□ □□ □□□ □□□ Office □□□ □□□□□?
* □□□ □□□ □□□□ □□ □□□ □□□□□?

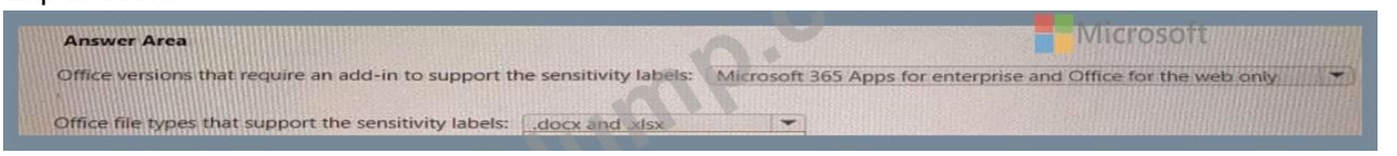
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □ □□□ 1 □□□□.



Answer:



Explanation:



NEW QUESTION: 45

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

NEW QUESTION: 46
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: 47
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
App1□□□ □□□□ □□ □□ □□□ □□□ □□□ □□□□ □□□□. App1□□ □□□ □□ □ □ □□□ □□□□ □□□□.
User1□ App1□□ □□□□ □□ □□□□□ Microsoft Defender for Cloud Apps □□□ □□□ □ □□□.
A. □□ □□
B. OAuth □ □□
C. Cloud Discovery □□ □□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 48
□□□ □□□□ □□□ □□□□ □□ □□□□.
Microsoft 365 □□□ □□□□.
□□ □□ □□(MFA)□ □□□□ Policy1□□□ □□□ □□□ □□□ □□ □□□□□.
□□□ □□□ □□□□ MFA□□ □□□□ □□□. □□ □□□ □□□□ □□ MFA□ □□□□ □□□.
Policy1□ □□ □□□ □□□□ □□□?
A. □□ □□□ □□□□ □□□ □□□ □□
B. □□□ □□□□□□ VPN □□
C. □□ □□
D. IP □□ □□□ □□□ □□□□ □□□ □□□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
□□□ □□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□ □□□ □. □ □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

contoso.com□ Azure AD□ □□□□□□ Azure AD Connect□ □□□□□.
□□ □□□ Azure AD□ □□□□□□?

A. □□1□

B. User1□ User2□

C. Group1□ User1□

D. □□1, □□□1, □□□2

Answer: (SHOW ANSWER)

Disabled accounts

Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD. The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user- and-contacts

NEW QUESTION: 50

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

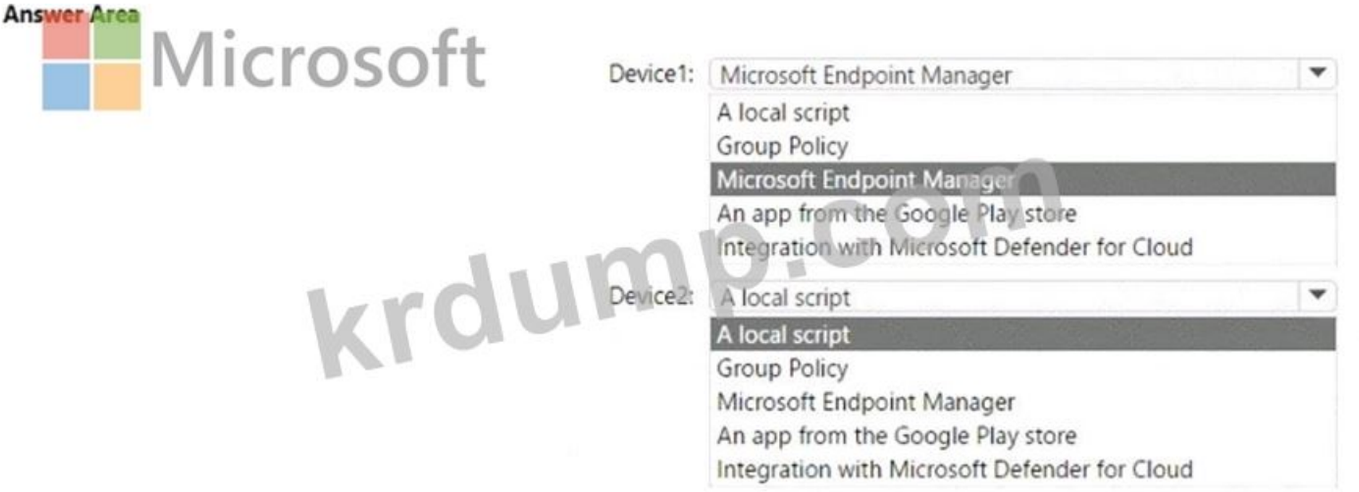
Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

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

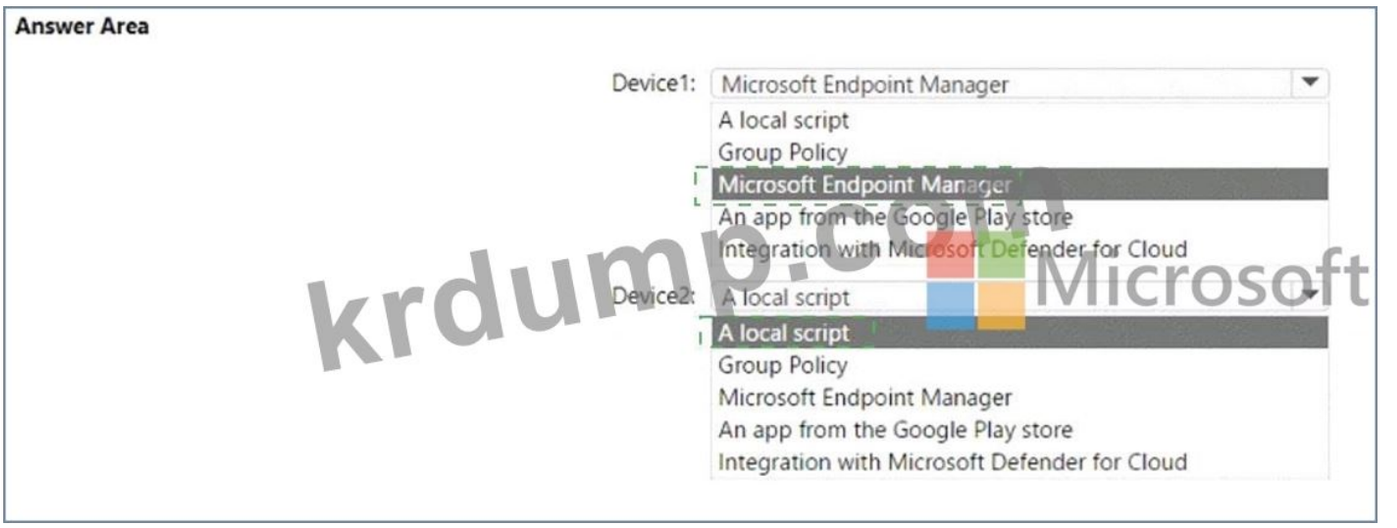
□ □□□ □□□□□ □ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□.

□□□□: □□ □□□ 1□□□□.

Answer Area



Answer:



Explanation:

NEW QUESTION: 51

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

Microsoft 365 E5 □□□ □□□□.

□□ □□ □□□ □□ □□□□□ □□□ □□□□□ □□□.

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

* Azure AD Identity Protection □□□ □□□□□.

□□□ □□□ □□□□□ Azure AD Connect□ □□□□ □□□. □□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

A. Single Sign-On □□□

B. □□□□ □□

C. □□□□ □□ □□

D. □□□□ □□ □□□

E. □□□□ □□ □□ □□□

Answer: (SHOW ANSWER)

NEW QUESTION: 52

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

Name	Member of Microsoft 365 role group
Admin1	Content Explorer List viewer Content Explorer Content viewer
Admin2	Security Administrator Content Explorer List Viewer

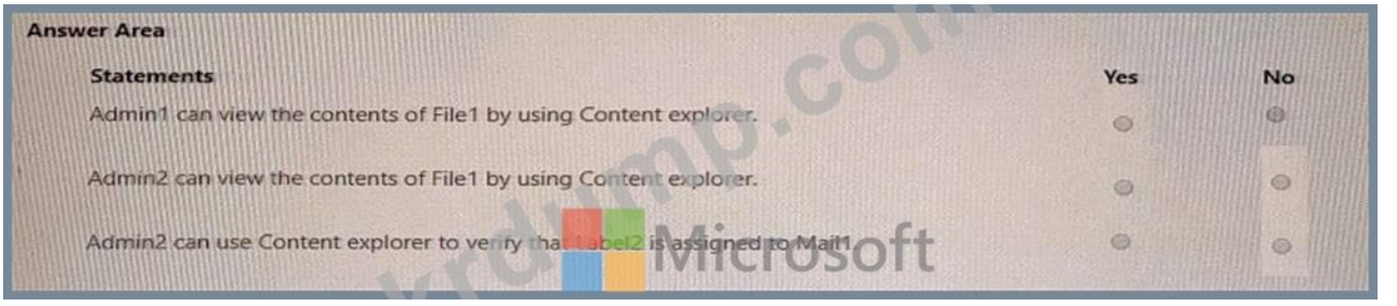
□□ □□ □□□ □□□ Microsoft 365□□ □□□□ □□□□.

Name	Type
Label1	Sensitivity
Label2	Retention

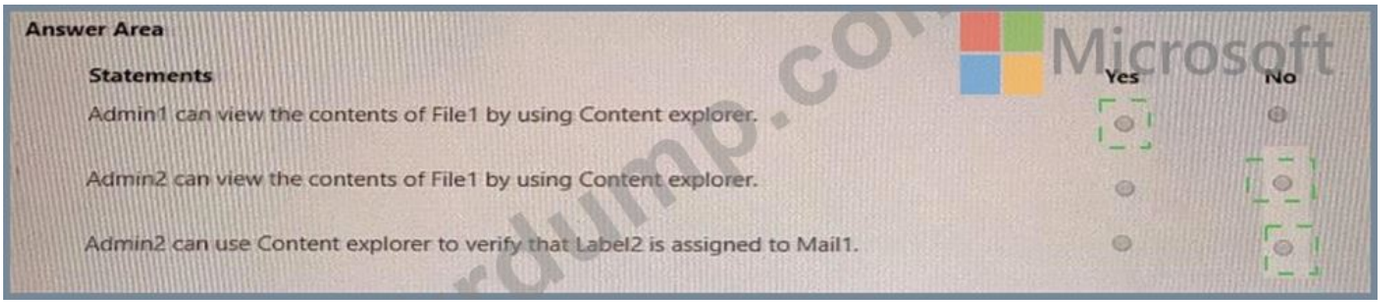
□□ □□ □□□ □□ Microsoft 365□ □□□□□ □□□□ □□□□□.

Name	Type	Label
File1	File in SharePoint Online	Label1
Mail1	Email message in Exchange Online	Label2

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

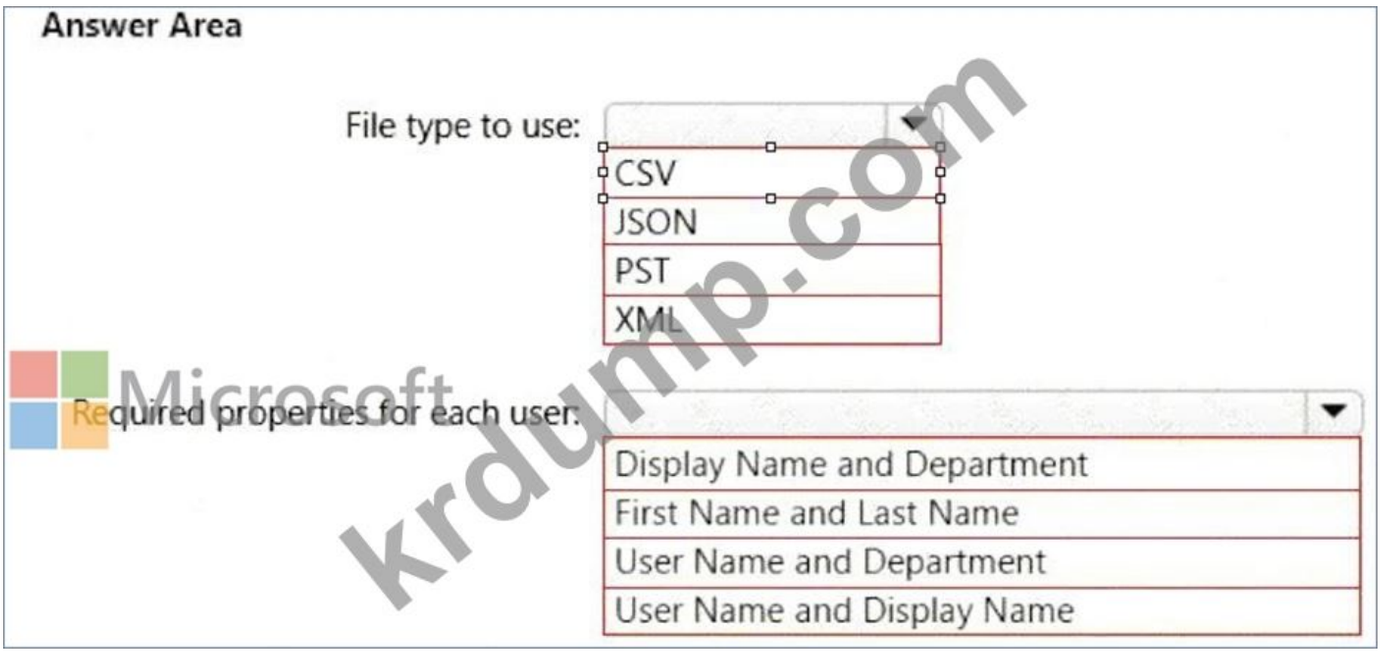


Answer:

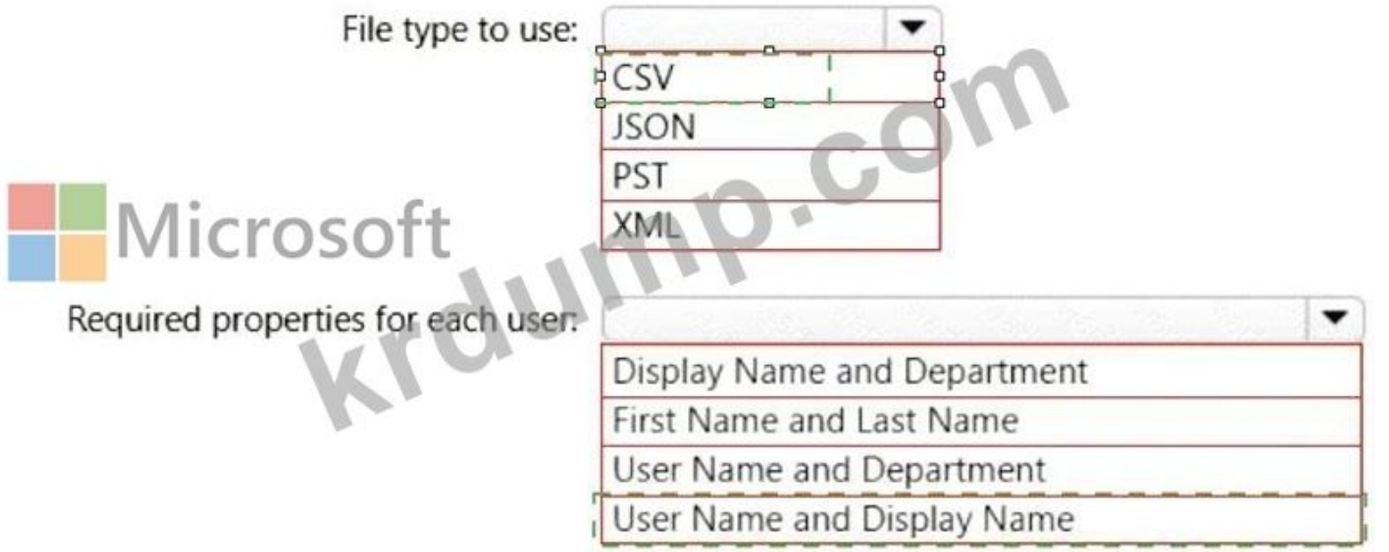


Explanation:

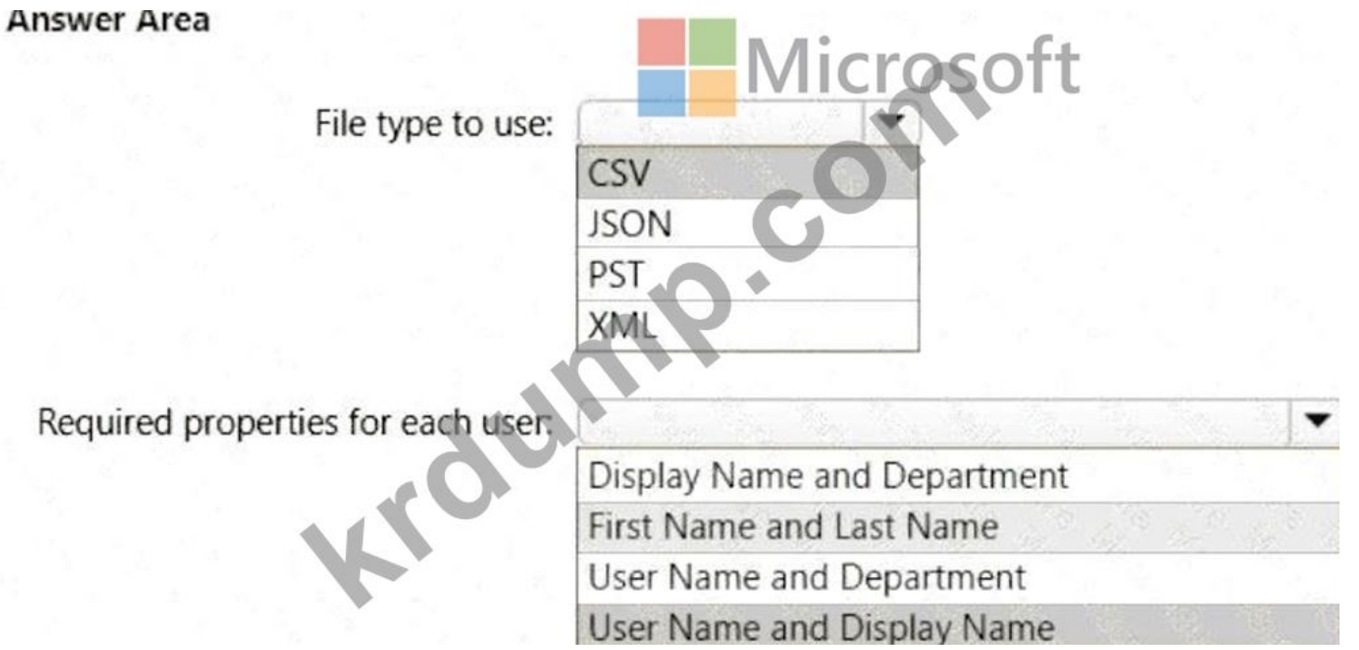
NEW QUESTION: 53
□□□
□□□□□ 100□□ □□□□ □□ □□ □□□□□ LDAP □□□□□ □□□□□.
□□□ Microsoft 365 □□□ □□□□□.
Microsoft 365 □□ □□□ □□□□ 100□□ □□□□ Microsoft 365□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □ □□ □□□□□.
□□□□: □□ □□□ 1□□□□.



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: 54

Microsoft 365 □□□□ □□□□.

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

□□□□ □□□□ □□ □□□□ □□□ □ □□□?

A. □□□ 8.1

B. □□□ □□□

C. □OS

D. □□□□□ □□□□□□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 55

Microsoft 365 □□□ □□□□.

□□ □□ □□□ □□□□ □□□.

* Microsoft 365 □□□ □□□ □□□□□.

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

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

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 56

□□□ □□ □□□ □□□□□ □□ □□□□ □□□□ □□□.

□□□ □□□□ □□□?

A. □□ □□

B. Azure AD □□ □□ ID □□(PIM)

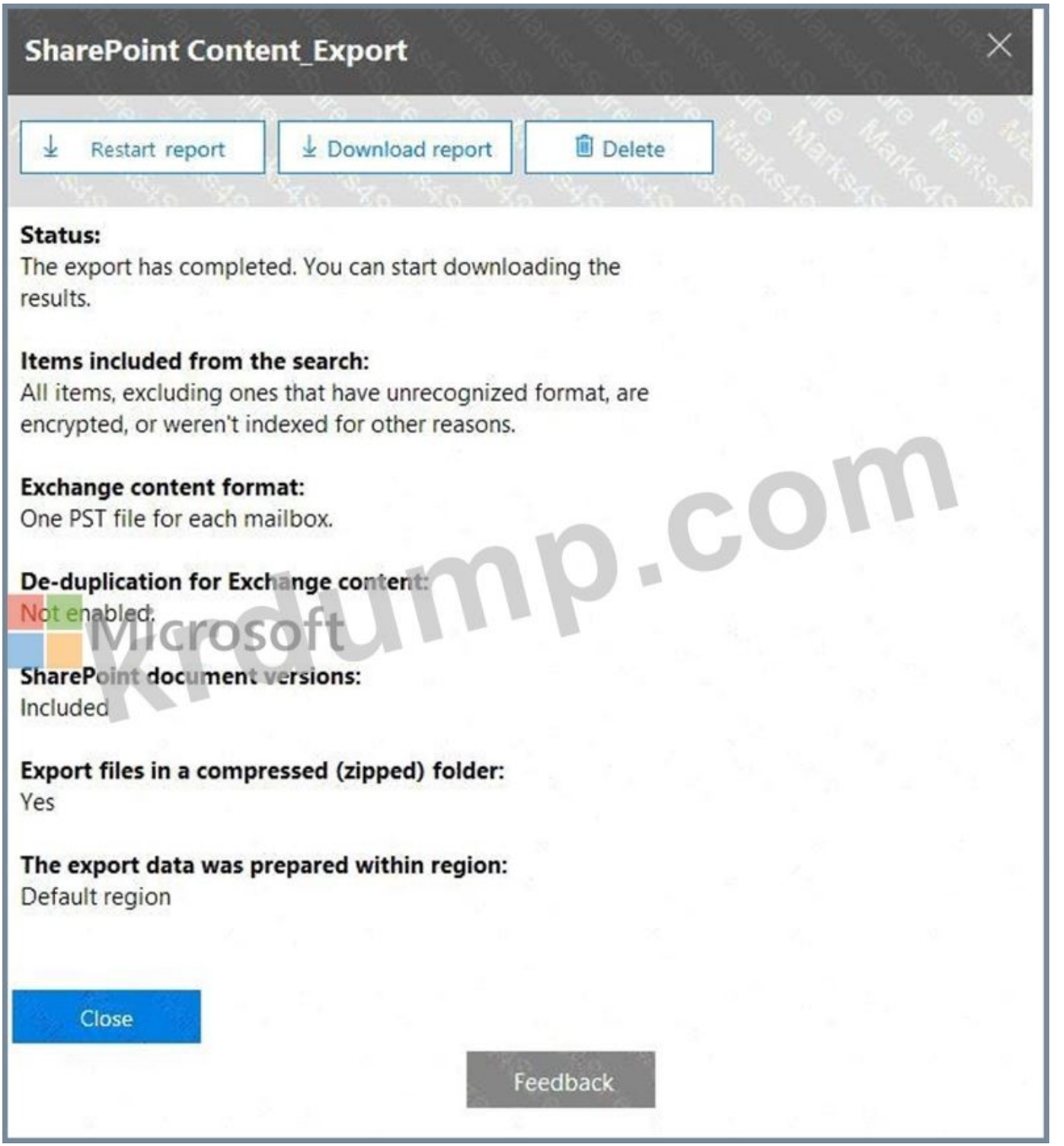
C. Azure AD ID □□

D. □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 57

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



□□□□ □□□□ □□□ □□□□□?

A. 10MB XLSX □□

B. 5MB MP3 □□

C. 5KB RTF □□

D. 80MB PPTX □□

Answer: B (LEAVE A REPLY)

Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files.

These types of files are considered to be unsupported file types.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?

view=o365-worldwide

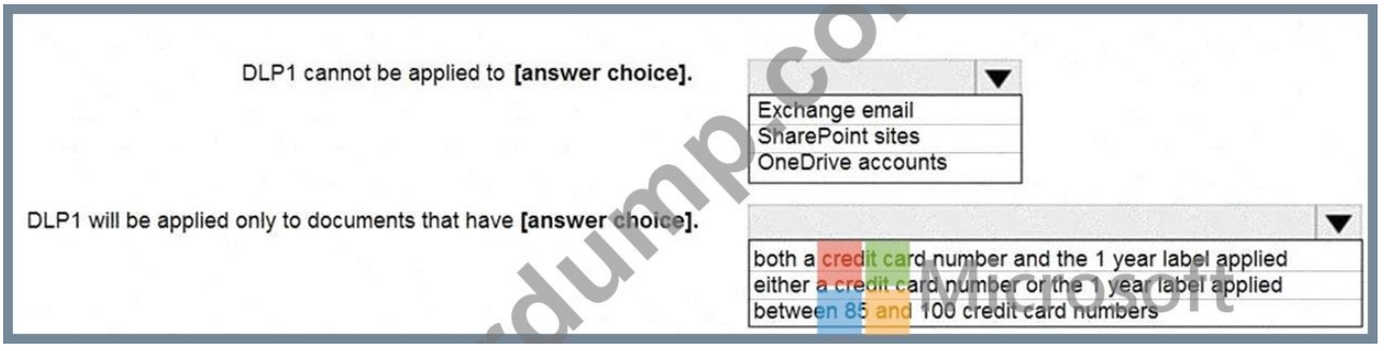
https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report

NEW QUESTION: 58

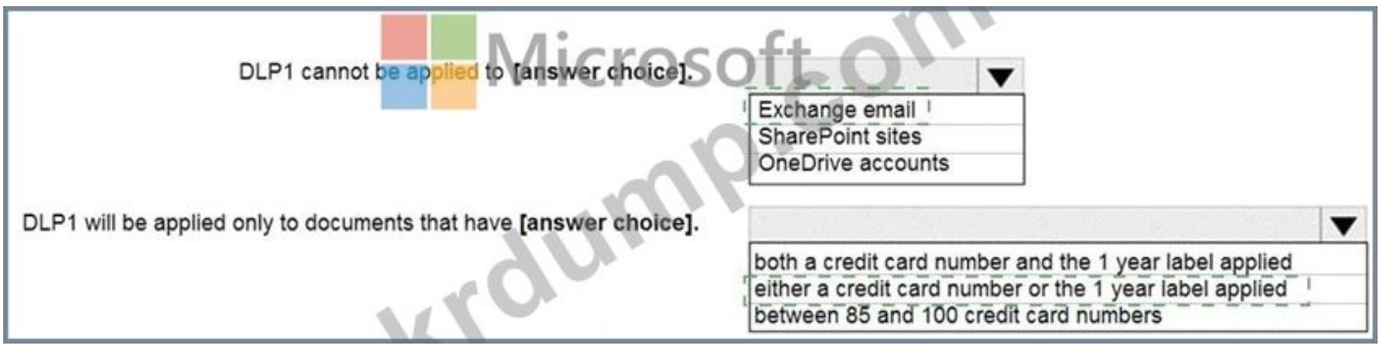
□□ □□□ □□ DLP1□□□ □□□ □□□ □□ □□(DLP) □□□ □□□□□.

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

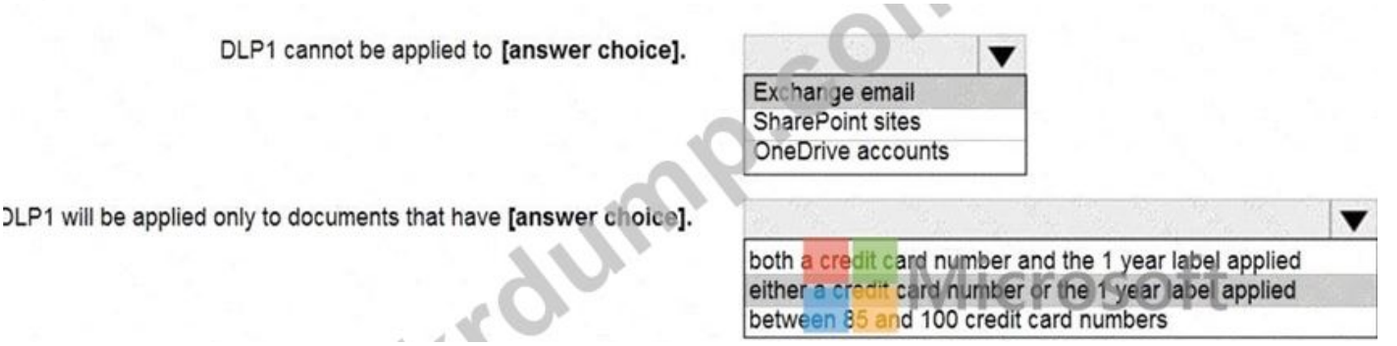
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

nce:

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

NEW QUESTION: 59

Microsoft 365 E5 □□□ □□□□.

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

www.contoso.com□ □□ □□□□□ □□ □□□□ □□□□□ Defender for Endpoint□ □□□ □ □□□.

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

□□□□: □□□ □□ 1□□□□.

A. □ □□□ □□□ □□□ □□□□.

B. □□□ □□ □□□□ □□□□ □□□□□□.

C. □□ □□□ □□□□□□.

D. □□ □□□ □□□□□.

E. □□□□ □□□□□.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 60

□□□ 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
Topic 4, FabrikamOverview
Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.
Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.
Existing Environment
Active Directory Environment
The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.
All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.
Fabrikam does NOT plan to implement identity federation.
Network Infrastructure
Each office has a high-speed connection to the Internet.
Each office contains two domain controllers. All domain controllers are configured as DNS servers.
The public zone for fabrikam.com is managed by an external DNS server.
All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.
All shared company documents are stored on a Microsoft SharePoint Server farm.
Requirements
Planned Changes
Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
Fabrikam plans to implement two pilot projects:
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 will be enabled in Microsoft 365 for the sales department users.
Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements
Fabrikam identifies the following technical requirements:
All users must be able to exchange email messages successfully during Project1 by using their current email address.
Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.
Application Requirements
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online.
App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.
Security Requirements
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

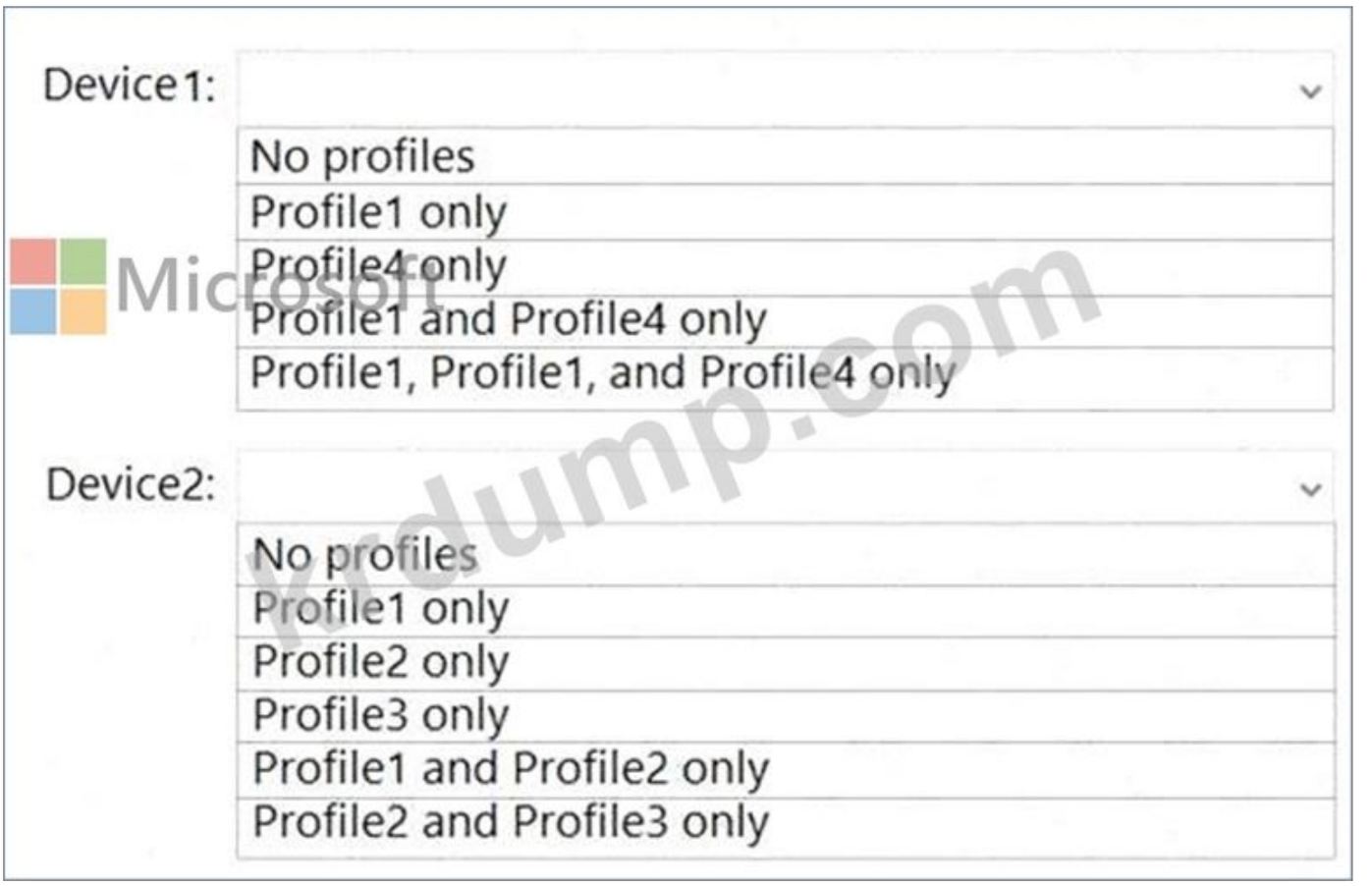
NEW QUESTION: 61
Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□ Intune□ □□□ □□□ □□□□.

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

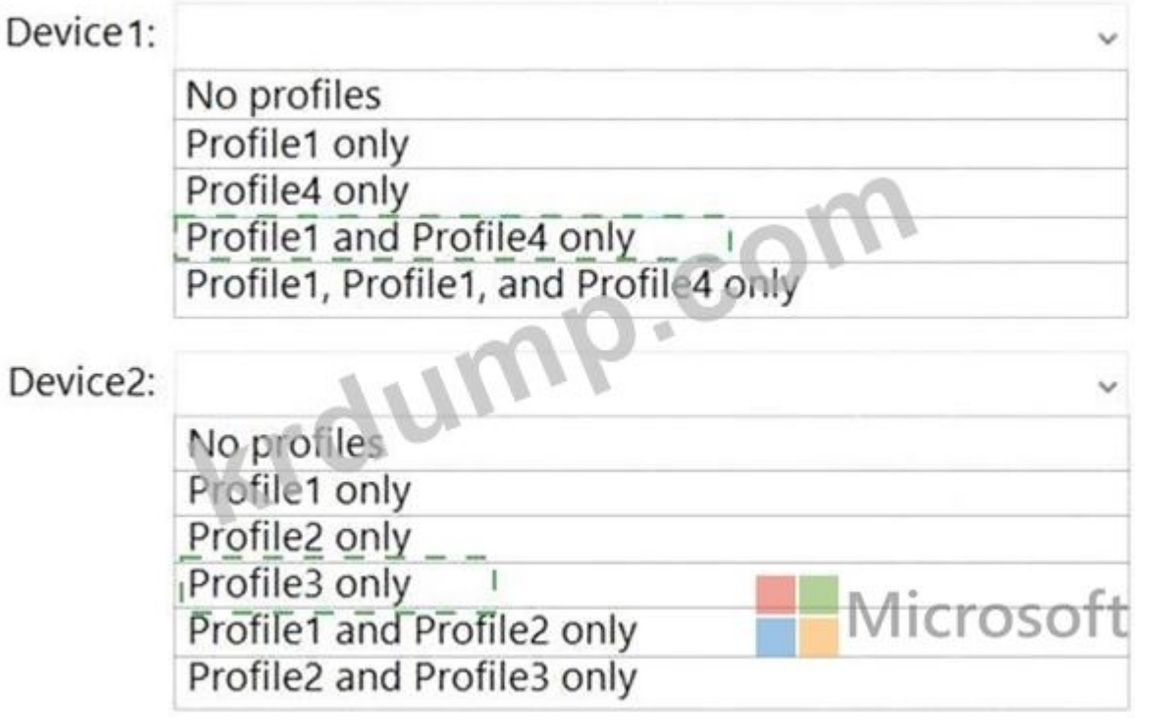
□□ □□ □□□ □□ □□ □□□□ □□□□.

Name	Platform	Assignments: Included groups	Assignments: Excluded groups	Scope tags
Profile1	Windows 10 and later	Group1	Group3	Tag1, Tag2
Profile2	Android Enterprise	All devices	Group2	Tag1, Tag2
Profile3	Android Enterprise	Group2, Group3	Group3	Tag1
Profile4	Windows 10 and later	Group3	None	Default

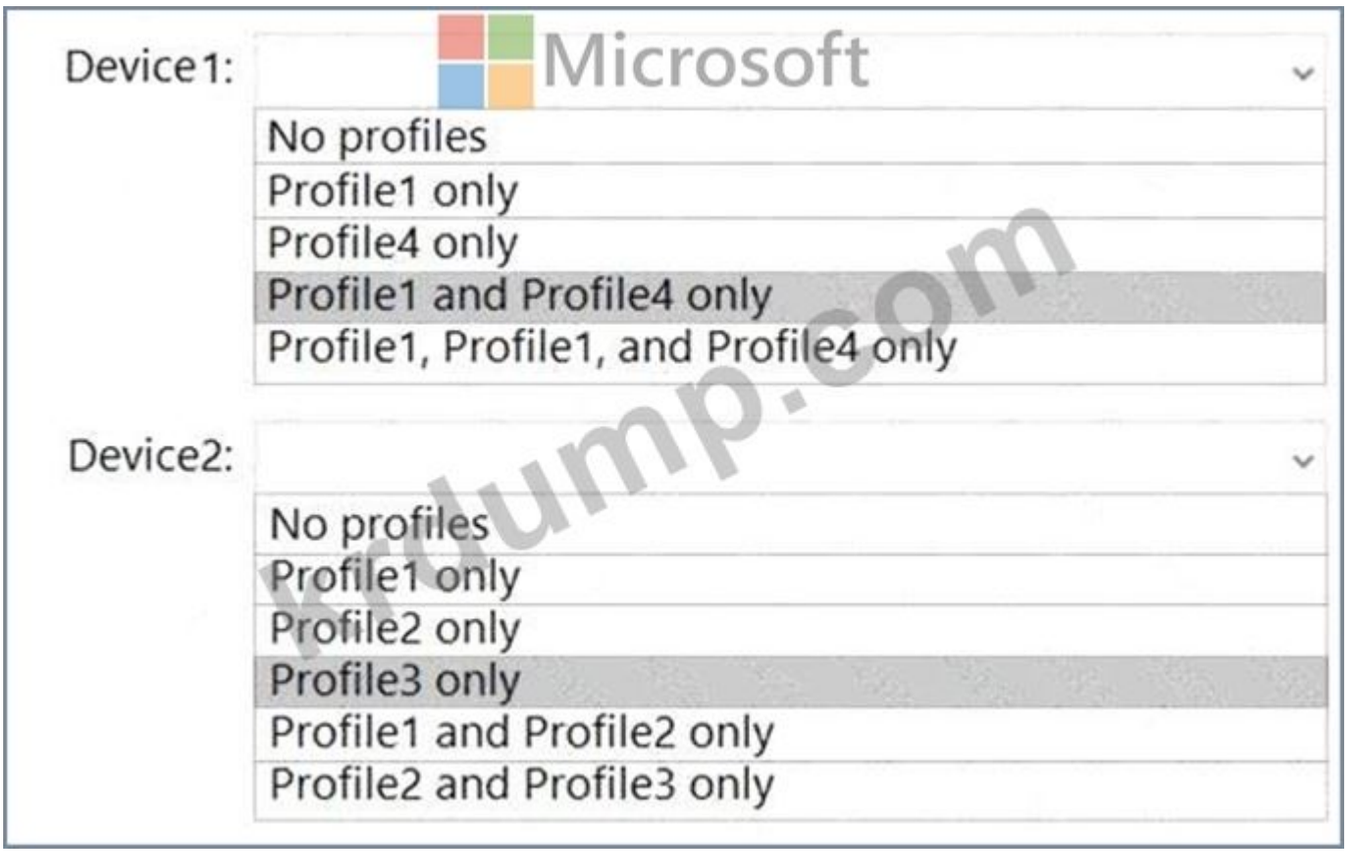
□ □□□ □□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 62

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

□□□□ □□□□ □□□ □□□ contoso.com□□□ Microsoft Entra □□□□ □□□□□□. (□ □ □□ □□□□□.) User2□ usef2@fabfikam.com□□ □□□□ □ Microsoft Entra □□□□ □ □□□ □□□□. User2□ Microsoft Entra ID□ □□□□ □□□□ □ □□□ □□□□ □□□. □□ □□: Microsoft Entra □□ □□□□ <abrlkam.com>□ □□□ □□ □□□□□ □□□□□. User2□□ user2@fabrikam.com□□ □□□□□□ □□□□□. □□□□ □□□ □□□ □ □□ □?

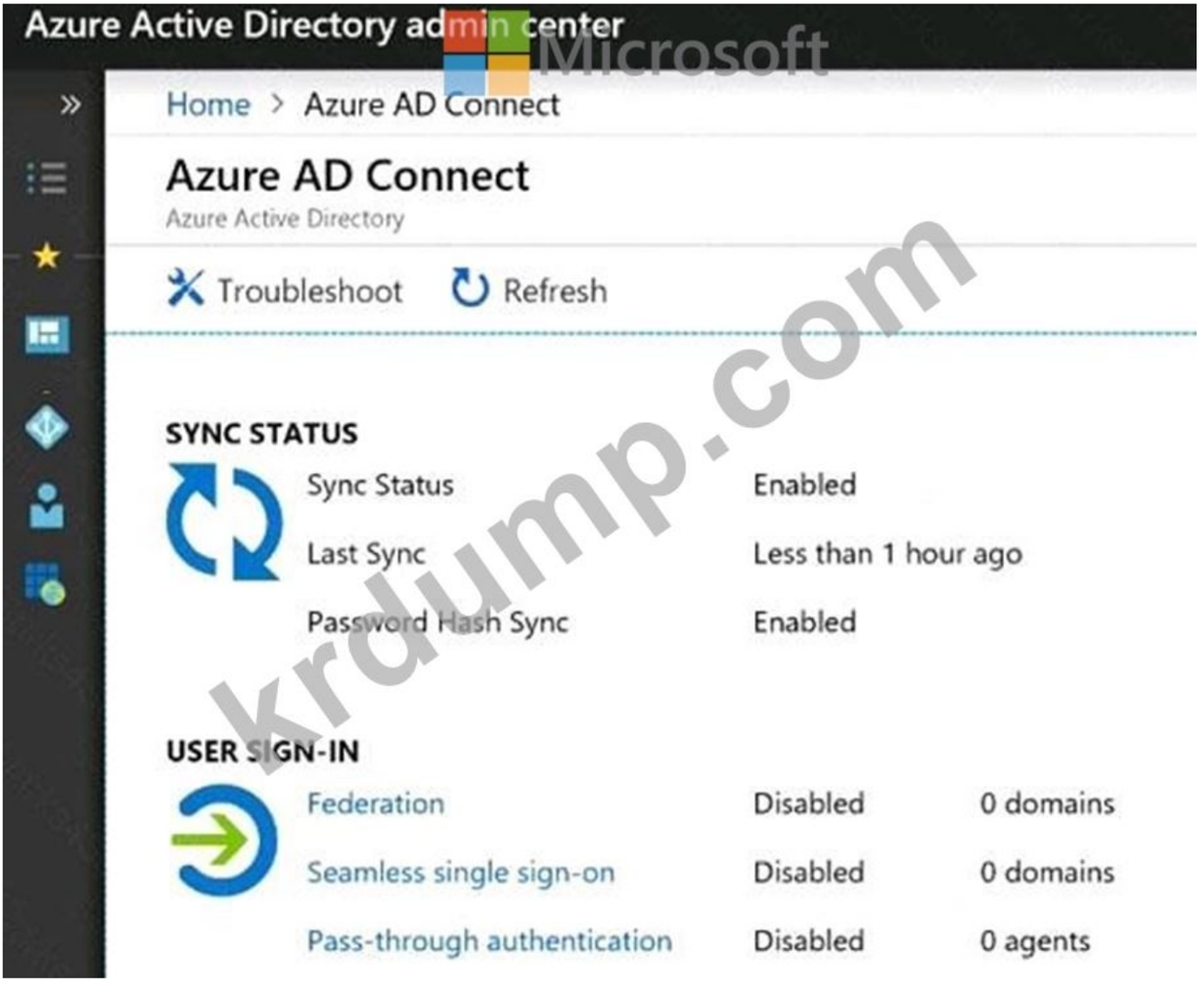
A. □

B. □□□

Answer: A (LEAVE A REPLY)

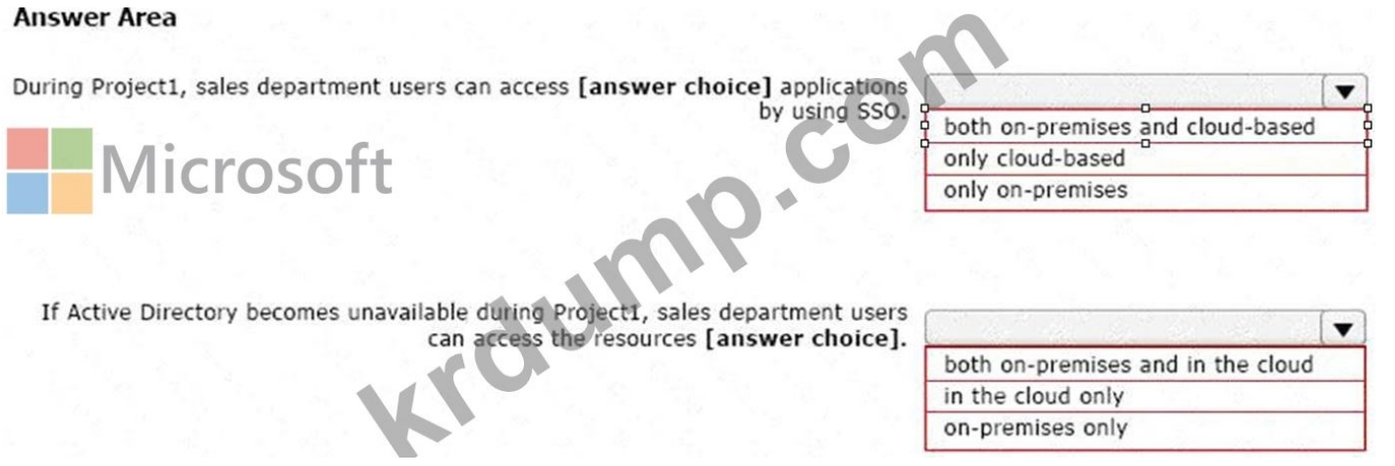
NEW QUESTION: 63
Microsoft 365 E5 □□□ □□□□.
□□ 7□ □□ □□□ IP □□□□ Microsoft Office 365□ □□□□ □□□□ □□□□ □□□.
□□□ □□ □□□?
A. Microsoft 365 □□ □□□□ □□ □ □□ □□ □□□□ □□□□□.
B. Microsoft 365 □□ □□□□ □□ □□□□ □□□□□.
C. Cloud App Security □□ □□□□ □□□ □ □□□ □□□□□.
D. Azure Active Directory □□ □□□□ □□□ □□□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 64
□□□
Microsoft 365 □□□□ □□□□.
□□ □□□ □□ Azure AD Connect□ □□□□□.



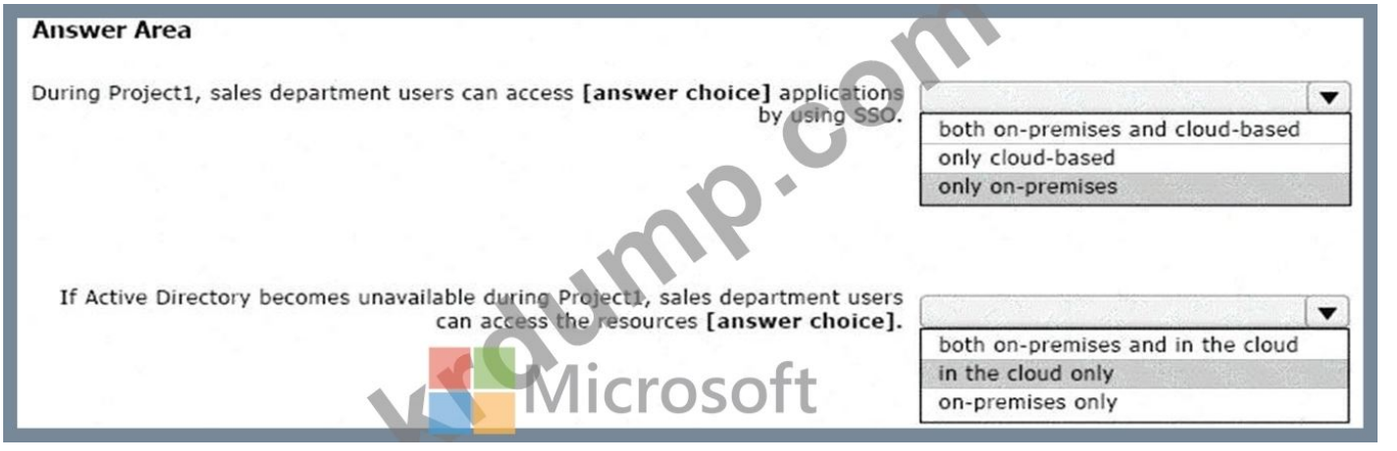
□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:



Box 1: only on-premises

In the exhibit, seamless single sign-on (SSO) is disabled. Therefore, as SSO is disabled in the cloud, the Sales department users can access only on-premises applications by using SSO.

In the exhibit, directory synchronization is enabled and active. This means that the on-premises Active Directory user accounts are synchronized to Azure Active Directory user accounts. If the on-premises Active Directory becomes unavailable, the users can access resources in the cloud by authenticating to Azure Active Directory. They will not be able to access resources on-

premises if the on-premises Active Directory becomes unavailable as they will not be able to authenticate to the on-premises Active Directory.
Box 2: in the cloud only

NEW QUESTION: 65
□□□ □□□ Microsoft 365□ □□□□ □□□□.
□□ □□□□ □□ Office 365□ □□ □□□□□ □□ □□□ □□ □□□□ □□□□ □□□. □ □□□□ □□□□□ □□□□ □ □□□ □□□ □□□ □□□□□ □□□.
□□□ □□□□ □□□?
A. Microsoft 365 □□ □□□ □□ □□□
B. Microsoft Purview □□ □□ □□□ □□□
C. Microsoft Entra □□ □□□ □□□□ □□□□
D. Microsoft 365 □□ □□□ □□□
Answer: (SHOW ANSWER)
Microsoft 365 Reports in the admin center
You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.
Which activity reports are available in the admin center
Depending on your subscription, here are the available reports in all environments.

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

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

NEW QUESTION: 66
Microsoft Defender for Endpoint□ □□□□ Microsoft 365 □□□ □□□□.
□□□ □□ □□□ Microsoft Defender for Endpoint□ □□□□ □□□□.
□□ 24□□ □□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□ □□□.
□□□ □□ □□□?
A. □□ □□□□ □□□ □□ □□□ □□□□.
B. Microsoft Purview □□ □□ □□□□ DLP(□□□ □□ □□) □□□ □□□□.
C. □□ □□□□□ □□ □□□ □□□ □□□ □□□□□.

D. Microsoft Purview □□ □□ □□□□ □□ □□ □□□ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Microsoft 365 □□□□ □□□□.
Microsoft 365 □□ □□□ □□□□ □□□□ □□□□□ □□□ □□□□□.
Microsoft 365 □□ □□□ □□□□ □□□□□ □□ Microsoft □□□ □□□ □□□□□?
A. □□□□□ Microsoft Defender□ □□□□□.
B. Microsoft Purview
C. Azure Arc
D. ID□ □□ Microsoft Defender
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

NEW QUESTION: 68
Microsoft 365 □□□ □□□□.
□□□ □□□ □□□ □□□□ □□□ □□□□ □□ □□ □□□ □□□ □□□ □□□ □□□ □□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□ □□(DLP) □□
B. □□ □□
C. □□ □□
D. □□□ □□ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 69
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: 70

□□ □□ □□ □□

□□□ □□□ Microsoft 365 E5 □□□□ □□□□ .

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

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

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

□□ □□□ □□□ □□□ □ □□□?

A. Device1, Device2, Device3, Device4, Device5

B. Device2, Device3, Device5□

C. Device2□ Device4□

D. Device1□ Device3□

E. Device2□

Answer: (SHOW ANSWER)

NEW QUESTION: 71

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

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

□□ cmdlet□ □□□□ □□□?

A. □□□ □□ □□

B. □□□□□□ □□

C. Execute-AzureAdLebelSync

D. □□□□ □□

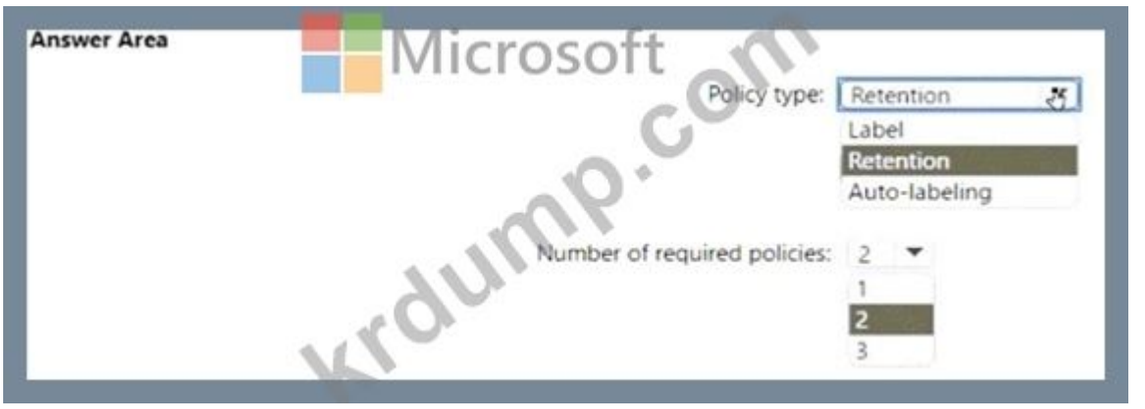
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72

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

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

□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

NEW QUESTION: 73

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

□□□□ Microsoft Teams, OneDrive □□ SharePoint Online□□ □□ □□□ □□□ □□□□□ □ □□□□ □□ □□□.

□□□ □□ □□□?

A. □□□ □□□ □□ □□□ □□□□.

B. □□□ □□ □□□ □□□ □□□□□.

C. □□□ □□□□ □□□ □□□□.

D. □□□ □□ □□ □□□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams

In organizations with Microsoft Defender for Office 365, Safe Attachments for SharePoint, OneDrive, and Microsoft Teams provides an additional layer of protection against malware. After

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

NEW QUESTION: 74
□□□□□ □□□□□□ Contoso.com□□ Active Directory □□□□ macOS, Windows 8.1, Windows 10 □□ Windows 11□ □□□□ 500□□ □□□ □□□□. □□ □□□ Microsoft Endpoint Configuration Manager□ □□□□ □□□□□. □□□□ Azure Active Directory(Azure AD)□ □□□□□□.
Microsoft 365 E5 □□□ □□□□ □□ □□□ □□□□ □□□□□. □□ □ □□ □□□ □ □□ □□□ □□□□□?
A. Windows 11 □ macOS□ □□
B. Windows 11□ □□
C. Windows 11, Windows 10-Windows8.1 □ macOS
D. Windows 11. Windows 10 □ Windows8.1□ □□
E. Windows 11 □ Windows 10□□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
User1□□□ □□□□ □□□ Microsoft 365 □□□ □□□□.
User1□ □□ □ □□ □□ □□ □□□□ Microsoft 365 □□ □□□ □□□ □ □□□ □□□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□ □ □□ □□ □□ □□□ □□ □□ □□ □□
B. Exchange □□ □□□ □□ □□ □□ □□
C. Azure Active Directory □□ □□□ □□ □□□
D. □□ □ □□ □□ □□ □□□ □□ □□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?
view=o365-worldwide

NEW QUESTION: 76
□□□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□□□ □□□ Microsoft Defender for Endpoint□ □□□□□□.

Microsoft Defender □□□□ □□ □□□□□ □□□ □□□ '□□□ □□'□ □□□ □□ □□□ □ □□ □ □ □□□□.
□□□□ □□□ □□ □□□ □□ □□□□□ □□□□ □□□□ □□ □□□, □□□ □□ □□ □□ □□□ □□□ □ □□□ □□□.
Microsoft Defender □□□□ □□□ □□□□ □□□?
A. □□□□ □□ □□
B. □□ □□
C. □□ □□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft 365 E5 □□□ □□□□.
SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.
SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Microsoft Defender for Office 365 □□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Microsoft 365 □□ □□□□ SecAdmin1□□ Exchange □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
You need to assign the Security Administrator role.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp

NEW QUESTION: 78
Microsoft Intune□ □□□ Microsoft 365 □□□ □□□□.
Intune□ □□□□ □□ iOS □□□ □□□ □ □□□□.

Microsoft Defender for Endpoint□ □□□□ □□ □□□ iOS □□□ □□□ □□□□□. Intune□ Defender for Endpoint □□ □□□ □□□□□.
Endpoint□ Defender□ □□□ □□□□□ □□□.
□□□ □□ □□□?
A. Intune□ □□ □□□□□.
B. □ □□ □□□ □□□□.
C. □□□□□ Microsoft Defender□ □□□□□□.
D. □□□ □□□□ □□□□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 79
User1□□ □□ □□□ □□□□ □□□?
□□ □□□ □□ □□ (□□□ □□ □□ □□□ □□□□□)
A. □□□□
B. □□ □□
C. □□ □□□
D. □□ □□
Answer: (SHOW ANSWER)
A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center. Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

NEW QUESTION: 80
□□ □□ □□□ □□□□ □□□□ Azure AD □□□□ □□□□.

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Exchange Administrator

□ □□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□ □□□ □□□□ □□□?
A. Microsoft Purview □□ □□ □□
B. Microsoft Entra □□ □□
C. Microsoft 365 □□ □□

D. Microsoft 365 Defender □□1

Answer: (SHOW ANSWER)

NEW QUESTION: 81

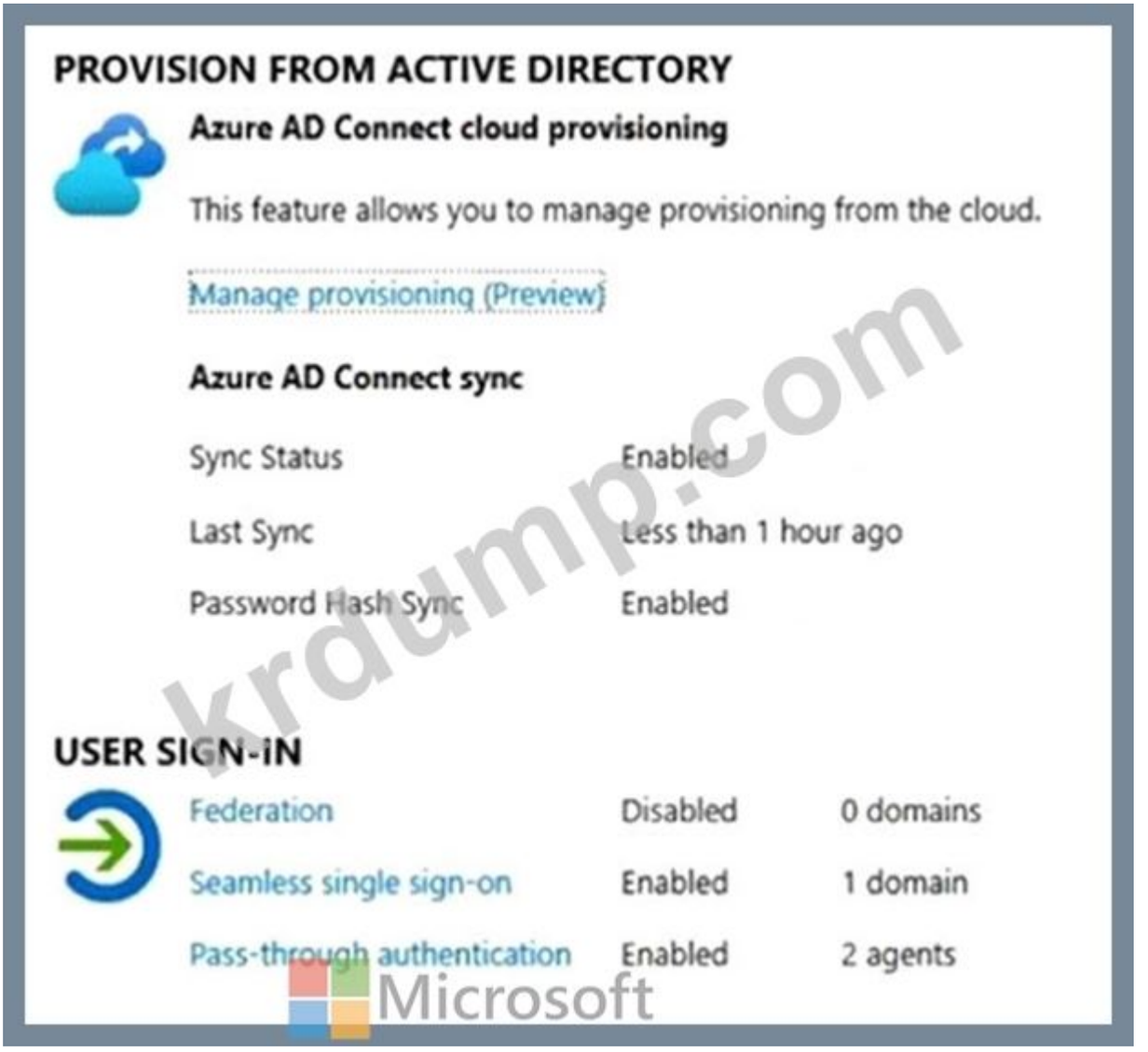
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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



User2□ user2@fabrikam.com□□ □□□□□□ Azure AD□ □□□□ □□□□□.
User2□ Azure AD□ □□□□ □□□□ □ □□□ □□□□ □□□.
□□□: Microsoft Entra □□ □□□□ User2□□ □□ □□ □□□ □□□□□. User2□□ user2@contoso.com□□ □□□□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)
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: 82
EU PII □□□□ □□ □□□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□ □ □□ □□ □□ □□□ □□ □□□□□.
B. Exchange □□ □□□ □□ □□
C. Exchange □□ □□□ □□□ □□ □□(DLP) □□
D. □□ □ □□ □□ □□ □□□ □□□ □□ □□(DLP) □□
Answer: A (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

NEW QUESTION: 83
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft 365 E5 □□□ □□□□.
SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.
SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Office 365 Advanced Threat Protection(ATP) □□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Azure Active Directory □□ □□□□ SecAdmin1□□ Teams □□□ □□□ □□□ □ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□

Answer: B (LEAVE A REPLY)

You need to assign the Security Administrator role.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365- worldwide

NEW QUESTION: 84

Microsoft 365 E5 □□□ □□□□.

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

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

□ □□□ □□ DLP □□□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.

Answer Area

Sender is condition: DLP1 only

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

File extension is condition: DLP1, DLP2, and DLP3

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

Answer:

Explanation:

NEW QUESTION: 85

Microsoft 365 E5 □□□ □□□□.

□□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□□ □□□.

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

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

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

R&D □□□ □□□□ Android□ iOS □□ □□□□ □□□□ □□□□ □□□.

□□ □□□ □□□□ App1□□□ Azure AD □□□□□□ □□□□□□□ □□□□ □ □□□ □□□. □□ □□ □□□□ 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 Azure AD 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: 86
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: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

NEW QUESTION: 87
contoso.com□□□ Azure AD □□□□ □□□□ Microsoft 365 □□□ □□□□. □□□□□ □ □ □□ □□□ □□□□ □□□□ □□□□.

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

User5□□ □□ □□□□ □□□ □□□ □□□ □□□□□.
User5□ □□□ □ □□ □ □□ □□ □□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□? □ □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. User2□ User4□ □□□□□.
B. User4□ □□□□□ □□□□□□.
C. Azure AD□ □□ □□□□ □□□□□ □□□□□□.
D. User1, User2, User4□ □□□□□.
E. User2□ User4□ □□□□□ □□□□□□.
F. Azure AD□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).
Only on users who are non-admins or in any of the following limited admin roles:
* Directory Readers
* Guest Inviter
* Helpdesk Administrator
* Message Center Reader
* Reports Reader
* User Administrator
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin- roles#available-roles

NEW QUESTION: 88
□□□
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

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

Answer Area

Microsoft 365 setting:

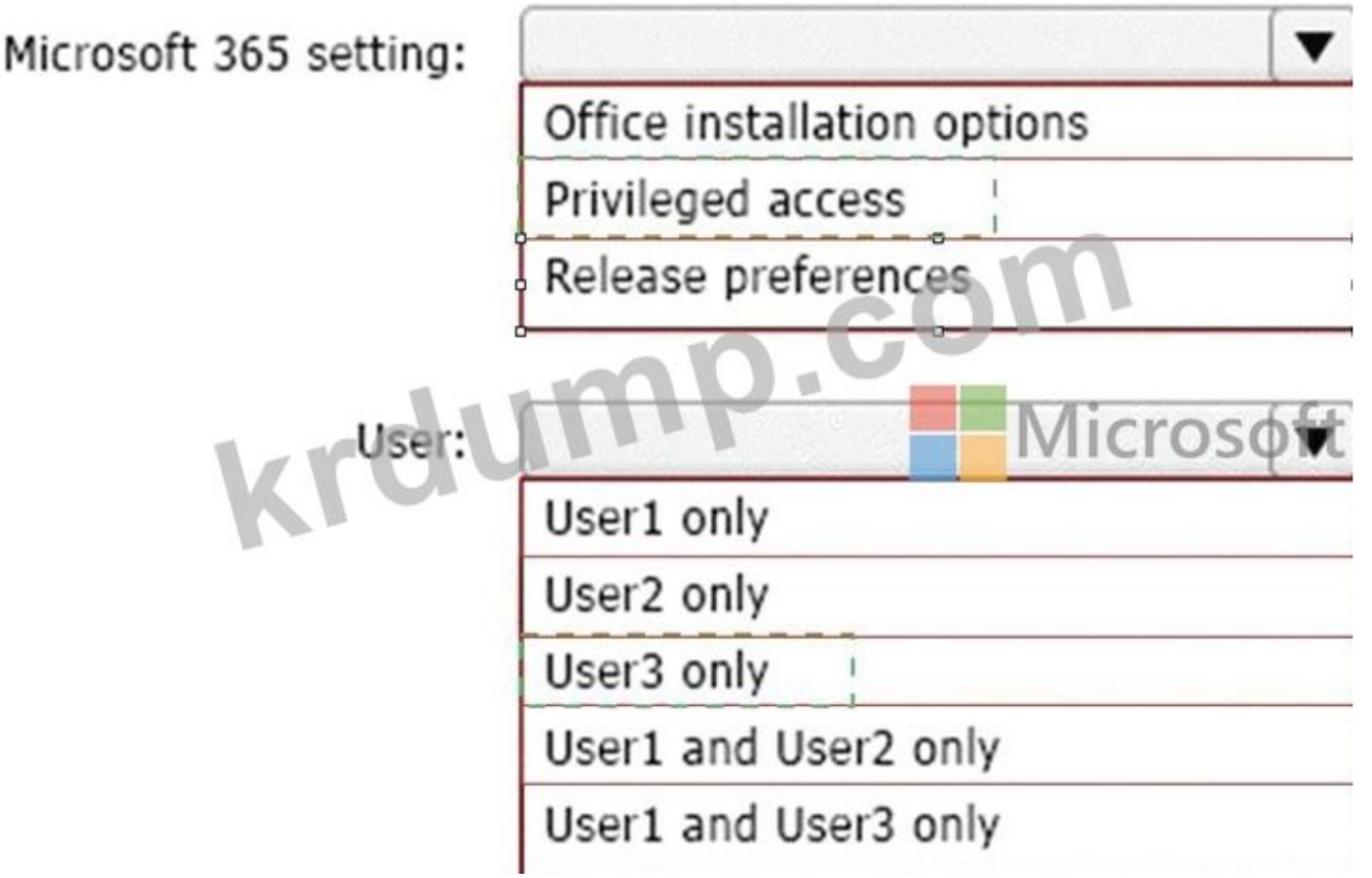
- Office installation options
- Privileged access
- Release preferences

User:

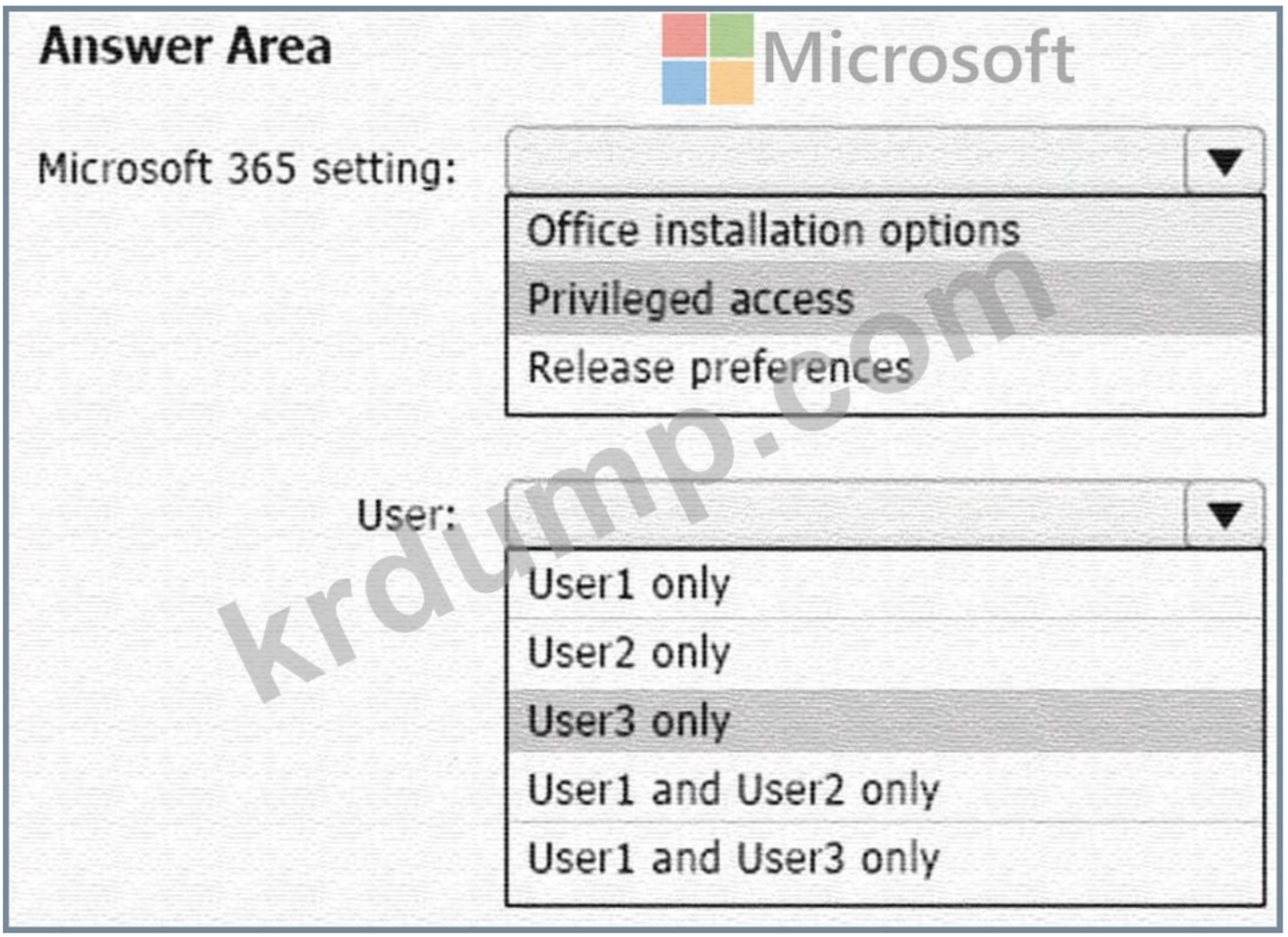
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

Answer:

Answer Area



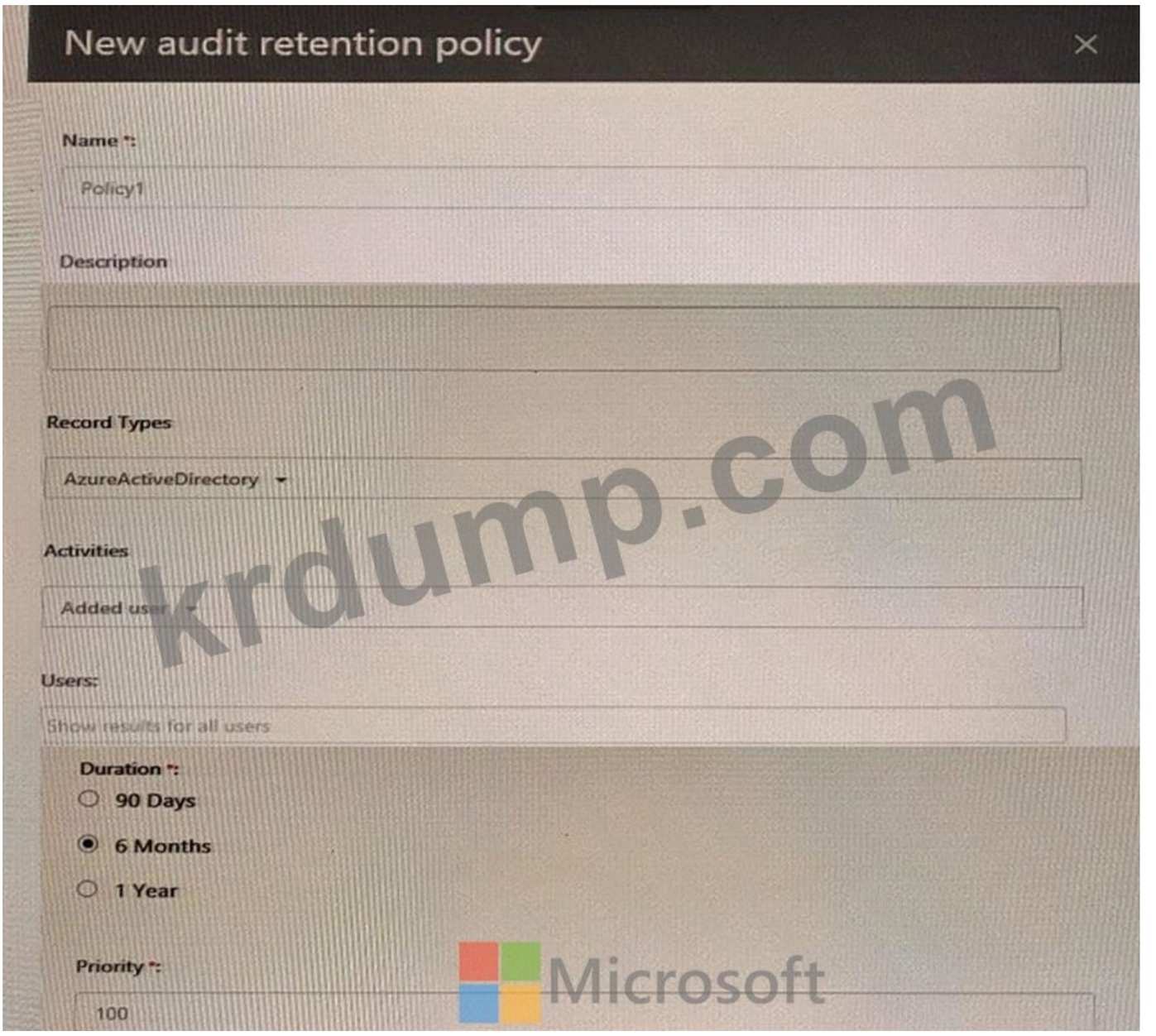
Explanation:



NEW QUESTION: 89

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

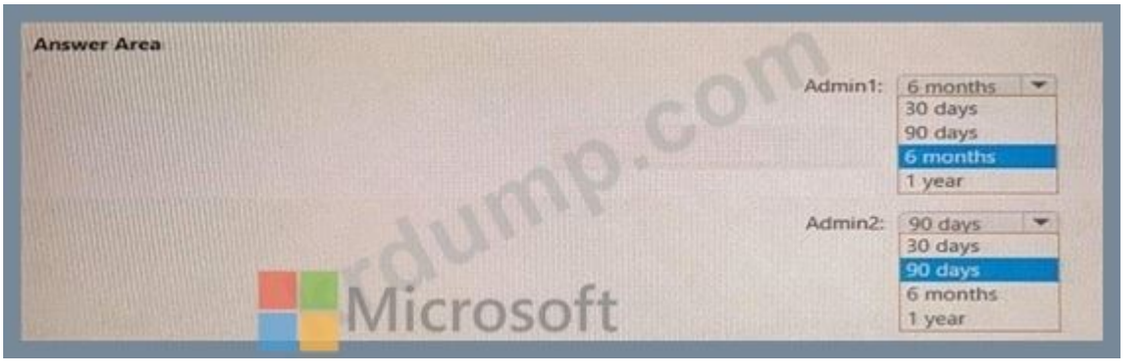
Name	License
Admin1	Microsoft Office 365 E5
Admin2	*None*



User1□□□ □□□ □□□ □□□□ □□ □□□□□.

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

□□ □□□ 1□□ □□□□□.



Answer:

NEW QUESTION: 90

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

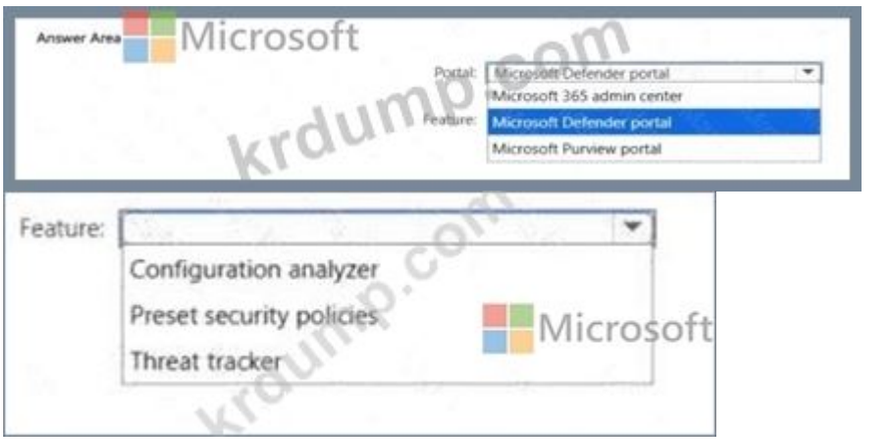
NEW QUESTION: 91

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

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

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

□□: □□ □□□ 1□□□□.



Answer:

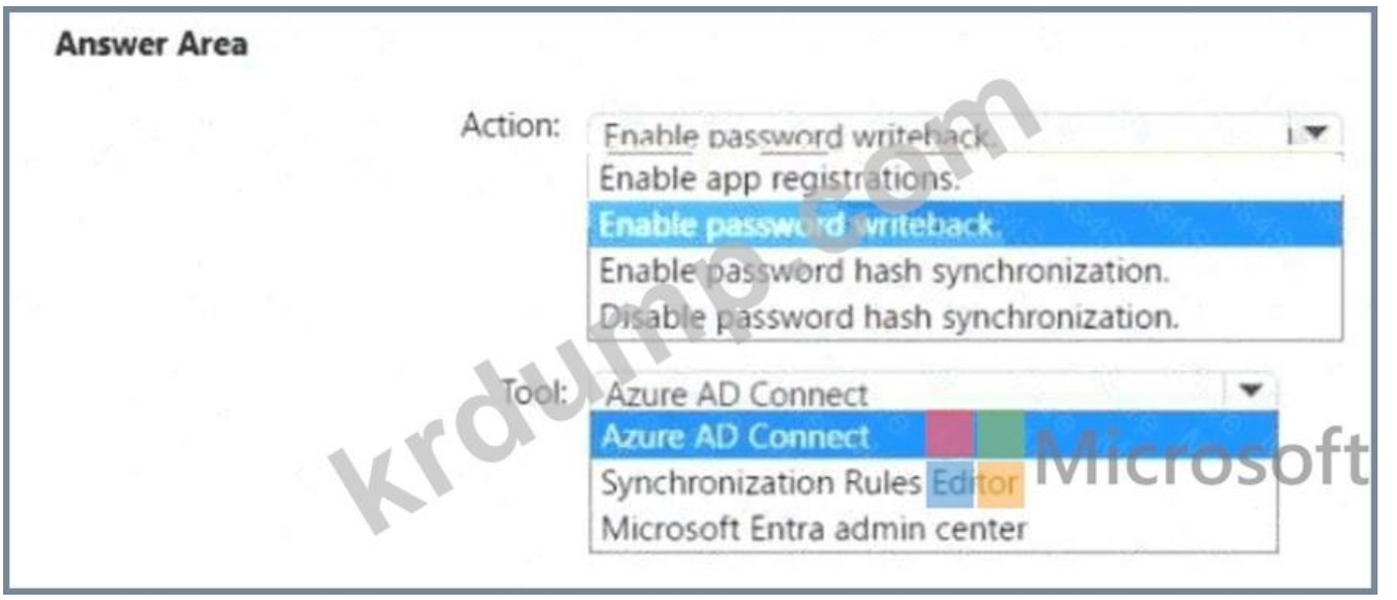
Explanation:

NEW QUESTION: 92

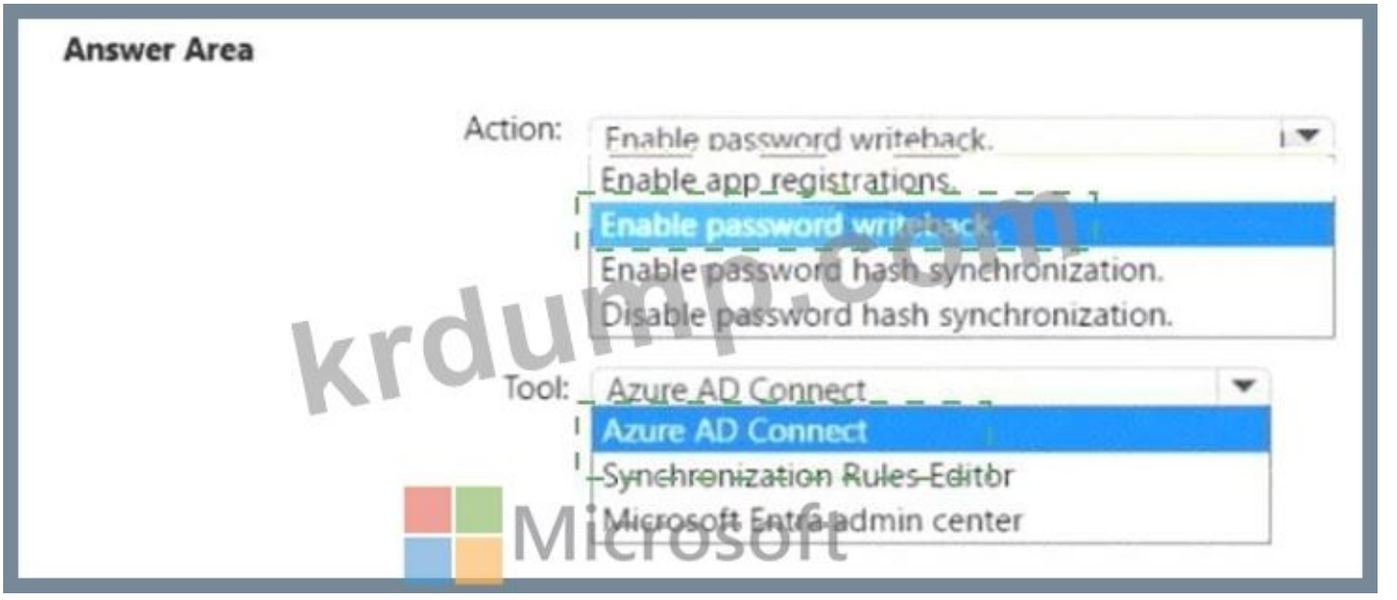
Admin4□ SSPR□ □□□ □ □□□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 93

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

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

□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows Server 2019□ □□□□ □□□ □□□□□ □□□□. □□□□□ □□□□ □□ □□□ Windows Server 2012 R2□□□.
□ □□□□□ Windows 10□ □□□□ 100□□ □□□□ Windows Server 2012 R2□ □□□□ Server1□□□ □□ □□□ □□□□ □□□□.
Server1□ □□□□ □□□□ □□□□ Windows 10 □□ □□ □□□ □□□ □□□□□.
Server1□ □□ □□ □□ □□(GPMC)□ □□□□□.
Server1□□ □□□□□ Windows □□□□ □□ □□ □□□ □□□□ □□□.
□□ □□: □□□ □□ □□□ Windows Server 2019□ □□□□. Windows 10 □□□□□ □□ □□□ □□□□□ Netlogon □□□ □□ □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

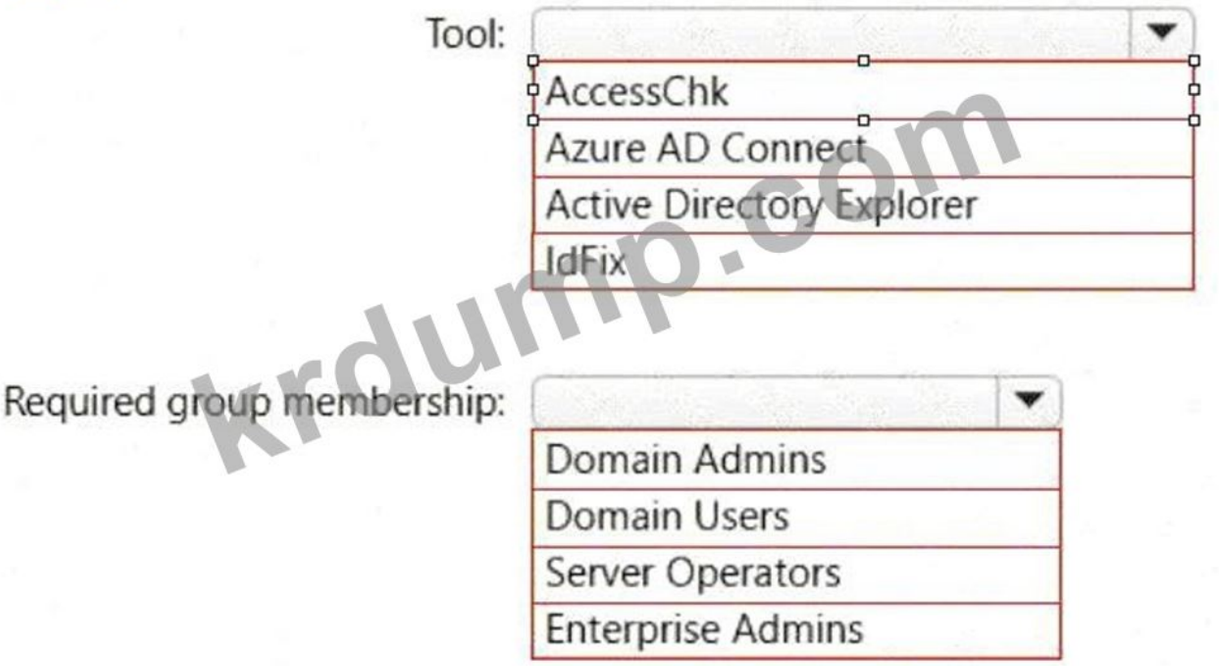
Answer: (SHOW ANSWER)

NEW QUESTION: 94

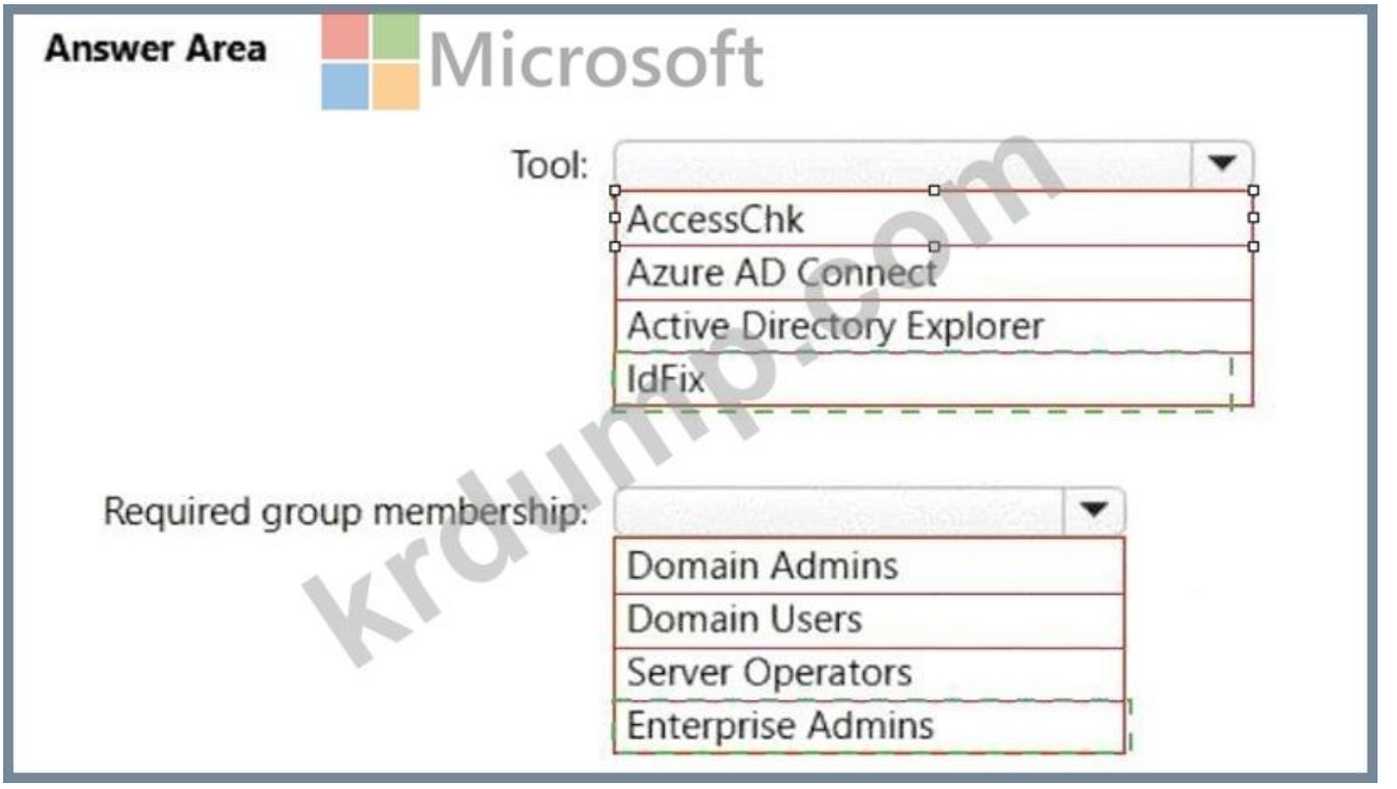
□□□

□□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft 365 E5 □□□ □□□□.
□□□□ □□□□ □□□ □□□□□.
□□□□ □□ □□□□ □□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

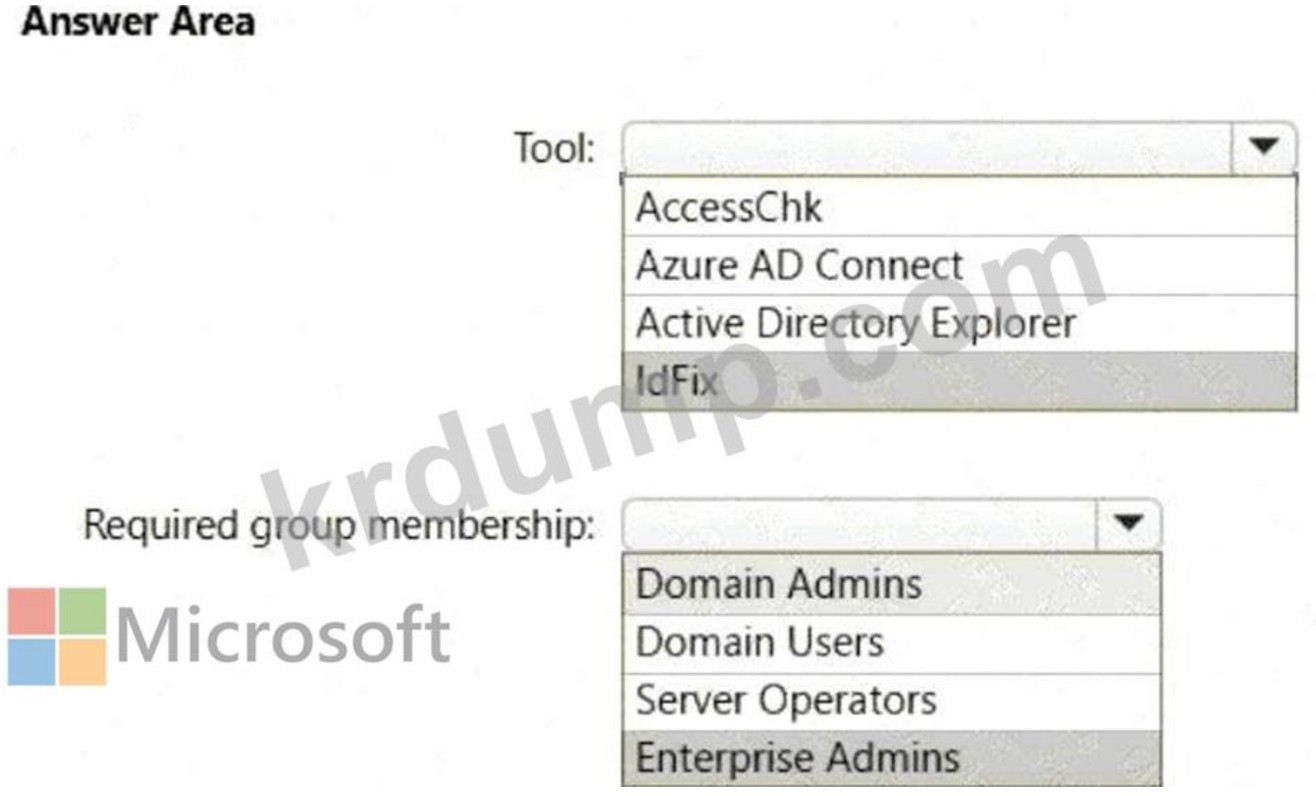
Answer Area



Answer:



Explanation:



Box 1: IdFix

Query and fix invalid object attributes with the IdFix tool

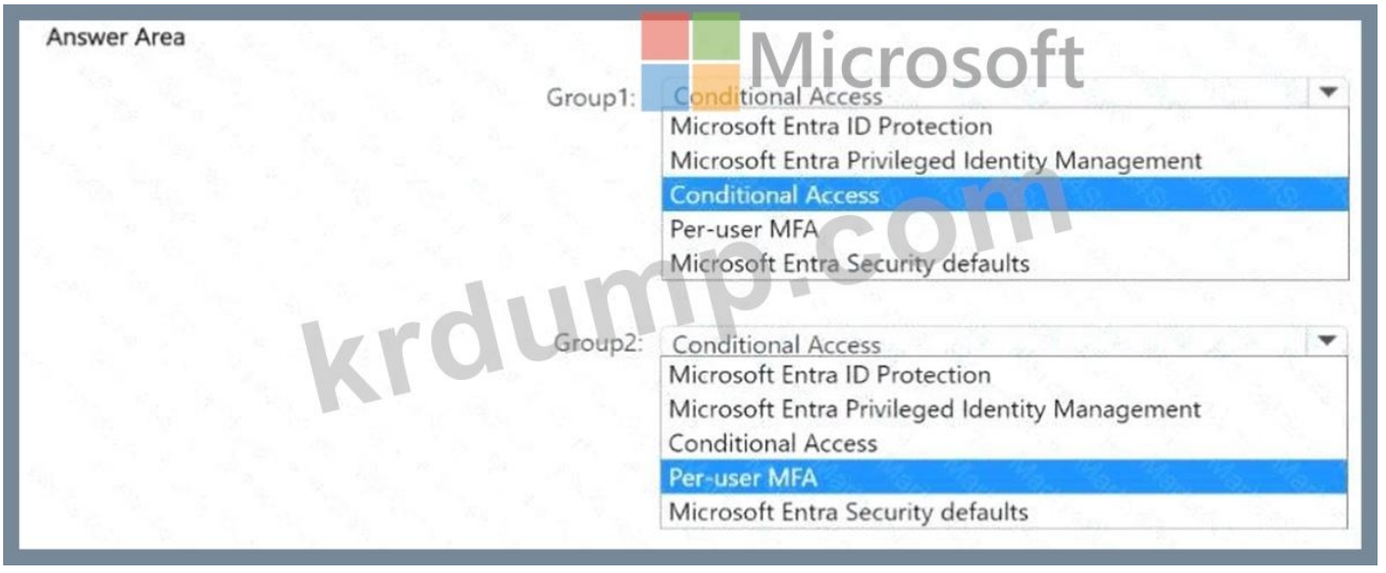
Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft

365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization

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

Reference:
https://microsoft.github.io/idfix/
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups

NEW QUESTION: 95
Group1□ Group2□□ □ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.
Group1 □ Group2□ □□□ □□ □□ □□ □□(MFA)□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Group1 □□□ Android □□□□ Microsoft Entra ID□ □□□ □□ MFA□ □□□□□ □□□□ □□□ □□□.
* □□ 2 □□□□ □□ □□□□ □□□□ Microsoft Exchange Online□ □□□□ □□ MFA□ □ □□□ □□□.
* □□□ □□□ □□□□□ □□□.
□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

Answer Area

NEW QUESTION: 96

Microsoft 365 E5 □□□ □□□□.

□□□ □□□ □□□□ □□□□ □□□.

□□ □□□ □□□□ □□□?

A. Microsoft Entra □□ □□

B. SharePoint □□ □□

C. Microsoft Purview □□ □□ □□

D. Microsoft 365 □□ □□

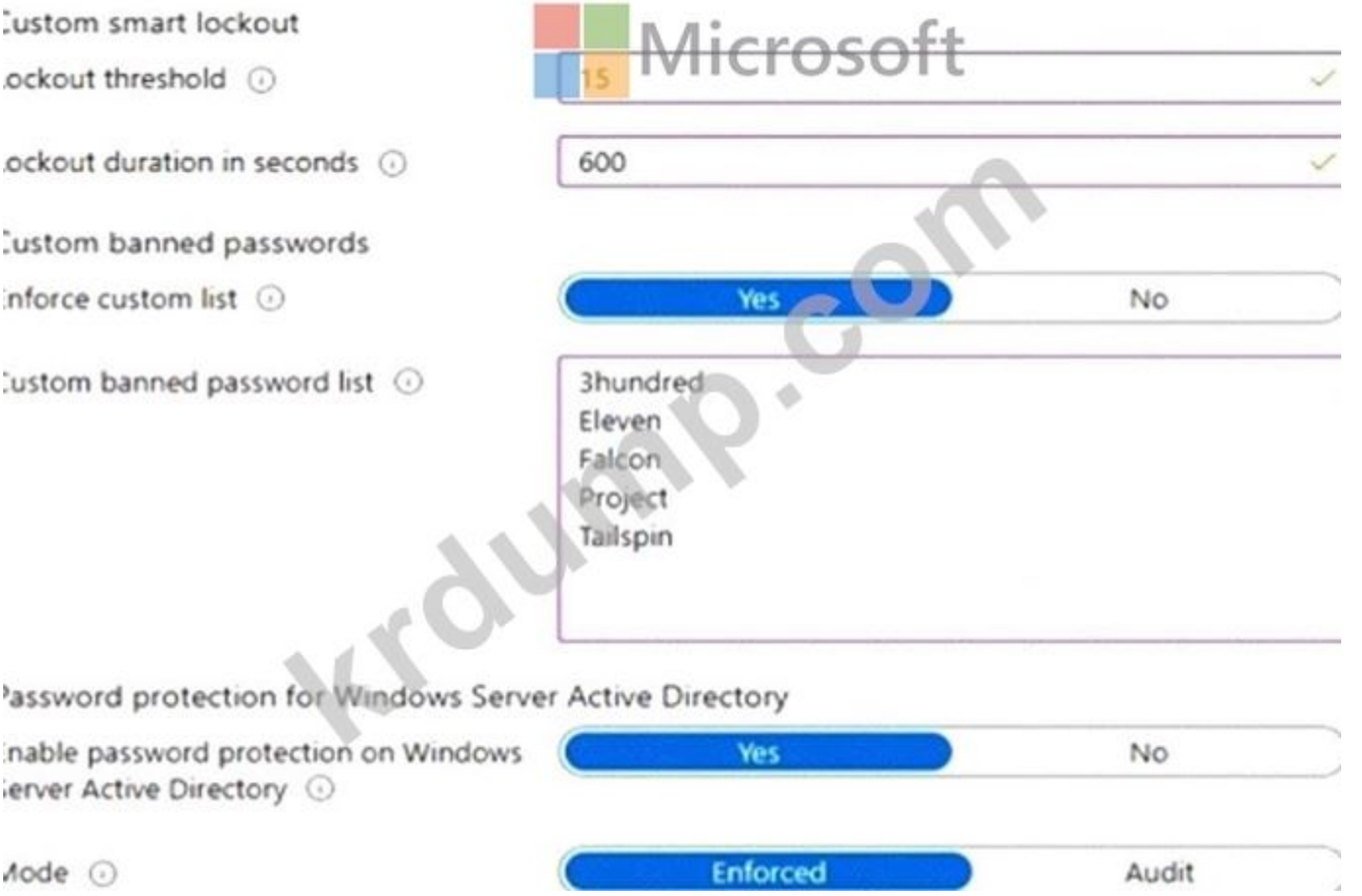
Answer: D (LEAVE A REPLY)

NEW QUESTION: 97

□□□

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

Azure AD □□ □□□ □□ □□□ □□ □□□□□.



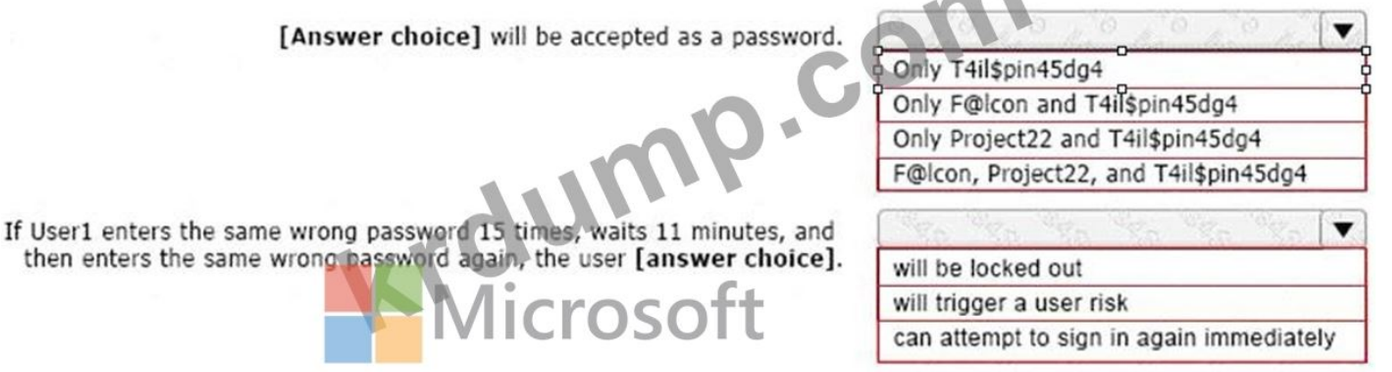
User1□ □□□ □□□□□ □□ □□□□□ □□□□□□□ □□□□□.

* □□
* □□□□22
* T4il$pin45dg4

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

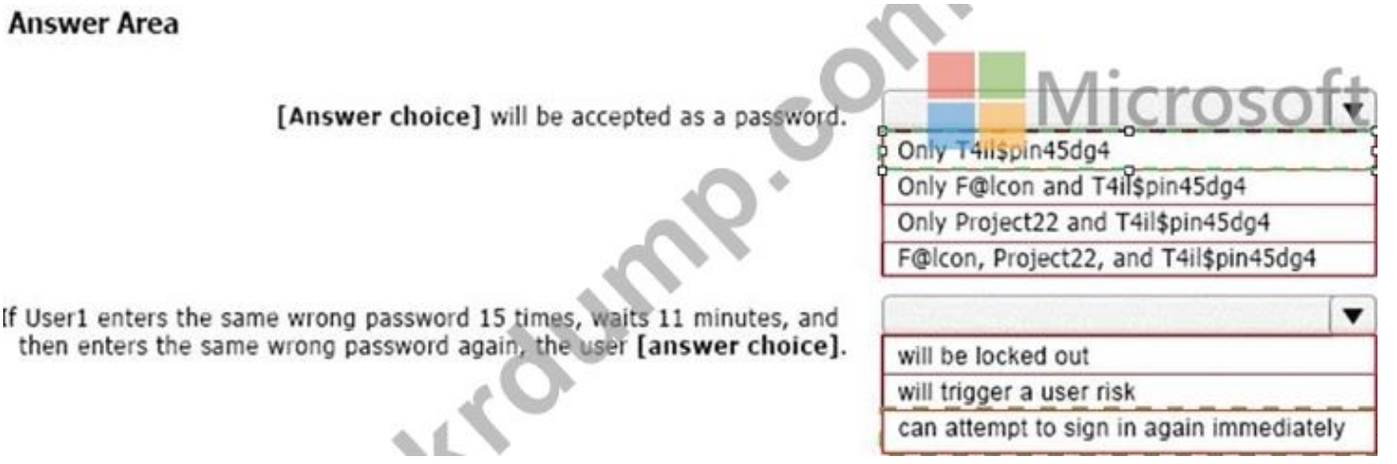
□□□□: □□ □□□ 1□□□□.

Answer Area

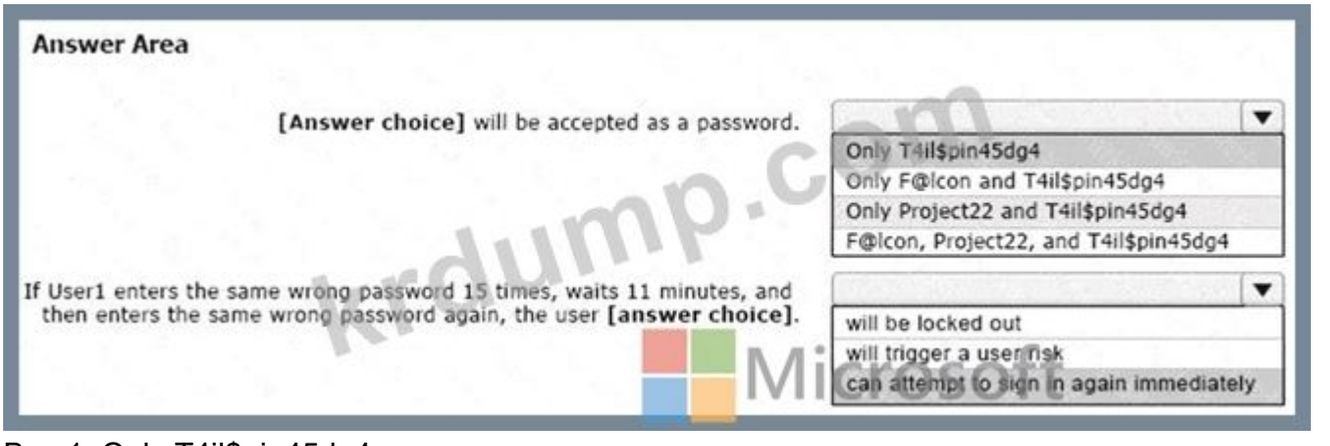


Answer:

Answer Area



Explanation:



Box 1: Only T4il$pin45dg4

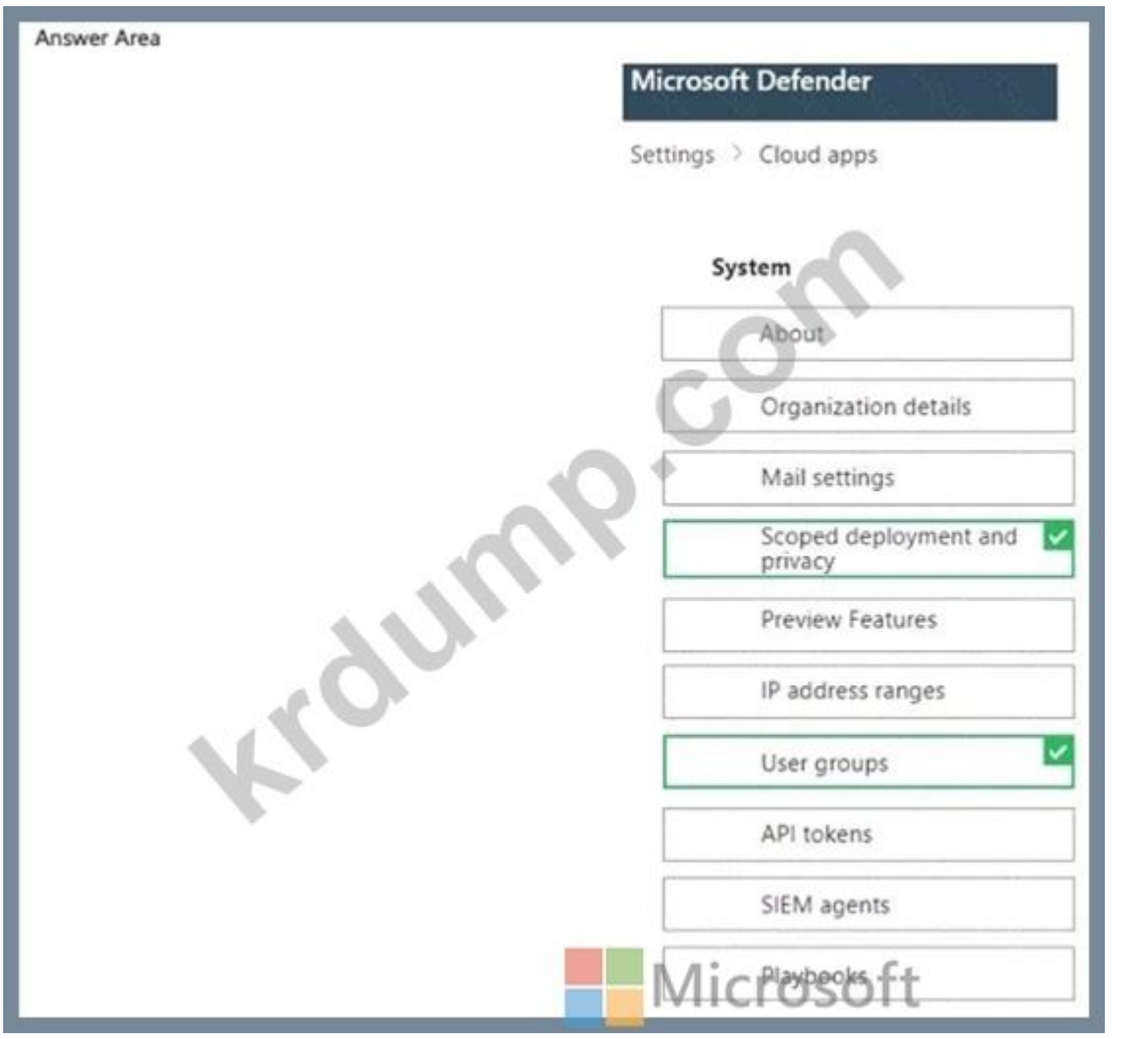
Box 2: can attempt to sign in immediately

Note: Manage Azure AD smart lockout values

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

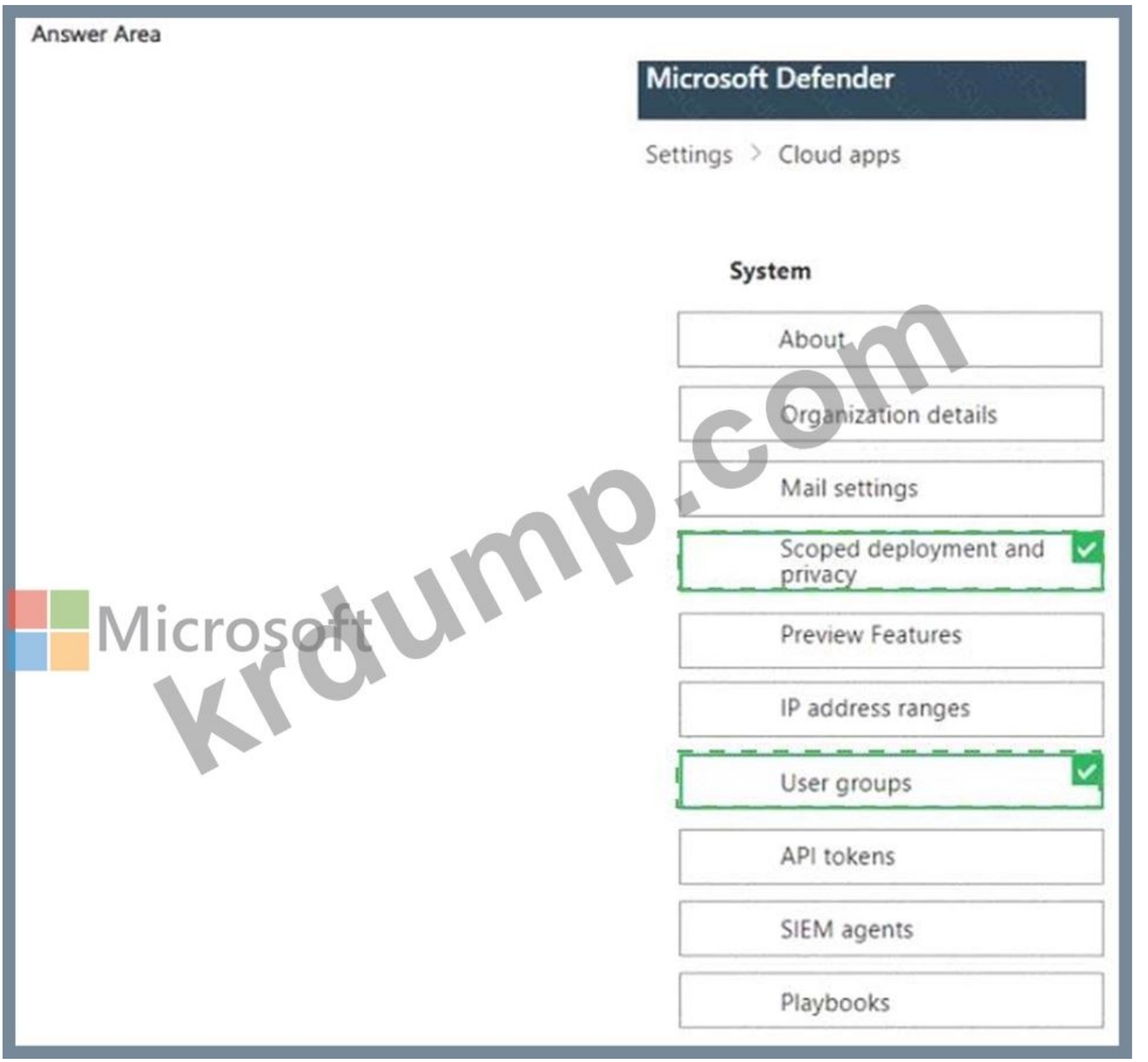
Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users. Customization of the smart lockout settings is not available for Azure China 21Vianet tenants.
To check or modify the smart lockout values for your organization, complete the following steps:
Sign in to the Entra portal.
Search for and select Azure Active Directory, then select Security > Authentication methods > Password protection.
Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.
The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.
Set the Lockout duration in seconds, to the length in seconds of each lockout.
The default is 60 seconds (one minute).
If the first sign-in after a lockout period has expired also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

NEW QUESTION: 98
□□ □□ □□□ □□□□ User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
User1□ □□□ 1,000□□ □□□ □□□□ □□ □, □□□□ □□ □□□□ □□□ □□ □□□ □□□ □□□□□. □□□ □□□□ □□□.
* User1□ □□□ □□□ □ □□ □□□□ □□□□□?
* User1□ □□□□ □□ □□□ □□ 2,000□□ □□□□ □□ □ □□□ □□□□ □□ □ □□ □ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

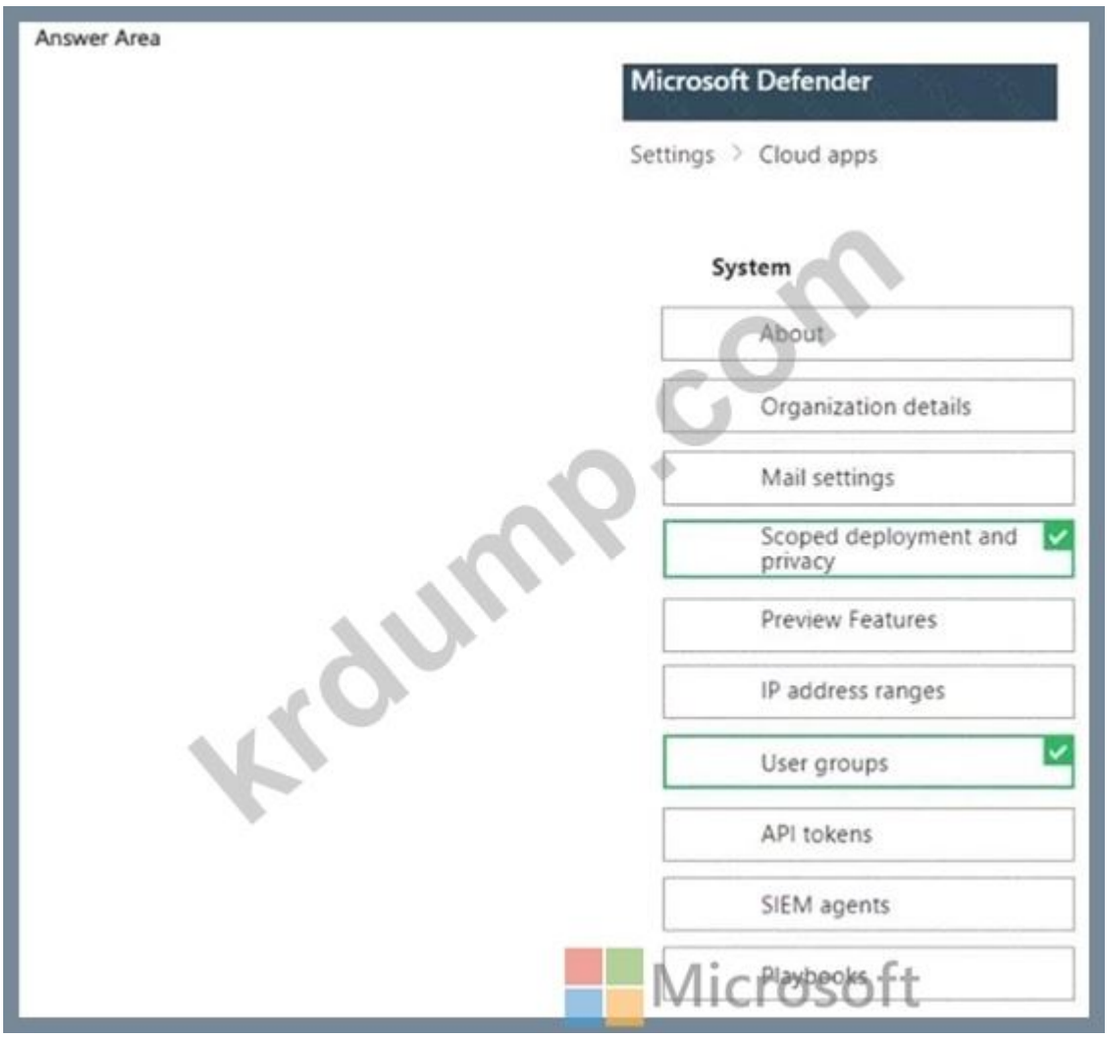

Answer Area
Microsoft Defender
Settings > Cloud apps
System
About
Organization details
Mail settings
Scoped deployment and privacy
Preview Features
IP address ranges
User groups
API tokens
SIEM agents
Playbooks
krdump.com
Microsoft

Answer:

Answer Area

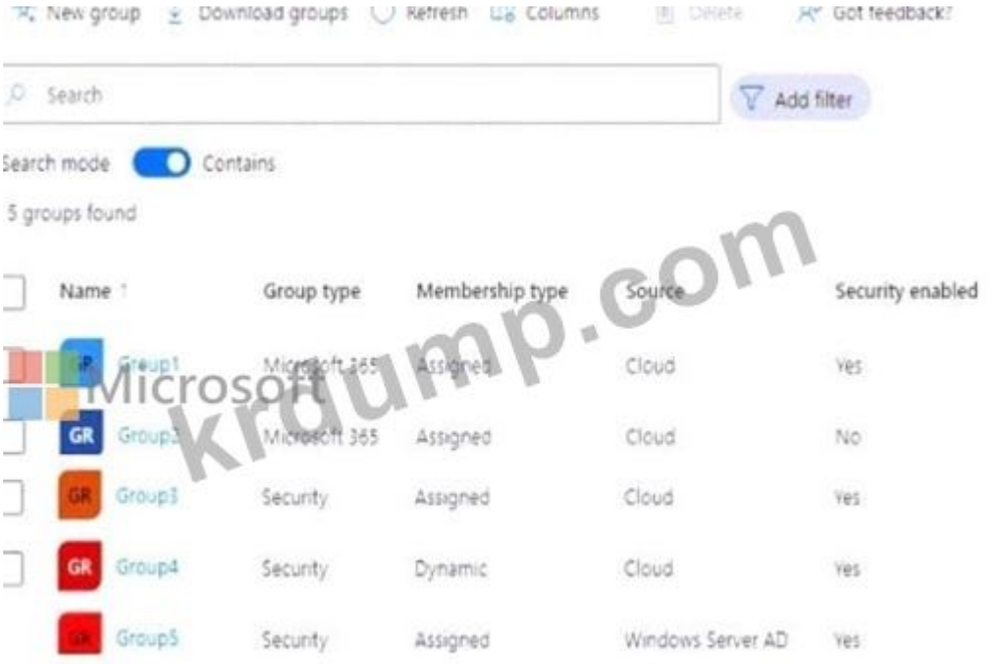


Explanation:



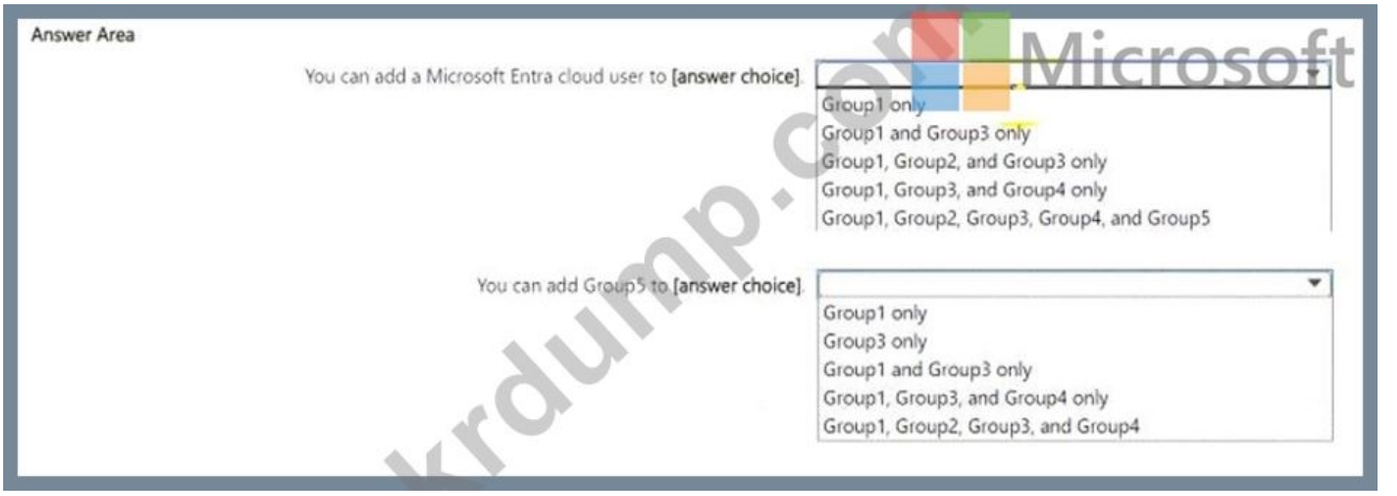
NEW QUESTION: 99

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

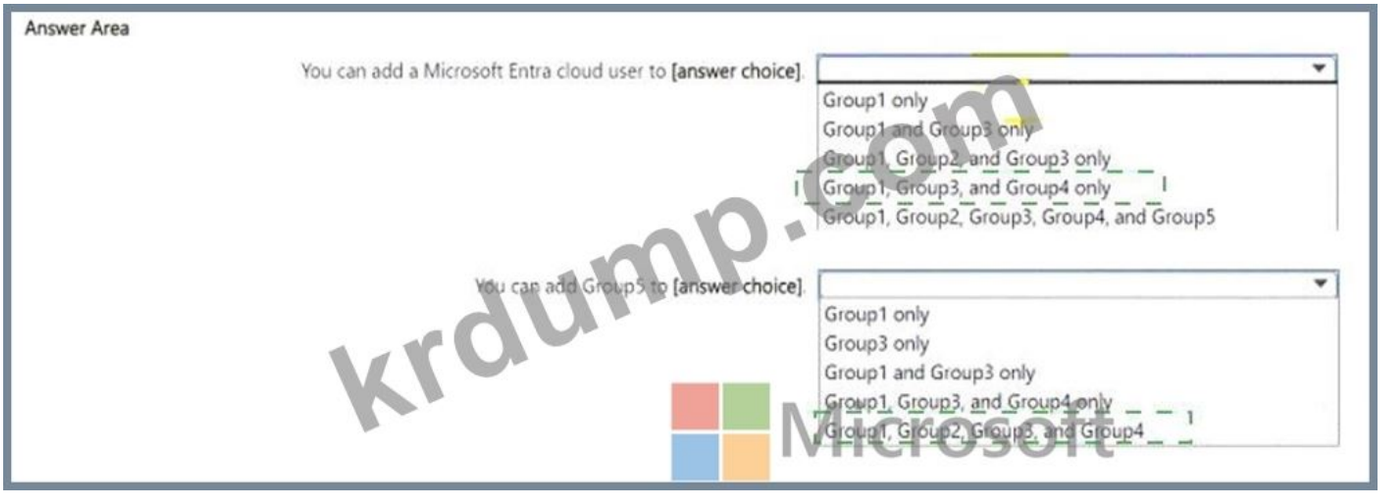


□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□ □ □□□□□.

□□□□: □□ □□ □□□ 1□□ □□□ □□□□.



Answer:



Explanation:

You can add a Microsoft Entra cloud user to: Group1, Group3, and Group4 only Group1: Microsoft 365 group with assigned membership type and security enabled.

Group3: Security group with assigned membership type and security enabled.

Group4: Security group with dynamic membership type and security enabled.

Group2 is not security enabled, so it cannot have security-related tasks assigned.

Group5 is sourced from Windows Server AD, which may limit direct cloud user additions.

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

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

NEW QUESTION: 100

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

* □□□ 11
* □□□□□
* □□□ OS

□□ □□□ Endpoint DLP □□□ □□□ □ □□□?

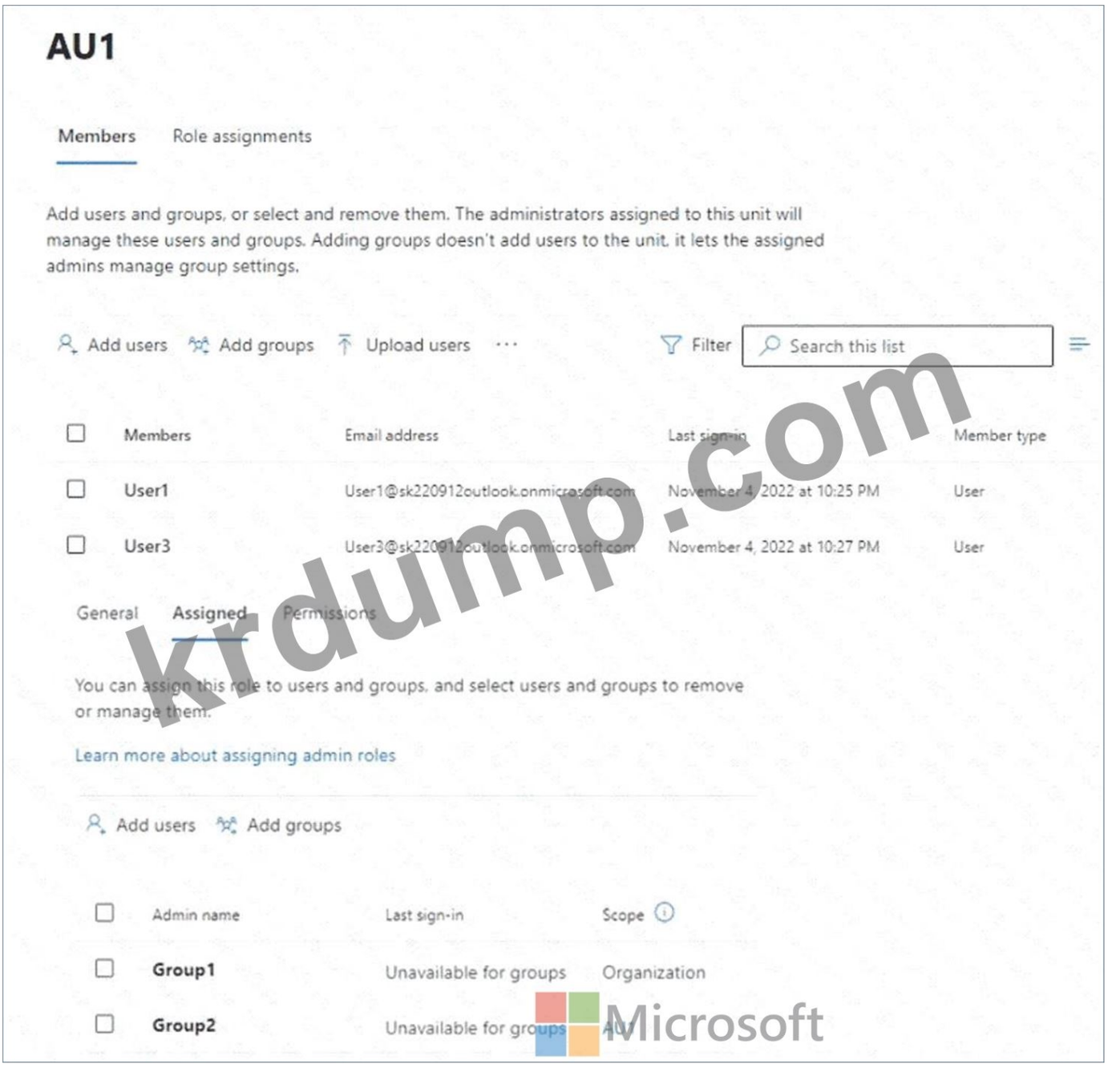
A. Windows 11□ □□
B. Windows 11 □ Android□ □□
C. Windows 11, Android □ iOS
D. Windows 11 □ iOS □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 101
contoso.com□□□ Azure AD □□□□ □□□ Microsoft 365 □□□ □□□□.
□□ □□□ □□□ □□□ □□□□□□ Contoso□□ □□□ □□□□□□ □ □□□.
□□ □□□ □□□□□ □□□ □□ □□□?
A. Microsoft Entra □□ □□□□ □□□ □□□ □□□ □□□□.
B. Azure AD Identity Protection□□ □□□ □□ □□□ □□□□□.
C. Microsoft Entra □□ □□□□ □□ □□ □□□ □□□□□.
D. Microsoft 365 □□ □□□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 102
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Member of
User1	Group1
User2	Group2
User3	None

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


AU1
Members
Role assignments
Add users and groups, or select and remove them. The administrators assigned to this unit will manage these users and groups. Adding groups doesn't add users to the unit. it lets the assigned admins manage group settings.
Add users
Add groups
Upload users
Filter
Search this list
Members
Email address
Last sign-in
Member type
User1
User1@sk220912outlook.onmicrosoft.com
November 4, 2022 at 10:25 PM
User
User3
User3@sk220912outlook.onmicrosoft.com
November 4, 2022 at 10:27 PM
User
General
Assigned
Permissions
You can assign this role to users and groups, and select users and groups to remove or manage them.
Learn more about assigning admin roles
Add users
Add groups
Admin name
Last sign-in
Scope
Group1
Unavailable for groups
Organization
Group2
Unavailable for groups
AU1

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


Answer Area
Statements
Yes
No
User1 can reset the password of User3.
User2 can reset the password of User3.
User2 can reset the password of User1.

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 103

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

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

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

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

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

Answer Area

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

Answer:

Answer Area

Explanation:

NEW QUESTION: 104

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

A. □□□□ □□ □□□
B. Azure AD ID □□
C. Azure AD Seamless Single Sign-On(Azure AD Se amless SSO)
D. □□□□ □□

Answer: D (LEAVE A REPLY)

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on- premises and cloud-based applications using the same passwords.
This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.
Note: Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on- premises directory in real time by using either Azure AD Connect or Azure AD Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.
Password writeback is supported in environments that use the following hybrid identity models:

Password hash synchronization
Pass-through authentication
Active Directory Federation Services
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback

NEW QUESTION: 105
□□□
□□ □□ □□ □□ □□□□ □□□ 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□□□□.

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

Answer:

Answer Area

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

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: 106

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

Name	Member of
User1	Group1
User2	Group2

□□ □□ □□□ □□□ □□□□□.

Name	Platform
Device1	Windows 10
Device2	Android

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

□ □ □□□ □□ □□□ □□: □

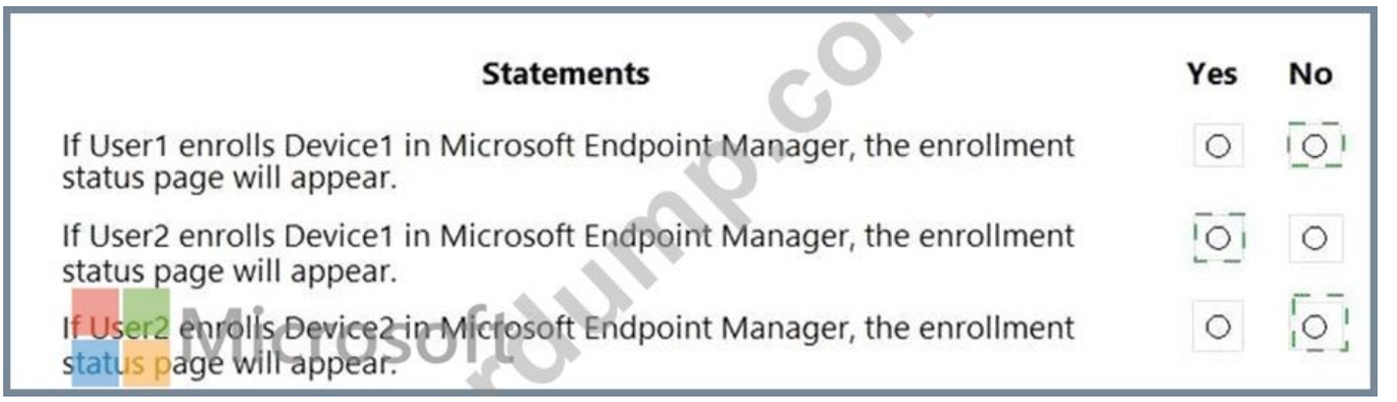
□□□□ □□ □□□ □□ □□□ □□□□□ □□: □

OOBE(Out-of-Box Experience)□ □□□□□□ □□□□ □□□ □□: □□□ □□: □□ 2 □□ □ □□□ □□ □□□ □□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

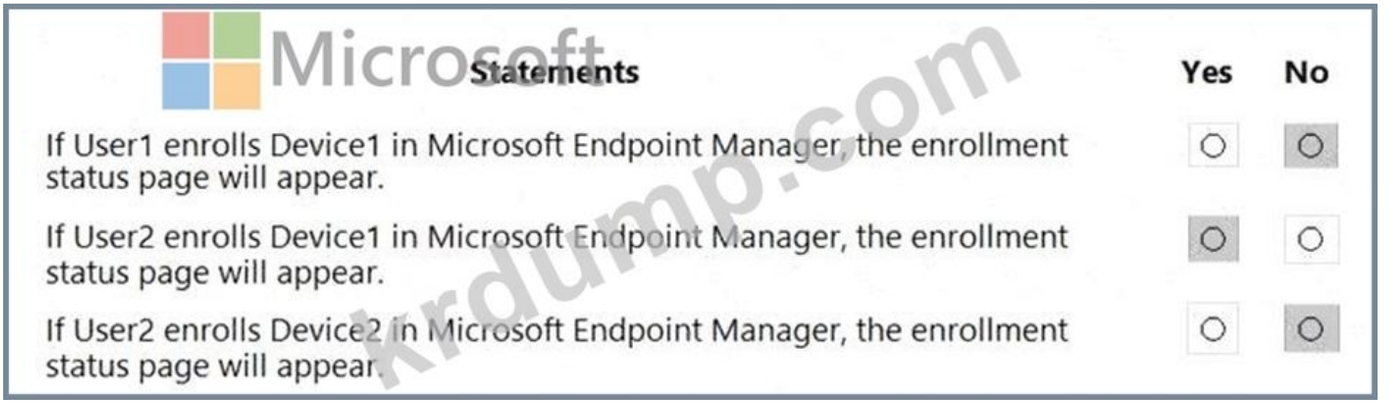
□□□□: □□ □□□ 1□□□□.

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

Answer:



Explanation:



Reference:

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

NEW QUESTION: 107

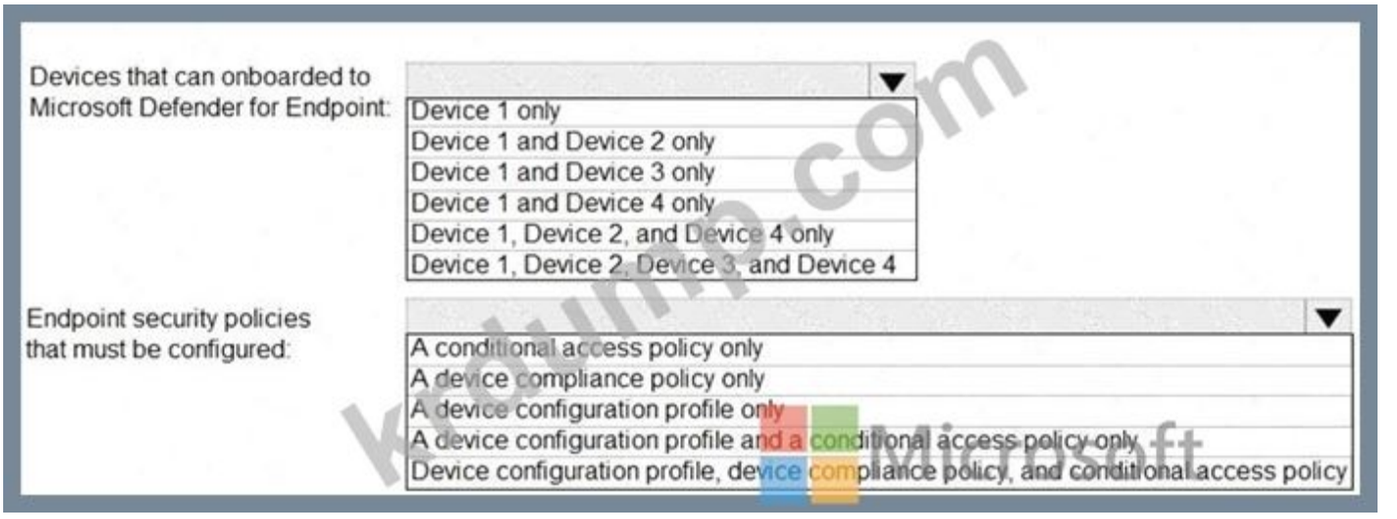
Endpoint□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□□ □□□□.

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

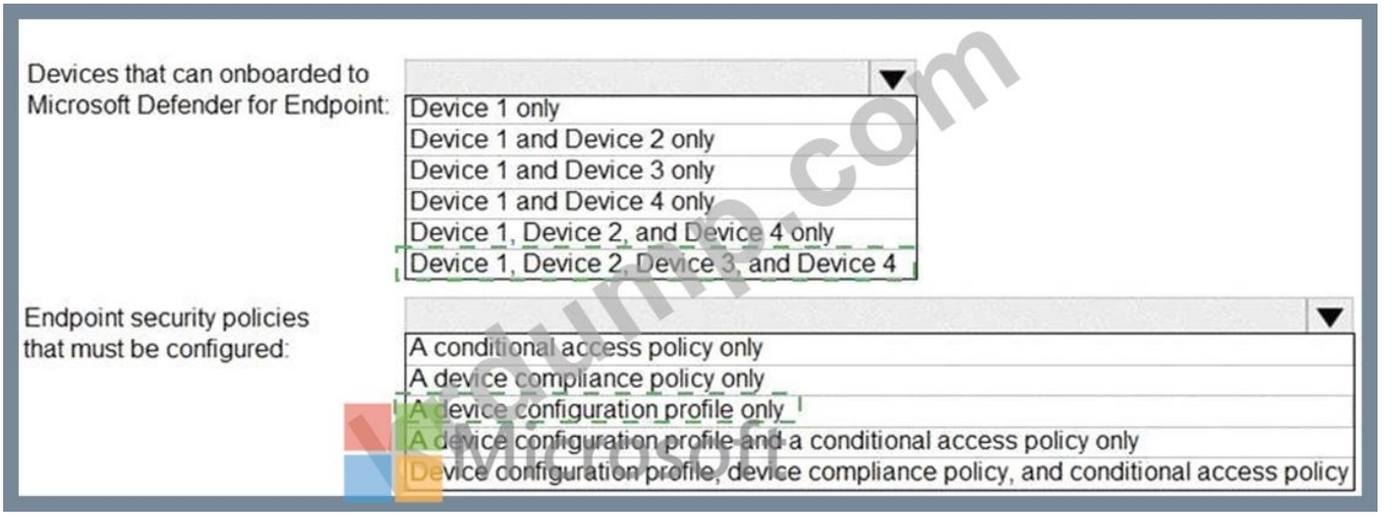
Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

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

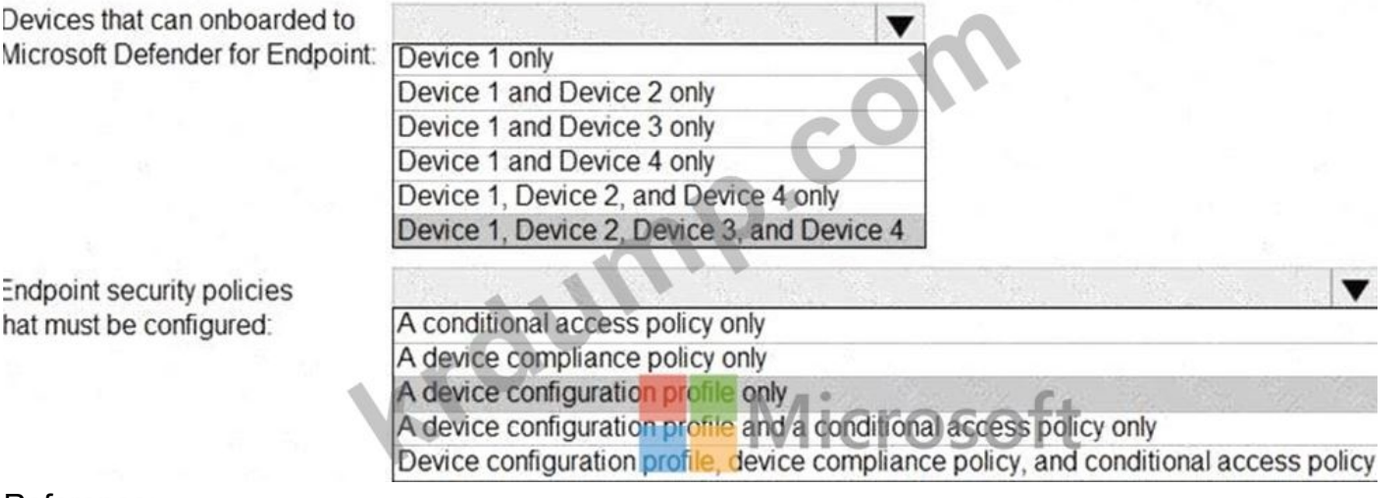
□□ □□□ Microsoft Defender for Endpoint□ □□□□ □ □□□, □□□ □□ Endpoint □□ □ □□ □□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?

view=o365-worldwide

NEW QUESTION: 108

Microsoft 365 E5 □□□ □□□□.

□□□□ Android □□ iOS □□□ □□□ □□□, Windows 11 □□ MacOS□ □□□□ □□□□ □ Microsoft 365 □□□□ □□□□□□.

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

□□ □□ □□□ □□□□ □□□?

A. □□□ □□

B. Microsoft Authenticator □

C. FID02 □□ □□ □

Answer: B (LEAVE A REPLY)

NEW QUESTION: 109

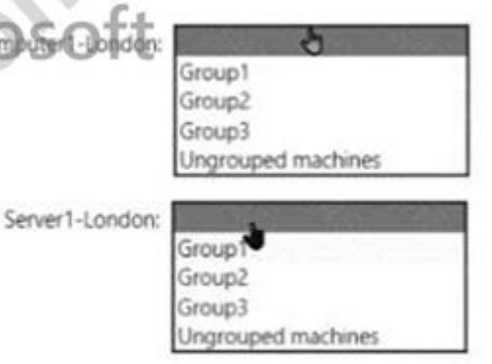
Endpoint□ Microsoft Defender□ □□□□□.

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

Name	Rank	Members
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 Area



Answer:

Explanation:

NEW QUESTION: 110

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

Azure AD □□□□ □□□□.

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

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

□□□□□ □□□ □□□□ □□□?

A. □□□□ □□□ Azure AD Connect □□□ □□ □□□ Azure AD Connect □□□ □□ □□

B. □□□□ □□□ Azure AD Connect □□□ □□ 3□□ Azure AD Connect □□□ □□ 1□

C. □□□□ □□□ Azure AD Connect □□□ □□ 6□□ Azure AD Connect □□□ □□ 3□

D. 3□□ Azure AD Connect □□□ □□□ □□□□ □□□ 3□□ Azure AD Connect □□□ □ □

Answer: (SHOW ANSWER)

Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect 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: 111

Microsoft 365 E5 □□□□ □□□□.

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

□□□□ Retention1□ □□□□□ □□ □□□□ □□□ □ □□□□.
□□ □□□□ Retention1□ □□□ □ □□□ □□□□ □□□.
□□□ □□ □□□?

A. □ □□ □□ □□□
B. □□ □□ □□ □□□ □□□□□!
C. □□ 1□ □□ □□ □□/□□ □□□ □□□□□.
D. □□ □□ CSV □□□□ □□□□ Retention1□ □□□□□.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 112

□□□ □□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□. □□□ □□ 1,000□□ Windows 10 □□□ □□□□.
10□□ □□□ □□□□□ □□ Microsoft Defender for Endpoint□ □□ □□(PoC) □□□ □□□ □□. □□□ □□□□ □□ Microsoft Defender for Endpoint □□ □□□□ □□□ □□□□□ □ □□□□.
□□ □□□ Microsoft Defender for Endpoint□ □□□□ □□□□□.
Microsoft Defender for Endpoint □□□□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?

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

Answer: B (LEAVE A REPLY)

Storage locations

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

* Machine information

- Stored in a Log Analytics workspace.

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

Reference:

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

NEW QUESTION: 113

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

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

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

Azure AD □□□□ □□□□□.

□□ □□□□ □□□□ Azure AD□ □□□□□□ □□□□□.

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

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

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

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

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

The question states that "all the user account synchronizations completed successfully". Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

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

NEW QUESTION: 114

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

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

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 115

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

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

□□ □□ □□(ASR) □□□ □□□ □□□□□. □□ □□□ ASR □□□ □□□□□?

A. Device 1, Device2, Device3□

B. Device3□

C. Device2□ Device3□

D. Device1, Device2, Devices □ Device4

Answer: C (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?

view=o365-worldwide#requirements

NEW QUESTION: 116

□□□

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

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

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

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

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

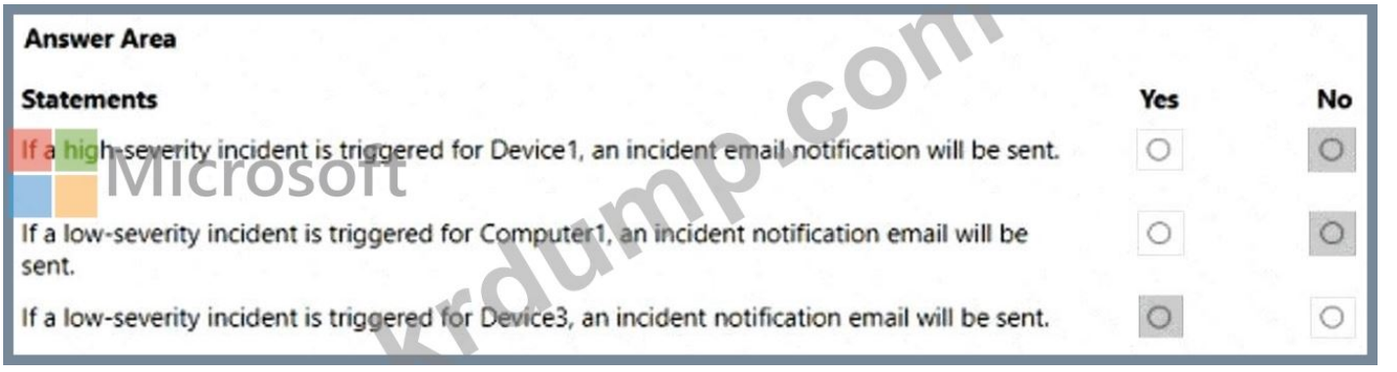
Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@contoso.com

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

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:



Box 1: No

Device1 is in Group2 as Name starts with Device and Tag contains Inventory.

However, the Group2 has alert severity low.

Box 2: No

Computer1 does not belong to either Group1 or Group2

Box 3: Yes

Device3 belongs to both Group1 and Group2.

Note: Understanding alert severity

Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.

The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

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

NEW QUESTION: 117

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

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

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

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

A. Device1□

B. Device1□ Device2□

C. Device1, Device2, Device3□

D. Device1, Device2, Device4□

E. Device1, Device2, Device3, Device4

Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 118

□□□□ contoso.com□□□ Microsoft Entra □□□□ Microsoft 365 □□□ □□□□. □□ □□ □□ Windows 10 □□□ □□□□ Microsoft 365 □□ □□□□□□. □□ □□□ □□ □□□ □ □□□.

contoso.com□ □□□□ □□ □□□□□ □□□ □□□□□ □□□.

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

A. Microsoft Authenticate □□ □□□□□.

B. Microsoft Entra □□□□□□ □□□□ □□□□□.

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

D. □□ □□□ contoso.com□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 119

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

Name	Type	Role assignments allowed	Security enabled
Group1	Security	No	Yes
Group2	Microsoft 365	Yes	No
Group3	Distribution	*Not applicable*	*Not applicable*

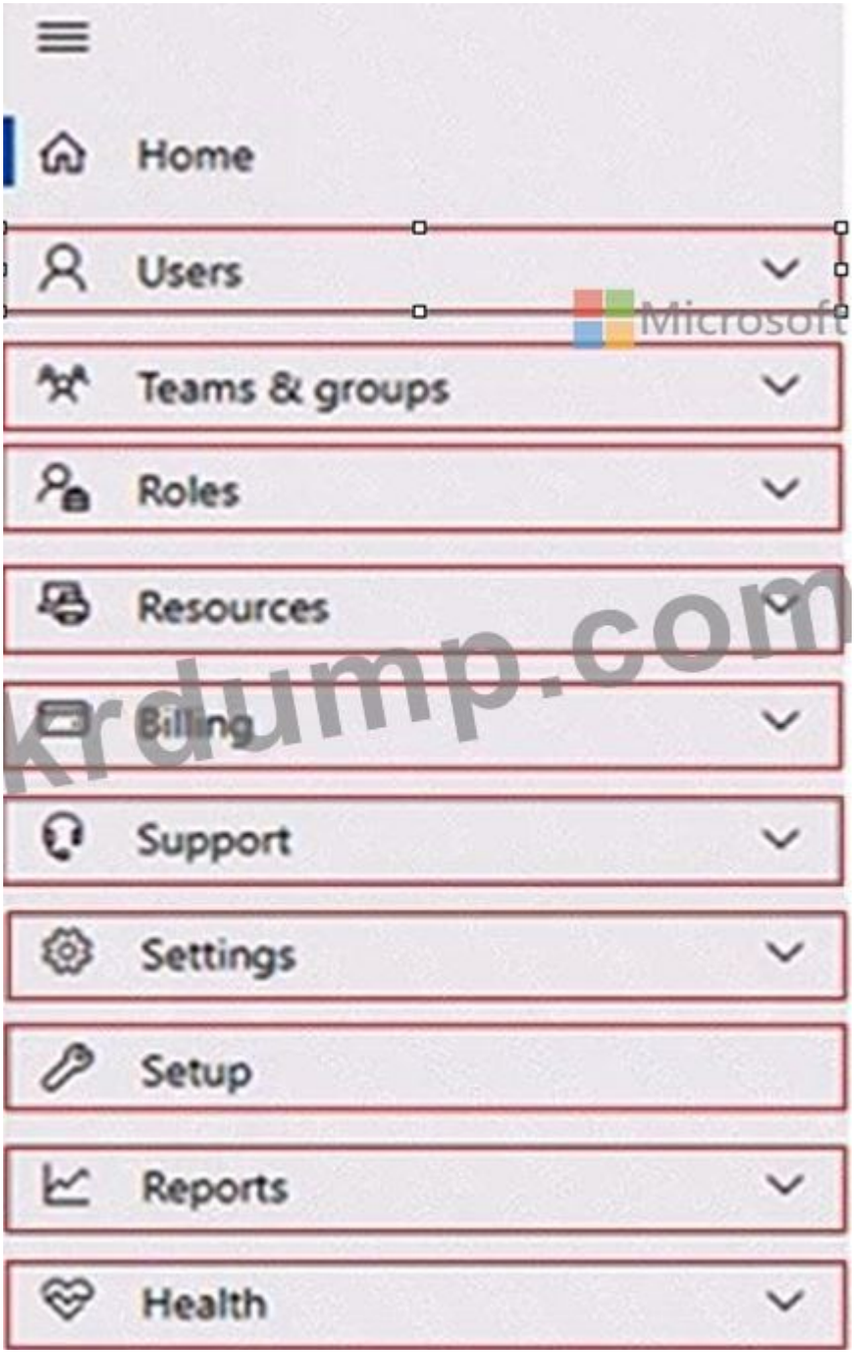
10□□ □□□ □□□□ □□□ □□ □□ □□□□□ □□□□ □ □□□□□ Microsoft 365 E5 □□□□□ □□□ □□□□□.

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

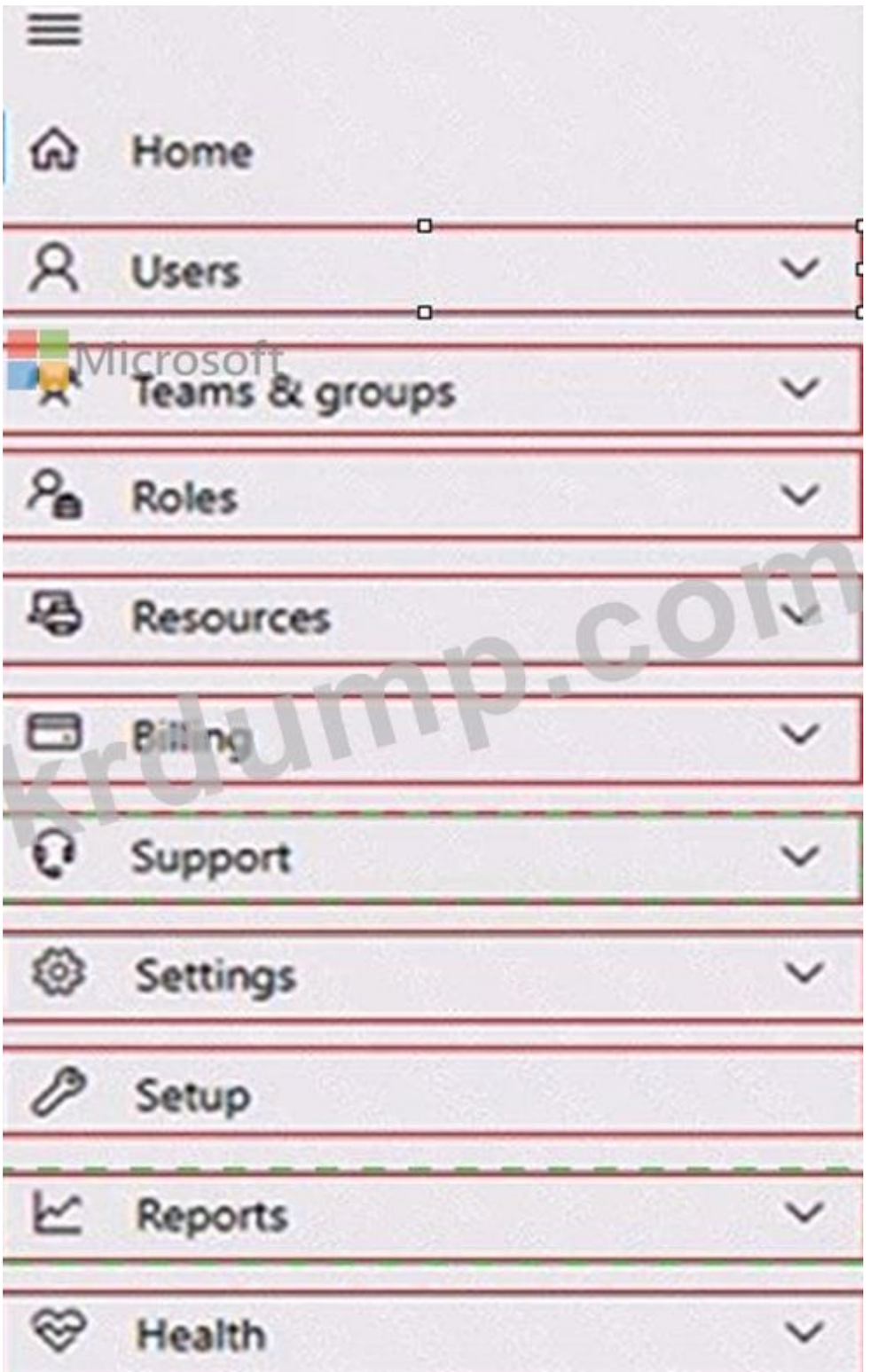
Answer:

Explanation:

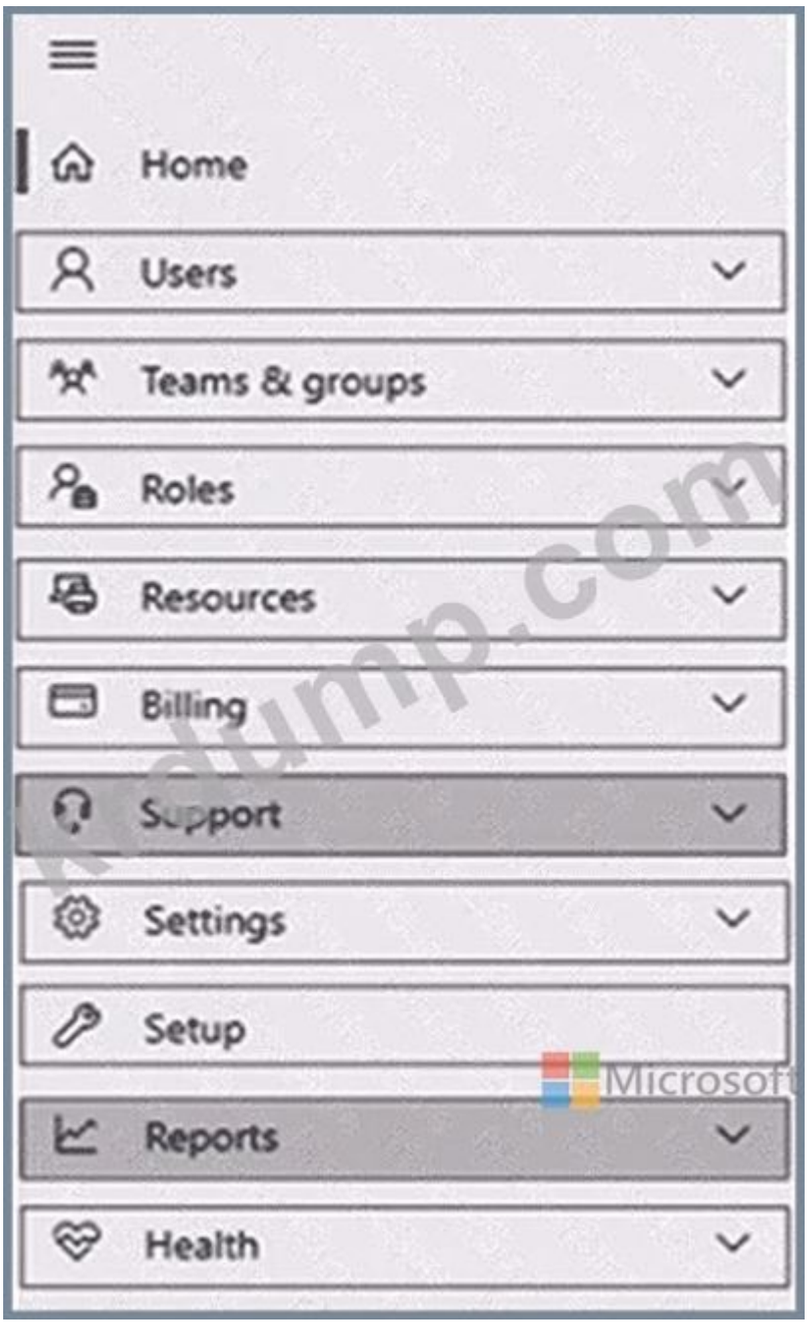
NEW QUESTION: 120
□□□
□□□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□□□ □□□.
□□□ □□ □□□ □□□□□.
Microsoft□ □□□ □□□ □□□ □□□□.
Microsoft 365 □□ □□□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □ □□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



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: 121
Microsoft 365 E5 □□□ □□□□.
□□□□ User1□□□ □□□ □□□□ □□□□.
□□□□ User1□ □□□□ □□□□□ □□ □□□ □□□□□.
* □□□ IP □□□□ Microsoft Exchange Online□ □□□□□□.
* □□□□ □□□□ Microsoft SharePoint Online□ □□□□□□.
* □□□□ □□□ □□□□ □□ □□□□ □□□ □□□ □□, □□ □□□□ □□□□ SharePoint Online□ □□□□□□. Azure AD Identity Protection□ User1□ □□ □□ □□□ □ □□ □□□ □□□□□?
A. □□ IP □□ □ □□□□ □□ □□□ □□□
B. □□ IP □□, □□□ □□ □ □□□□ □□ □□□ □□
C. □□ IP □□□
D. □□ IP □□ □ □□□ □□
E. □□□□ □□ □□□ □□ □ □□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 122
□□: □ □□□□ □□□ □□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□ □ □□□ □□□.
□□□ □□ □ □ □□□ □□□□ □□□ □□□ □ □□□□. □□□ □□ □□□ □ □□ □□ □□□ □□□□ □□ □□ □□□□.
□ □□□ □□□ □□ □□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft 365 E5 □□□ □□ Office 365□ Microsoft Defender□ □□□□ □□□□.
□□, □□, □□□□□□ □□□□ □□ □□ □□ □□ □□ □□□□ □□□□ □□ □□□ □□ □□ □□□.
□□□: □□□ □□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □

B. □□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 123

Microsoft 365 E5 □□□□ □□□□.

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

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

□□□□: □□ □□□ 1□□□□.

Answer:

Answer Area

Explanation:

NEW QUESTION: 124

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

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

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

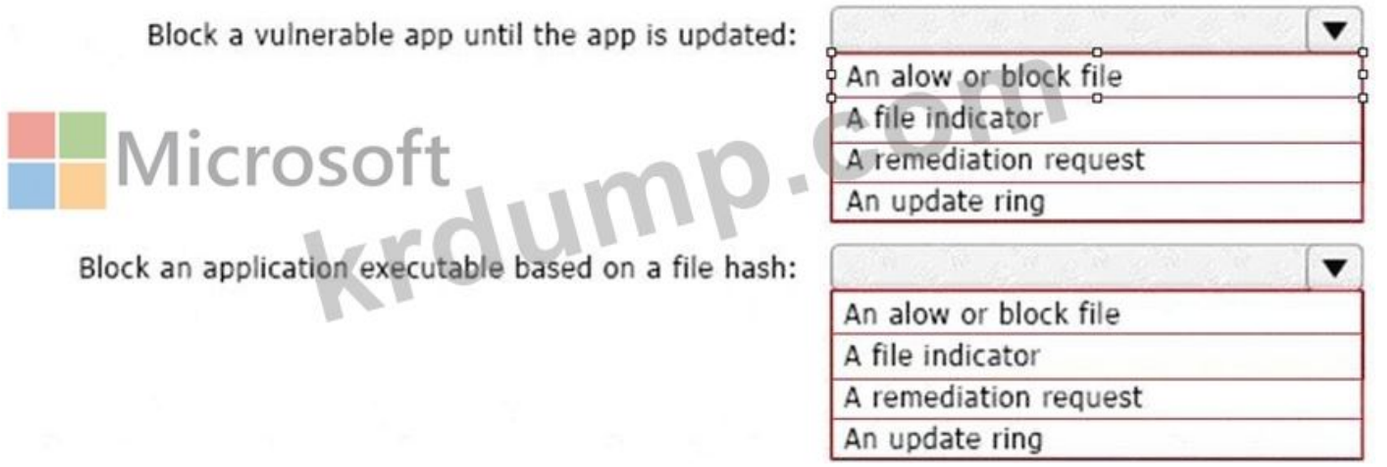
Microsoft 365 E5 □□□ □□ Office 365□ Microsoft Defender□ □□□□ □□□□.

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

□□□: □□□ □□ □□ □□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)

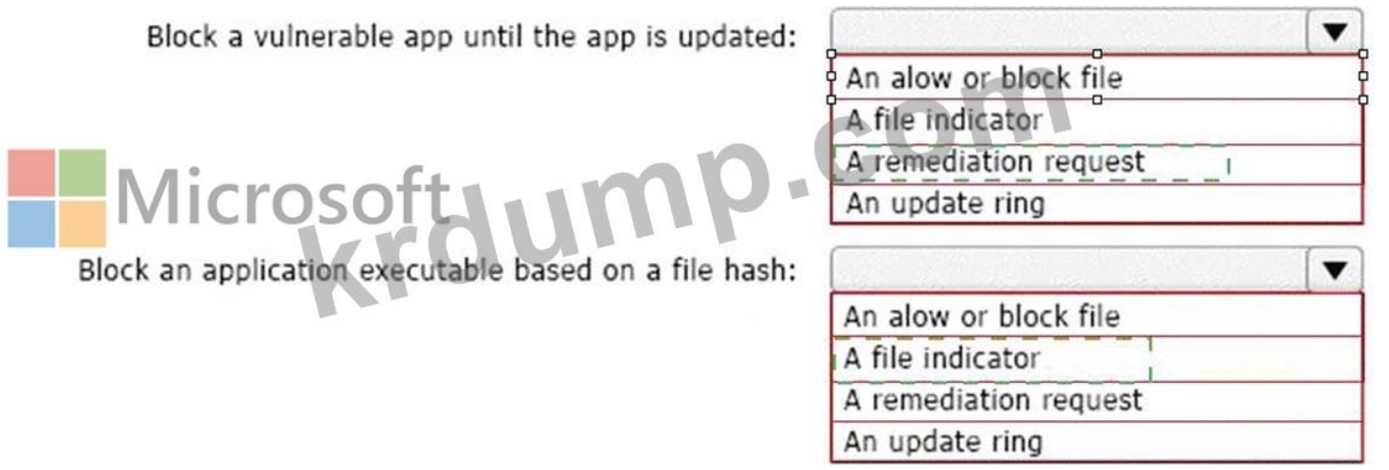
NEW QUESTION: 125
□□□
Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□ Windows 11 □□□ Microsoft Defender for Endpoint□ □□□□□.
□□ □□ □□□ □□□□□ Defender for Endpoint□ □□□□ □□□.
* □□ □□□□□ □□□ □□□ □□ □□□□□.
* □□ □□□ □□□□ □□□□□□ □□ □□□ □□□□□.
□□□□ □□□ □□□ □□□□□ □□□.
□ □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□ □.
□□□□: □□ □□□ 1□□□□.

Answer Area

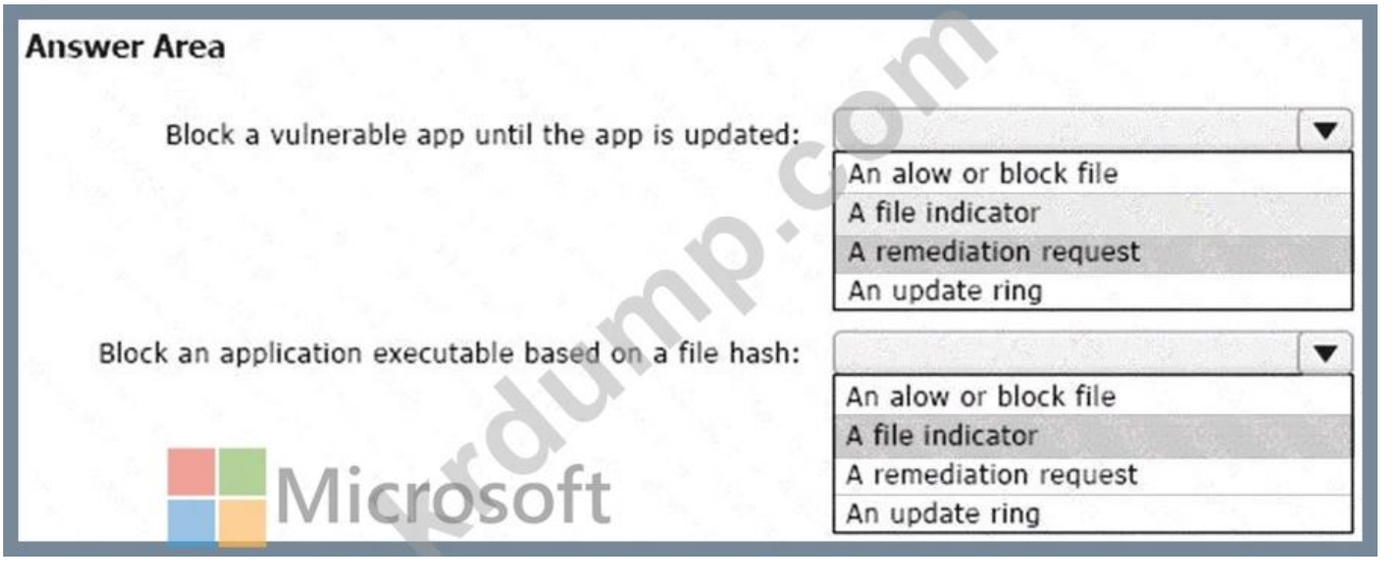


Answer:

Answer Area



Explanation:



Box 1: A remediation request

Block a vulnerable app until the app is updated.

Block vulnerable applications

How to block vulnerable applications

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

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

Select Request remediation.

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

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

Pick a Remediation due date and select Next.

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

Review the selections you made and Submit request. On the final page you can choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.
Box 2: A file indicator
Block an application executable based on a file hash.
While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.
The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-block-vuln- apps

NEW QUESTION: 126
□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.

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

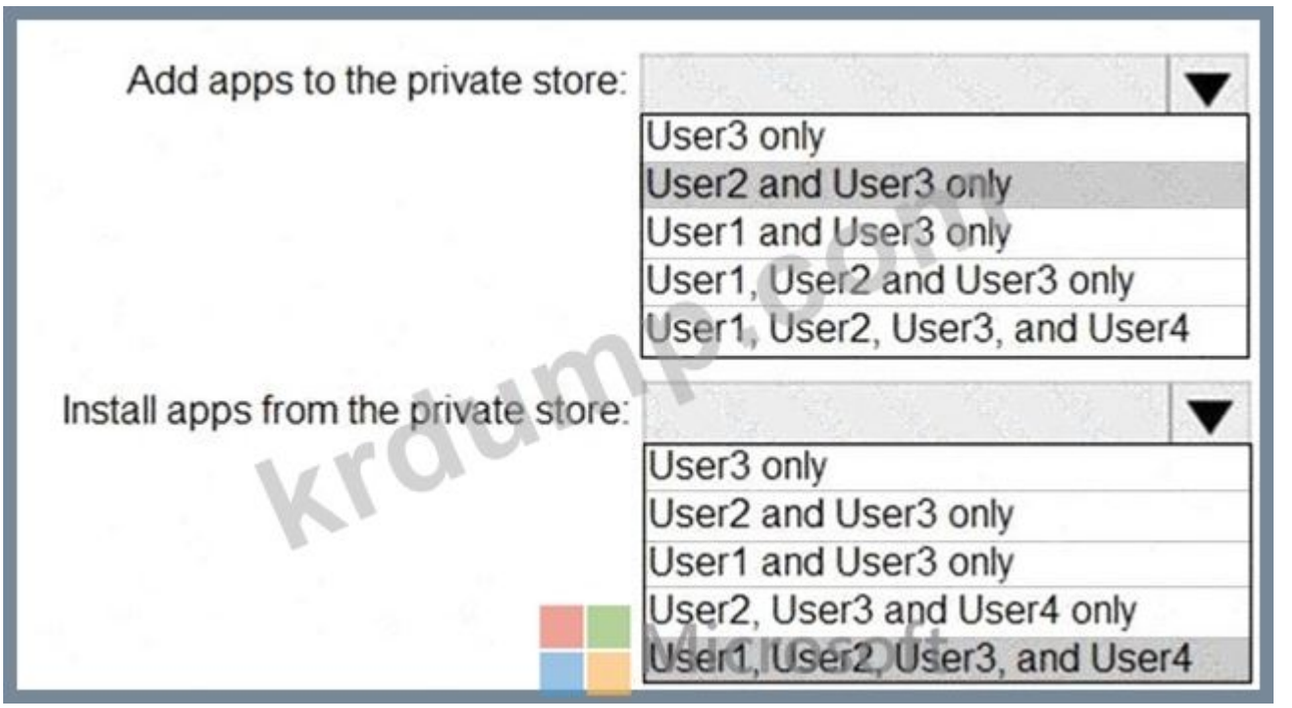
□□ □□ □□□ □□ □□□□□ Microsoft Store for Business □□□ □□□□□.

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

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

Answer:

Explanation:



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

NEW QUESTION: 127
Microsoft 365 □□□ □□□□.
□□ □□ □□□ □□ □□□□.

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

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

Answer:

Explanation:

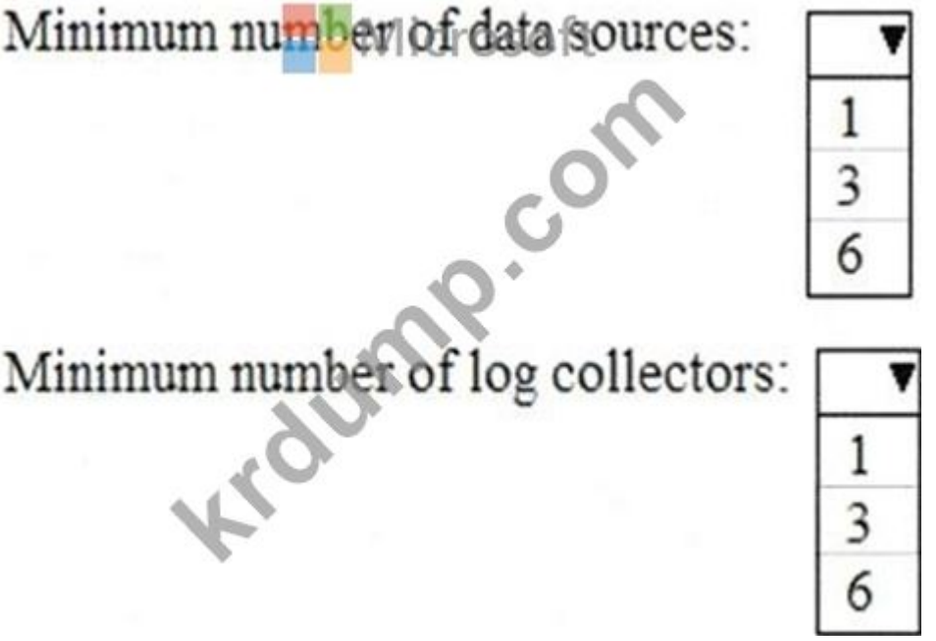
Answer Area

NEW QUESTION: 128

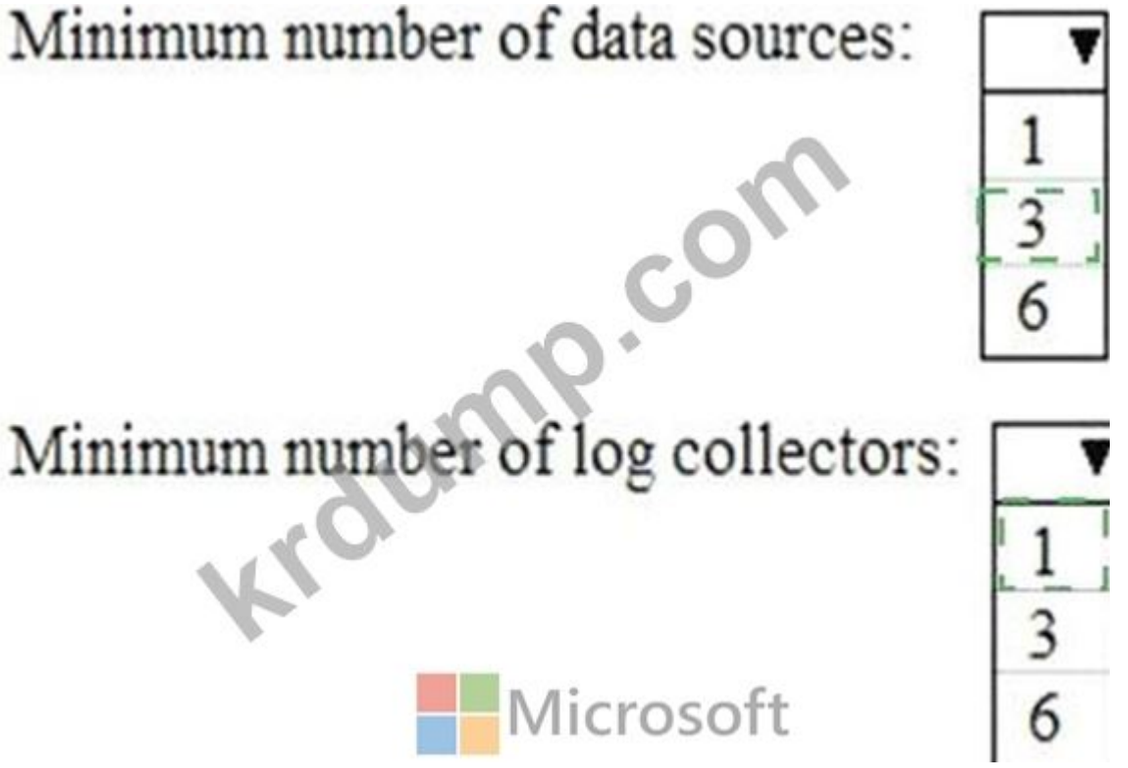
□□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□.

Microsoft Cloud App Security□□ □□□□ □□ □□ □□□ □□ □ □□ □□□ □□ □□□□ □? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

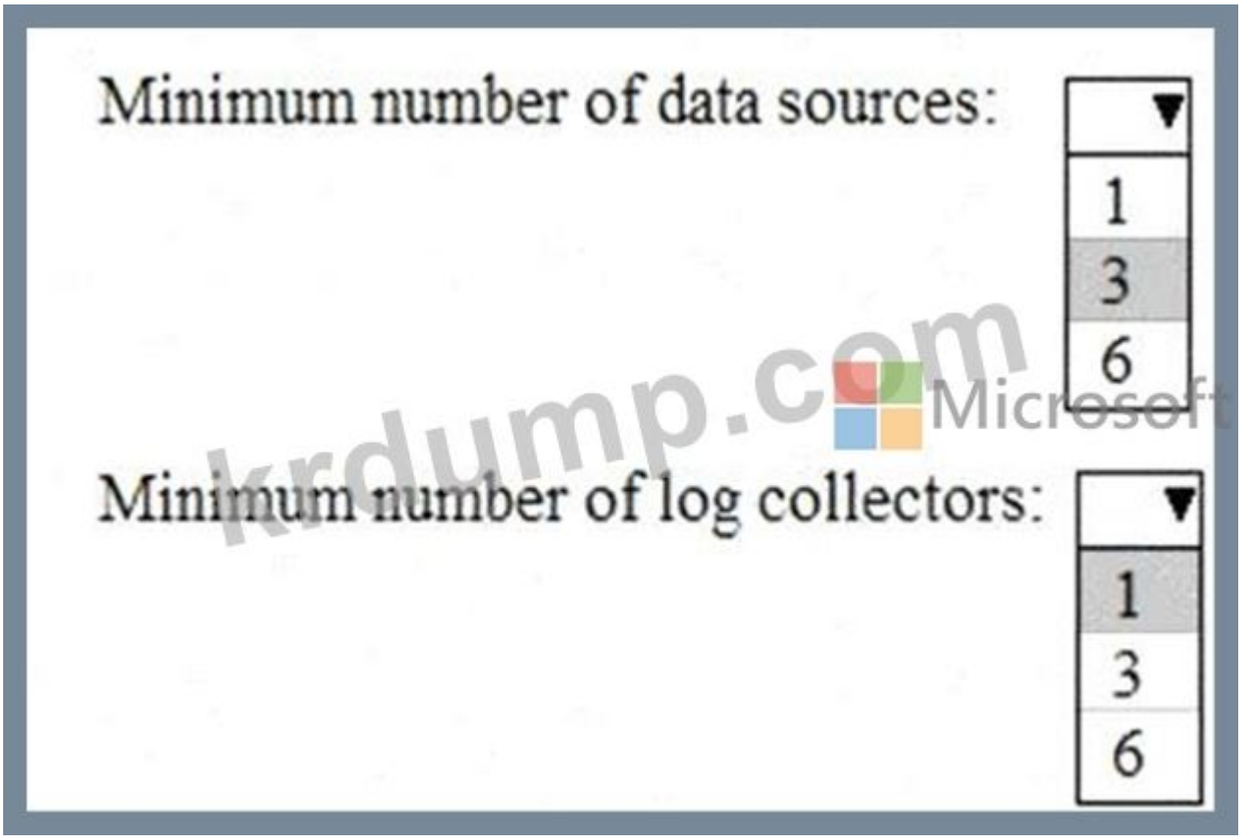
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



References:

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

Topic 3, Litware Inc.

Case Study

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. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
General Overviews
Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.
Environment
Existing Environment
The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.

Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.
Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	MacOS
Device4	iOS
Device5	Android

Litware.com contains the security groups shown in the following table.

Name	Members
UserGroup1	All the users in the Montreal office
UserGroup2	All the users in the Seattle office
DeviceGroup1	All the devices in the Montreal office
DeviceGroup2	All the devices in the Seattle office

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

The verified domain is linked to an Azure Active Directory (Azure AD) tenant named litware.com.

Audit log search is turned on for the litware.com tenant.

Problem Statements

Litware identifies the following issues:

Users open email attachments that contain malicious content.

Devices without an assigned compliance policy show a status of Compliant.

User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.

Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

Requirements

Planned Changes

Litware plans to implement the following changes:

Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.

Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.

Implement data loss prevention (DLP) policies to protect confidential information.

Grant User2 permissions to review the audit logs of he litware.com tenant.

Deploy new devices to the Seattle office as shown in the following table.

Name	Platform
Device6	Windows 10
Device7	Windows 10
Device8	iOS
Device9	Android
Device10	Android

Implement a notification system for when DLP policies are triggered.
Configure a Safe Attachments policy for the litware.com tenant.
Technical Requirements
Litware identifies the following technical requirements:
Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Azure AD.
Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
User2 must be granted the permissions to review audit logs for the following activities:
- Admin activities in Microsoft Exchange Online
- Admin activities in SharePoint Online
- Admin activities in Azure AD
Users must be able to apply sensitivity labels to documents by using Office for the web.
Windows Autopilot must be used for device provisioning, whenever possible.
A DLP policy must be created to meet the following requirements:
- Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
- Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
The principle of least privilege must be used.

NEW QUESTION: 129
□□ □□ □□(MFA) □□□ □□□□ Microsoft 365 □□□ □□□□.
Microsoft Secure Score□ □□□□ □□ □□ □□□□ □□ □□ □□ □□□ □□□□□ □□□ □□ □□□ □□ □□□ □□□□ □□ □□□ □□ □□ □□□□□.

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

A. □□ □□□ □□□□□.

B. □□□ □□□□ □□□□□.

C. □□□□□ □□□ □□□□□.

D. Microsoft Defender for Identity □□□ □□□□□.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 130

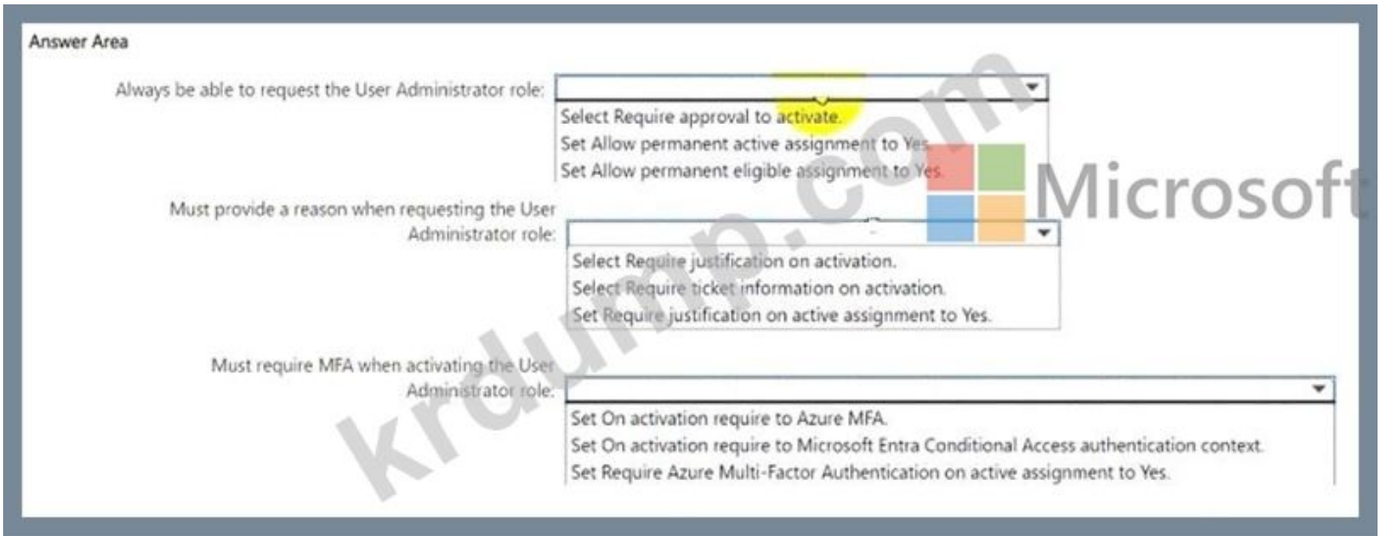
Microsoft 365 E5 □□□ □□□□.

Microsoft Entr a□□ □□□ □□□ □□□ □□ Privileged Identity Management(PIM)□ □□□□ □□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.

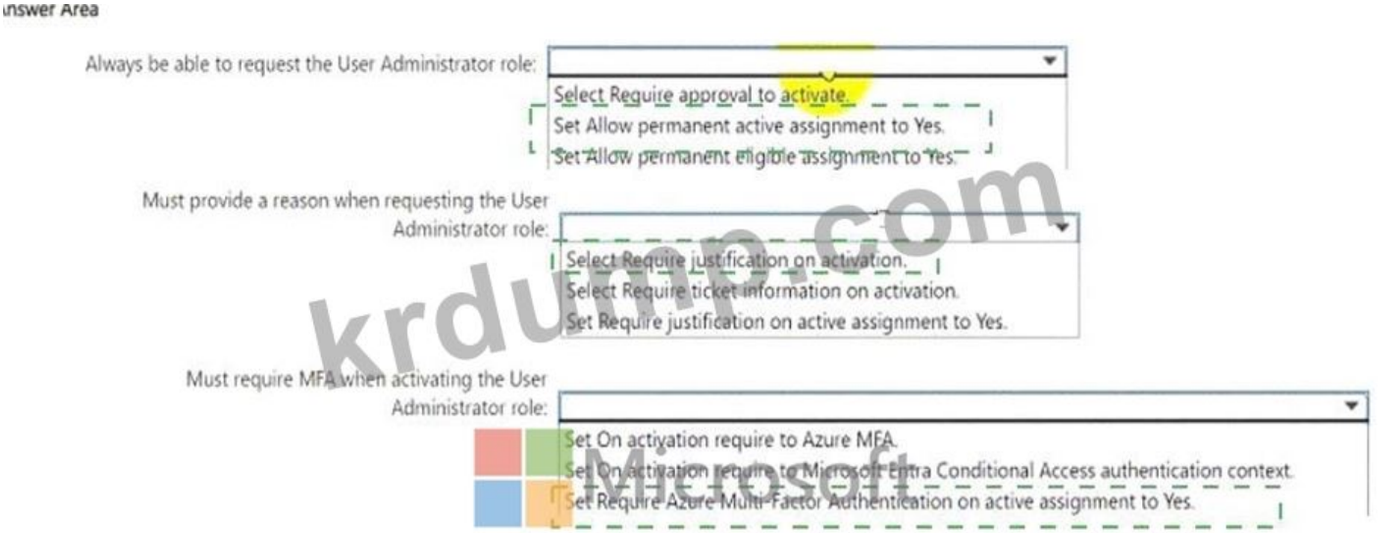
* □□ □□□ □□□ □□□ □□□ □ □□□□.

* □□□ □□□ □□□ □□□ □ □□□ □□□□ □□□.

* □□□ □□□ □□□ □□□□ □ □□ □□ □□(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: 131
□□ □□ □□ □□ □□□□ □□□□ □□□ Microsoft Store for Business□ □□□ Microsoft 365 □□□□ □□□□.

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

□□ □□□□ Windows 10 Enterprise □□□ □□□ □□□□.
□□ □□□□□ Microsoft Store for Business□ □□ □ □□□ □□□ □□□□□.

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

□□□□: □□ □□□ 1□□□□.

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

Answer:

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

Explanation:

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

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

NEW QUESTION: 132

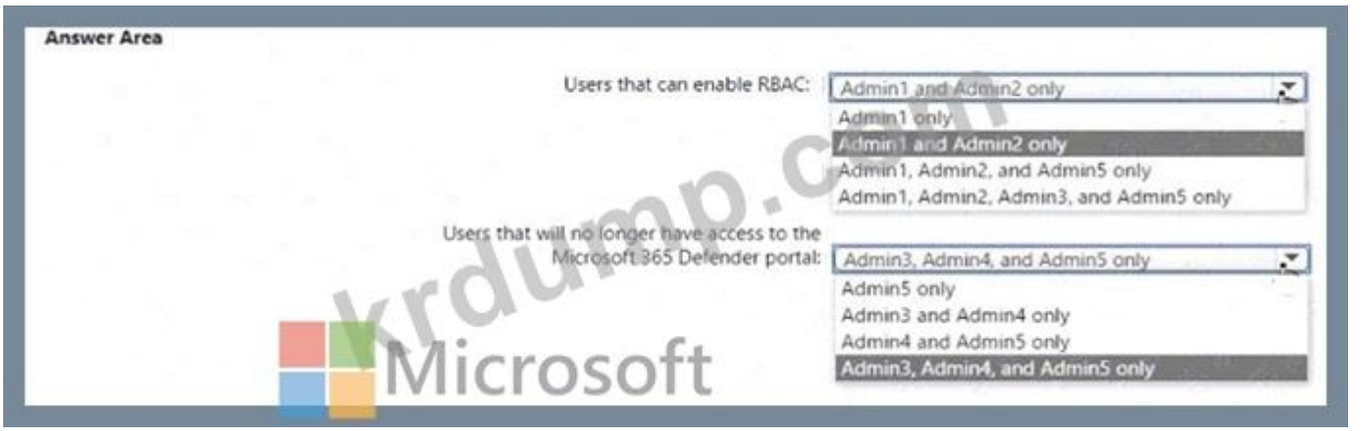
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

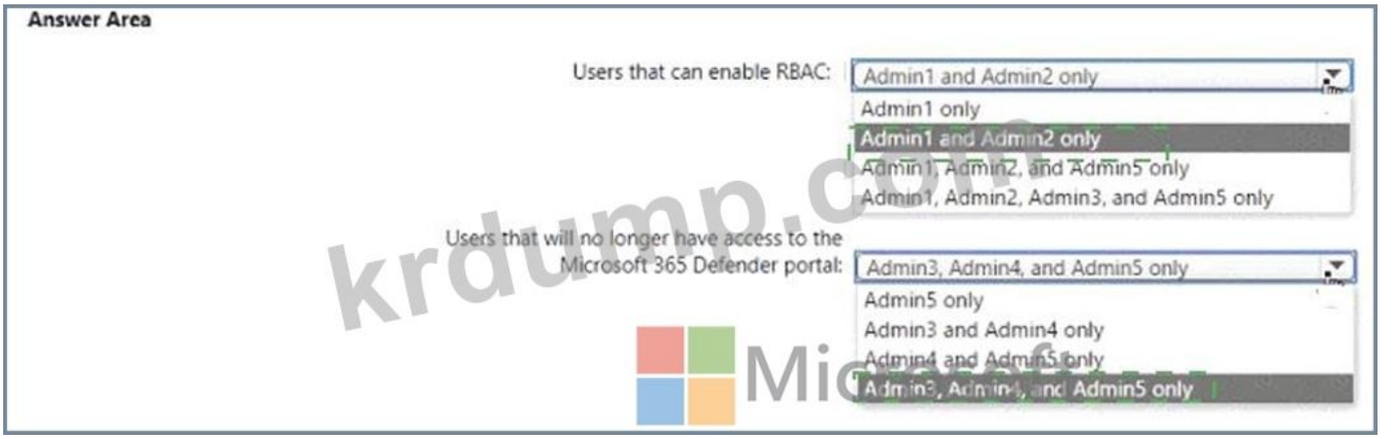
Microsoft Defender for Endpoint □□□ □□□□□□.
Microsoft 365 Defender □□□ □□ □□□□ □□□□□ □□ □□ □□□ □□(RBAQ)□ □□ □□□ □□□.

□□ □□□□ RBAC□ □□□□ □ □□, □□ □□□□ RBAC□ □□□□ □ Microsoft 365 Defender □□□ □ □□ □□□□ □ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □ □□□□.

□□ □□: □□□ □□□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 133

□□ □□□□ Defender for ID □□□ □□□□ □□□?

A. □□1

B. □□2

C. □□3

D. □□4

E. □□5

Answer: (SHOW ANSWER)

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: 134

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

Name	Type
User1	User
Group1	Microsoft 365 group
Group2	Mail-enabled security group
Group3	Distribution group

Shared1□□□ □□□ □□ □□□□ □□□□.

Shared1□ □□ ID□ □□□ □□□ □ □□□?

A. User1□ Group3□

B. User1, Group2, Group3□ □□

C. User1□ Group1□

D. User1□

E. User1□ Group2□

Answer: E (LEAVE A REPLY)

NEW QUESTION: 135

Microsoft 365 E5 □□□ □□□□.

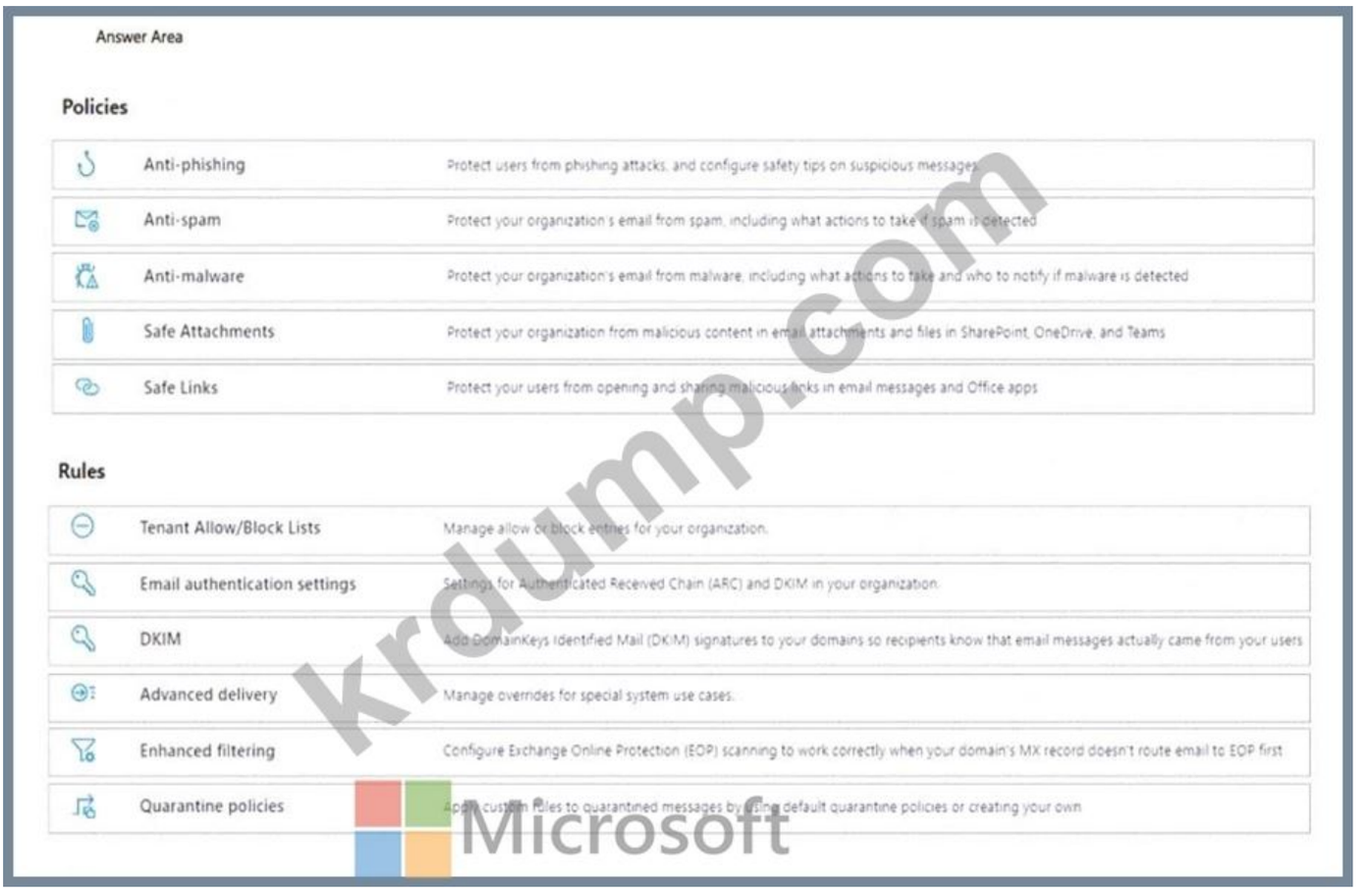
□□ □□ □□□ □□□□□ Microsoft 365□ □□ □□ □□□ □□□□ □□□.

* User 1□□□ □□□□ □□□ 30□□ □□ □□□ □□□□ □□□ □□□□ □□□□□.

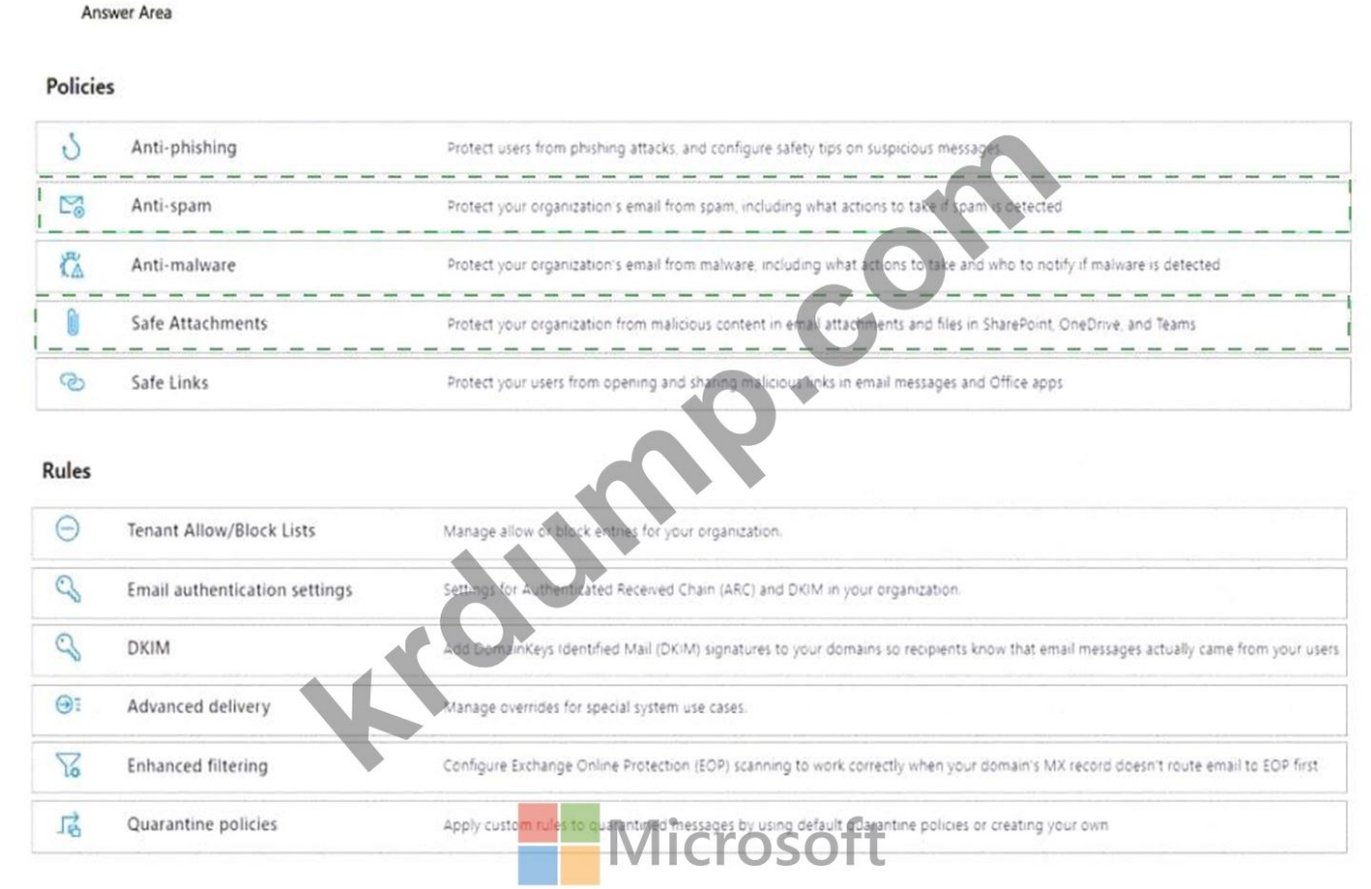
* □□ □□□ □□□□ □□ □□□ □□□ □□□□□.

Microsoft Defender for Office 365□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□□□ □ □ □□□□ □□□ □□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.



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: 136
Admin1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□□ Branch□□ □□□ □□□ □□□ □□□□□□!
Admin1□□ Branch1 □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Admin1□ □□□ □□□ Branch1□ □□□ □□□□ □□□ □ □□□ □□□.
* Admin1□ Branch1□ □□□□ □□□□ □□□□ □□□, □□□ □□□□ □□, □□□ □□ □□□ □□□□ □□□.
Branch1 □□□□ □□□ □□□□ □□, Admin1□□□ □□ □□□ □□□□ □□□? □□ □□ □□ □□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 137
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □ □□ □□ □□□□ □□□ □ □□□, □□ □□□ □□ □□ □ □□□□ □□□□.
□□□□□ Active Directory □□□□ □□□□ □□□□.
Azure AD □□□□ □□□□□.
□□ □□□□ □□□□ Azure AD□ □□□□□□ □□□□□.
□□ □□(OU)□ 10□ □□□ □□□ Azure AD□ □□□□□ □□ □□ □□□□□□. □□ □□ □□□ □□□ □□□□□ □□□□□□□□.
Azure AD Connect Health□ □□□□ □□ □□□ □□ □□□□ □□□□□ □□□□□□ □□ □□□.
10□□ □□□ □□□ Azure AD□ □□□□□□□ □□□□ □□□.
□□ □□: Azure AD Connect□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: B (LEAVE A REPLY)

NEW QUESTION: 138
Group1□□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□. □ □□□ □□□□ □□ Microsoft Defender□ □□□□□.
□□□□ □□□ □□□□□.
Group1 □□□□ □□ IT □□□ □□ □□ □□□ □□□□ □□□ □□ □□□□ □□ □ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?

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

NEW QUESTION: 139
Microsoft 365 E5 □□□□ □□□□.
□□□□□ Microsoft Office 365 □□ □□□ □□□□ □□□ □□□□□ □□□ □□□□ □□ □.
□□□ □□□□□ □□□ □□□□ □□□?
A. □□□□ □ □□□ Microsoft Defender
B. Microsoft Apps □□ □□
C. Microsoft 365 □□ □□
D. Microsoft Purview □□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 140
Site1□□□ Microsoft SharePoint Online □□□□ □□□ Microsoft 365 □□□ □□□□. Site1□ □ □□ □□ □□□ □□□□.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	2
File4.bmp	3
File5.doc	3

Site1 □□□□□□ □□ □□ □□□ □□□ □□□□□.

Name	Role
User1	Owner
User2	Visitor

□□ □□ □□□ □□□ Policy1□□□ □□□ □□□ □□ □□(DLP) □□□ □□□□.

□□'□ □□□ □□□ □ □□□1□ □□□2□□ □□□□ □□□ □□ □□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 141

Microsoft 365 E5 □□□ □□□□.
□□□□ Microsoft Defender for Endpoint□ □□□ □□□□ □□□□ □□□□ □□□□.
Defender for Endpoint□ Microsoft Defender for Cloud Apps□ □□□ □□□□□ □□□□ □□ □□.
Cloud Discovery□ App1□□□ □□□ □ □□ □□□□□□.
Microsoft Edge□□ App1□ □□□□ □□ □□□□ □□□. □□□□ □□□ □□□ □ □□□ □□□.
□□ □□□ □ □□□ □□□□ □□, Defender for Endpoint□ Defender for Cloud□ □□□□ □ □ □□□ □□□□ □□□?

Answer:

Explanation:

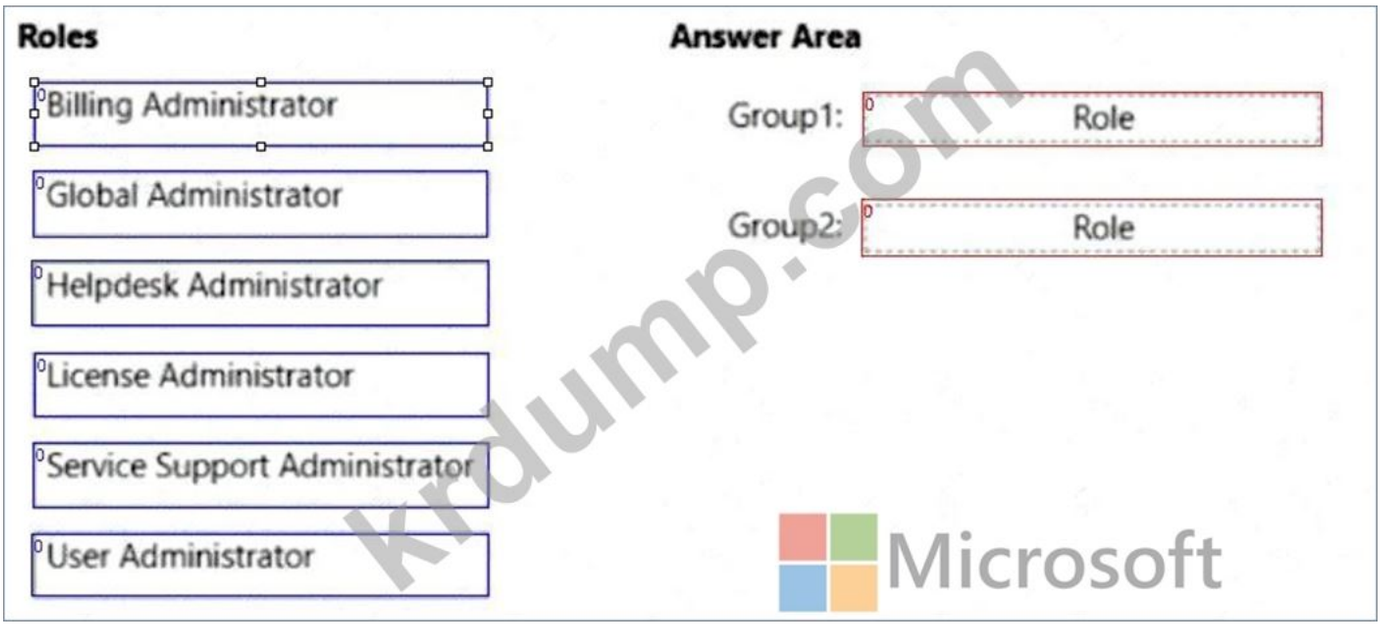
NEW QUESTION: 142
Microsoft 365 □□□ □□□□.
□□ □□ □□□ □□□□ □□ □□ □□□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□□ □□□□ □□□□□.
□□□ □□□□ □□□□ Microsoft SharePoint □□ □□□ □□□□□ □□□ □□□□ □□ □ □□□ □□□□□. □□ □ □□ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□ □□□.
□□□□: □□ □□□ 1□□□□.

A. □□ □□□ □□□
B. □□□ □□ □□
C. □□□ □□ □□
D. □□□ □□ □□
E. □□□ □□ □□(DLP) □□
Answer: A,E (LEAVE A REPLY)
A: Classifiers
This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.
Where you can use classifiers
Classifiers are available to use as a condition for:
Office auto-labeling with sensitivity labels
Auto-apply retention label policy based on a condition
Communication compliance
Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.
Data loss prevention
E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp

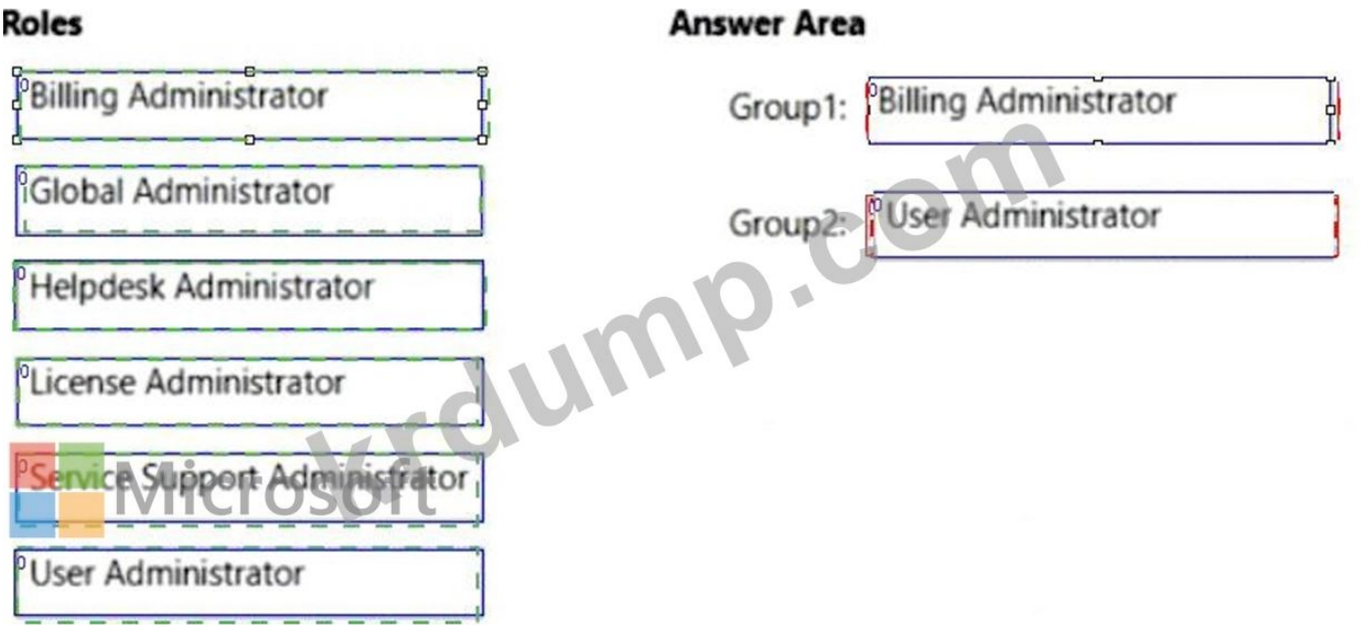
NEW QUESTION: 143
□□□ □ □□
Group1□ Group2□□ □ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.
□ □□□ □□ □□ □□□ □□□ □□□ □ □□□ □□□□ □□□.

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

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



Answer:



Explanation:

Box 1: Billing admin
manage service request
Purchase new services
Etc.
Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.
Box 2: User admin
User admin
Assign the User admin role to users who need to do the following for all users:
- Add users and groups
- Assign licenses
- Manage most users properties
- Create and manage user views
- Update password expiration policies
- Manage service requests
- Monitor service health
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles

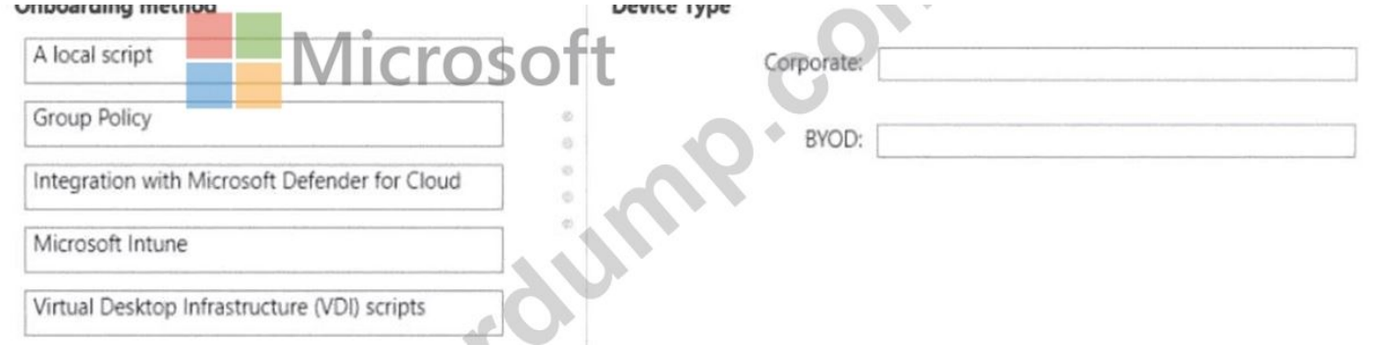
NEW QUESTION: 144
□□ □□ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

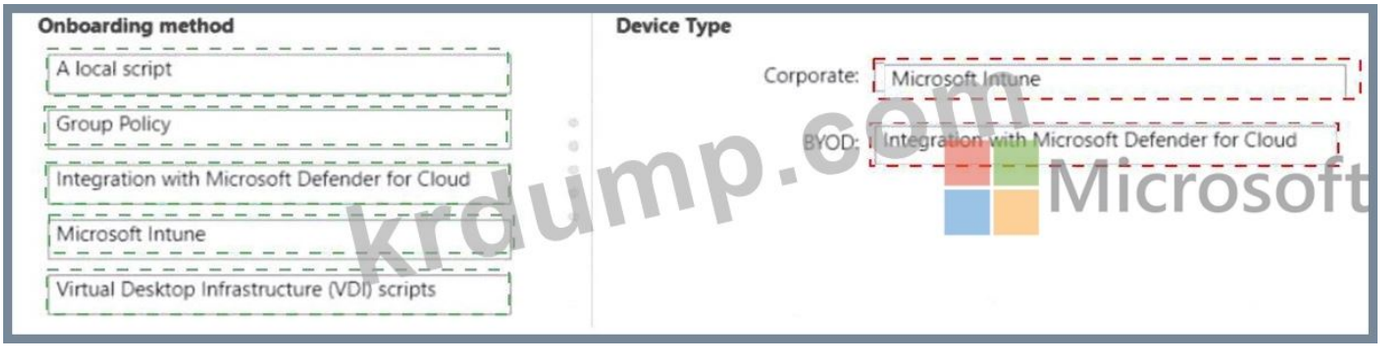
Microsoft Defender for Endpoint□ □□□ □□□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.

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

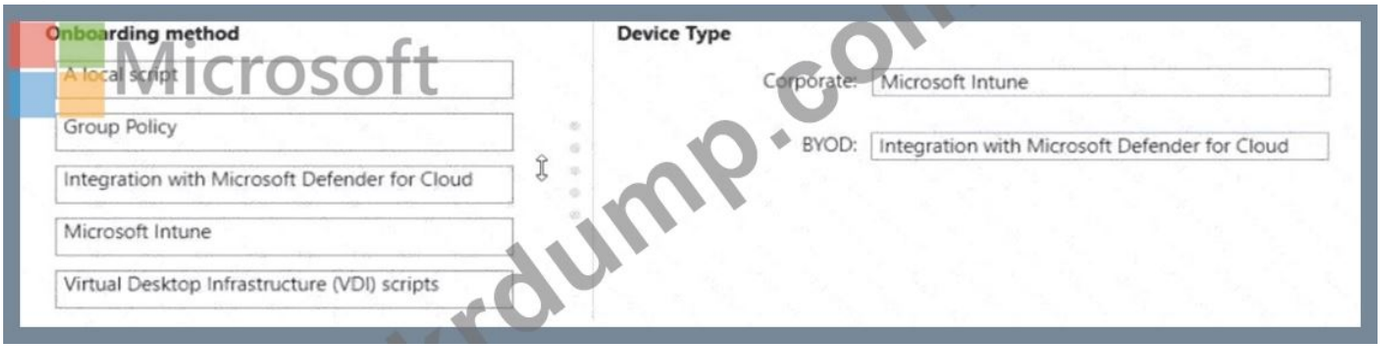
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



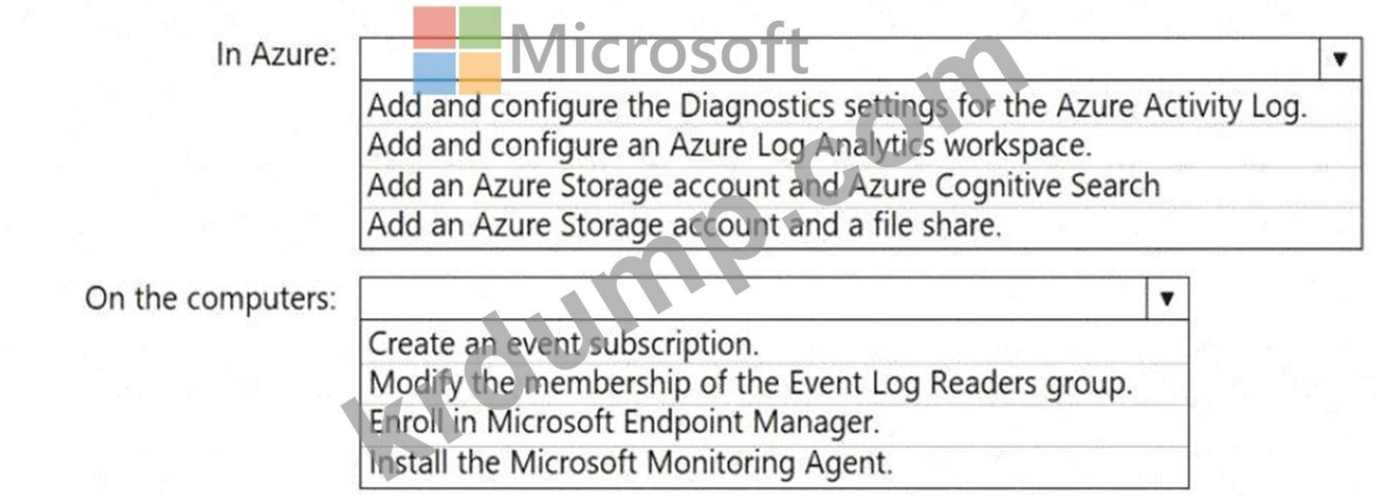
NEW QUESTION: 145

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

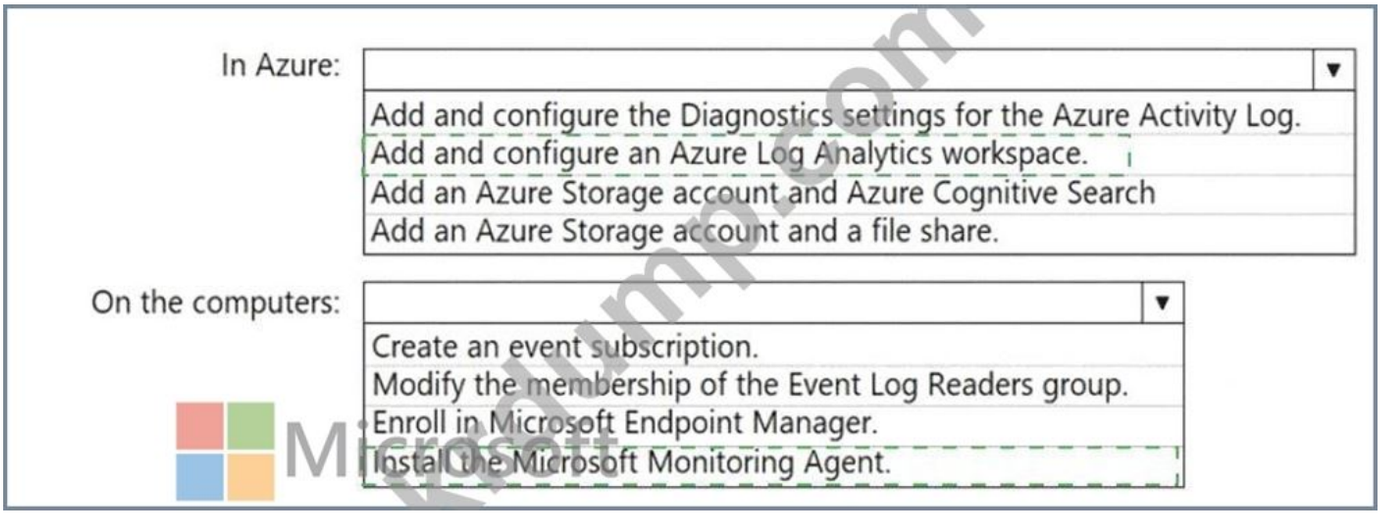
□□□□ □□□ □□ □□□□ □□□□ □□□□□□ □□□.

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

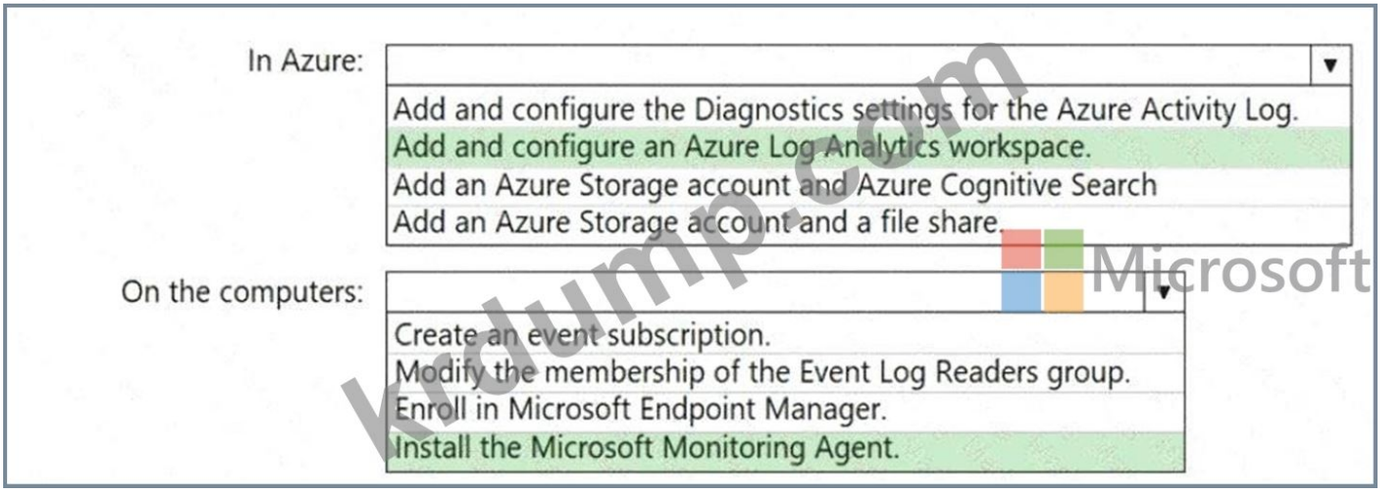
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Reference:

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

NEW QUESTION: 146

Microsoft J65 E5 □□□ □□□□.

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

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

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

NEW QUESTION: 147
Microsoft Defender for Endpoint□ □□□□ Microsoft 365 E5 □□□ □□□□.
Endpoint□ Microsoft Defender□□ □□ □□ □□ □□ □□ □□□ □□□.
□□□□ File1.exe□□ □□□ □□□□□□ □□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□ □□ □□□
C. □□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 148
Microsoft 365 □□□ □□□□.
□□□ □□ onmicrosoft.com □□□□ □□□□ □□□. □□ □□□□ □□□□ □□□ □□□ □□□ □ □□□ □□□.
□□□ □□□ □ □□ onmicrosoft.com □□□□ □□ □□ □□□□□?
A. 1
B. 2
C. 5
D. 10
Answer: C (LEAVE A REPLY)
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: 149
□□ □□ □□□ □□□ Microsoft Endpoint Manager□ □□□ □□□ 3□ □□□□.

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

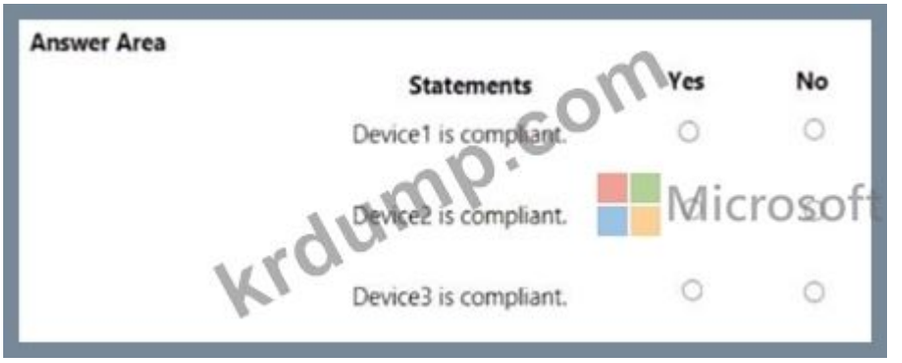
Endpoint Manager□ □□ □□ □□□ □□ □□ □□ □□□□□.

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

□□ □□ □□□ □□□ □□ □□ □□□□ □□□□.

Name	Assigned to
Policy1	Group3
Policy2	Group2

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



Answer:

Explanation:

NEW QUESTION: 150

□□□

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

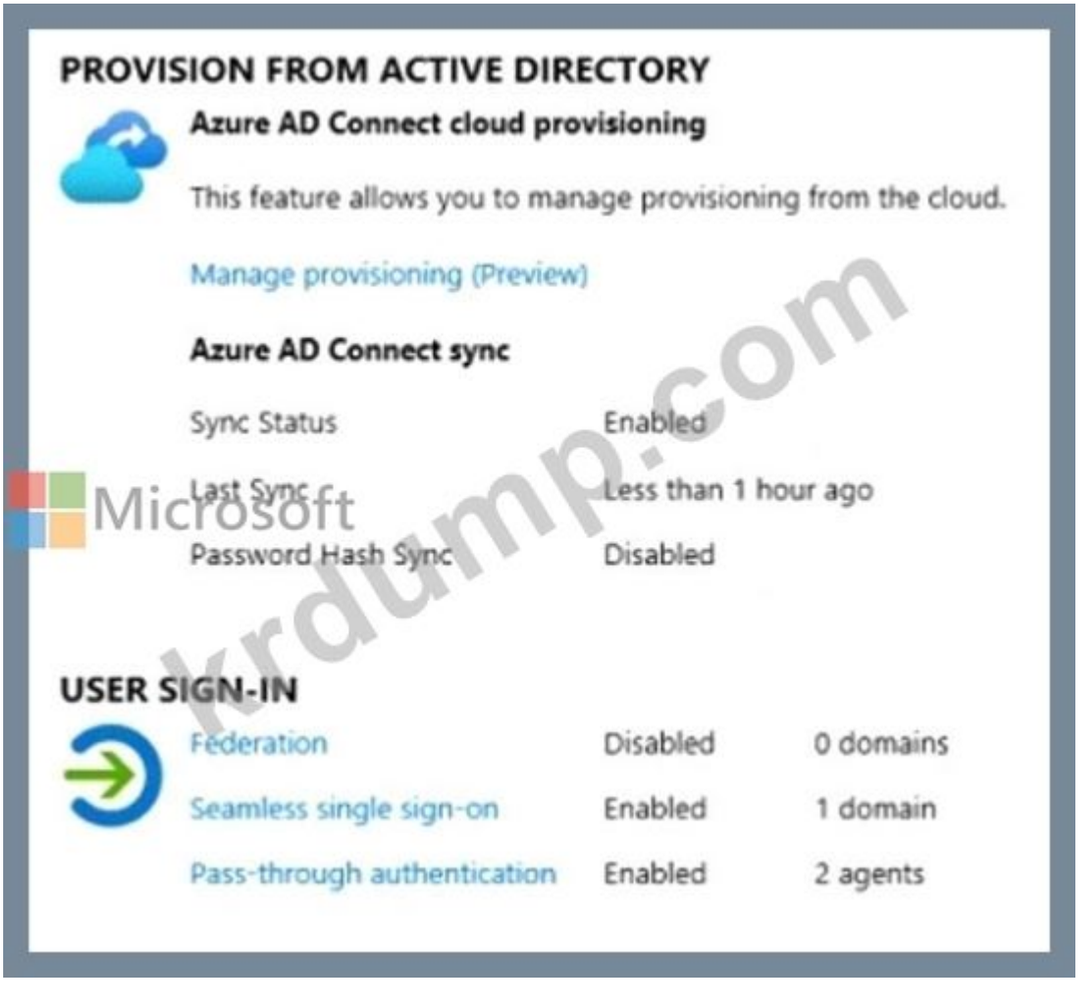
* □□□□□

* □□.□□□□□

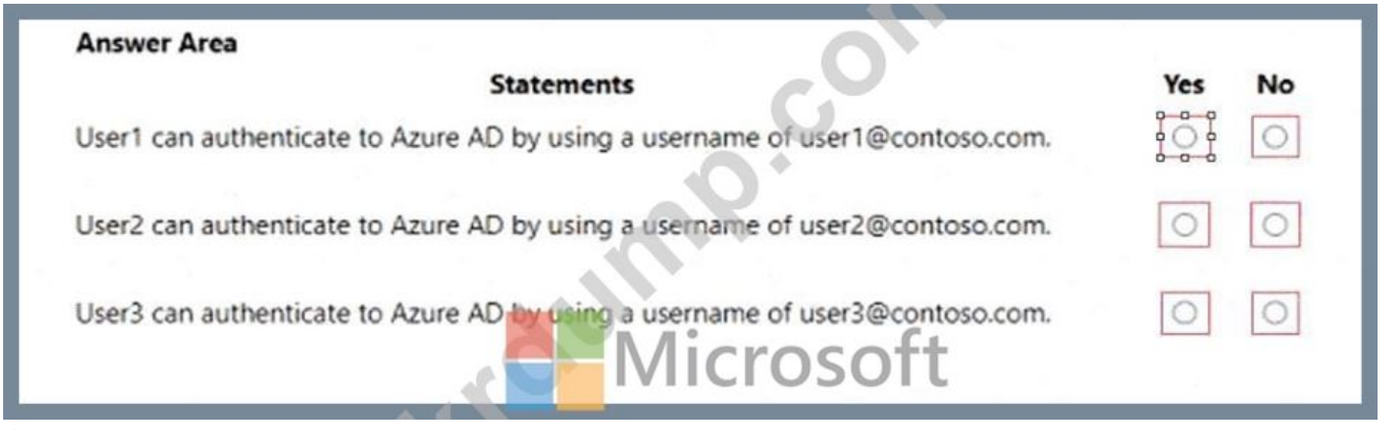
□□□□□□ □□ □□ □□ □□ □□□□ □□□□ □□□□.

Name	UPN suffix
User1	Contoso.com
User2	East.contoso.com
User3	Fabrikam.com

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



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



Answer:

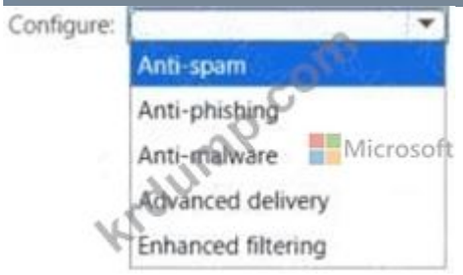
Explanation:
Box 1: Yes
The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.
Box 2: No
The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.
Box 3: No
The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

NEW QUESTION: 151
Windows 10 □□ 21H1□ □□ □□□ □ □□□□ □□□□□□.
□□□□ □□ □□□□ □□□□ □□□. □□□□ □□□ □□□□ □□ □□□□□ □□□.
□□□□□ □□□ □□ □□□?
A. □□ □□ □□□□□ □□ □□ □□□□□ □□□□□.
B. □□ 21H1 □□□ □□□□ □□ □□ □□□□□ □□ 21H1 □□□ □□□□ □□ □□ □□ □□□ □□□□□.
C. □□ □□ □□□□□ 21H1 □□ □□□ □□□ □□ □□ □□□□□ □□□□□.
D. □□ 21H1 □□□ □□□□ □□ □□ □□□□□ □□ □□ □□□□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 152
□□ □□ □□□ □□□□ User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Role
Admin1	Exchange Administrator
Admin2	Security Administrator
Admin3	User Administrator

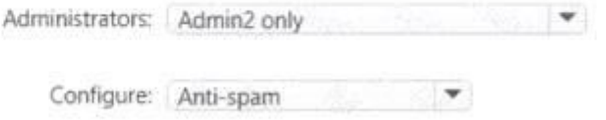
□□□1□ □□□ □□□ 1,000□□ □□ □ □□ □□□ □□□ □□□□□□ □□□□□. □□ □□□ □□□□ □□□.



Answer:

Explanation:

Answer Area



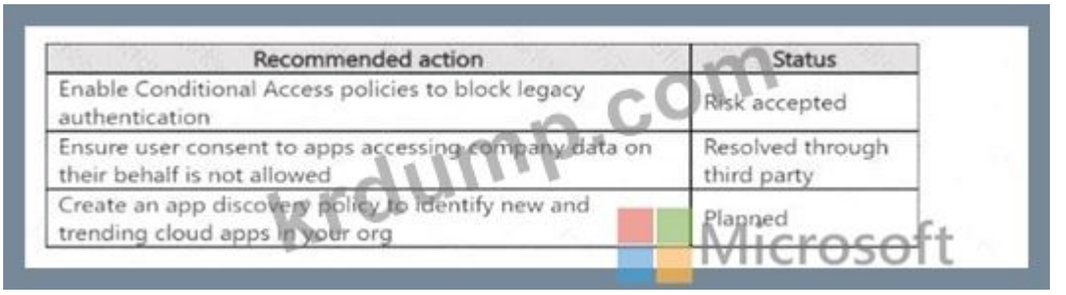
NEW QUESTION: 153

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

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

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

□□ □□ □□□ □□ □□ □□□ □□□ □□□□□ □□□□□.



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

□□□□ □ □□ □□□ □□□ □□□□□?

A. 4

B. 16

C. 7

D. 0

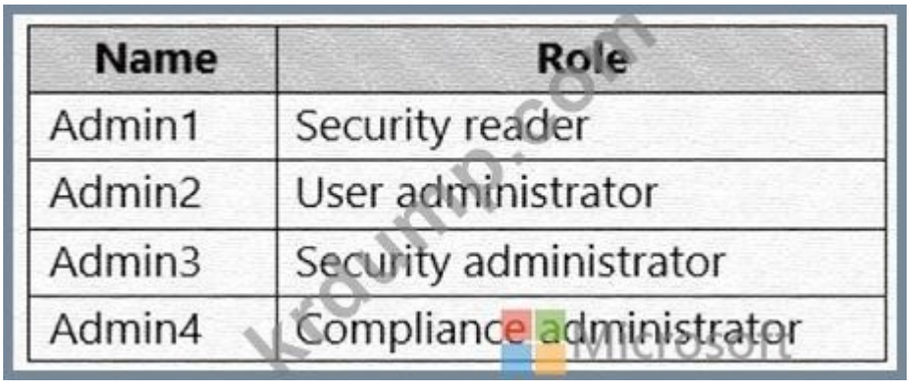
E. 13

Answer: C (LEAVE A REPLY)

NEW QUESTION: 154

Azure AD Identity Protection □□ □□ □□□□ □□□□□ □□□□□.

□□ □□ □□□ □□□□ □□□□.



Name	Role
Admin1	Security reader
Admin2	User administrator
Admin3	Security administrator
Admin4	Compliance administrator

□□ □□□□ □□ □□ □□□□ □□□□ □□ □□□?

A. Admin2, Admin3, Admin4□

B. Admin1, Admin2, Admin3, Admin4

C. Admin2 □ Admin3□

D. Admin3□

E. Admin1 □ Admin3□

Answer: E (LEAVE A REPLY)

By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or Security Administrators will automatically be added to the recipients list.

NEW QUESTION: 155

□□□□□ □□□□□□ Active Directory □□□□ Microsoft Endpoint Configuration Manager □ □□□ □□□□ □□□□.

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

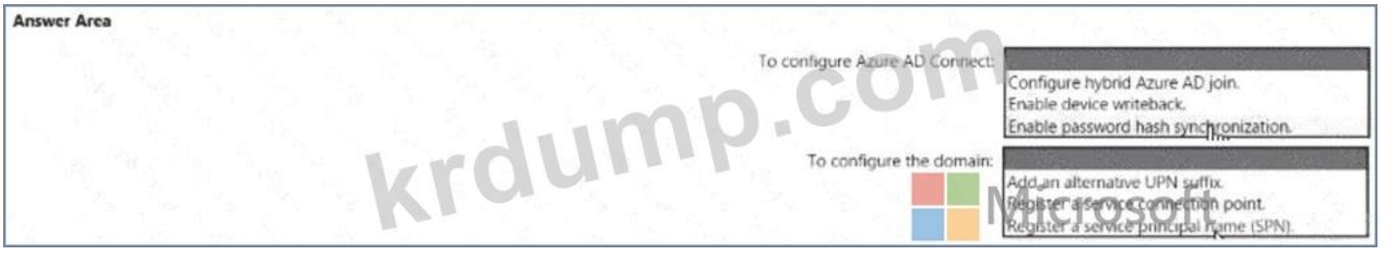
Azure AD Connect□ □□□□ □□□ □□ □ □□ □□□ Azure Directory(Azure AD)□ □□□ □□□. □□ □□ □□□□ □□□□□□□.

□□ □□□ □□□ □□□□□.

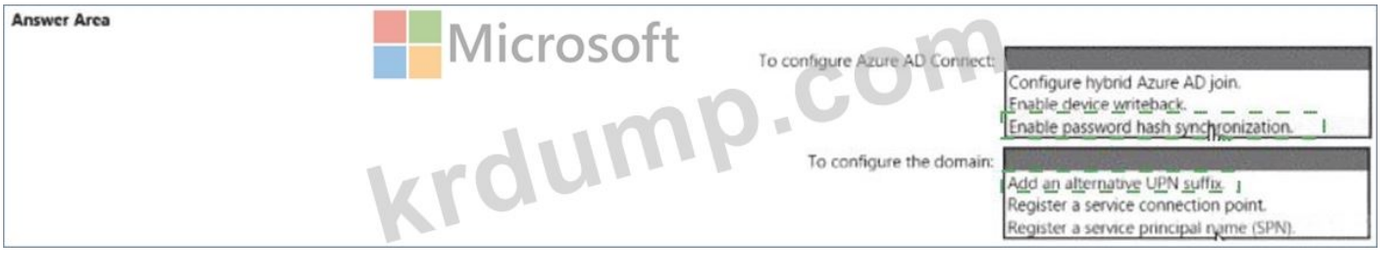
□□ □□□ □□□□□ Azure AD Connect□ □□□□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 156

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

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

□ □□□ Microsoft Intune□ □□□□ □□□□□.

□□ □□□ □□□ □□□□□ □□ □□□□ □□□□□ □□□.

□□ □□□ □ □□□ □□□□□?

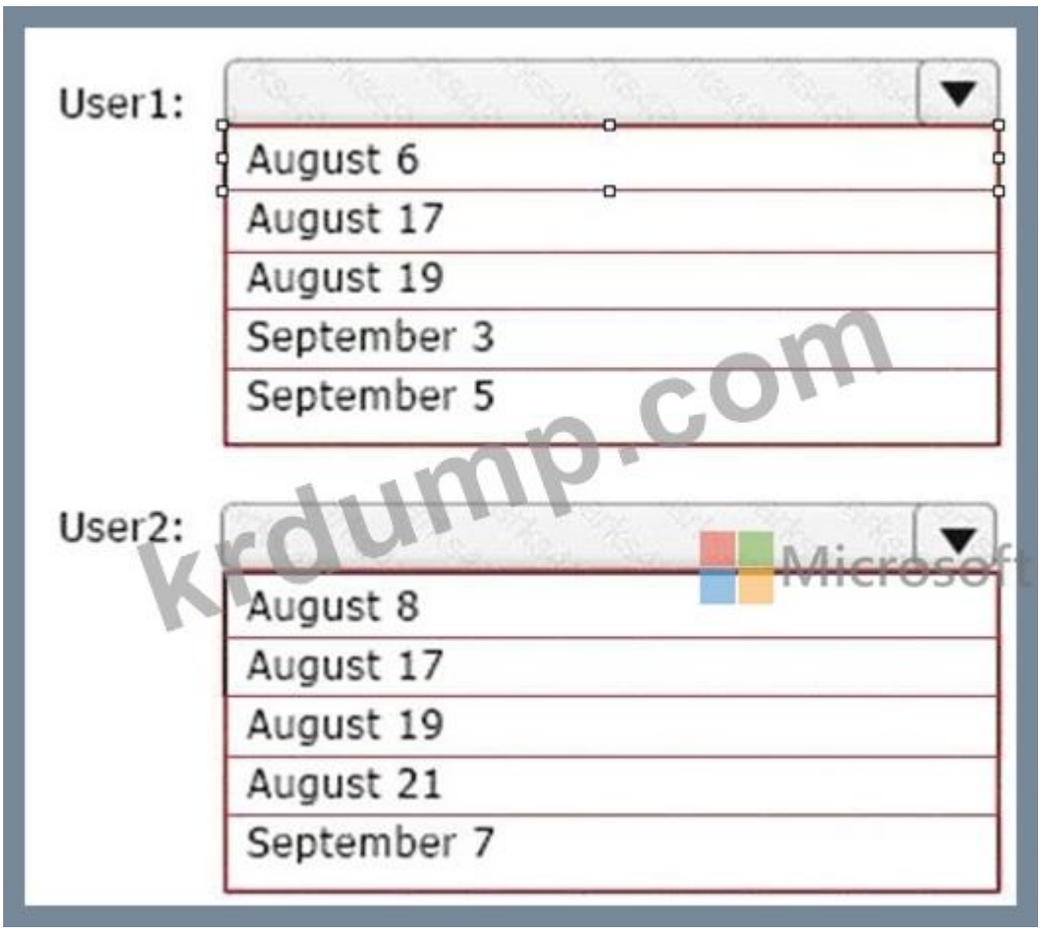
A. Device1□ Device4

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

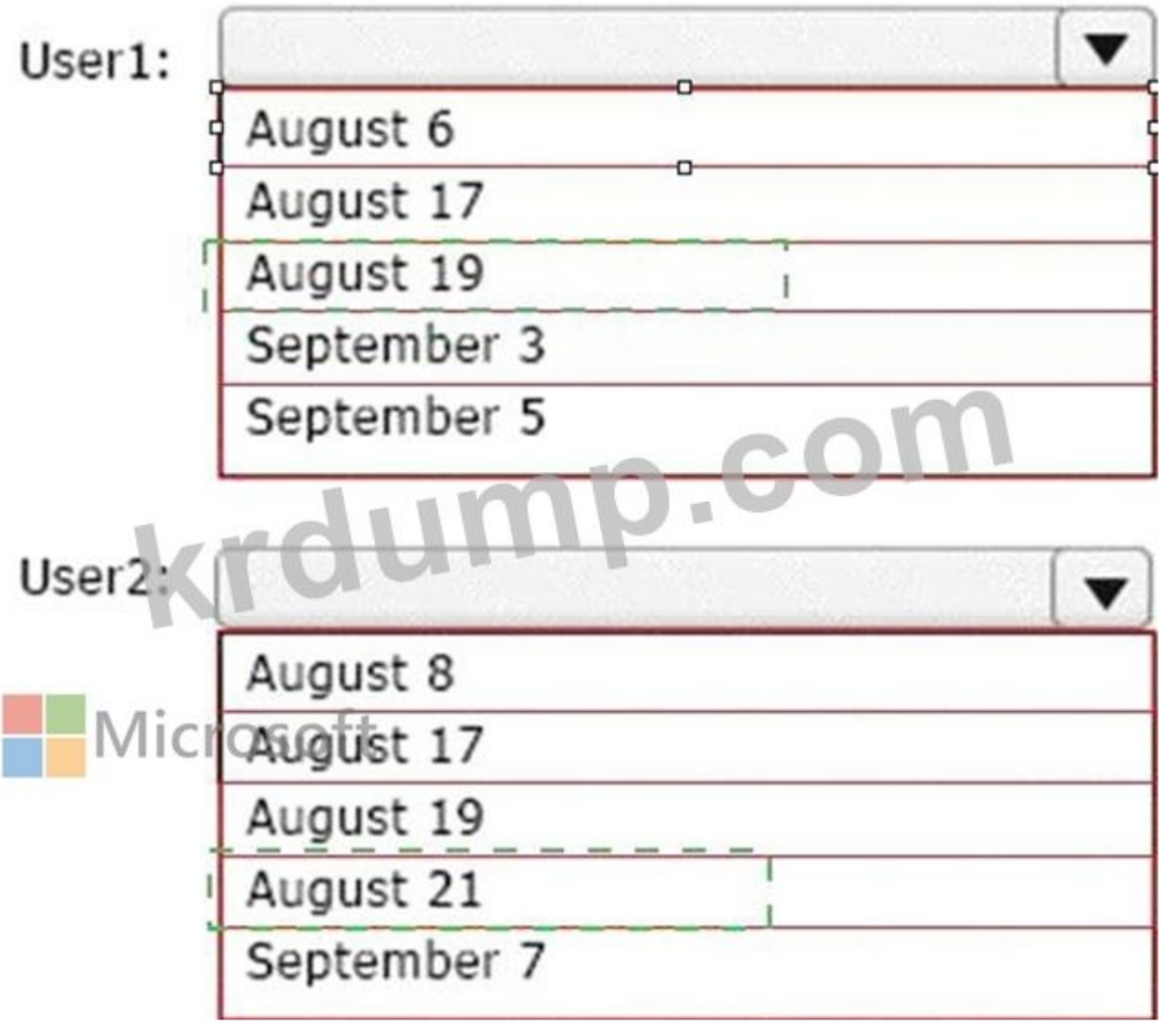
NEW QUESTION: 157
□□□
Microsoft 365 E5 □□□ □□□□.
8□ 1□□□ Azure AD Identity Protection□□ □□ □□□ □□□ □□ □□ □□ □□ □□□ □ □□□□.
* □□ : □□ □□□
* □□□: Azure AD □□ □□ □□ □□
* □□ □□: □□
* 8□ 3□□ User1□ User2□□ □ □□ □□□□ □□□□.
□□□□ □□ □□ □□□ □□□ □□□□ Azure Multi-Factor Authentication(MFA)□ □□□□ □□□□□.

User	Date
User1	August 5
User2	August 7

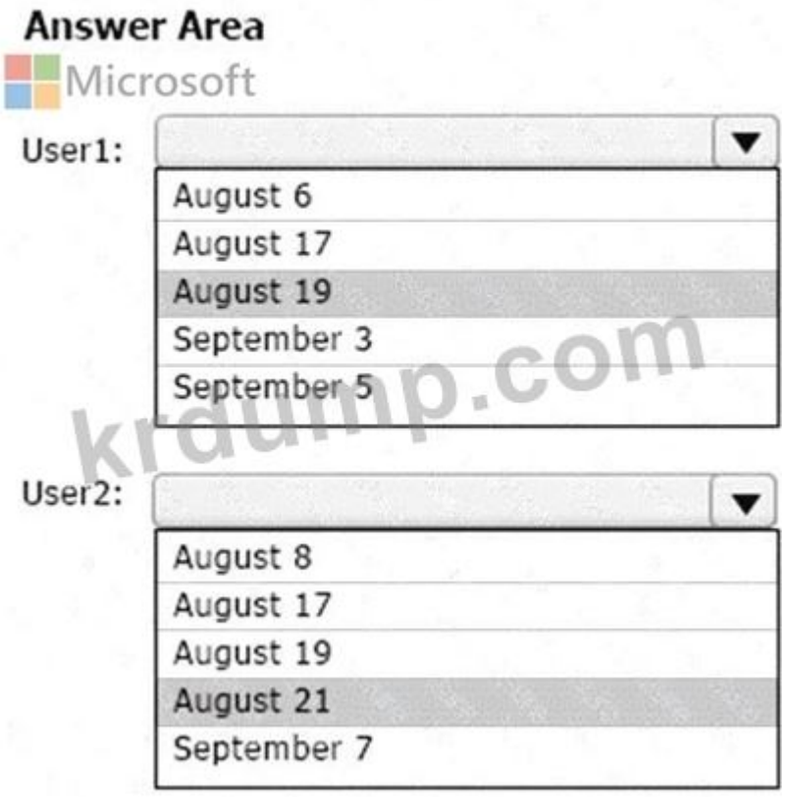
User1□ User2□ □□ □□□□ Azure MFA □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Box 1: August 19

Note: Security defaults will trigger a 14 day grace period for registration after a user's first login and security defaults being enabled. After 14 days users will be required to register for MFA and will not be able to skip.

Conditional Access by itself without Azure Identity Protection does not allow for the 14 day grace period.

Identity Protection includes the registration policy that allows registration on its own with no apps assigned to the policy. If a Conditional Access policy requires Multi-Factor Authentication, then the user must be able to pass that MFA request.

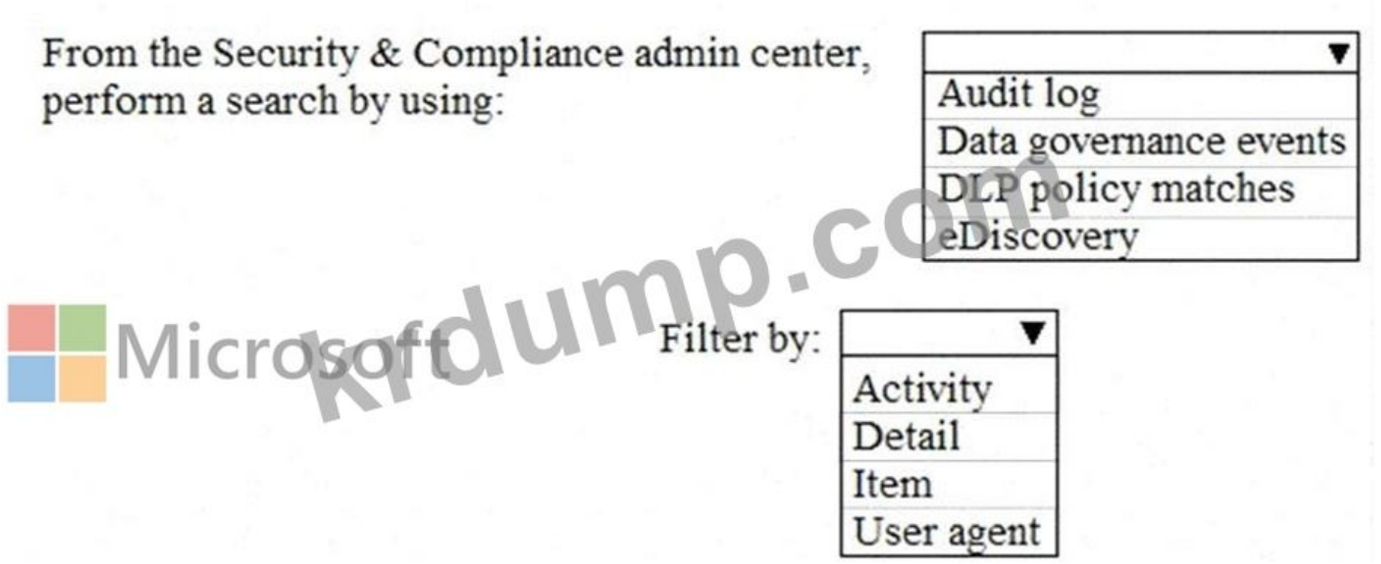
Box 2: August 21

Reference:

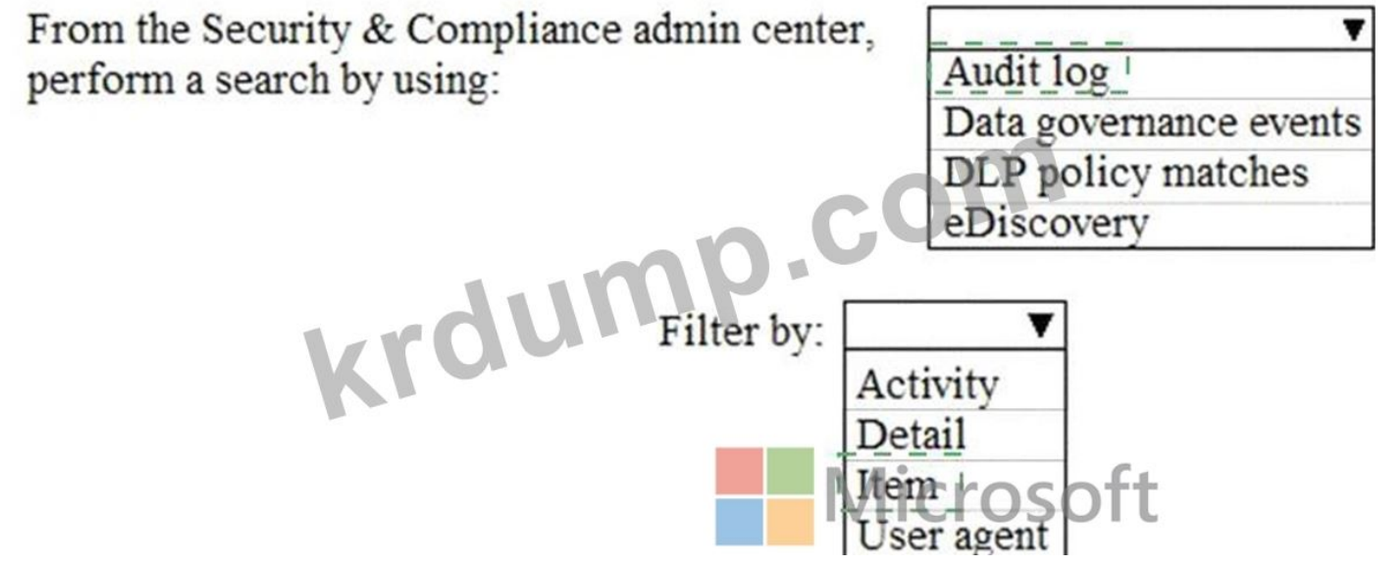
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

NEW QUESTION: 158

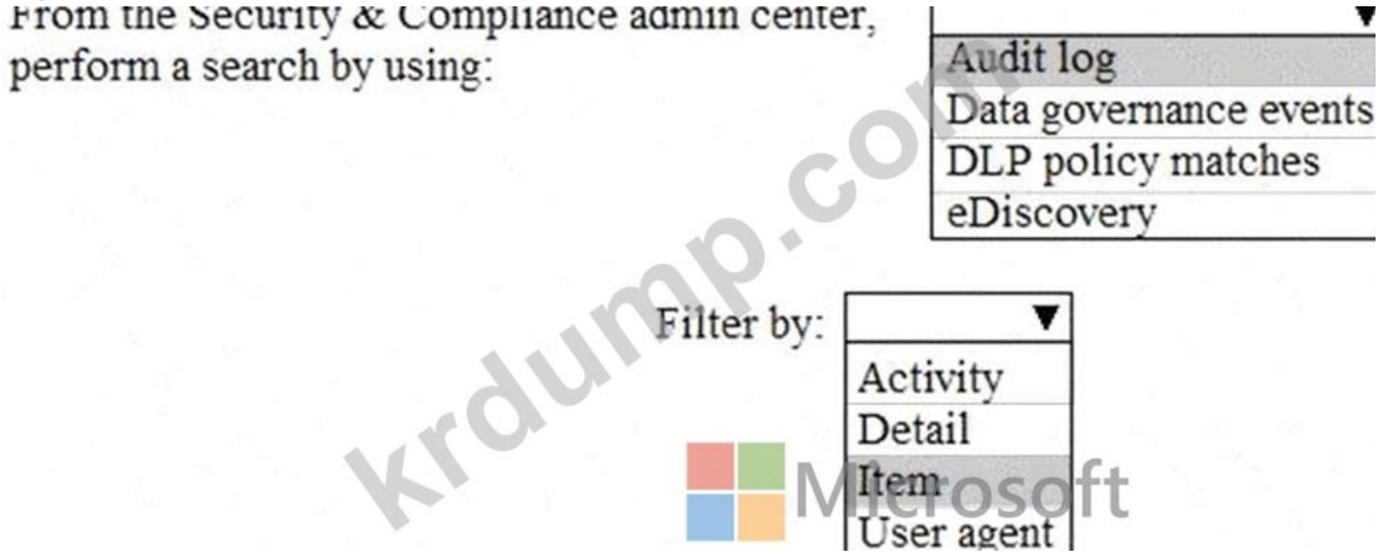
SharePoint □□□□ □□ □□ □□□ □□□□ □□□. □□□ □□ □□□? □□□□ □□□ □ □□ □□□ □□□□□□. □□: □ □□□ 1□□□□.



Answer:



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: 159

Microsoft 365 □□□ □□□□.

□□ □□□ □□ □□□ □□ □□□□.

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

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

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

File1.docx□ □□ □□□□ □□□□□?

A. 2023□ 1□ 1□

B. 2024□ 1□ 1□

C. 2023□ 1□ 31□

D. 2024□ 1□ 31□

E. □□ □□

Answer: D (LEAVE A REPLY)

Retention wins over deletion.

Note:

Explanation for the four different principles:

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

2. Etc.

Reference:

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

NEW QUESTION: 160

User1□ User2□□ □ □□ □□□□ □□□□ Microsoft 365 □□□□ □□□□. □□ □□□ □ □□ □□ □□□ □□□□.

□□□ 2□ 4□□□ Microsoft SharePoint Online □□□□□□ □□□ □□□□ □□□□□ □□ □□, □ □□□□□ 2□□ □□ □□□□□.

User1□ □ □□ □□□ □□ □□□?

A. 5

B. 10
C. 2
D. 25
Answer: (SHOW ANSWER)

NEW QUESTION: 161
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft 365 □□□ □□□□.
□□□□ □-□□□□ □□□□□ □□□□ □□ □□ Microsoft SharePoint Online □□□□ □□ □□□ □□□□ □□ □□□.
□□□: Endpoint Management □□ □□□□ □□ □□ □□□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
You need to create a trusted location and a conditional access policy.

NEW QUESTION: 162
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft 365 E5 □□□ □□□□.
SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.
SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Office 365 Advanced Threat Protection(ATP) □□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Azure Active Directory □□ □□□□ SecAdmin1□□ □□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: B (LEAVE A REPLY)

NEW QUESTION: 163
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □□, □□ □□□□ □□□ □□ □ □□□□.

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

Microsoft 365 E5 □□□ □□□□.

SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.

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

□□ □□: Microsoft 365 □□ □□□□ SecAdmin1□□ SharePoint □□□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: (SHOW ANSWER)

NEW QUESTION: 164

□□□

Microsoft 365 E5 □□□ □□□□.

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

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

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

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

□□□□: □□ □□□ 1□□□□.

Answer Area

To identify when users have compromised credentials, configure:

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

To enable self-remediation, select:

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

Answer:

Answer Area

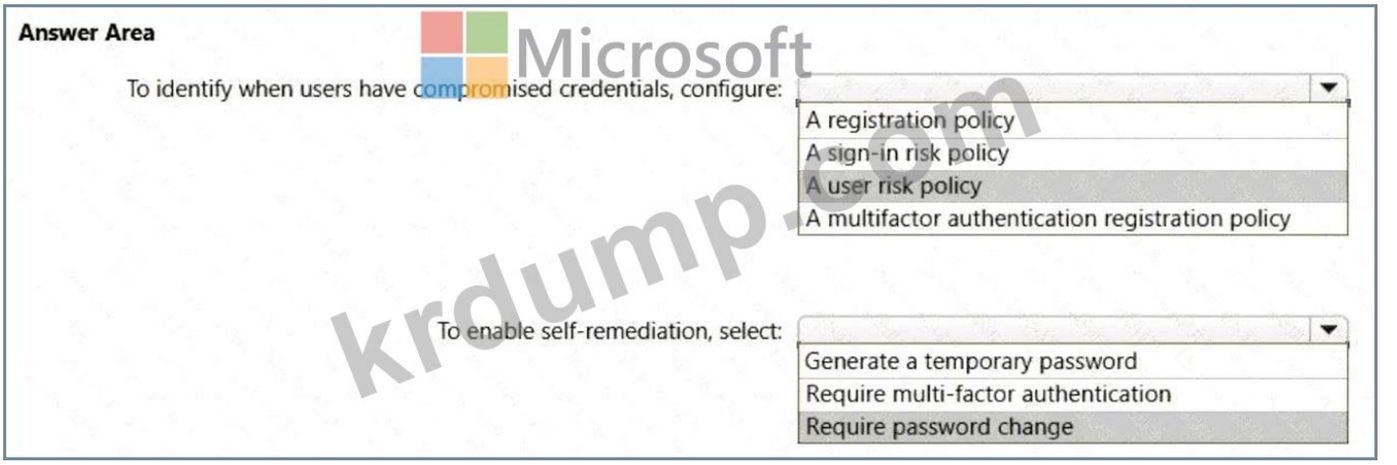
To identify when users have compromised credentials, configure:

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

To enable self-remediation, select:

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

Explanation:



Box 1: A user risk policy

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

User risk-based Conditional Access policy

Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:

Block access

Allow access but require a secure password change.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.

Box 2: Require password change

Provide users that have compromised credentials with the ability to self-remediate.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators Reference:

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection- policies#user-risk-based-conditional-access-policy

NEW QUESTION: 165

Microsoft 365 E5 □□□ □□□□.

SecAdmin1□□□ □□□ □□□ □□ □□□ □□□ □□□□.

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

□□ □□: Azure Active Directory □□ □□□□ SecAdmin1□□ Teams □□□ □□□ □□□□ □.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: A (LEAVE A REPLY)

NEW QUESTION: 166
□□ □□ □□□ Microsoft Endpoint Manager □□□ Device1□□□ Windows 10 □□□ □□□ Microsoft 365 □□□□ □□□□.

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

A. Policy2□ □□□
B. Policy3□ □□□
C. □□ □□
D. □□□ □□□!
Answer: B (LEAVE A REPLY)

NEW QUESTION: 167
Microsoft 365 E5 □□□ □□□□. □□□□ Site1□□□ Microsoft SharePoint Online □□□□ □□□□ □□□□. Site1□□ □□ □□□ □□□□ □□□□.
* □□.docx
* □□□□.docx
* □□jmportant.docx
Microsoft Defender Cloud □□□ □□ □□□ □□□ □□□ □□ Policy1□□□ □□ □□□ □ □□□.

Policy1□ □□ □□□ □□□□□?

A. ImportantFile.docx□
B. Filejmportant.docx□
C. ImportantFile.docx □ Filejmportant.docx□
D. File.docx, ImportantFile.docx, Filejmportant.docx
E. □□.docx□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 168
□□□ Microsoft 365 E5 □□□□ □□□□.
Microsoft Exchange Online □□□ □□ □□□ □□□□ □□□□□ □□ □□□ □□□□□ □ □□.
□□ □□ □□□ □□ □□□?
A. □□□ □□□□□□.
B. Microsoft 365 □□ □□□ □□□□□□.
C. □□□ □□ □□ □□□ □□□□□.
D. □□□□□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Microsoft Purview auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization.
This capability provides visibility into the activities performed across your Microsoft 365 organization.
Note: Permissions alert policies
Example: Elevation of Exchange admin privilege
Generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in Exchange Online.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview
https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies

NEW QUESTION: 169
Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□ □□□ □□ □□□ □□□□□.


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

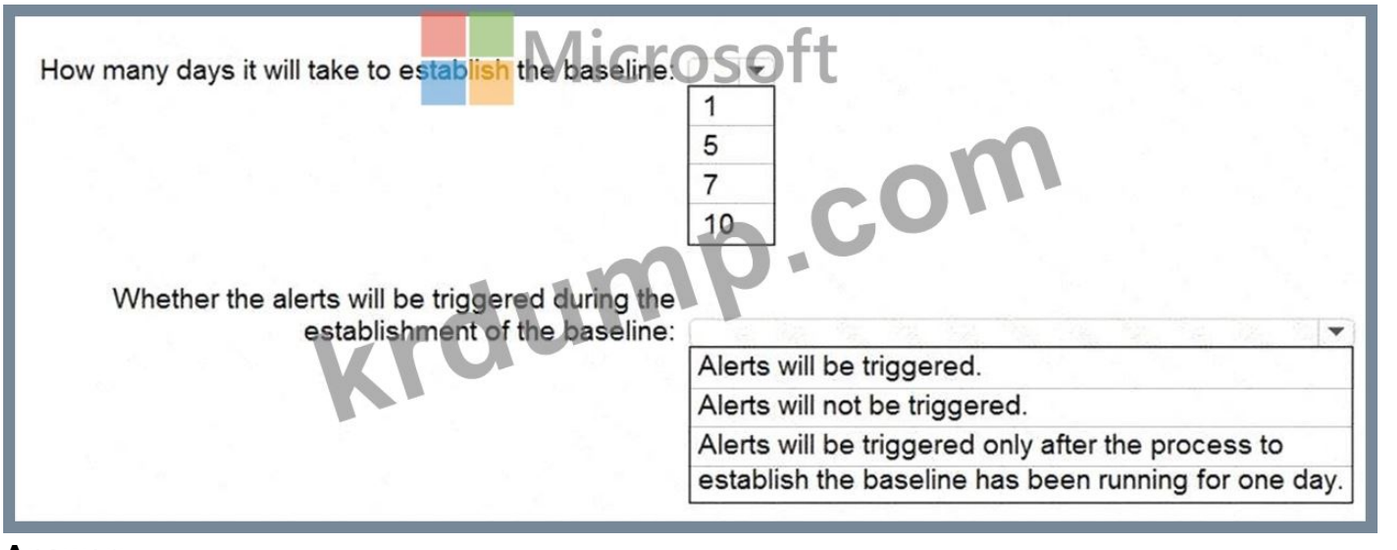
□□ □□□ □□□□ □□□.

* □□□□□ □□□ □□ □□□□ □□□□ □ □□□ □□□□?

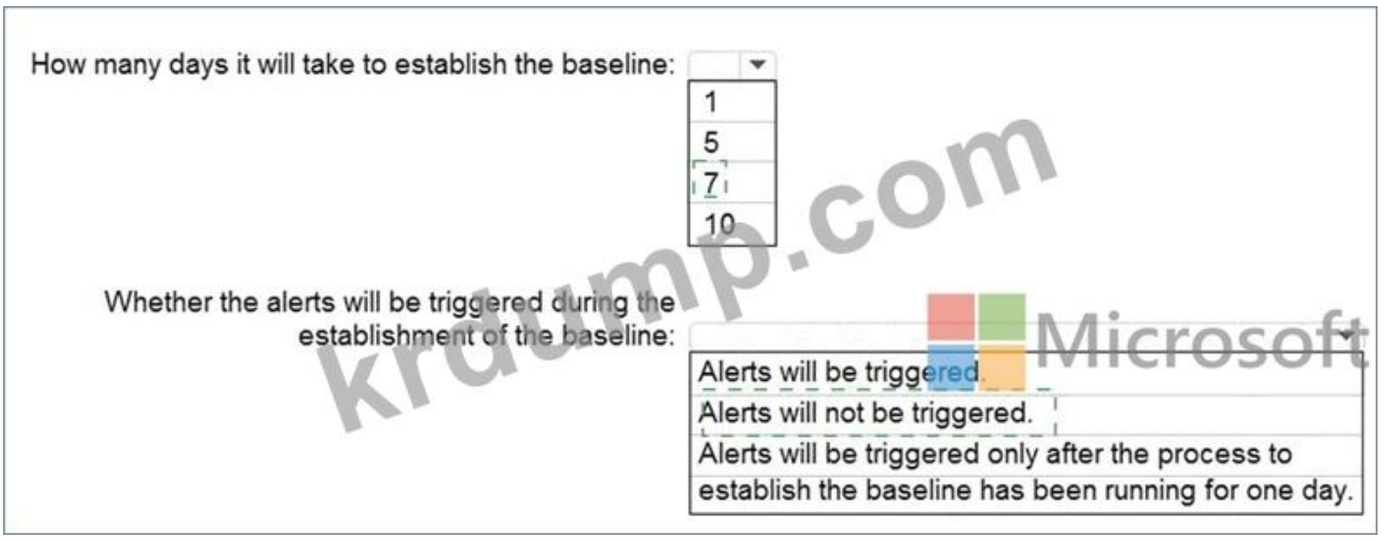
* □□□□ □□□□ □□ □□□ □□□□□ □□.

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

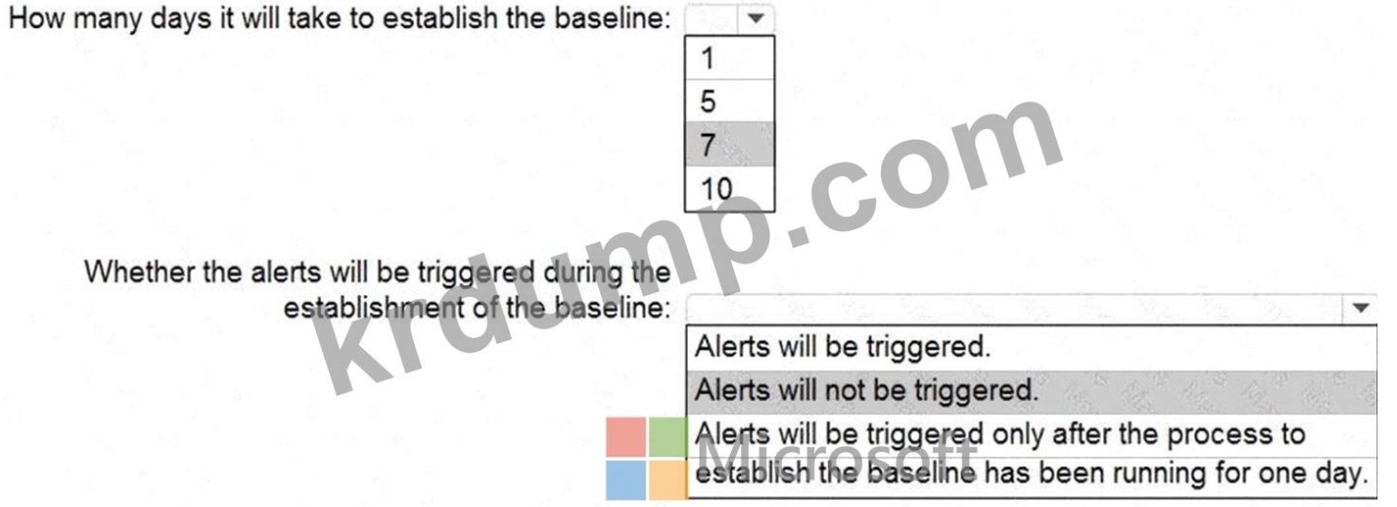
□□□□: □□ □□□ 1□□□□.


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

Answer:



Explanation:



ence:

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

NEW QUESTION: 170

Microsoft 365 E5 □□□ □□□□.

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

□□□ DLP □□□□ □□ □□□ □□□ □ □□□?

A. □□□ □□ □□

B. □□□ □□ □□

C. □□□

D. □□□ □□□

Answer: C (LEAVE A REPLY)

Apply retention labels to content automatically if it matches specific conditions, that includes cloud attachments that are shared in email or Teams, or when the content contains:

Specific types of sensitive information.

Specific keywords that match a query you create.

Pattern matches for a trainable classifier.

Note: Retention policies can be applied to the following locations:
Exchange mailboxes
SharePoint classic and communication sites
OneDrive accounts
Microsoft 365 Group mailboxes & sites
Skype for Business
Exchange public folders
Teams channel messages (standard channels and shared channels)
Teams chats
Teams private channel messages
Yammer community messages
Yammer user messages
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-exchange-conditions-and-actions

NEW QUESTION: 171
□□□□□ contoso.com□□□ Active Directory □□□□ □□□□. □ □□□□□ □□ □□ □ □ □□ □□□ □□□□ □□□□.

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

Answer Area

Statements	Yes	No
User2 will synchronize to the Microsoft Entra tenant.	○	○
Group2 will synchronize to the Microsoft Entra tenant.	○	○
User3 will synchronize to the Microsoft Entra tenant.	○	○

Answer:

Answer Area

Statements	Yes	No
User2 will synchronize to the Microsoft Entra tenant.	○	○
Group2 will synchronize to the Microsoft Entra tenant.	○	○
User3 will synchronize to the Microsoft Entra tenant.	○	○

Explanation:

Answer Area

Statements	Yes	No
User2 will synchronize to the Microsoft Entra tenant.	○	●
Group2 will synchronize to the Microsoft Entra tenant.	●	○
User3 will synchronize to the Microsoft Entra tenant.	■	○

NEW QUESTION: 172

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

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

□□□□: □□ □□□ 1□□□□.

Settings to configure in Azure AD: ▼

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune: ▼

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

Answer:

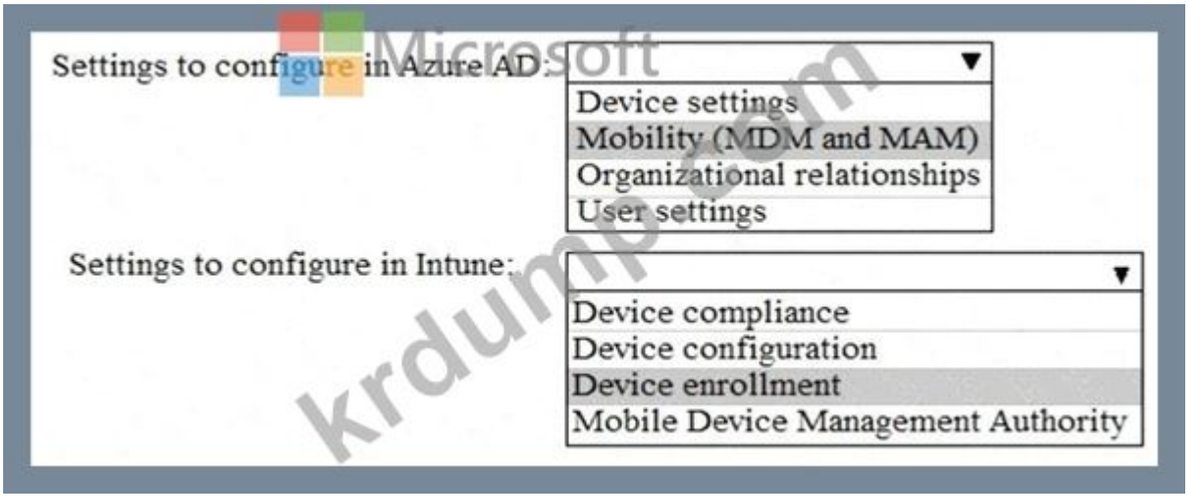
Settings to configure in Azure AD: ▼

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune: ▼

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

Explanation:



References:

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

NEW QUESTION: 173

Microsoft 365 □□□ □□□□.

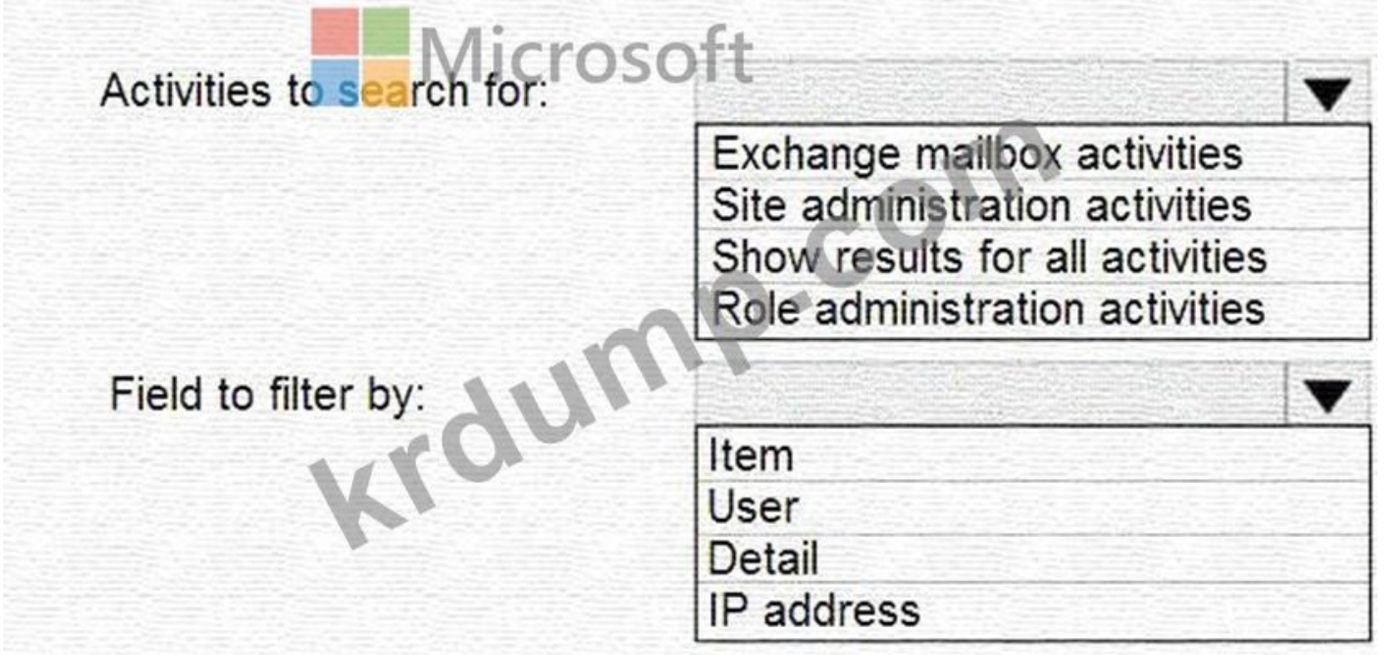
□□□ □□□□□ 51.40.15.0/24□ IP □□ □□□ □□□□□.

Exchange Online □□□□ □□ □□□□□ □□□□□ Role1□□□ □□□ □□□□□□.

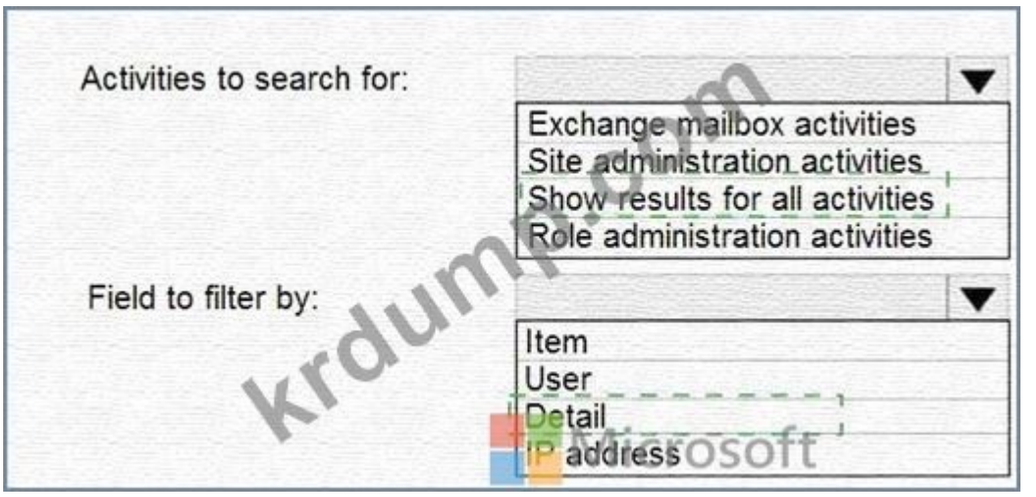
□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□.

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

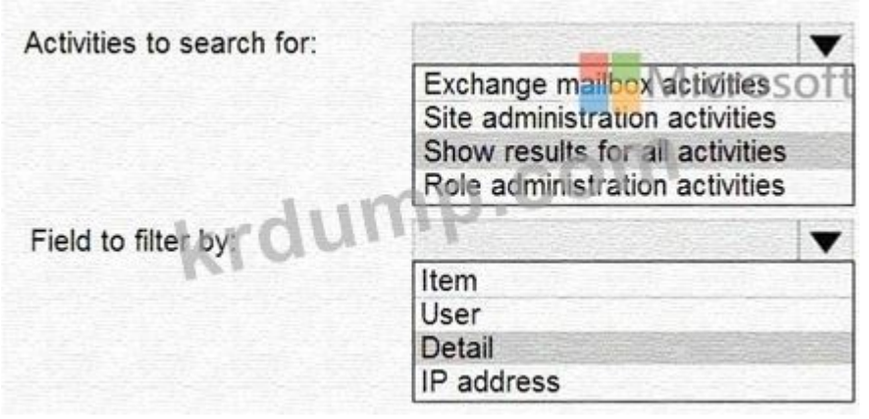
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 174

Azure Advanced Threat Protection(ATP)□ □□□□ Microsoft 365 E5 □□□ □□□□.

Azure ATP□□ □□ □□□ □□□□ □□□.

□□ □□□ □□□□ □□□?

A. □□ □ □□ □□ □□ □□

B. Microsoft Defender □□ □□

C. Microsoft 365 □□ □□

D. Azure Advanced Threat Protection □□

E. □□□□ □ □□ □□

Answer: D (LEAVE A REPLY)

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: 175

Microsoft 365 E5 □□□ contoso.com□□□ Azure AD □□□□ □□□□.

□□ □□□□ 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
- [ ] Helpdesk Administrator
- [ ] Hybrid Identity Administrator
- [ ] License Administrator

Explanation:

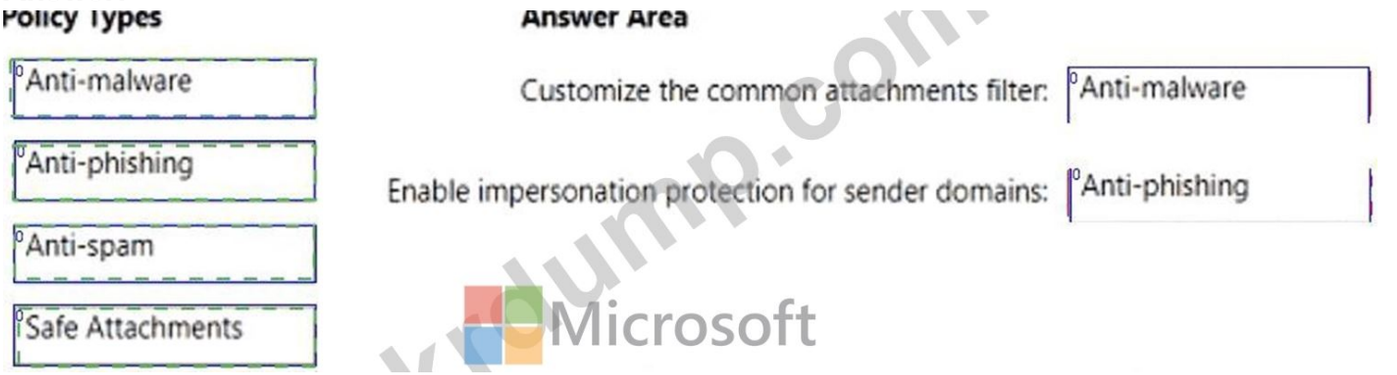
Answer Area

NEW QUESTION: 176

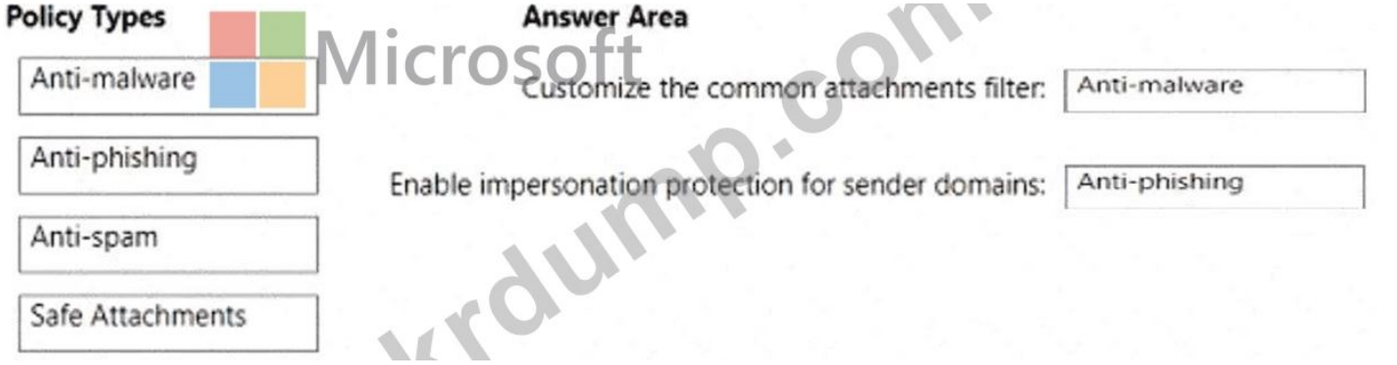
Office 365☐ Microsoft Defender☐ ☐☐☐☐ Microsoft 365 ☐☐☐ ☐☐☐☐.

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

Answer:



Explanation:



Box 1: Anti-malware

Customize the common attachments filter.

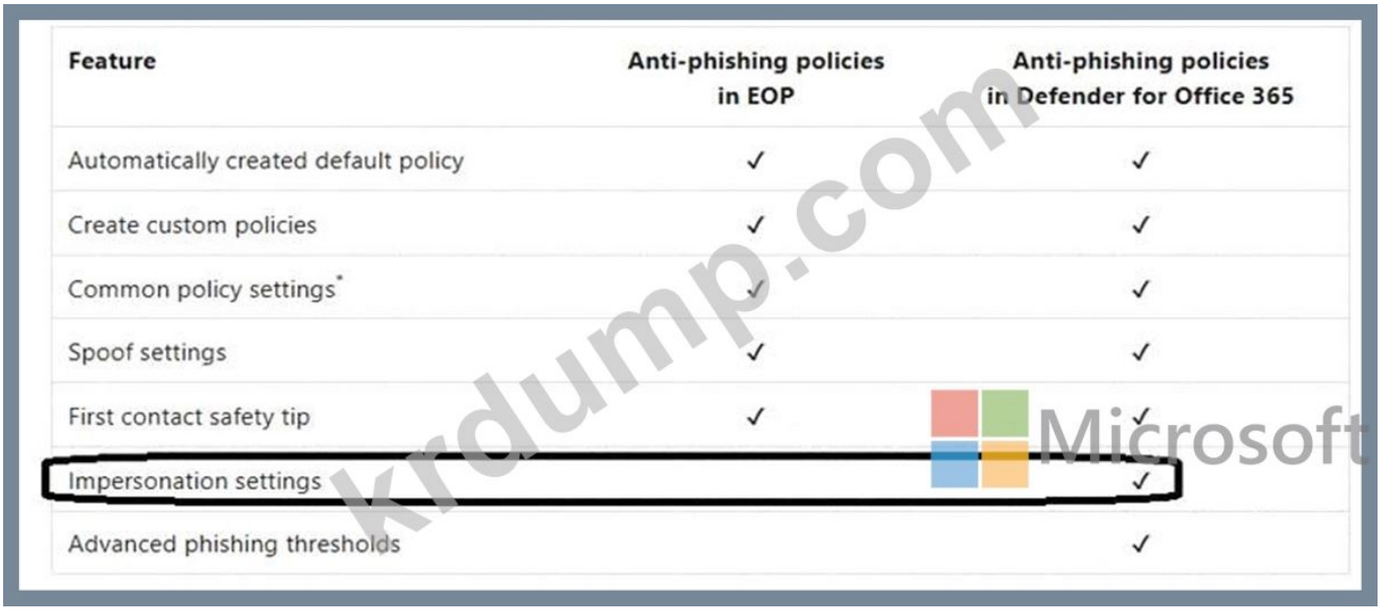
See step 5 below.

1. Use the Microsoft 365 Defender portal to create anti-malware policies In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & Collaboration > Policies & Rules > Threat policies > Anti-Malware in the Policies section. To go directly to the Anti-malware page, use https://security.microsoft.com/antimalwarev2

2. On the Anti-malware page, select Create to open the new anti-malware policy wizard.

On the Name your policy page, configure these settings:

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



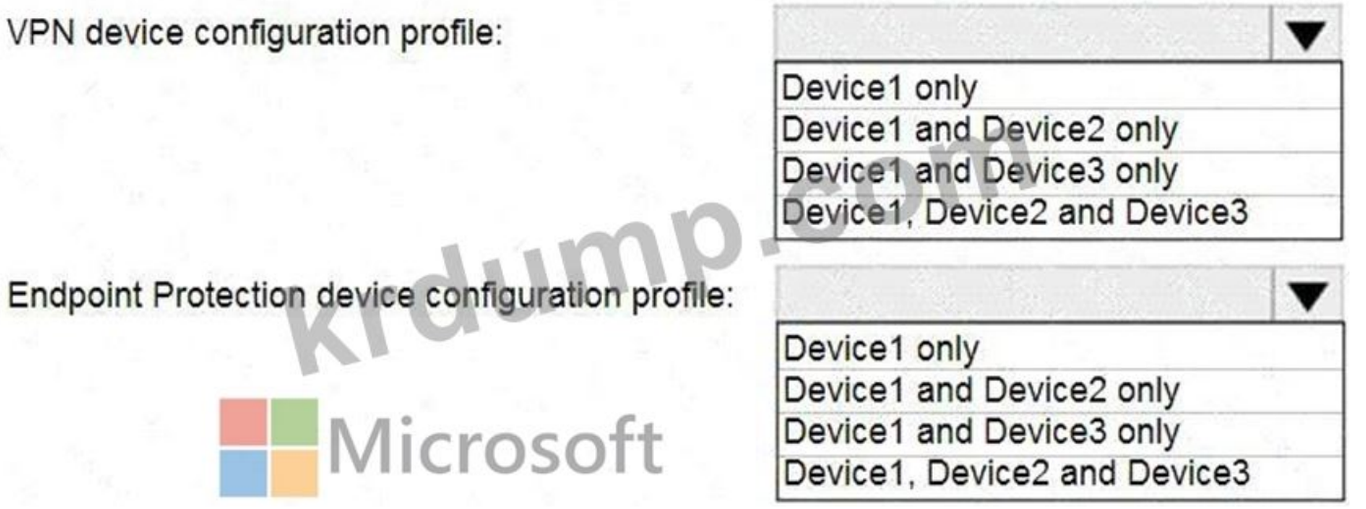
Feature	Anti-phishing policies in EOP	Anti-phishing policies in Defender for Office 365
Automatically created default policy	✓	✓
Create custom policies	✓	✓
Common policy settings*	✓	✓
Spoof settings	✓	✓
First contact safety tip	✓	✓
Impersonation settings		✓
Advanced phishing thresholds		✓

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

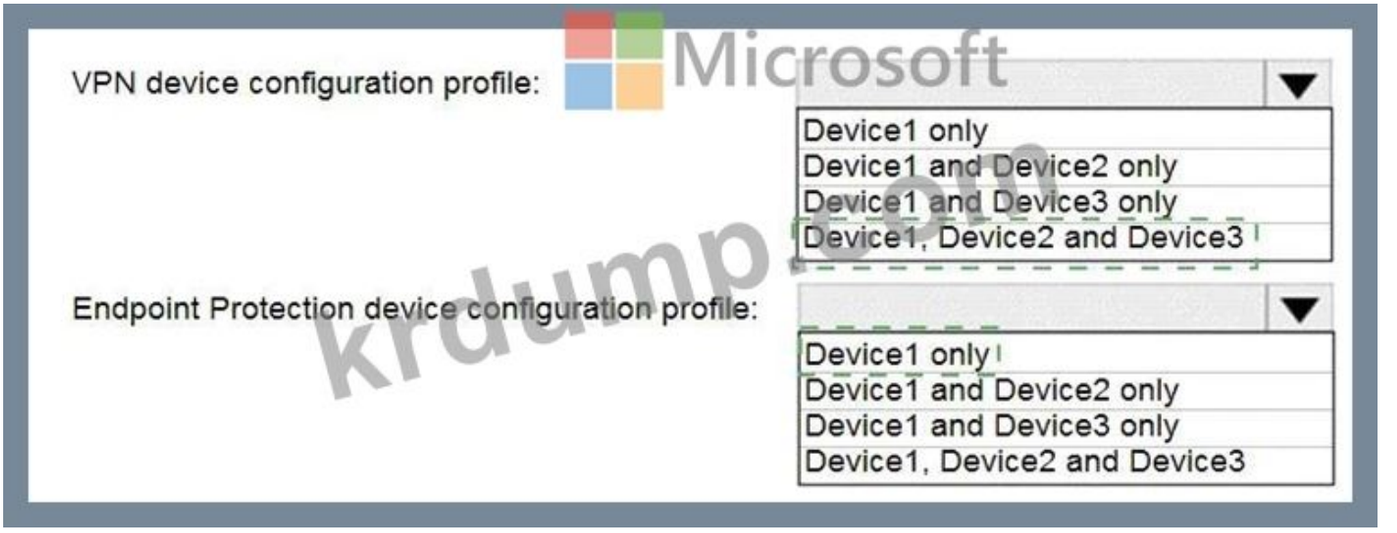
NEW QUESTION: 177
Microsoft Intune□ □□□ □□□□□ □□□□ Microsoft 365 □□□□ □□□□. □□□□□ □ □ □□ □□□ □□ □□□□□.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

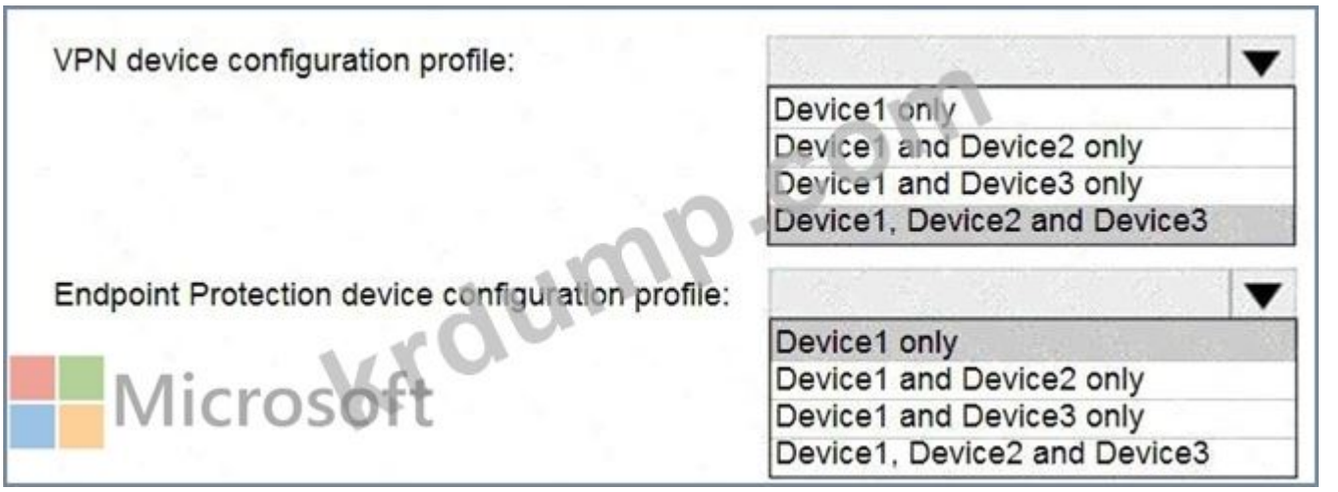
Microsoft Endpoint Manager□□ □□□ □□ □□ □□ □□□ □□□ □□□□□.
* VPN □□ □□ □□□□ □□□□ VPN □□□ □□□□□.
* Endpoint Protection □□ □□ □□□□ □□□□ □□ □□□ □□□□□.
□□□ □□ □□□ □□□□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

NEW QUESTION: 178
□□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft Entra □□□□ □□□□□.
□□ □□□□ □□□□ Microsoft Entra □□□□ □□□□□□ □□□□□. □□ □□(OU)□ 10 □ □□□ □□□ Microsoft Entra □□□□ □□□□□ □□ □□ □□□□□□. □□ □□ □□□ □□□ □□□□□ □□□□□□□□.
Microsoft Entra Connect Health□ □□□ □□ □□ □□□ □□ □□□□ □□□□□ □□□□□ □ □ □ □□□□.
10□□ □□□ □□□ Microsoft Entra □□□□ □□□□□□□ □□□□ □□□.
□□ □□: Microsoft Entra Connect□□ Microsoft Entra □□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

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

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

□□□ □□ VPN □□□□ □□□□ □□□□□.
□□□ □ □□ □□ □□□ □□□□□?
A. 5
B. 3
C. 1

D. 4

Answer: (SHOW ANSWER)

NEW QUESTION: 180

Label1□ Label2□□ □ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □ □□ □□ Microsoft Purview□ □□□□ Device1□□□ Windows □□□ □□□□ □□□□. Device1 □□ □□ □□ □□ □□ □□□ □□□□ □□□□.

Name	Location	Sensitivity label
File1.docx	C:\Temp\	Label1
File2.docx	C:\Temp\Folder1\	Label2
File3.docx	C:\Temp\Folder2\	Label1

□□ □□□ □□ Policy1□□□ □□□ □□□ □□ □□(DLP) □□□ □□□□.

Answer Area

Answer:

Explanation:

NEW QUESTION: 181

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

□□□ □□ □□□ Microsoft □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□.

□□□ □□□□ □□□?

A. □□□□ □□

B. Microsoft □□ □□

C. □□ □□□

D. □□ □□

E. □□ □□

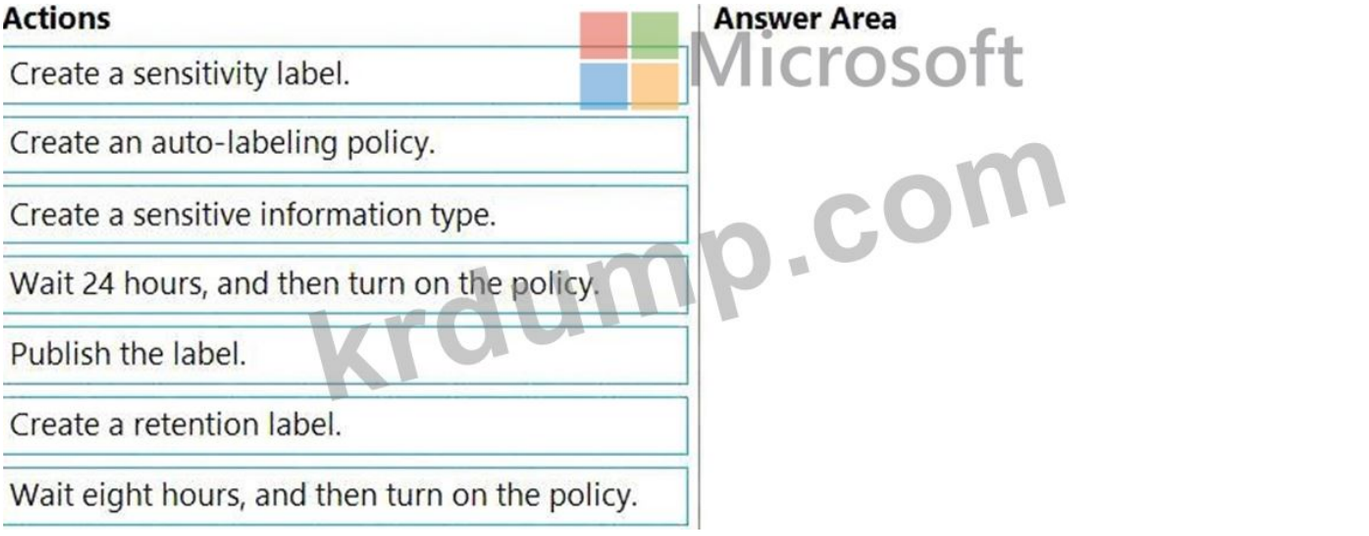
Answer: (SHOW ANSWER)

NEW QUESTION: 182

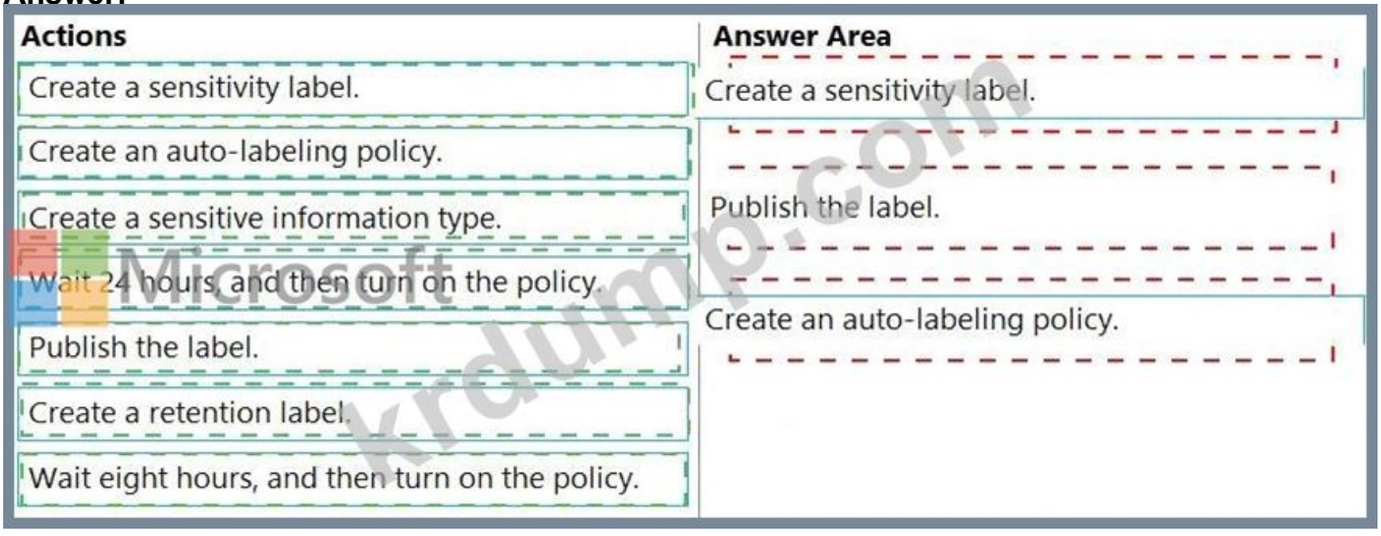
Site1□□□ Microsoft SharePoint Online □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Site1□□ □□□□ □□□ □□□ □□□ □□□□ □□□ □□□□ □□□.

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



Answer:



Explanation:

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

NEW QUESTION: 183
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
□□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft Entra □□□□ □□□□□.
□□ □□□□ □□□□ Microsoft Entra □□□□ □□□□□□ □□□□□.
□□ □□(OU)□ 10□ □□□ □□□ Microsoft Entra □□□□ □□□□□ □□ □□ □□□□□ □. □□ □□ □□□ □□□ □□□□□ □□□□□□□□.
Microsoft Entra Connect Health□ □□□ □□ □□ □□□ □□ □□□□ □□□□□ □□□□□ □ □ □ □□□□.
10□□ □□□ □□□ Microsoft Entra □□□□ □□□□□□□ □□□□ □□□.
□□ □□: Microsoft Entra Connect□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?

A. □
B. □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 184
Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□□□ □□□□ □□□ □□ □□□□ □□□ □ □□□ □ □□□□□.
□□ □□□ □□ □ □□□□ □□ □□□□ □□□□ □□□ □□□□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?

A. □□□ □□ □□ □□□ □□□□□.
B. □□□ □□□ □□(EDM) □□□□ □□□□.

C. Sec-RegulacoryComplianceUI cmdlet□ □□□□□.
D. Sec-LabelPolicy cmdlet□ □□□□□.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide

NEW QUESTION: 185
□□□ □□ □□□ □□□□□ □□ □□ □□□ □□□□ □□□.
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: 186
Microsoft 365 E5 □□□ □□□□.
□□□□ □□□ □□□ □□□□ □□□□ □ App1□□□ □□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□□.
□□□□ □□ □□□□□□ □□□□ □ □□□□ □□□ □□ □□ □□ □□□ □□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□ □□
B. □□ □□
C. □□ □□ □□(MFA)
D. □□□ □□□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 187
Microsoft 365 E5 □□□ □□□□. □ □□□□ Windows 11 □□□ □□□□ □□□□ □□□□ □□□□.
Microsoft Defender for Endpoint□ □□□ □□□□ □□□□□. □□□ □□□ □□□□ □□ Defender for Endpoint□ □□□□□.
Defender for Endpoint□ □□□ □ □□□ □□ URL□ □□ IP □□□ □□□□□ □□□□ □□ □. □□□ □□ □□□?
A. □□ □□□ □□□□□.
B. □□ □□□ □□□□□□.
C. □□□□ □□ □□□ □□□□□.
D. □□ □□ □□□ □□□□□.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 188

□□□□□ Azure Active Directory(Azure AD) □□□□ Microsoft Endpoint Configuration Manager □□□ □□□□.

□□ □□ □□□ □□ □□□□.

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

□□ □□□ □□□□ □□□□□.

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

□□ □□□ □□□□ □□□?

A. Device1, Device2, Device3

B. Device3□

C. Device2□ Device3□

D. Device2□

E. Device1□

Answer: (SHOW ANSWER)

NEW QUESTION: 189

Microsoft 365 E5 □□□ □□□□.

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

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

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

□□□ □□□□ □□□?

A. □□ □□

B. MFA □□ □□

C. □□□ □□□ □□

D. □□ □□□ □□□□ □□□(SSPR)

Answer: D (LEAVE A REPLY)

Self-remediation with self-service password reset

If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.

Reference:

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

protection-remediate-unblock

NEW QUESTION: 190
500□□ Windows 10 □□□□□ □□□□ Microsoft 365 E5 □□□□ □□□□. □□□□□ Microsoft Intune□ □□□□ □□□□.
Endpoint □□□ □□□□ □□□□ □□□ □□□ □□□□□.
Endpoint □□□ □□□□□ □□□□ Windows □□ □□□□□ □□□□□ □□□. □□□ □□ □□□?
A. Endpoint □□ □□ □□ □□□□ □□□□□.
B. □□ □□ □□□ □□□□.
C. Windows 10 □□ □□ □□□□ □□□□.
D. □□ □□□□ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 191
Youi □□□□□□ Active Directory □□□□ □□□□ □□□□.
□□ □□□□ □□□□□ Microsoft Entra □□□□ □□□□.
Microsoft Entra Connect Sync□ □□□□ □□□□ □□ □□□□□□□. □□ □□ □□□ □ □ □□□ □□□ □□□□□□□□□.
□□□ □□ □□□ □□□□□ Microsoft Entra ID Protection□ □□□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Microsoft Entra □□ □□□□ □□ □□□□ □□□□□□.
B. Microsoft Entra Connect□□ □□□□ □□ □□□□ □□□□□□.
C. Microsoft Entra Connect□□ □□□□ □□□ □□□□□□.
D. Microsoft Entra □□ □□□□ □□ □□□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
NEW QUESTION: 192
□□□□□□ Azure AD□ □□□□ adatum.com□□□ Active Directory □□□□ □□□□ □□ □□.
□□ □□□□□ 100□□ □□□ □□□ □□□□.
□□ □□□□ □□ □□□ □□□□ □□□□ □□□ □□□□□.
□ □□□ 3□□ □□ □□□ city □□ □□ □□□□ □□□.
□□□ □□ □□□?
A. □□□ □□□□□ Windows PowerShell□□ Gec-ADUser □ Sec-ADUser cmdlet□ □□□□ □.
B. Azure Cloud Shell□□ Gec-ADUser □ Sec-ADUser cmdlet□ □□□□□.
C. □□□ □□□□□ Windows PowerShell□□ Gec-MgUser □ Updace-MgUser cmdlet□ □□ □□□.
D. Azure Cloud Shell□□ Gec-MgUser □ Update-MgUser cmdlet□ □□□□□.
Answer: A (LEAVE A REPLY)
The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active

Directory (Azure AD). Therefore, the city attribute must be changed in the on-premise Active Directory.
You can use Windows PowerShell on a domain controller and run the Get-ADUser cmdlet to get the required users and pipe the results into Set-ADUser cmdlet to modify the city attribute.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.
Other incorrect answer options you may see on the exam include the following:
1. From the Azure portal, select all the Azure AD users, and then use the User settings blade.
2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set-AzureADUser cmdlets.
3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
4. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.
Reference:
https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser

NEW QUESTION: 193
□□ □□□□ □□□□ □□□ □□□ □□□ □□ □□ □□ □□□ □□□ □ □□□ □□□□ □□□.
□□□ □□□ □□ □□ □□□□ □ □□□□?
A. 1
B. 4
C. 7
D. 31
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

NEW QUESTION: 194
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□ □ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Compliance Manager □□□ □□□□□ User1□ □□□□□ □□□.

□□ □□: Microsoft 365 □□ □□□□ User1□□ □□ □□ □□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

NEW QUESTION: 195

Project1□ □□□ □□□□□ □□□□ □□□□.
□□□□□ □□□ □□□ □□□□ □□ □□ DNS □□□□ □□□□ □□□ □□□□ □□□.
□□ DNS □□□□ □□□□ □□□?

A. □□□(A)

B. □□□ □□

C. □□□(TXT)

D. □□(CNAME)

Answer: (SHOW ANSWER)

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)

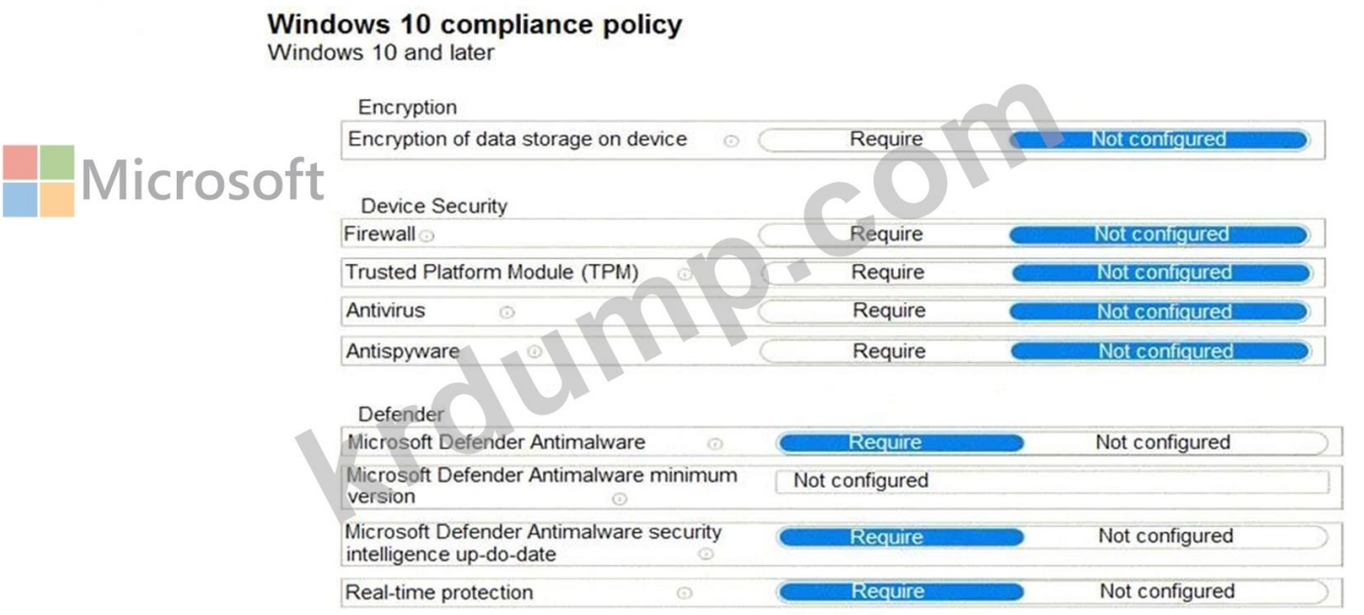
Reference:
https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns- hosting-provider

NEW QUESTION: 196

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

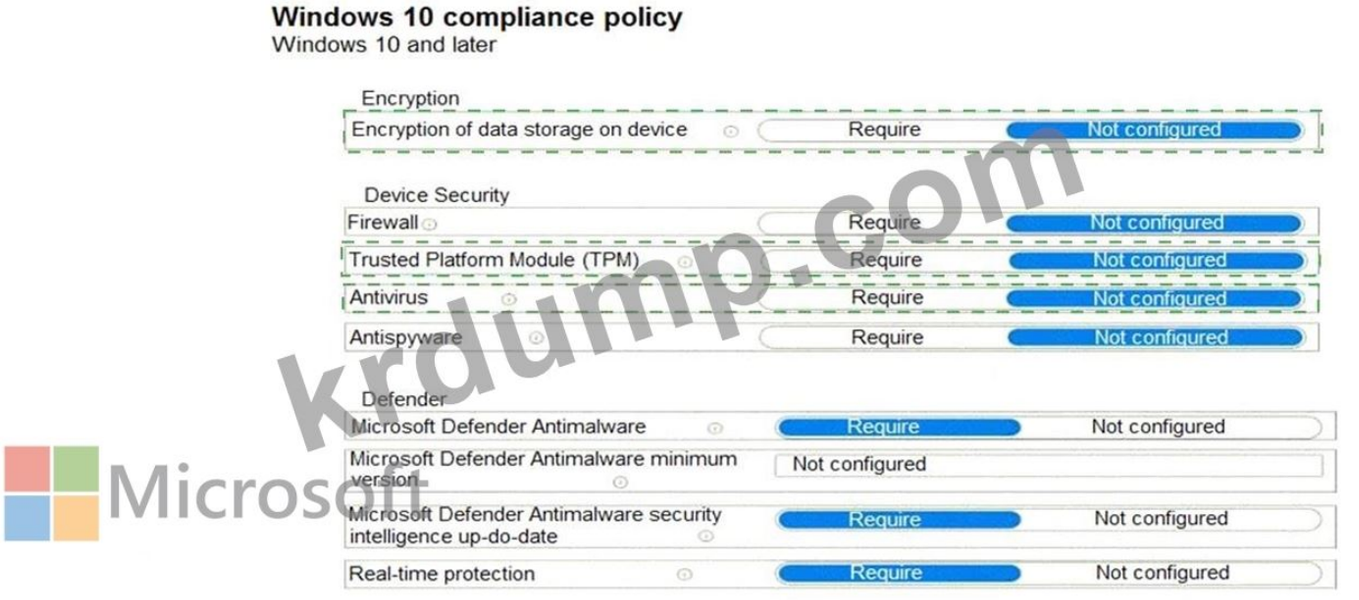
□□ □□□□ □□ □□□□ □□□ □□□□□.
□□ □□□ □□□ □□□□□ □□□□ □□□ □□□□ □□□.
□□ □□□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □ □□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

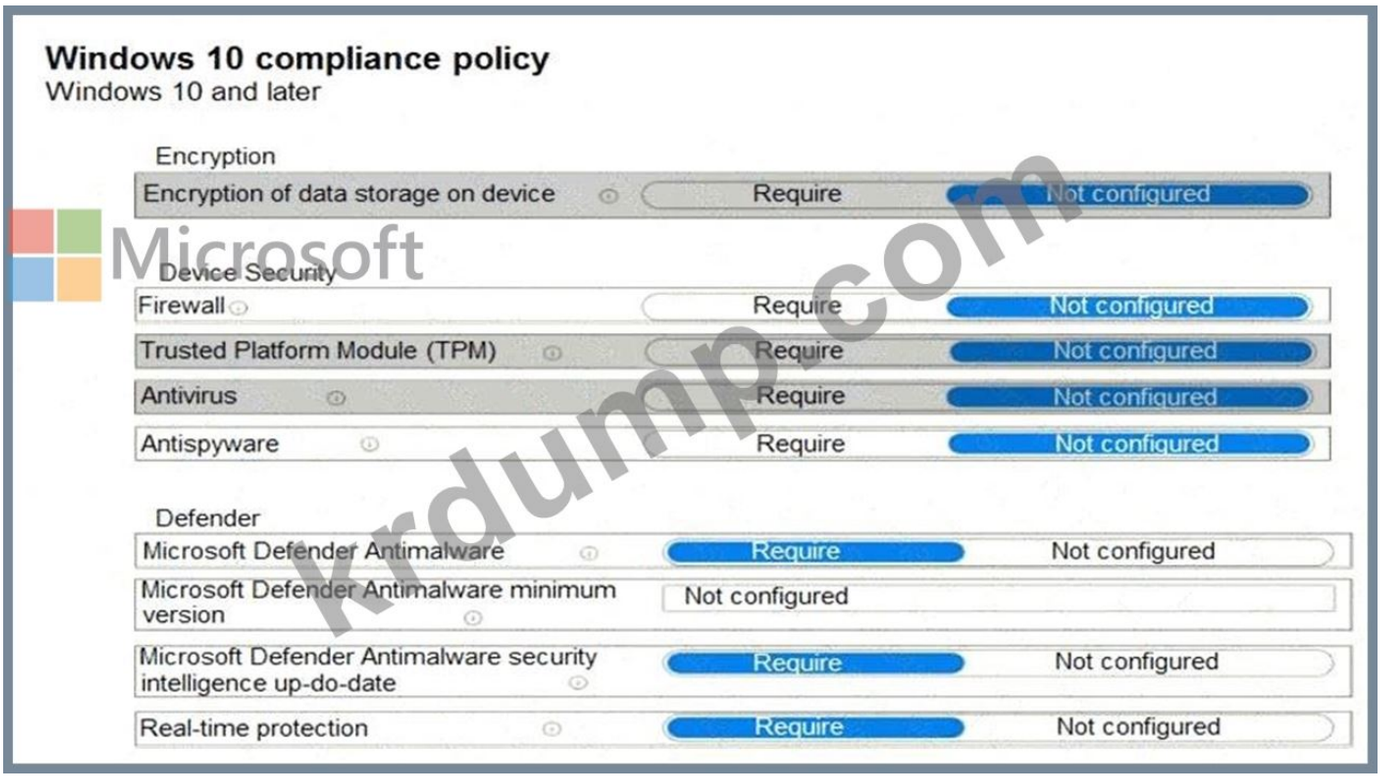


Answer:

Answer Area



Explanation:



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

NEW QUESTION: 197
□□ □ □□ □□ □□ □□□ □□□□ Microsoft 365 □□□ □□□□.
□□ □□ □□□□□ □□□ □□ □□□ □□ □□□ □□□□□.
□□ □□□□ □□□ □ □□ □ □□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□ □.
□□□□: □□□ 1□□ 1□□□□.
A. □□□□ □□ □□
B. □□□ □□ □□
C. □□ □□□ □□□□□
D. □□ □□□□
E. □□□□□ □□□□□.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 198

□□, □□, □□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Microsoft Entra ID Protection□ □□□□ □□□□.
□□ □□□□ □□□(VDI)□ □□□□. □□ VDI □□□ □□□ □□□□.
□□□□ □□□□ VDI□□ Microsoft 365□ □□□□□.
□□ VDI □□□□ □□ □□□ □□□□ □□ Microsoft 365□ □□□□ □ □□□ □□□□□.
VDI □□□□ Microsoft□ □□□□□ □□ □□ □□□ □□□□ □□□ □□□.
365. □□□□ ID □□□ □□□□ VDI □□□ □□□□ □□□□ □□□.
A. Microsoft 365□ ExpressRoute
B. □□□ □ □□ □□
C. □□□ □□□ □□
D. □□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 199
Endpoint□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□ □□□□.
Microsoft Defender for Endpoint□□ □□ □□ □□ □□ □□ □□□ □□□.
□□□□ File1.exe□□ □□□ □□□□□□ □□ □□□□ □□□.
A. □□ □□ □□□
B. □□□
C. □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 200
Microsoft Defender for Endpoint□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□□ □□□ □□ □□ □□ □ □□ □□□ □□□ □□□□□.
Device1□□□ □□□ □□□□ □□□□ □□□□ □□□□□.
□ □□□□ □□□ □□ □□□?
A. □□□ □□□□ □□□□□□ □□□□□.
B. Microsoft □□ □□□ - □□□ □□ □□□ □□□□□.
C. □□ □□□ □□□□□.
D. Defender for Endpoint□ Microsoft Intune□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 201
User1□□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□□□□ Microsoft 365 □□□ □□□□□□.
Cloud App Security □□ □□□□ □□ □□□ □□□ □□□ □□□□ □ □□□ □□□ User1 □□ □□□□□□ □□□□ □□□.
□□ □□: Azure Active Directory □□ □□□□ User1□□ □□ □□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□

B. □

Answer: B (LEAVE A REPLY)

NEW QUESTION: 202

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

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

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

A. User1□ User2□

B. □□□□!

C. User!□ User3□

D. User1, User2, User3

E. User2onry

Answer: D (LEAVE A REPLY)

NEW QUESTION: 203

Microsoft 365 □□□ □□□□.

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

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

□□ □□: Windows PowerShell□□ □□□ □□ □□□ □□ New-complianceSecurityFilter cmdlet□ □□□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: B (LEAVE A REPLY)

NEW QUESTION: 204

□□ □□ □□□ □□□ □□□ 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: 205
Microsoft 365 □□□ □□□□.
□□□ onmicrosoft.com □□□□ □□ □□ □□□□ □□□□ □□□. □□ □□□□ □□□□ □□□ □□□ □□ □□□□ □□□.
□□□ □□□ □ □□ onmicrosoft.com □□□□ □□ □□ □□□□□?

A. 1

B. 2

C. 10

D. 5

Answer: A (LEAVE A REPLY)

NEW QUESTION: 206
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□

□ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □ □□□□.
Windows 10□ □□□□ □□□□ □□□□.
□□□ Windows 10 □□□ □□□□ □□□.
□□ □□: □□ □□□ □□□□ □ □□□ □□□□ □□□□ □□□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 207

contoso.com□□□ Azure AD □□□□ □□□□ Microsoft 365 □□□ □□□□. □□□□□ □ □ □□ □□□ □□□□ □□□□ □□□□.
Microsoft Entra □□ □□□ □□□ □□□□□□ User1□ User2□ □□□□ □ □ □□ □□□?
□□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area

Explanation:

NEW QUESTION: 208

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

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

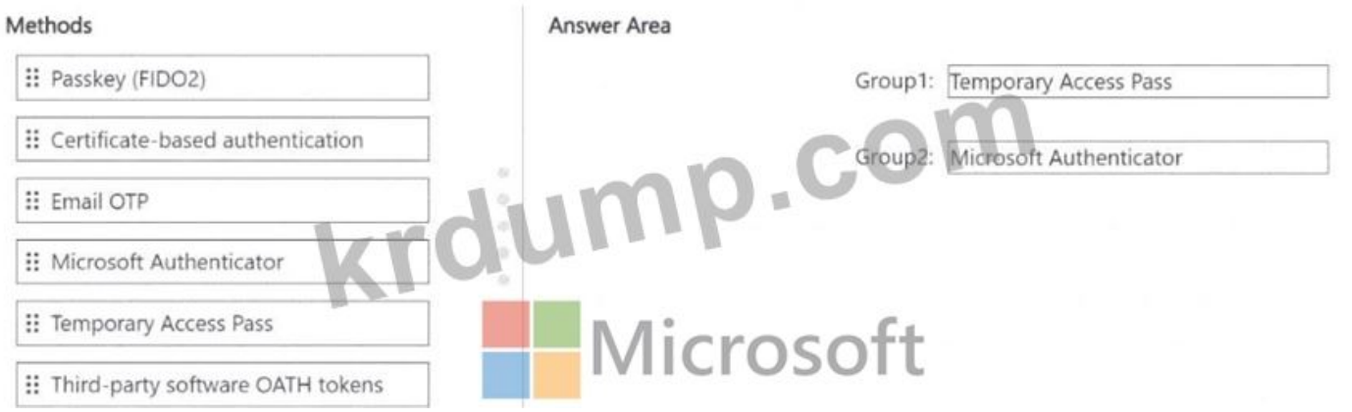
* □□2□ □□□□ □□ □ □□□(PKI)□ □□□□ □□□ □ □□□ □□□.

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

□□: □□ □□□ 1□□□□.

Answer:

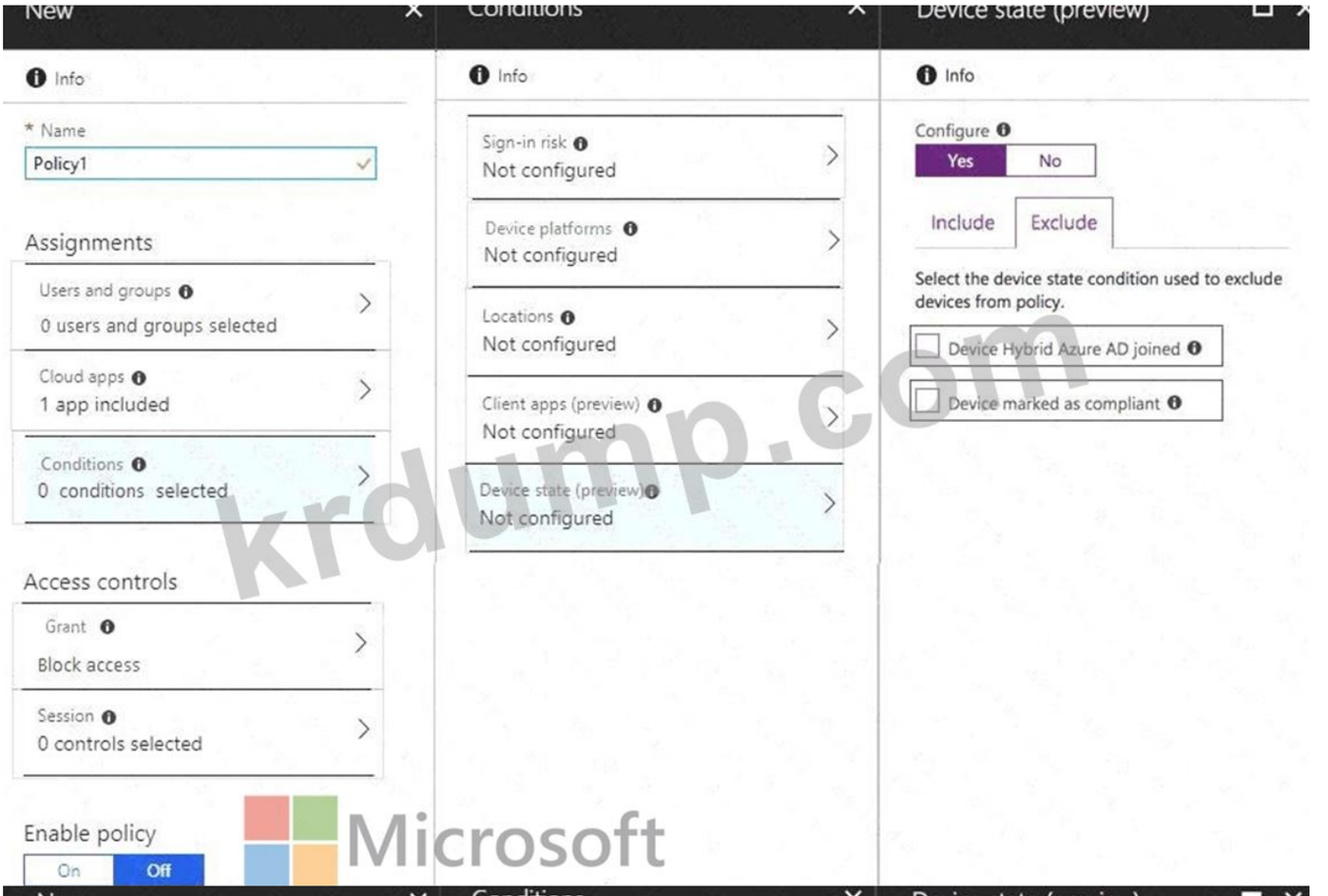
Explanation:

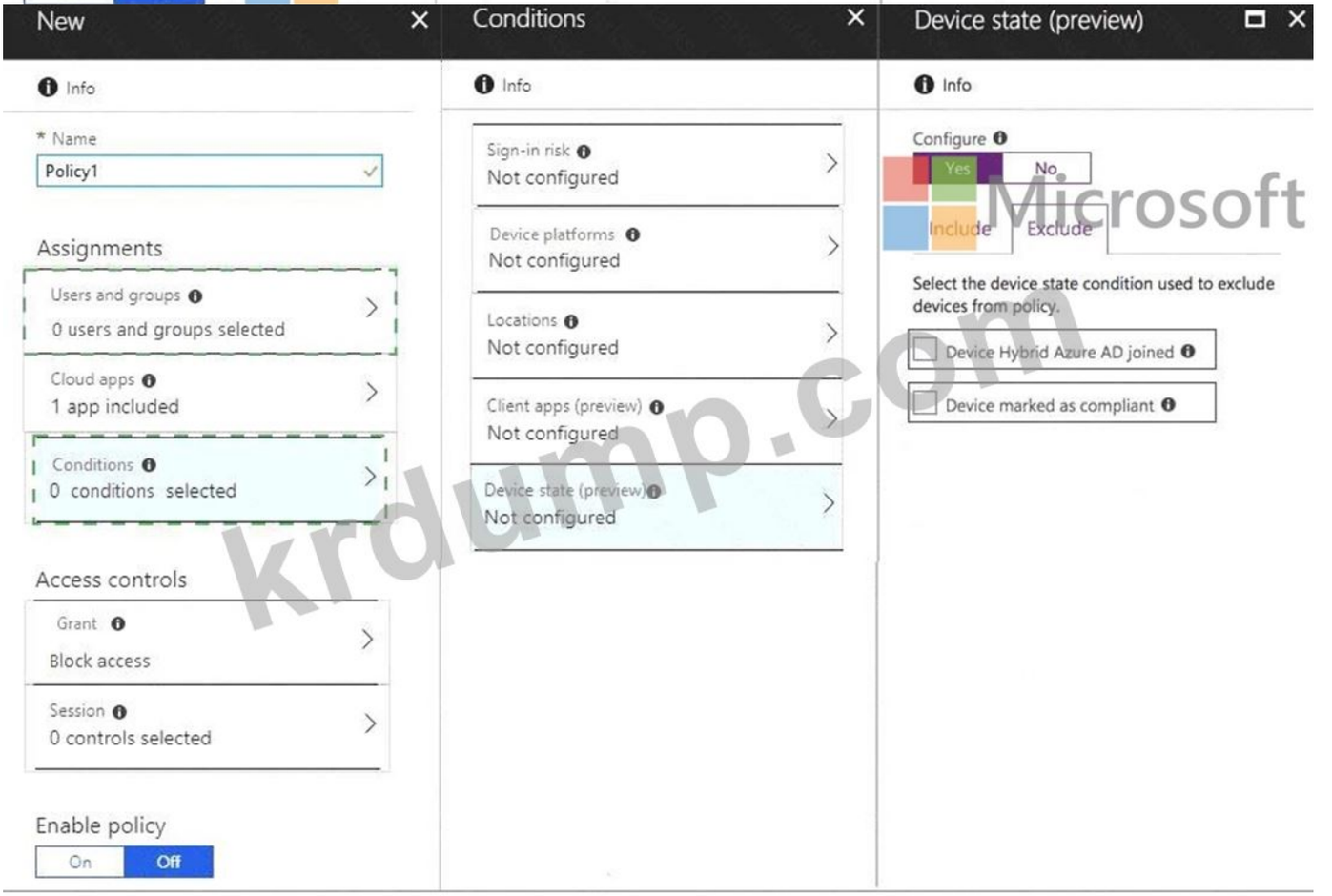


NEW QUESTION: 209
Microsoft 365 □□□ □□□□.
□□ □□□□□ Microsoft 365 Apps for enterprise □□□□□ □□□□□.
□□□□ Microsoft 365 □□ □□□□ □□□ □□□ □□ □□□ □□ □□□□□ □□ □□□.
Microsoft 365 □□ □□□□ □□□ □□□□ □□□?
A. □□□□ □□ □□ □□
B. □□□□
C. □□□ □□ □□
D. □□ □□ □□□□ □□ □□ □□
Answer: A (LEAVE A REPLY)

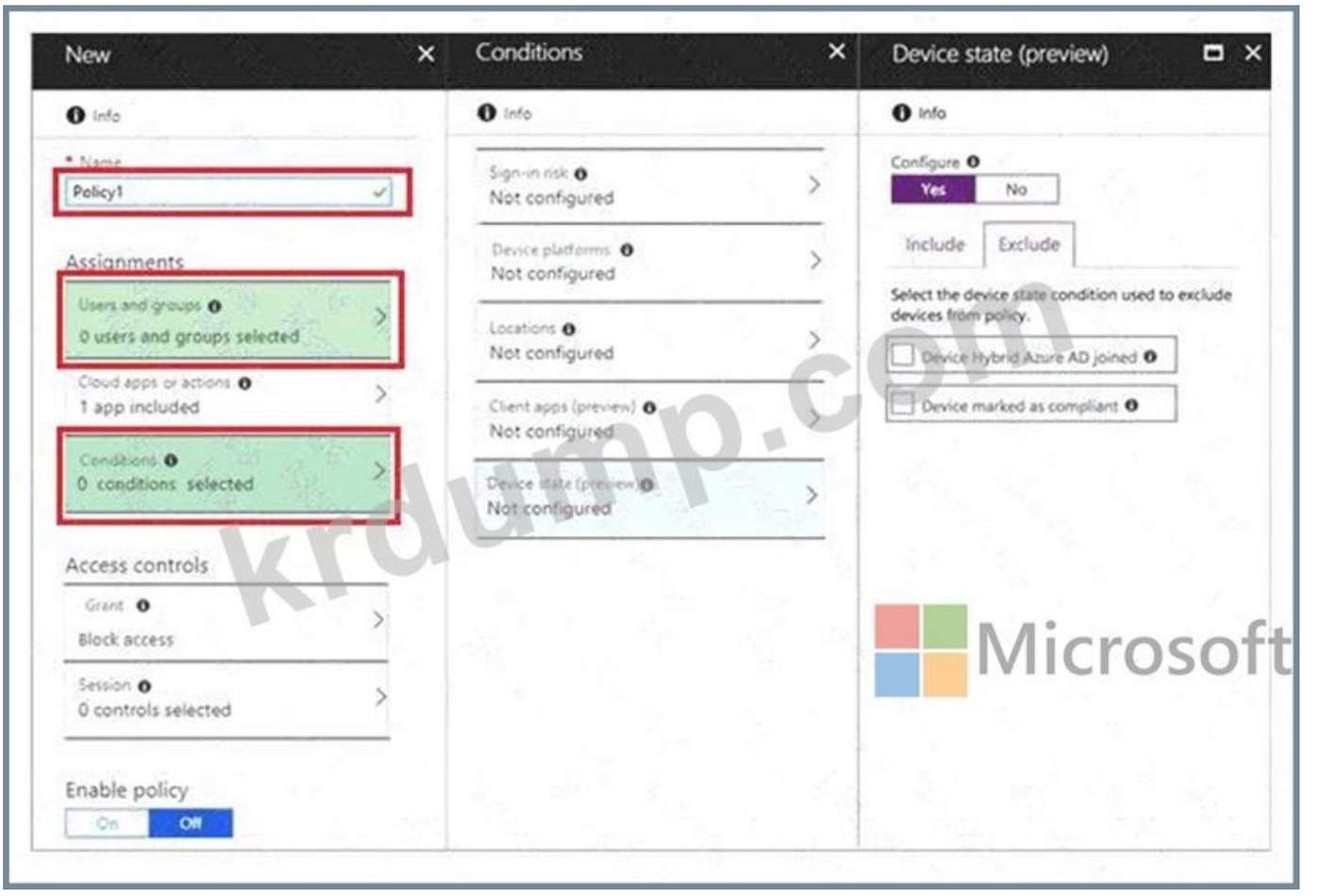
NEW QUESTION: 210
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □□ □□□ □□□□
Retention1□□□ □□□ □□ □□□□ □□□□.
User1□ □□□ □ □□ Retention1□ □□□□ □□□ □□□□ □□□□ □□□ □ □□□ □□ □□□.
Microsoft Exchange Online PowerShell□□ □□ cmdlet□ □□□□ □□□?
A. Start-MpScan
B. Start-AppBackgroundTask
C. Start-ManagedFolderAsslstant
D. □□ □□□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 211
□□ □□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□□ □□□.
Exchange Online□ □□□□ □□□ □□□□□.
Policy1□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.





Explanation:



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

Topic 2, A. Datum

Case 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: 212
Microsoft Defender for Endpoint□ Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□ □.
□□ □□□ Windows 11□ □□□□ Microsoft Entra□ □□□□ □□□□.
□□□□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□ □□□ □□□□ Intune □□□□□ □□□ □□ □□□ □□ □□□ □□□□ □□ □□□.
□□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. □□ □□□□ □□□ □□ □□□ □□□□□.
B. □□□ □□□□ □□ □□ □□□ □□□.
C. □□ □ □□□□ □□ □□□ □□□□□.
D. □□□ □□ □□□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 213
Microsoft 365 □□□ □□□□.
Microsoft Exchange Online □□□ □□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□. □ □□ □□ □□□?
A. Exchange □□ □□□□ □□□□ □□□□.
B. Microsoft 365 □□ □□□□ □□ □□□ □□□ □□□□□□□.
C. Microsoft 365 □□ □□□□ □□□ □□ □□□ □□□ □□□□□.
D. Microsoft Outlook □□□□□□□ □□ □□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 214
Microsoft 365 F5 □□□ □□□□.
100□□ □□□ Windows 10 □□□ □□□ □□□□□.
□□□ □□□ □□□ Windows 10 □□□ □□□□ □□□. □□□ □□ □□ □□□ □□□□ □ □□.
□□ 24□□ □□ □□□□ □□□□.
Microsoft □□□□□□ □□□(App-V) □□
□□ □□□ □□□□ □□□?
A. □□□ 10 □□, □□ 1909
B. □□□ 10 □□, □□ 2004
C. □□□ 10 □□, □□ 1909

D. Windows 10 Enterprise, □□ 2004

Answer: D (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/windows/release-health/release-information

https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported-configurations