Microsoft.MS-102-KR.v2026-06-01.q252

□□□□:	MS-102-KR
□□□□:	Microsoft 365 Administrator (MS-102 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	252
□□:	v2026-06-01
# □□ □:	177
# □□ □□□:	2520
https://www.krdump.com/Microsoft.MS-102-KR.v2026-06-01.q252.html	

NEW QUESTION: 1
□□□ □□□□ □□□ Microsoft SharePoint Online □□□□□ □□□□ □□□ □□□ □ □□□ □□□□□ □□□ □□□. □□□ □□ □□□?
A. Microsoft Purview □□ □□ □□□□ DLP(□□□ □□ □□) □□□ □□□□.
B. SharePoint Online □□□□□ □□□ □□□□.
C. Microsoft 365 Defender □□□□ □□ □□□ □□□□.
D. SharePoint Online □□ □□□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
□□ □□ □□□ □□□□ □□□□ Azure AD □□□□ □□□□.

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Exchange Administrator

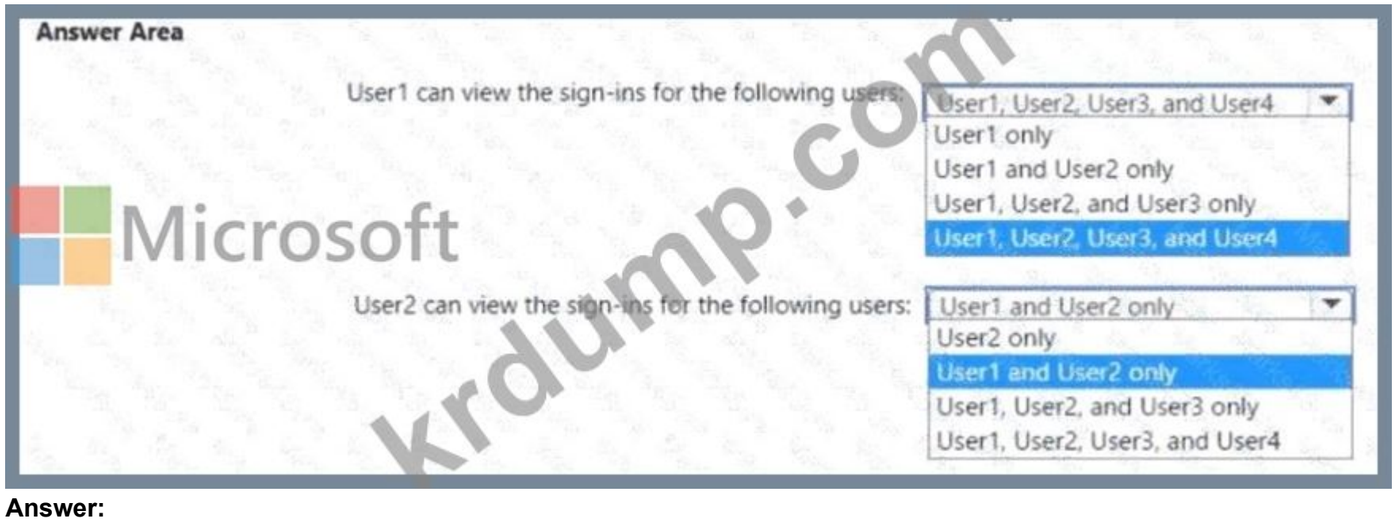
□ □□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□ □□□ □□□□ □□□?
A. Microsoft 365 □□ □□
B. Microsoft Purview □□ □□ □□
C. Microsoft 365 Defender □□1
D. Microsoft Entra □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
Microsoft 365 E5 □□□ □□□□.
Endpoint□ Microsoft Defender □□□□ □□□□ □□□.

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

NEW QUESTION: 4
Microsoft Defender for Endpoint□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□□ □□□ □□ □□ □□ □ □□ □□□ □□□ □□□□□.
Device1□□□ □□□ □□□□ □□□□ □□□□ □□□□□.
□ □□□□ □□□ □□ □□□?
A. Microsoft □□ □□□ - □□□ □□ □□□ □□□□□.
B. Defender for Endpoint□ Microsoft Intune□ □□□□□.
C. □□ □□□ □□□□□.
D. □□□ □□□□ □□□□□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
contoso.com□□□ Azure AD □□□□ □□□□ Microsoft 365 □□□ □□□□. □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.
Microsoft Entra □□ □□□ □□□ □□□□□□ User1□ User2□ □□□□ □ □ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

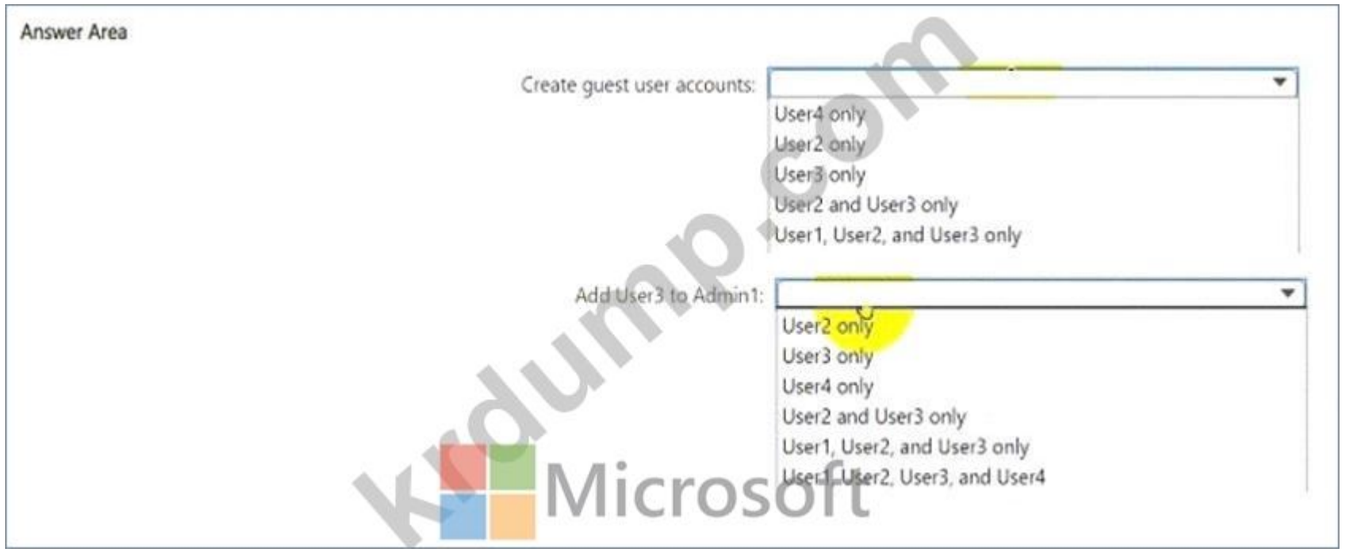
Explanation:

NEW QUESTION: 6

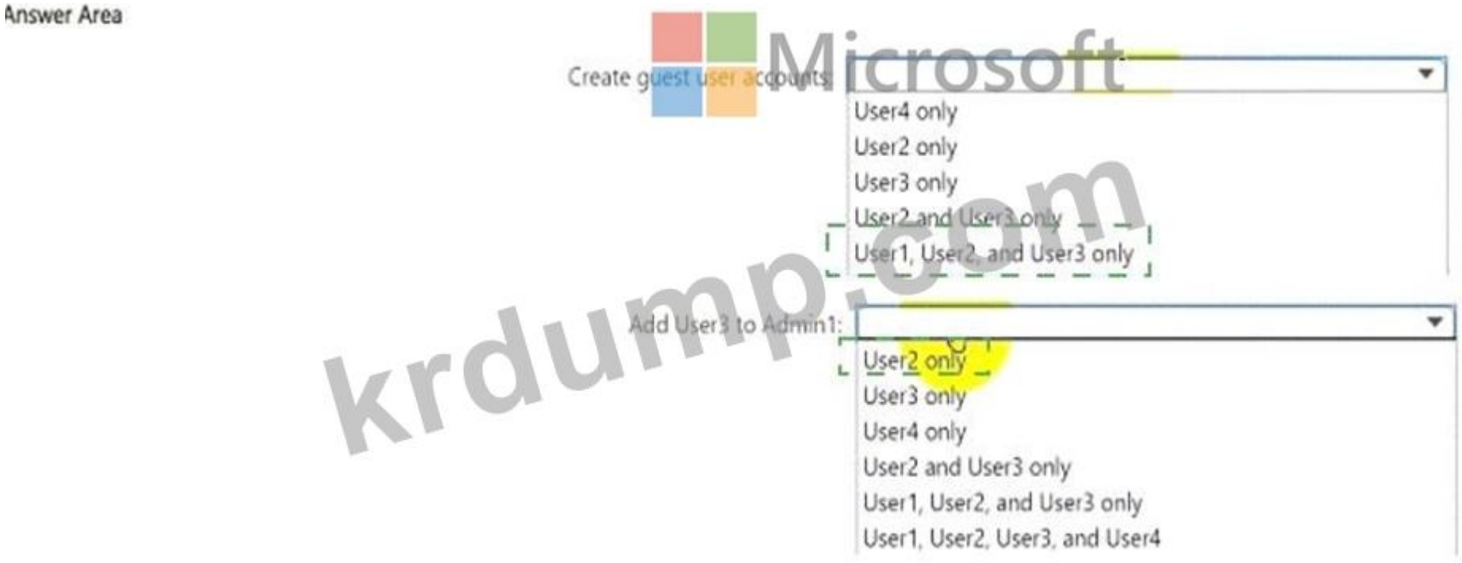
□□□ □□□□ □□ □□ □□ □□ □□□□ □□□ Microsoft Entra □□□□ □□□□.

Name	Role
User1	Privileged Role Administrator
User2	User Administrator
User3	Security Administrator
User4	Billing Administrator

□□□□□ Admin1□□□ □□ □□□ □□□□□. Admin1□ □□ □□□ □□□□ □ □□□□□. □□ □□ □□□□ □□ □□□ □□□□.
□□ □□ □□□ □□□ □ □□ □□□□ □□□□ □□□.



Answer:



Explanation:
Create guest user accounts: User1, User2, and User3 only
User1: Privileged Role Administrator role has the ability to manage role assignments in Azure AD, including creating guest accounts.
User2: User Administrator role can manage user accounts, including creating guest accounts.
User3: Security Administrator role does not typically include permissions for creating guest accounts, but in some configurations, they might have limited guest user management capabilities.
Add User3 to Admin1: User2 only
User2: User Administrator role has the permissions to add users to security groups like Admin1.

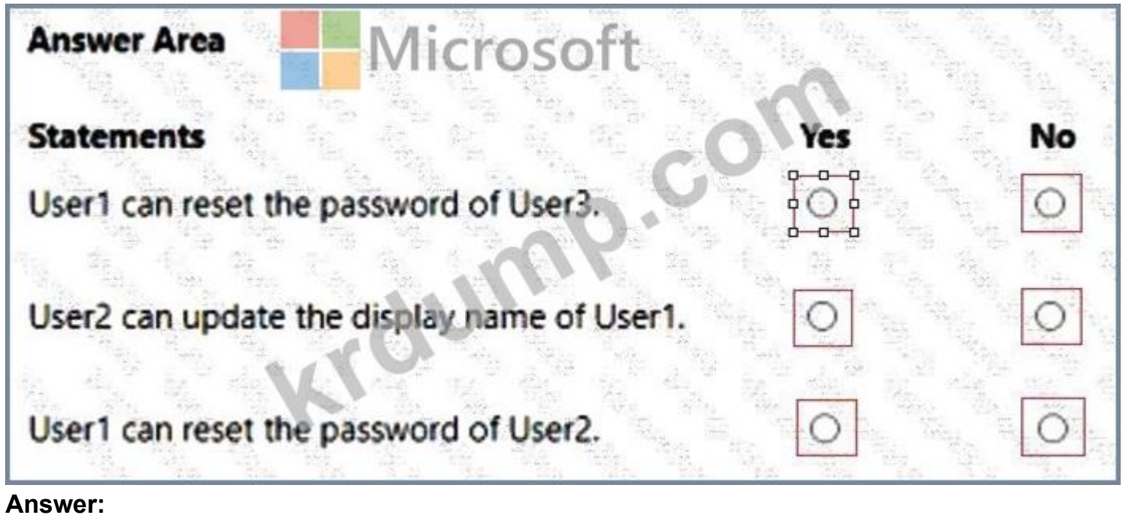
NEW QUESTION: 7

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
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: 8
□□□
□□ □□ □□□ □□ □□□ □□□ Azure AD □□□□ □□□□.

Name	Members
AU1	User1, User2
AU2	User3

□□□ □□ □□□□ □□□□:
* AU1 □ AU2□ □□□□ □□□□ □□□ User1□□□ □□□□□□.
* AU1□ □□□ □□□□ □□□ User2□□ □□□□□□.
* □□□□ □□□ □□□□ □□□ User3□□□ □□□□□□.
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

Box 1: No

User1 is assigned the Password Administrator for AU1 and AU2.

User3 is in AU2. User3 is User Adminstrator.

Password administrators cannot reset User Administrators passwords.

Note: Password Administrator

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

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

Box 2: Yes

Box 3: No

User1 is assigned the Password Administrator for AU1 and AU2.

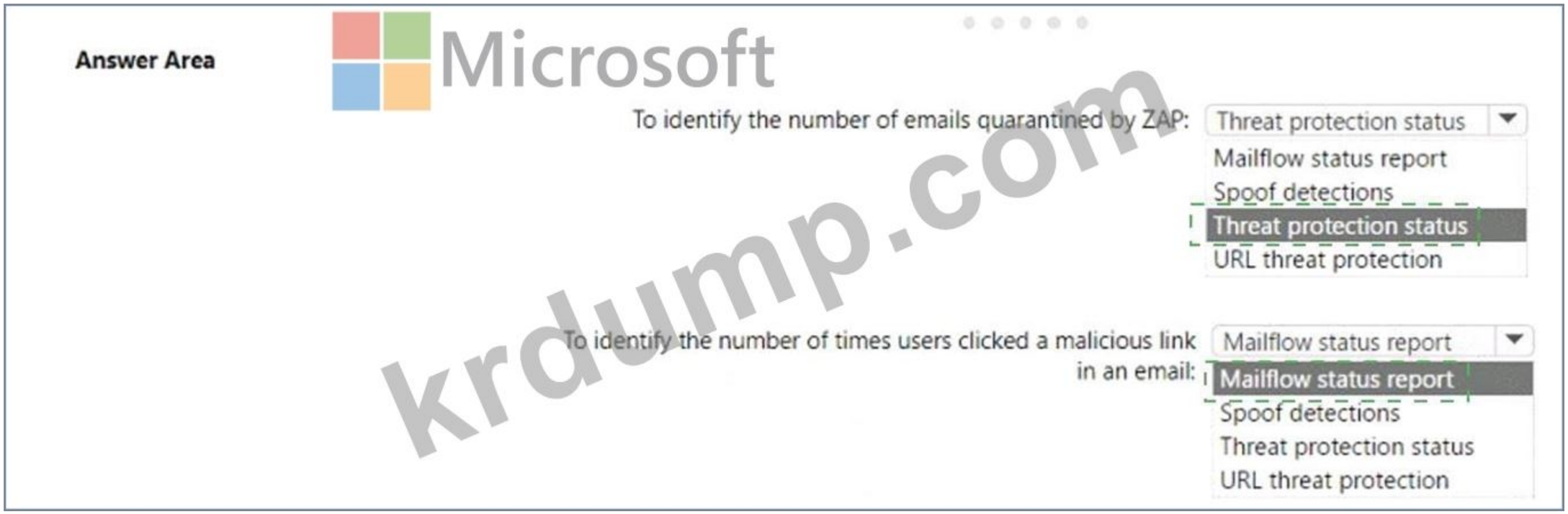
User2 is in AU1. User2 is User Adminstrator.

Password administrators cannot reset User Administrators passwords.

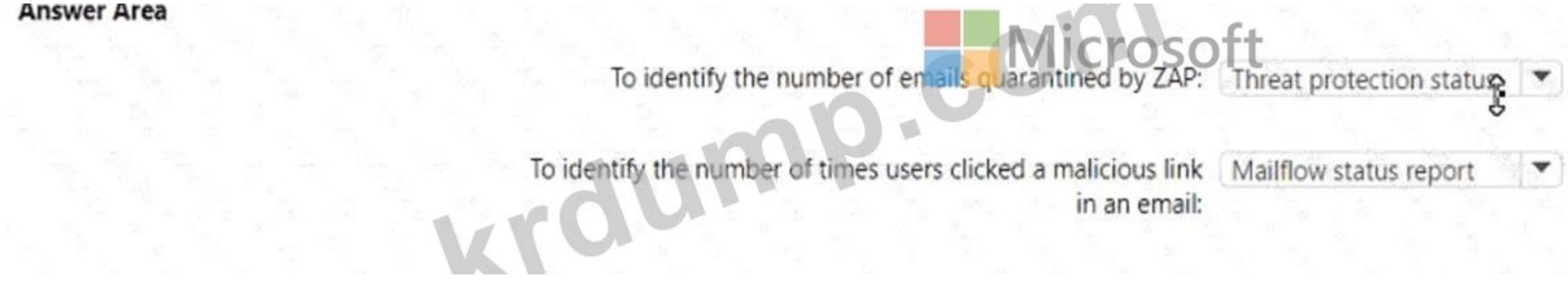
Note: User Administrator
Can manage all aspects of users and groups, including resetting passwords for limited admins.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

NEW QUESTION: 9
Office 365□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□□ □□ □□ □□ □□ □□□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□□□.
□□ □□□ □□□□ □□□.
* ZAP(□□□□ □□ □□)□ □□□ □□□ □□□ □
* □□□□ □□□ □□□□□ □□ □□□ □□□ □□ □□ □□□ □ □□ □□□□ □□□□ □□□? □□□□ □□□□ □□□ □□□ □□□□□□. a. □□: □ □□□ 1□□□□.

Answer:



Explanation:



NEW QUESTION: 10

□□□

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

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

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


Settings > Endpoints > computer1
computer1
Microsoft
Device summary
Risk level
None
Device details
Domain
adatum.com
OS
Windows 10 64-bit
Version 21H2
Build 19044.2130

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

Answer Area

Computer1 will be a member of **[answer choice]**.

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of **[answer choice]**.

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

Answer:

Answer Area

Computer1 will be a member of **[answer choice]**.

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of **[answer choice]**.

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

Explanation:

Answer Area

Computer1 will be a member of **[answer choice]**.

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of **[answer choice]**.

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

Box 1: Group3 and Group4 only
Computer1 has no Demo Tag.
Computer1 is in the adatum domain and OS is Windows 10.
Box 2: Group1, Group2, Group3 and Group4

NEW QUESTION: 11
Sitel□□□ Microsoft SharePoint □□□□ □□□ Microsoft 365 E5 □□□ □□□□. Site!□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Number of IP addresses in the file
File1	2
File2	3

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

Name	Content contains	Policy tip	If there is a match, stop processing	Priority
Rule1	3 or more IP addresses	Tip1	No	0
Rule2	1 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

Site1□ DLP1□ □□□□□.
□ □□□ □□ □□ □□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 12

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

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

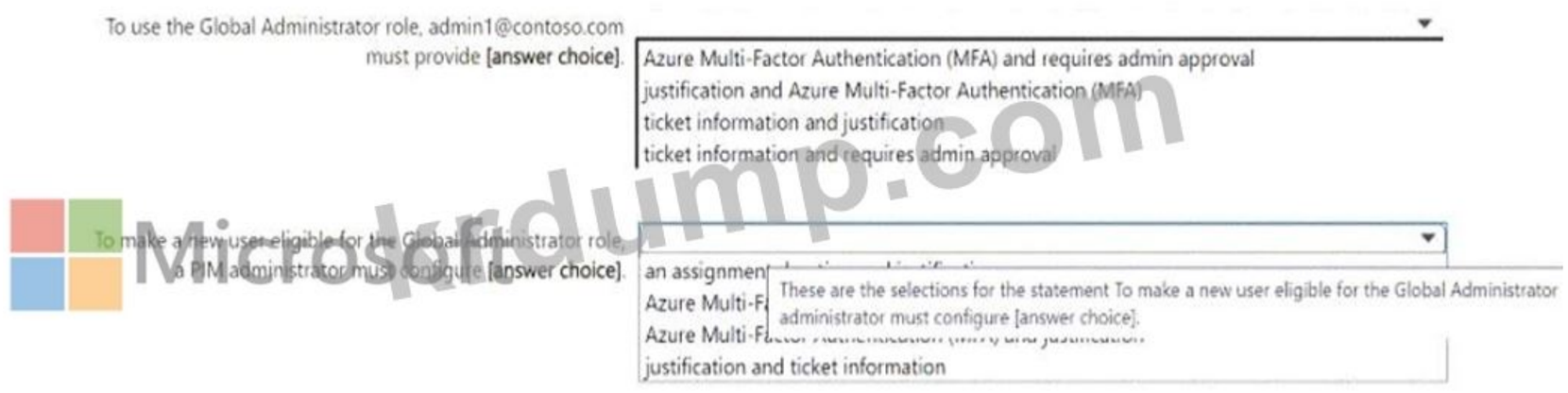
User5□□ □□ □□□□ □□□ □□□ □□□ □□□□□.
User5□ □□□ □ □□ □ □□ □□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □ □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. User2□ User4□ □□□□□.
B. User4□ □□□□□ □□□□□□.
C. Azure AD□ □□ □□□□ □□□□□ □□□□□□.
D. User1, User2, User4□ □□□□□.
E. User2□ User4□ □□□□□ □□□□□□.
F. Azure AD□□ □□ □□□□ □□□□□.
Answer: A,E (LEAVE A REPLY)
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: 13
Microsoft 365 □□□ □□□□.
Microsoft Entra Privileged Identity Management(PIM)□□ □□ □□□ □□ □□□ □□□ □□□ □□ □□ □□□ □□□□□.

admin1@contoso.com□□□ □□□□ □□□ □□□ □□□ □□□□ □□□□.

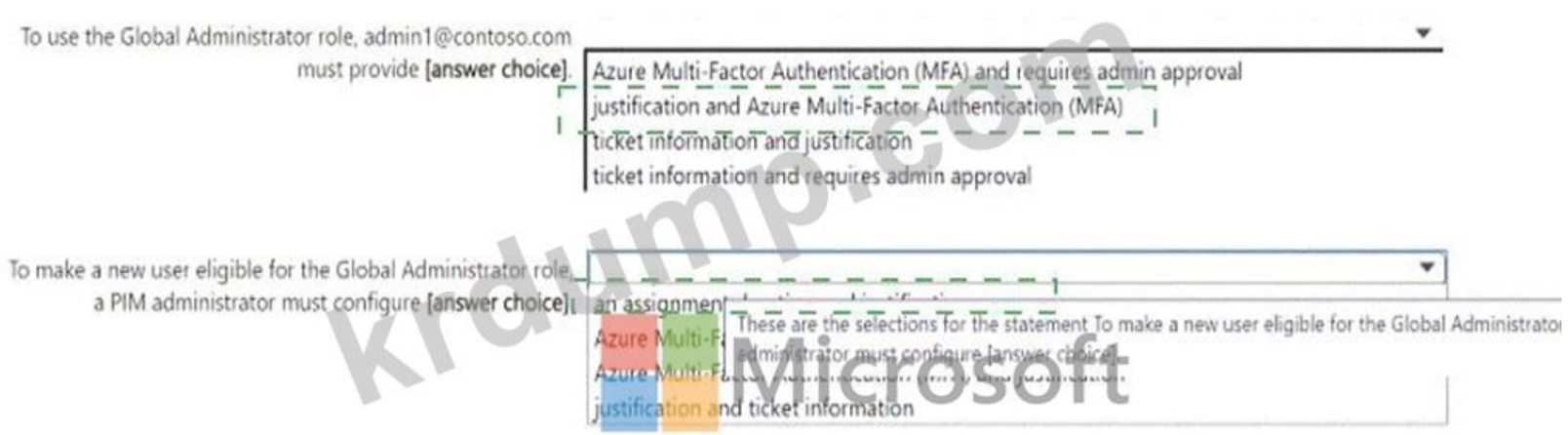
□□□ □□□ □□□□ □ □□□ □□□□ □□ □□□ □□□□□ □□□□ □□□ □□□□□□.

Answer Area



Answer:

Answer Area



Explanation:

To use the Global Administrator role, admin1@contoso.com must provide: Azure Multi-Factor Authentication (MFA) The role settings indicate that " Require Azure Multi-Factor Authentication " is set to " Yes " for active assignments. Therefore, admin1@contoso.com must provide Azure MFA to use the Global Administrator role.

To make a new user eligible for the Global Administrator role, a PIM administrator must configure: an assignment that expires after 15 day(s) The settings show that eligible assignments expire after 15 days. Therefore, to make a new user eligible, a PIM administrator must configure an assignment with this expiration period.

NEW QUESTION: 14

□□□ □□□□ □□□ □□□ □ □□□□□□□ □□□□.

Microsoft Defender Advanced Threat Protection(Microsoft Defender ATP)□ □□□ □□□ □□ □□□□□ □□□ □□□ □□□□ □□ □□□□ □□□ □□ □□□.

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

A. □□□ □□ □□ □□

B. □□/□□ □□ □□

C. □□ □□ □□

D. □□□

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage- indicators

NEW QUESTION: 15

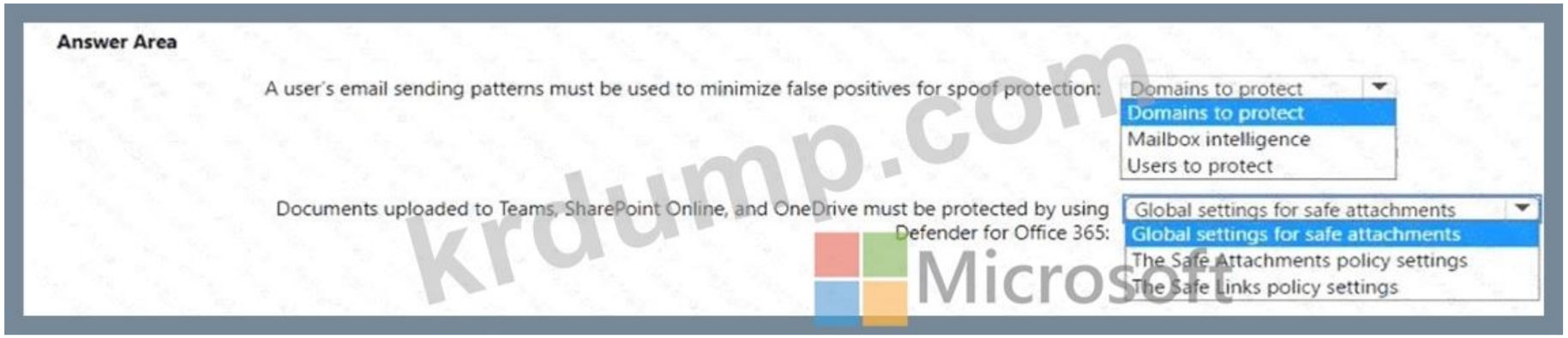
Microsoft 365 E5 □□□ □□□□.

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

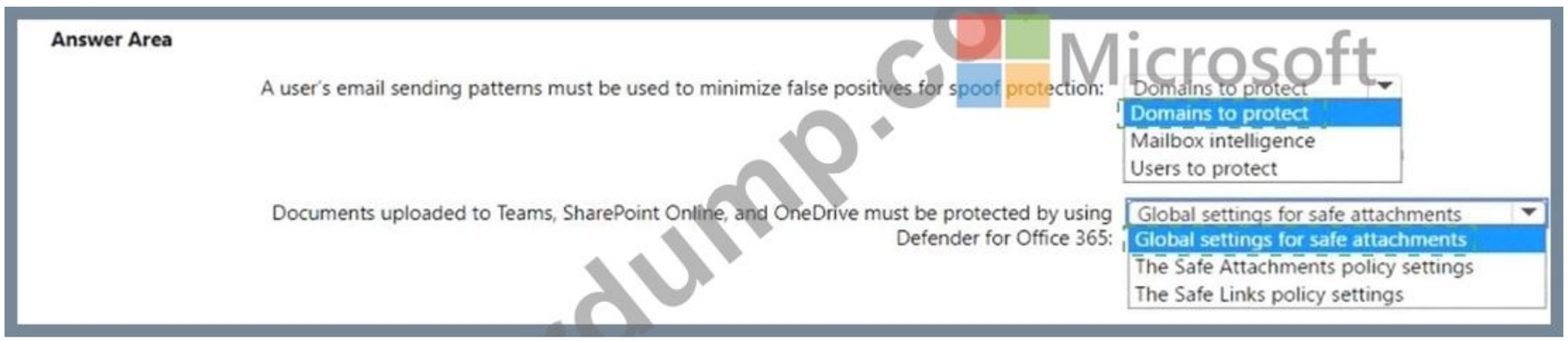
* □□□□ □□□ □□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□□ □□□.

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

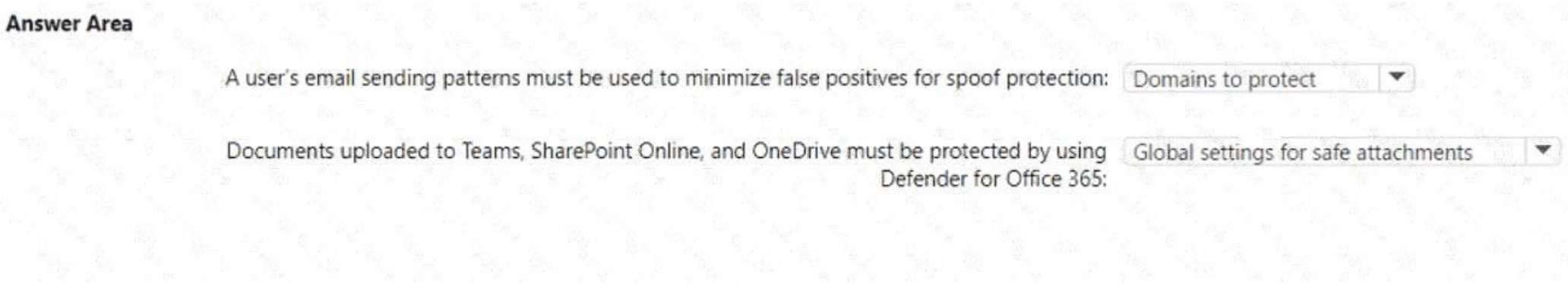
□ □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□□□ □□□ □□□ □□□□□□. □□: □ □□□ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 16

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

□□ □□ □□ □□ □□□□.

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

Microsoft Endpoint Manager□ □□□□ □□□□ □□ □□□ □□□□□.
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

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

Answer:

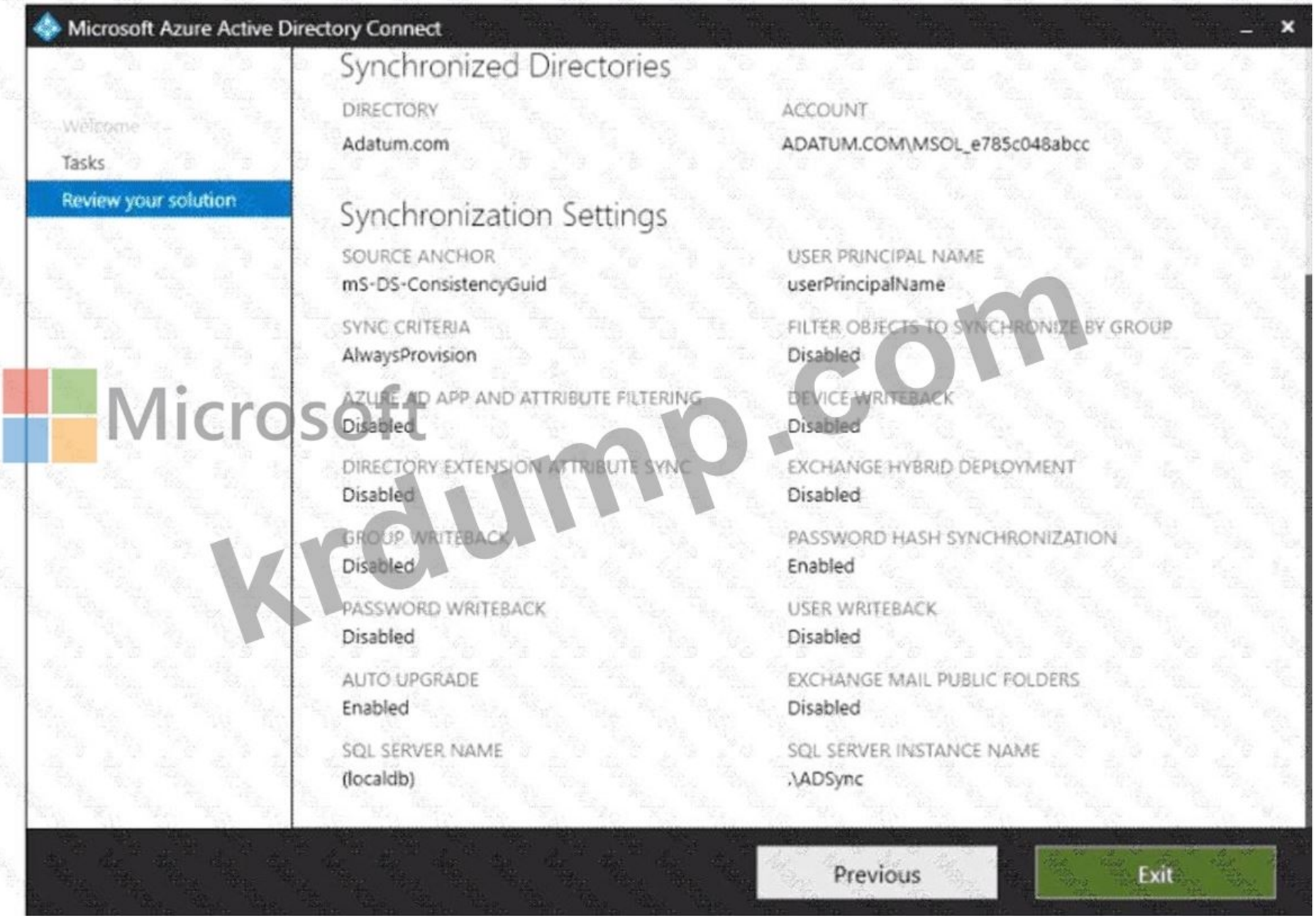
Statements	Yes	No
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

Explanation:

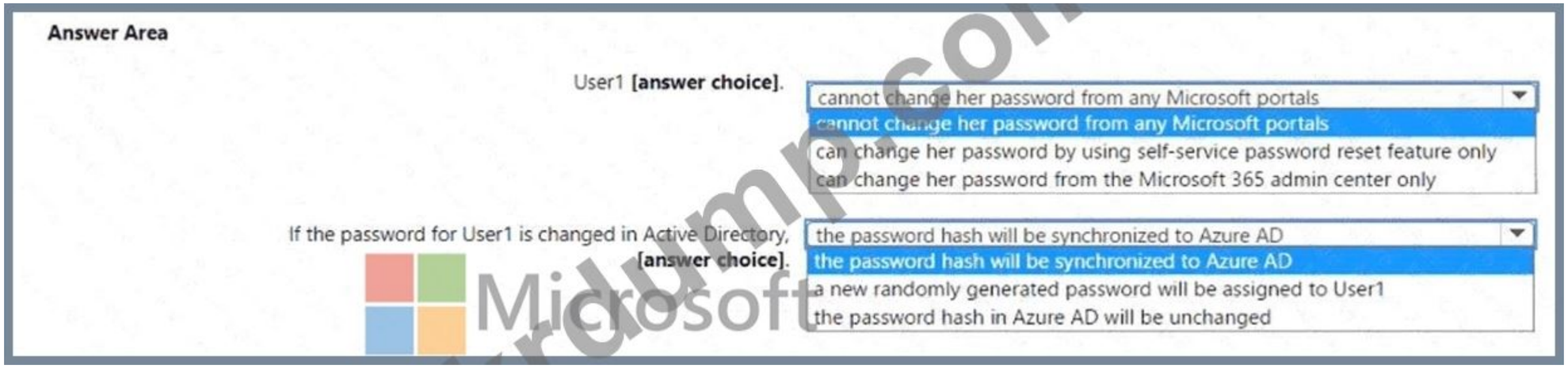
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy
https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy

NEW QUESTION: 17
Microsoft 365 □□□□ □□□□.
Microsoft 365 □□ □□□ □□□□ □□□□ □□□□□ □□□ □□□□□.
Microsoft 365 □□ □□□ □□□□ □□□□□ □□ Microsoft □□□ □□□ □□□□□?
A. Microsoft □□□□ □ □□
B. Azure □□□
C. Azure □ □□□□□□ □□□
D. Azure □□□
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

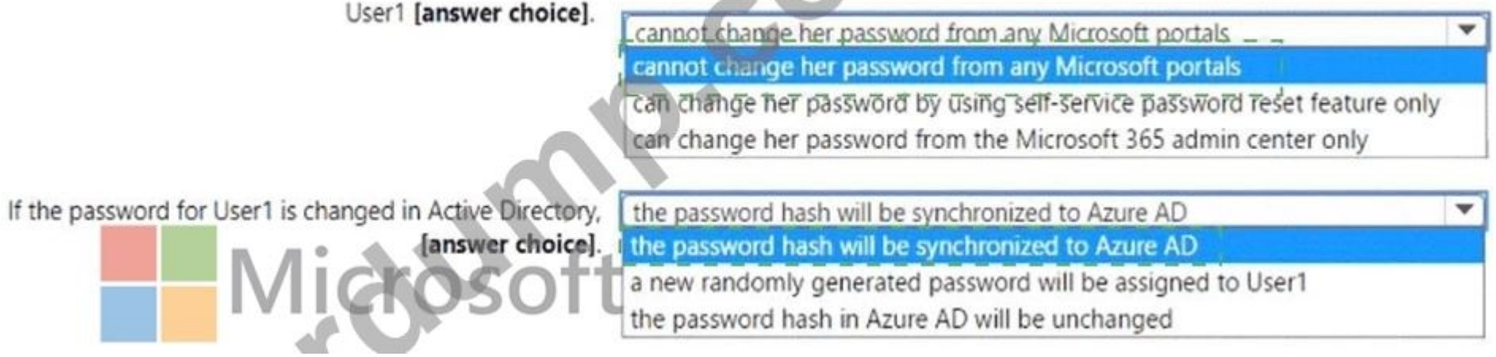
NEW QUESTION: 18
□□□ Microsoft 365□ □□□□□□ □□□□□□.
User1□□□ □Ł□□□□ □□□□ Azure AD□ □□□□□□.
Azure AD Connect□ □□ □□□ □□ □□□□□.



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



Answer:



Explanation:

NEW QUESTION: 19

Microsoft 365 E5 □□□ □□, □□□□ □□ Microsoft Defender□ □□□□ □□□□. OAuth □ □□□ □□ □ □□□ □□□□ □□□.

□□ □□: Defender for Cloud Apps□ API □□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 20

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□□□□.

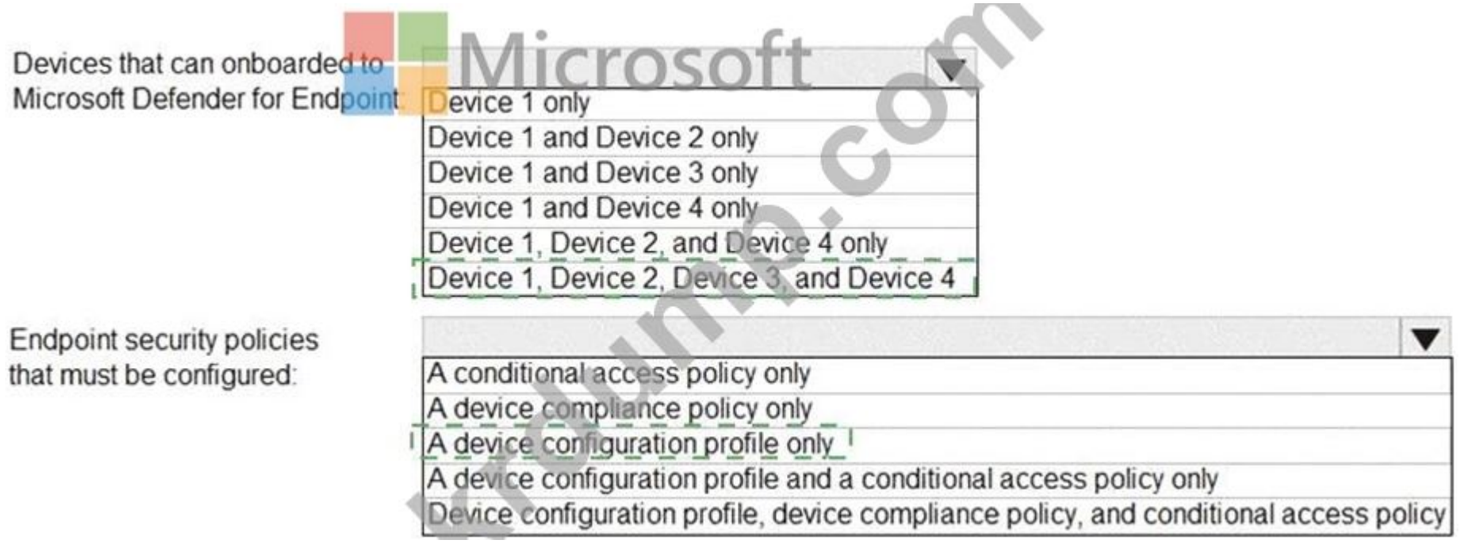
Devices that can onboarded to Microsoft Defender for Endpoint:

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

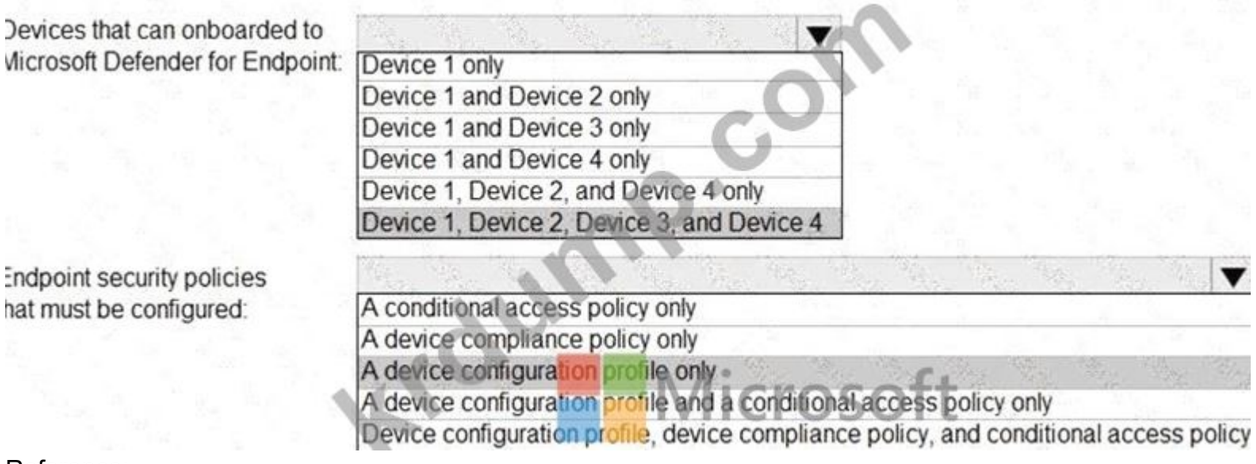
Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?view=o365-worldwide

NEW QUESTION: 21
Microsoft Defender for Endpoint□ □□□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□. Microsoft Defender for Cloud Apps□ Defender for Endpoint□ □□□□□. □□ 30□ □□ □□ □□ □□□ □□ □□ □□ □□□□ □□□□ □□□. □□□ □□ □□□?
A. □□ □□ □□ □□□ □□
B. Cloud Discovery □□ □□□ □□
C. □□ □□ □□ □□□ □□□□.
D. Cloud Discovery □□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)

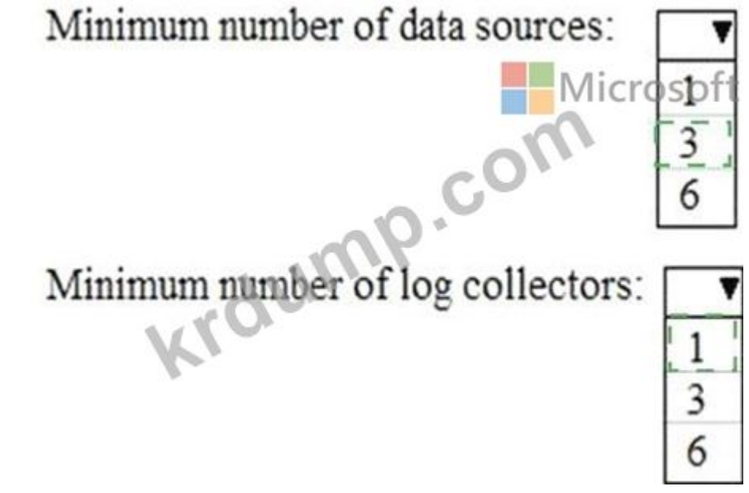
NEW QUESTION: 22

□□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□.

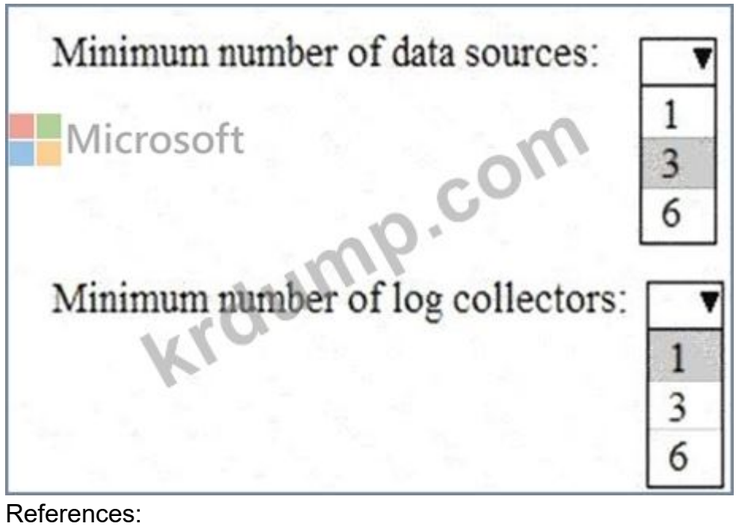
Microsoft Cloud App Security□□ □□□□ □□ □□ □□□ □□ □ □□ □□□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:



Explanation:



References:

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

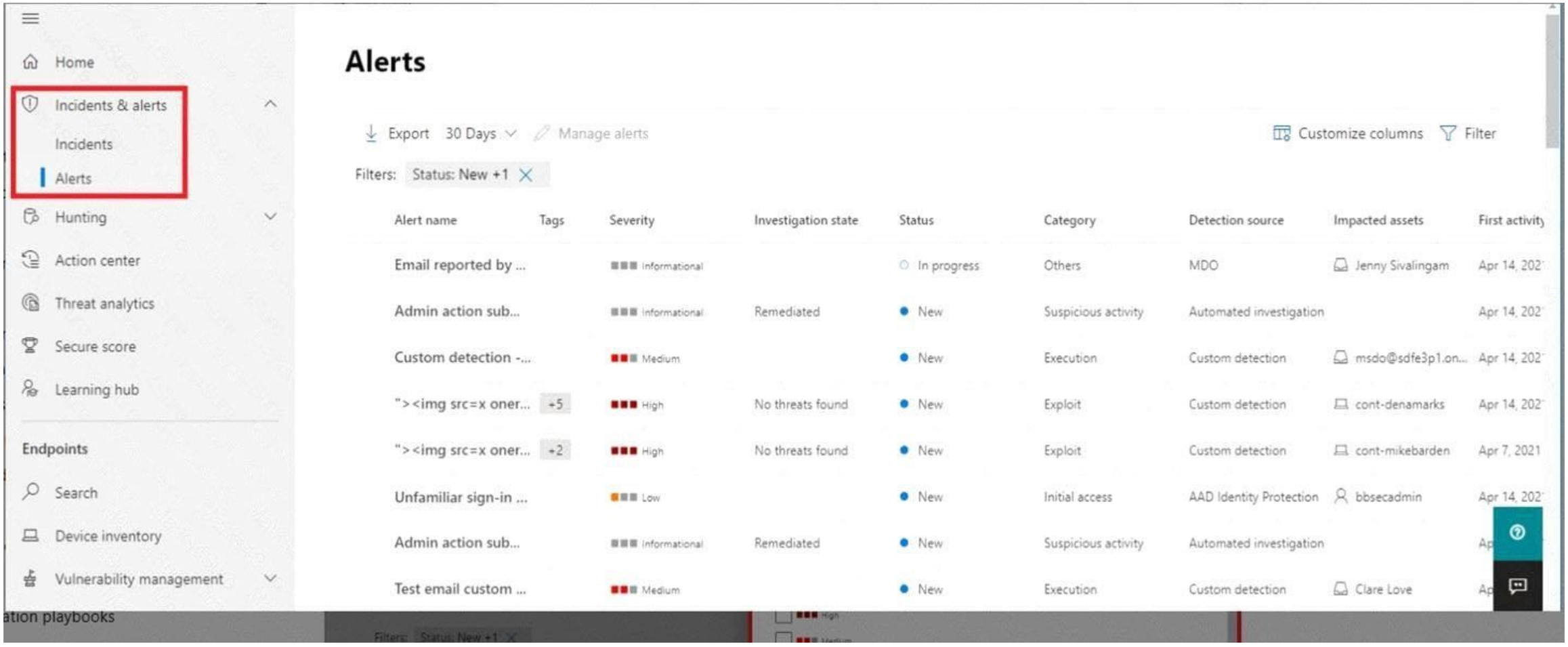
NEW QUESTION: 23
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□□1□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□□.
□□□ □□□ □□□□ User1□ □□□□ □□□.
□□□ □□□□ □□□?
A. Exchange □□ □□
B. Microsoft Purview □□ □□ □□
C. Microsoft 365 □□ □□
D. Microsoft 365 Defender □□
E. Microsoft Entra □□ □□
Answer: (SHOW ANSWER)
Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.
Remove a user from the Restricted entities page in the Microsoft 365 Defender portal In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use https://security.microsoft.com /restrictedentities.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted- users-portal-after-spam

NEW QUESTION: 24
Microsoft 365 IS □□□ □□ Microsoft Defender for Cloud Apps□ □□□□□. Microsoft Entra 10□□ App1□□□ □□□□ □□ □□□□□. Appl□ □□ □□□ □□□ □□□□ □□□. □□ □□□ □□ □ □□?
A. □□□□ □□ Defender□ □□ □□ □ □□□ □□(SIEM) □□□□□ □□□□□.
B. □□□□ □□ Defender□ □ □□□□ □□□□□.
C. App1□ □□□ □□□ AppControl□ □□□□□.
D. App1□ □□ □ □□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 25
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□ □□ Microsoft 365 □□ □□ □□□ □□□ □□□□□.
□□ □□ □□(PII)□ □□□ Microsoft Teams □ SharePoint Online□ □□□ □□□ □□□□□.
PII□ □□□ □□ □□□ □□ □□□□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□□ □□ □□(DLP) □□
C. □□ □□
D. Microsoft Cloud App Security □□
Answer: B (LEAVE A REPLY)
Reference:

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

NEW QUESTION: 26
Microsoft 365 Defender □□□□ □□□ □□□□ □□□□.
□□□ □□□ □□□ □□□□ □□□□□?
A. 30□
B. 60□
C. 3□□
D. 6□□
E. 12□□
Answer: C (LEAVE A REPLY)
Data retention information for Microsoft Defender for Office 365
By default, data across different features is retained for a maximum of 30 days. However, for some of the features, you can specify the retention period based on policy. See the following table for the different retention periods for each feature.
Defender for Office 365 Plan 1
* Alert metadata details (Microsoft Defender for Office alerts)
90 days.
Note: By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the top of the list so you can see it first.



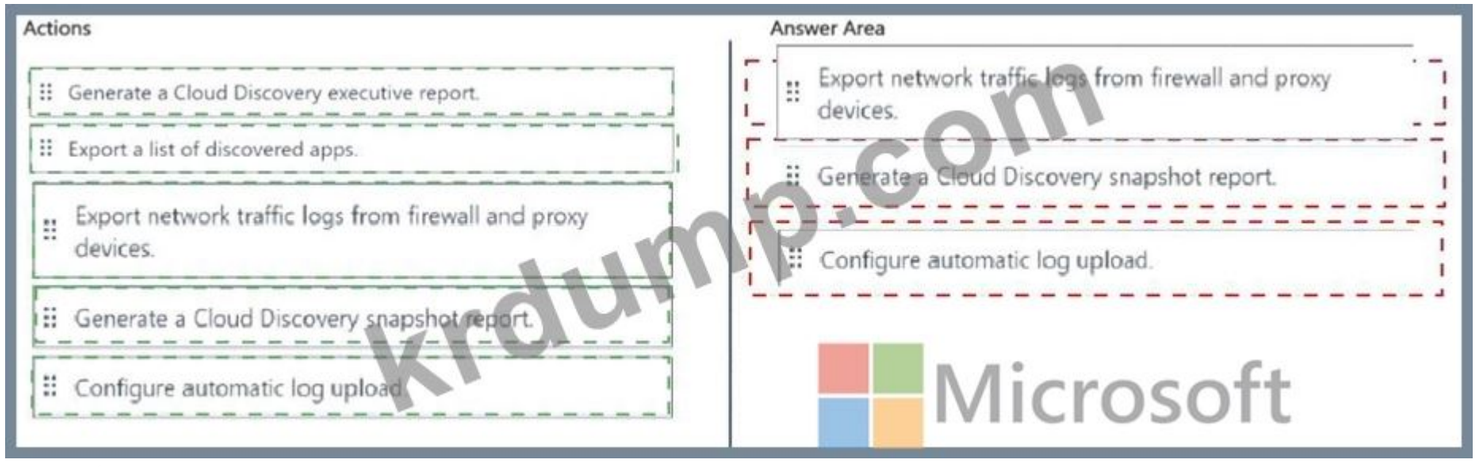
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention

NEW QUESTION: 27
100□□ Windows 10 □□□ □□□ Microsoft 365 E5 □□□□ □□□□.
□□□□ □□□ □□□ □□□□ Windows 10 □□ □□ □□□□ □□□ □□□□□.
□□□□□ □□□ □□□□ □□□?
A. □□□□□□□ □□□
B. Microsoft Defender Exploit Guard
C. Microsoft Defender Credential Guard
D. BitLocker □□□□ □□□(BitLocker)
Answer: C (LEAVE A REPLY)

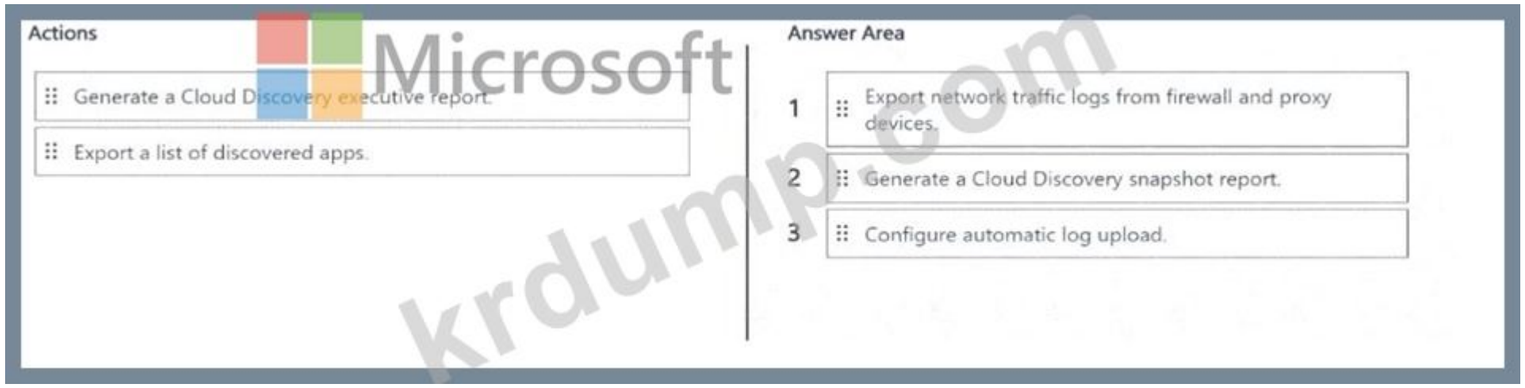
NEW QUESTION: 28
Microsoft 365 E5 □□□ □□ □□□□ □□ Microsoft Defender□ □□□□ □□□□.
□□□ □□□ □□□□ □□□ □□□□ □□□□ □□ □□□□□ □□□□ □□□□ □□□□□ Cloud Discovery□ □□□□ □□□.

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

Answer:



Explanation:



NEW QUESTION: 29
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: 30
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: 31
□□□ □□□ Microsoft 365□ □□□□ □□□□.
□□□ □□□ □□□ □□ □□□ □□□□ □□□□□.
□□ □□ '□□'□□□ □□□ □□□ □□□ □□□□ □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Exchange □□ □□□ □□ □□ □□
B. Exchange □□ □□□ □□ □□
C. Microsoft 365 □□ □□ □□□ □□□ □□ □□(DLP) □□
D. Microsoft 365 □□ □□□ Dace □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
□□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft 365 □□□ □□□□.
□□□□ □□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□□□□ Active Directory □□ □□□ □□□ □□□□ □□□.
* □□□□ Microsoft Entra Self-Service Password Reset(SSPR)□ □□□ □ □□□ □□□.
□□□ □□□□ □□□?
A. □□□□ □□
B. Microsoft Entra Seamless Single Sign-On(Microsoft Entra Seamless SSO)
C. Microsoft Entra ID □□
D. □□□□ □□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 33

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

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

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

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

□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 34
Microsoft 365 □□□ □□□□.
□□ □□ □□□ □□□□□ □□□ DLP(□□□ □□ □□) □□□ □□□□ □□□.
□□ □□□ □□□ □□□ □ □□□?
A. SharePoint □□□
B. OneDrive □□
C. □ □□ □ □□ □□□
D. □□□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
□□□ □□ □□□ □□□□□ DLP □□□ □□□□ □□□.
□□ □□□ □□□□ □□□?
A. □□□ □□ □□
B. Insider □□ □□ □□
C. □□□ □□
D. □□□ □□□
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

NEW QUESTION: 36
□□□ □□□ Microsoft 365□ □□□□ □□□□.
□□ □□□□ □□ Office 365□ □□ □□□□□ □□ □□□ □□ □□□□ □□□□ □□□. □□□□□ □□□□□ □□□□ □ □□□ □□□ □□□ □□□□□ □□□.

□□□ □□□□ □□□?

A. Microsoft 365 □□ □□□ □□ □□□

B. Microsoft Purview □□ □□ □□□ □□□

C. Microsoft Entra □□ □□□ □□□□ □□□□

D. Microsoft 365 □□ □□□ □□□

Answer: D (LEAVE A REPLY)

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: 37

Microsoft 365 E5 □□□ □□ □□□□ □□ Microsoft Defender□ □□□□ □□□□. □ □□□□ Windows 11 □□□ □□□□ □□□□ □□□□ □□□□.

□□□ □□□□ □ □□□□ □□□□□ Cloud Discovery □□□ □□□□ □□□□ □□□. □□□□ □□□□ □□ □□□ □□ □□□?

A. □□ □□□ □□□□.

B. □□□ Azure Monitor Agent□ □□□□□.

C. □□□□ □□□□□ □□□ □□□ □□□□□.

D. □ □□ □□□ □□□□.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 38

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

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

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

□□ □□ □□□ □□ □□ □□□ □□□ □□□□□ □□□□□.

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

□□□□ □ □□ □□□ □□□ □□□□□?

A. 0
B. 7
C. 4
D. 13
E. 16

Answer: (SHOW ANSWER)

NEW QUESTION: 39

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

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 40

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

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

Microsoft Store Business□ □□ □□□□ □□□ □□ □□ □□□□□.
Microsoft Store for Business□□ □□ □□□□ □□□□ □□□ □□ □□□□□.
□□ □□□ □□□ □□□ □ □□□?
A. Device2, Device3, Device5□
B. Device2□ Device4□
C. Device1, Device2, Device3, Device4, Device5
D. Device1□ Device3□
E. Device2□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
Project1□ □□□ □□□□□ □□□□ □□□□.
□□□□□ □□□ □□□ □□□□ □□ □□ DNS □□□□ □□□□ □□□ □□□□ □□□.
□□ DNS □□□□ □□□□ □□□?
A. □□□(A)
B. □□□ □□
C. □□□(TXT)
D. □□(CNAME)
Answer: C (LEAVE A REPLY)
When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
Text (TXT)
Mail exchanger (MX)
incorrect answer options you may see on the exam include the following:
alias (CNAME)
Host (A)
host (AAA)
Pointer (PTR)
Name Server (NS)
host information (HINFO)
pointer (PTR)
Reference:
https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns- hosting-provider

NEW QUESTION: 42
Microsoft Defender for Endpoint□ □□□□ Microsoft 365 E5 □□□ □□□□.
Endpoint□ Microsoft Defender□□ □□ □□ □□ □□ □□ □□□ □□□.
□□□□ File1.exe□□ □□□ □□□□□□ □□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□
B. □□ □□
C. □□ □□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 43
Azure □□□ Microsoft 365 E5 □□□ □□□□.
Microsoft Defender XDR□ □□□ □ □□ □□□□□ □□□□.
Azure□□ □□□□□ IP □□□ □□□ □□□□□ □□ □□□ □□□□□□ □□□.
□□□ □□□□□□ □ □□□ □□□□ □□, Azure□ Microsoft Defender XDR□ □□□□ □ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.
Answer Area

Answer:
Answer Area

Explanation:

NEW QUESTION: 44
Microsoft 365 E5 □□□ □□□□. □□ □□ □□ □□□□ □□□□ □□□. □□ □□□ □□□□ □□□?
A. Microsoft Purview □□ □□ □□
B. Microsoft Entra □□ □□
C. Intune □□ □□
D. Exchange □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 45
□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□: User1
UPN: user1@contoso.com
□□□ □□: user1@marketmg.contoso.com
MFA □□ □□: □□□□□
User1□ user1@marketing.contoso.com □□□ □□□ □□□□ □□□ Outlook□ □□□□□□ □□ □□□□ □□□□ □ □□□□.
User1□ user1@marketing.contoso.com□ □□□□ □□□ Outlook□ □□□□ □ □□□ □□□□ □□□.
□□□ □□ □□□?
A. User1□ MFA □□ □□□ □□□□□.
B. User1□ □□□□□ □□□□□□.
C. User1□ □□ □□ □□□ □□□ □□□□□.
D. User1□ UPN□ □□□□□.
Answer: D (LEAVE A REPLY)
Microsoft's recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN's to match.
Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user's email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only needs to remember a single name.
Configure the Azure AD multifactor authentication registration policy
Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.
Reference:
https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname

NEW QUESTION: 46
□□□ □□ 3□□ □□ 1□□ □□□ □□□□. □□□ □□□ □□□□□.

□ □□□ Microsoft 365 □□□□ □□□□ □□ □□ □□□ □□□ □□□□□.
□□ □□□□ □□□□□□ □□ □□ □□□ □□□□□ □□ Microsoft 365 □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. Microsoft Intune □□ □□ □□
B. Azure AD □□□ □□□
C. Microsoft Intune □□ □□ □□□
D. Azure AD □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 47
□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.

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

□□ □□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□□ □ □□□□?
A. Mailbox1□ Site1□
B. Mailbox1, Account1, Site1□
C. Account1□ Site1□
D. Mailbox1, Account1, Site1, Channel1
E. Account1, Site1, Channel1□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

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

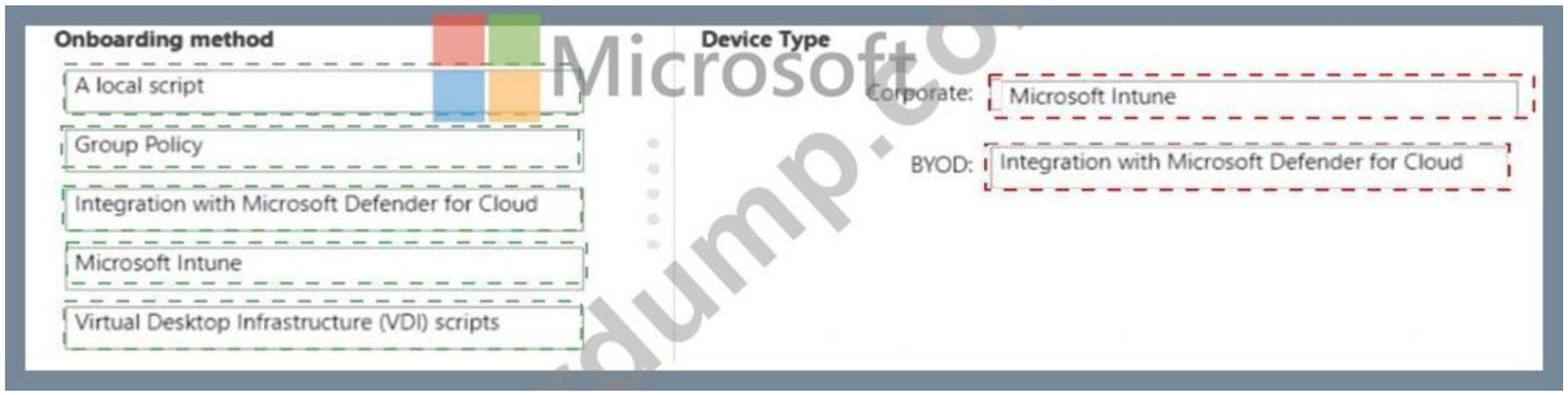
Type	Number of devices	Operating system	Enrollment status
Corporate	150	Windows 11	Azure AD-joined, Microsoft Intune-managed
Bring your own device (BYOD)	25	Windows 11	Unmanaged

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

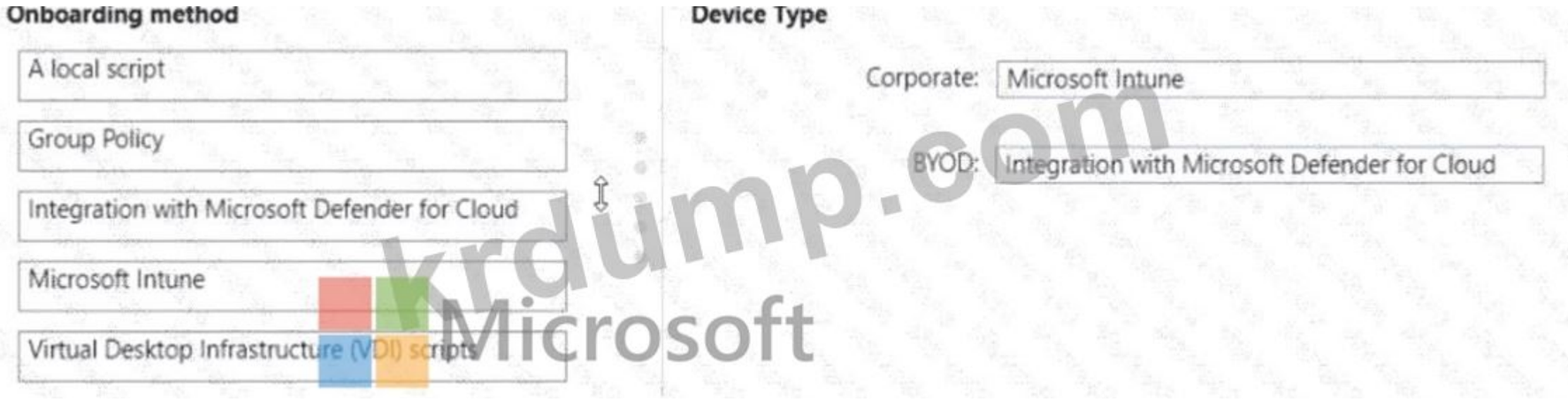
□ □□□ □□□ □□□□□ □ □□□ □□□□ □□□? □□□□□ □□□ □□□ □□□ □□□ □□ □□□□ □□□□□□. □ □□□ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □ □□ □□ □□□ □□□□□□ □□□□□ □□□□ □□□□ □ □□ □□□□.

□□□□: □□ □□□ 1□□□□.

Answer:



Explanation:



NEW QUESTION: 49

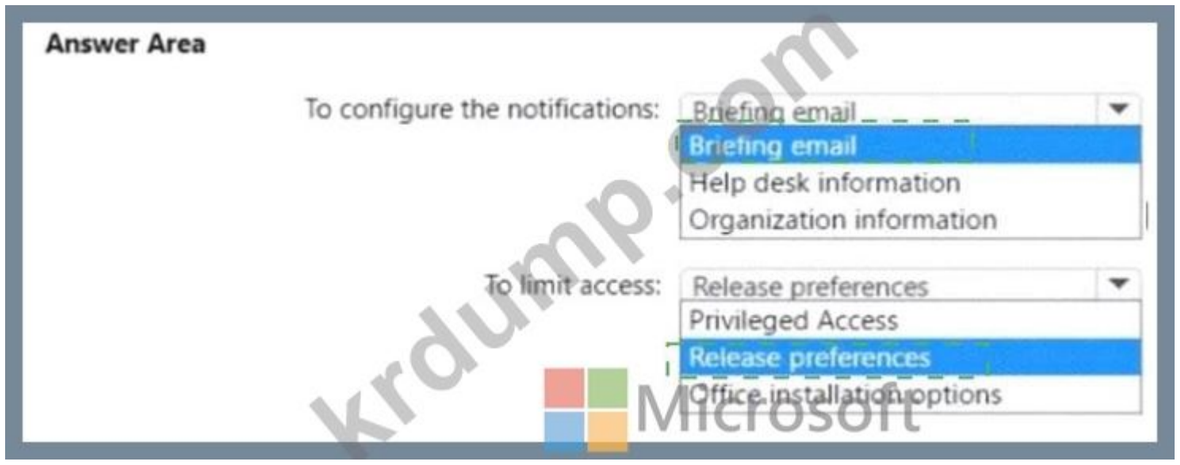
Office 365 □□□ □□ □□□ □□□□ □□□ □ □□ □□□□□ □□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.

Answer Area

Answer:



Explanation:

NEW QUESTION: 50
Microsoft Defender for Endpoint□ □□□□ Microsoft 365 □□□ □□□□.
□□□ □□ □□□ Microsoft Defender for Endpoint□ □□□□ □□□□.
□□ 24□□ □□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□ □□□.
□□□ □□ □□□?
A. Microsoft Purview □□ □□ □□□□ DLP(□□□ □□ □□) □□□ □□□□.
B. □□ □□□□ □□□ □□ □□□ □□□□.
C. □□ □□□□□ □□ □□□ □□□ □□□ □□□□□.
D. Microsoft Purview □□ □□ □□□□ □□ □□ □□□ □□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
□□□□□ □□□□□□ 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. Windows 10 □ Windows8.1□ □□
B. Windows 11□ □□
C. Windows 11, Windows 10-Windows8.1 □ macOS
D. Windows 11 □ Windows 10□□ □□
E. Windows 11 □ macOS□ □□

Answer: E (LEAVE A REPLY)

NEW QUESTION: 52
Microsoft 365 □□□ □□□□.
□□□□ □□ Microsoft Defender□ □□□□□□ Microsoft Defender□ □□□□□.
□□ □□□ 4□ □□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area

Explanation:

Answer Area

NEW QUESTION: 53
□□□□□ Active Directory □□□□□ □□□□ □□□□.
Microsoft 365□ □□□□□.
□□□□ □□□□ □□□ □□□□□.
□□□□ ID□ □□ □□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Active Directory□ □□□ □ □□ □□ □□□□ Microsoft 365 □□□□ □□□□□ □□□ □ □□□ □□□.
* □□□ □□□□□ 10□ □□□□□ □□□.
□□□: □□□□ □□□ □□□□ Microsoft Entra Password □□□ □□□□□. □□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Microsoft 365 E5 □□□ □□□□.
□□□□ □□□ □□□ □□□□ □□□□ □ App1□□□ □□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□□.

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

NEW QUESTION: 55
Microsoft 365 ES □□□ □□□□.
Microsoft Defender for Endpoint□ Microsoft Intune□ □□□□□.
Intune□ □□□ □ □□□ Defender for Endpoint□ □□□□ □□□□□□ □□ □□□.
□□□: □□□□□ □□ □ □□(EDR) □□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Azure AD □□□□ Microsoft 365 E5 □□□ □□□□. □□□□□ □□ □□ □□□ □□□□ □□□□□.

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

Endpoint□ Microsoft Defender□ □□□ □□□□□.
Microsoft Defender for Endpoint□□ □□ □□ □□□ □□(RBAC)□ □□ □□□ □□□□□.
Microsoft 365 Defender □□□□ □□ □□□□□ □ □ □□ □□□□ □□□□ □□□.
□□ □□□□ □□□□ □□□?
A. □□□3
B. □□□2
C. □□□4
D. □□□1
Answer: (SHOW ANSWER)

NEW QUESTION: 57
Microsoft 365 E5 □□□ □□ □□□□ □□ Microsoft Defender□ □□□□ □□□□.
App1□□□ □□□□ □□ □□□□.
□□ □□ □□□ □□□□ App1□ □□ □□ □□□□ □□□□ □□□.
* □□□ □□□ □□□ □□□□□ □□□□□.

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

Answer:

Explanation:
Answer Area

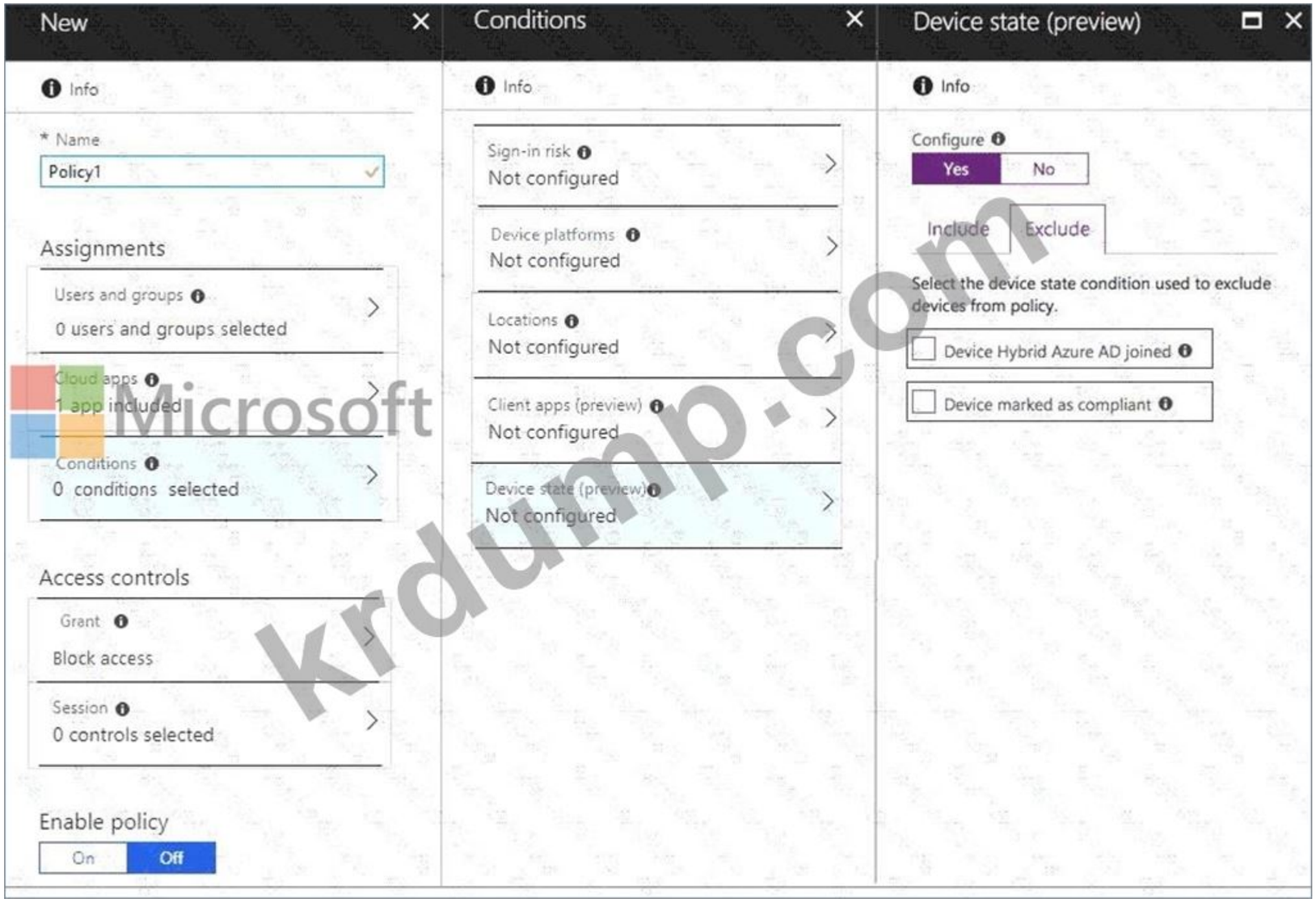
NEW QUESTION: 58
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
User1□ □□□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□□ □□□ □□□ □□□□ □□□□. □□□ □□□ □□□□ User1□ □□□□ □□□. □□ □□□ □□□□ □□□?
A. Microsoft 365 □□ □□

B. Microsoft Entra □□ □□
C. Exchange □□ □□
D. Microsoft Defender □□
E. Microsoft Purview □□
Answer: (SHOW ANSWER)

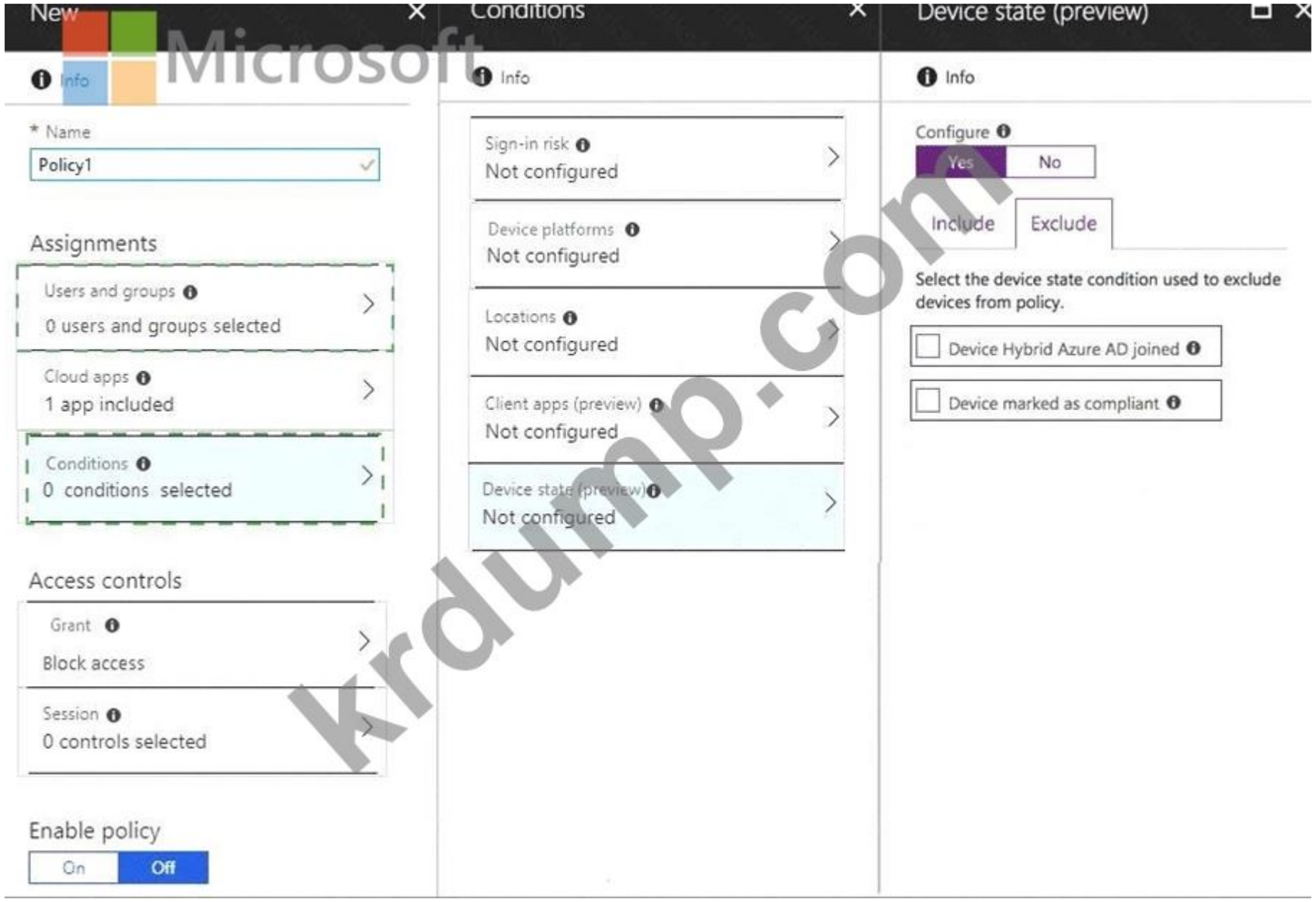
NEW QUESTION: 59
Windows 10 □□ 21H1□ □□ □□□ □ □□□□ □□□□□□.
□□□□ □□ □□□□ □□□□ □□□. □□□□ □□□ □□□□ □□ □□□□□ □□□.
□□□□□ □□□ □□ □□□?
A. □□ □□ □□□□□ □□ □□ □□□□□ □□□□□.
B. □□ □□ □□□□□ 21H1 □□ □□□ □□□ □□ □□ □□□□□ □□□□□.
C. □□ 21H1 □□□ □□□□ □□ □□ □□□□□ □□ 21H1 □□□ □□□□ □□ □□ □□□□□ □□□□□.
D. □□ 21H1 □□□ □□□□ □□ □□ □□□□□ □□ □□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 60
Group1□ Group2□□ □ □□ □□□ □□□ Microsoft 365 □□□□ □□□□.
Microsoft Teams□ □□□□ Group1□ □□ □□ Group2□ □□□ □□□□ □□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□ □□□□ □□ □□□□□ □□□ □□□□ □ □□□.
□□□ □□□□ □□□?
A. □□□□□□ □□ □□
B. Azure Active Directory(Azure AD)□ □□□ □□
C. □□□ □□ □□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 61
□□ □□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□□ □□□.
Exchange Online□ □□□□ □□□ □□□□□.
Policy1□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

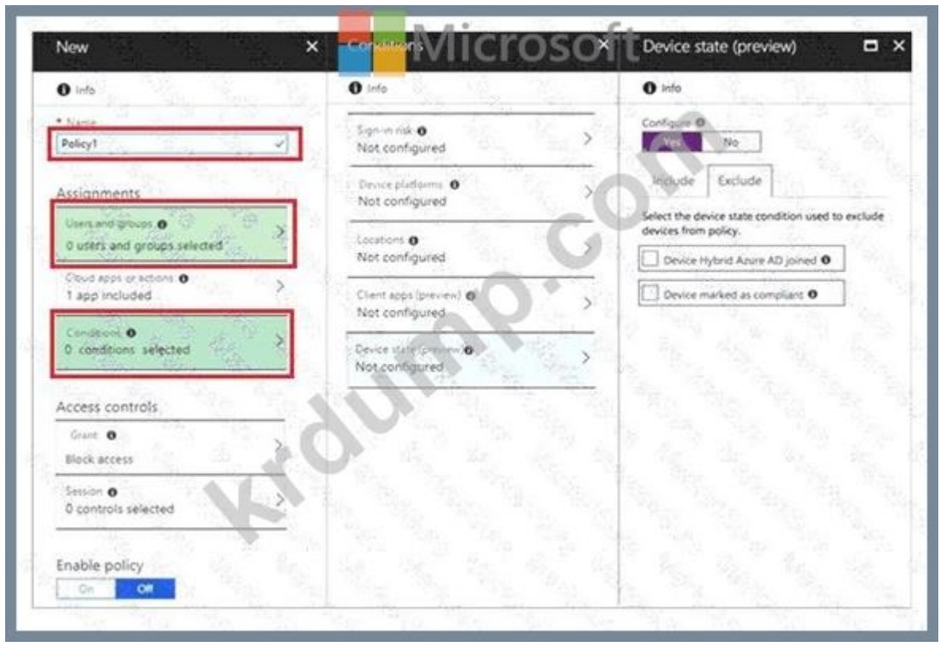

New
Info
* Name
Policy1
Assignments
Users and groups
0 users and groups selected
Cloud apps
1 app included
Conditions
0 conditions selected
Access controls
Grant
Block access
Session
0 controls selected
Enable policy
On
Off
Conditions
Info
Sign-in risk
Not configured
Device platforms
Not configured
Locations
Not configured
Client apps (preview)
Not configured
Device state (preview)
Not configured
Device state (preview)
Info
Configure
Yes
No
Include
Exclude
Select the device state condition used to exclude devices from policy.
Device Hybrid Azure AD joined
Device marked as compliant

Answer:



Explanation:

Suggested answer:



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

NEW QUESTION: 62

Microsoft 365 E5 □□□ □□□□.

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

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

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

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

□□□ □□□□ □□□?

A. □□ □□

B. MFA □□ □□

C. □□□ □□□ □□

D. □□ □□□ □□□□ □□□(SSPR)

Answer: (SHOW ANSWER)

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: 63
Office 365□ Microsoft Defender□ □□□□ Microsoft 365 □□□ □□□□.
□□□ □□ □□ □□ □□ □□ □□ □□□ □□□□□.
□□ □□ □□□ □□ □□□ □ □□ □□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. □□ □□
B. □□□ □□ □□
C. □□ □□
D. □□□ □□
E. □□□ □□
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 64
Microsoft 365 E5 □□□ □□ Microsoft Defender for Endpoint□ □□□□□. □□□□ □□□ □□□ □□□ □□□□□.

Name	Platform
Device1	Windows 11
Device2	Android
Device3	Linux

□□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□.

Name	Template
Policy1	Microsoft Defender Antivirus
Policy2	Device Control

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

Answer:

Explanation:

NEW QUESTION: 65

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

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

□□ □□□□ □□□ □ □□ □□ □□ □□□ □□□□□.

* □□ : AntiSpam1
* □□□□ : 0
* □□□ □□□, □□ □ □□□□ □□□□□.
o □□□: User3
o □□ : Group1
* □□ □□□, □□ □ □□□ □□
o □□ : □□2
* □□□ □□
o □□ □□□ □□□ 100□□ □□□□□
* □□ : AntiSpam2
* □□□□ : 1
* □□ □□□, □□ □ □□□□ □□□□□.
o □□□: User!o □□: Group2
* □□ □□□, □□ □ □□□ □□
o □□□: User3
* □□□ □□
o □□ □□□ □□□ 50□□ □□□□□
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 66

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

Defender for Cloud Apps□□ □□□ □□ □□□ □□□□□ □□□□ □□□ □□□ □□□□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□ □□□□ □ □□□?

□□□ □□□ □□□ □□□□ □□□□□.

A. □□□ □□ □□ □□

B. □□ □□□□
C. □□□ □□
D. □□□□ □□ □□
E. Microsoft Power Automate □□□□
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 67
Endpoint Security□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□ □□□ □□ □□□ Endpoint Security Manager □□□ □□□□ □□□.
□□ □□□ □□□ □□□ □ □□□?
A. □□ □□ □□ □ □□ □□
B. Microsoft 365□ □□
C. □□ □□
D. □□, □□ □□ □□, Microsoft 365 □ □□
E. □□ □□ □□, Microsoft 365 □ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Office 365□ Microsoft Defender□ □□□□□□?
□□ □□□□□ □□□□ □□□□ □□□□□.
□□□□□□ □□□ □□□□ □□□□□ □□□ □□ □□ □□□ □□□ □□□.
□□□□□ □ □□□□ □□□ □□ □ □□ □□ □□□ □□□□□?
A. 7
B. 45
C. 30
D. 15
Answer: (SHOW ANSWER)

NEW QUESTION: 69
Microsoft 365 ES □□□ □□□□.
Microsoft 365 Defender □□□□ □□□ Microsoft Secure Score□ □□□□□.
□□ □□ □□□□ □□□ □□□□ □□□□□.
□□ □□ □□□ □□□□ □□□ □□□□ □ □□□ □□□.
□□ □□□ □□□□ □□□?
A. □□ □□ □□
B. □□□ □□ □□ □□
C. □□ □□
D. □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 70

Microsoft 365 E5 □□□□ □□□□.
□□□ □□ □□□□ □□□ □□ □□□ □□ □□□□ □□ □□□□□ □□□ □□ □□□ □□□ □□□.
□□ □ □□ □□□ □□□ □ □□□□? □ □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. □□ □□ □□
B. □□□ □□□ □□
C. Microsoft Cloud App Security □□ □□
D. □□□ □□ □□(DLP) □□
E. □□□□□□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 71
□□ □□□□ Defender for ID □□□ □□□□ □□□?
A. □□1
B. □□2
C. □□3
D. □□4
E. □□5
Answer: A (LEAVE A REPLY)
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: 72
□□□ Microsoft 365 □□□ □□□□ □□□□.
Microsoft Entra □□ □□ □□□□ □□ □□□ □□ □□ □□ □□□□□ □□ Microsoft Authenticator □□□ □□□□□.

□□□□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□ □□□. □ □□□□ □□□ □□□ □□ □□□□□□ □□□□ □□□?
A. □□□□□□□ 365 □□□□
B. □□□□□□□ □□
C. □□□□□□□ □□□

D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Microsoft 365 □□□□ LinkedIn □□ □□□□ □□□□.
LinkedIn □□□□ □□□□ LinkedIn □□□□ □□□□ Microsoft 365□ □□□ □□□□□.
LinkedIn □□□□ □□□□ □□□ □□□ □ □□□?
A. Microsoft OneDrive for Business □□
B. Microsoft SharePoint Online □□ □□□□□
C. Microsoft 365 □□□
D. Azure □□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin-data?view=o365-worldwide

NEW QUESTION: 74
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□ Policy1□□□ □□□ □□□□□ □□ □□ □□□ □□□□.

Policy1□ User1□ □□□□□.

User1□ 24□□ □□ □□ □ □□ □□ □□□ □□□ □□ □□□□□?

A. 720

B. 30

C. 1000

D. 1030

Answer: A (LEAVE A REPLY)

NEW QUESTION: 75

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

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

GPS □□□ □□□ □□□ □□□□ □□□ □□□ □□□ □□ □□□□□.
□ □□□ □□ □□□□ □□□ □ □□□?

A. Userl1□

B. User1□ User3□

C. User1, User2, User3, User4

D. User2□ User4□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 76

Montreal Users □ Seattle Users OU□ □□ □□□ □□ □□□ □□□□□ Microsoft Entra Connect Sync□ □□□□ □□□.
□□□ □□ □□□?

A. PowerShell□□ Add-ADSyncConnectorAttributeInclusion cmdlet□ □□□□□.

B. Microsoft Entra Connect □□□□□ □□□ □□ □□□ □□□ □□□□□.

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

D. PowerShell□□ Start-ADSyncSyncCycle cmdlet□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 77

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

* □□□ 10
* □□□□□
* □□□ OS

□□ □□□□ Endpoint DLP □□□ □□□ □ □□□?

A. Windows 10□ □□

B. Windows 10 □ Android□ □□

C. Windows 10 □ macOS □□

D. Windows 10, Android □ iOS

Answer: (SHOW ANSWER)

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

NEW QUESTION: 78
□□ □□ □□□ 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. □□ □□
B. Policy3□ □□□
C. Policy2□ □□□
D. □□□ □□□!
Answer: B (LEAVE A REPLY)

NEW QUESTION: 79
□□□□□ Endpoint□ Microsoft Defender□ □□□□ □□□□.
□□ □□□□ Microsoft Defender for Endpoint□ □□□□ □□□ □□□□□.

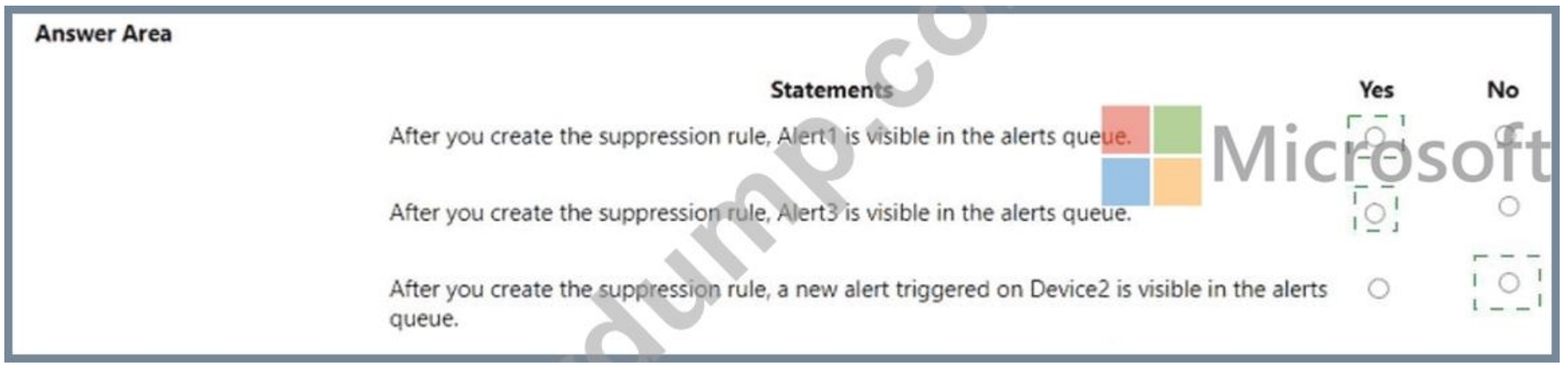
Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

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

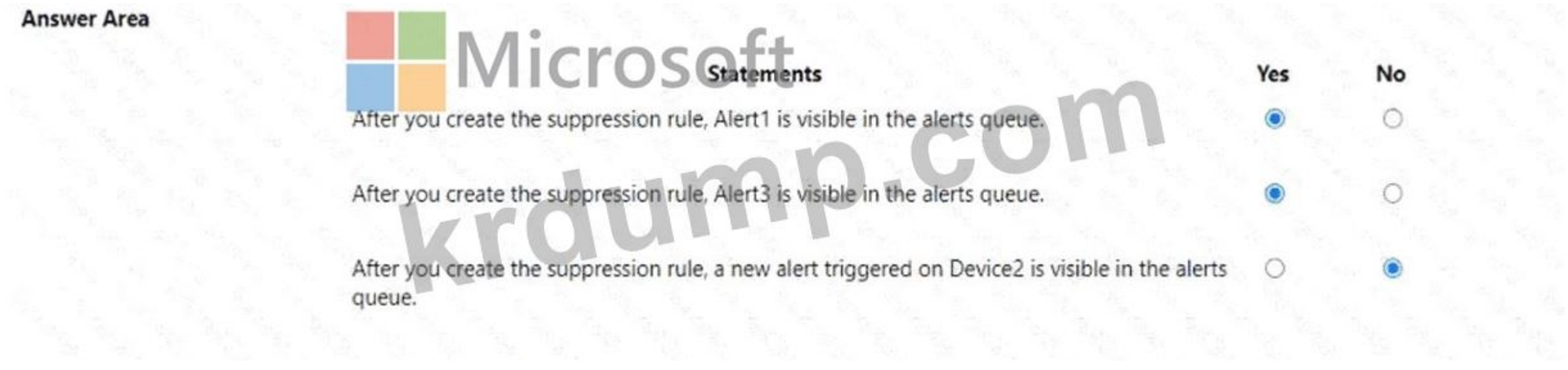
Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

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

Answer:



Explanation:

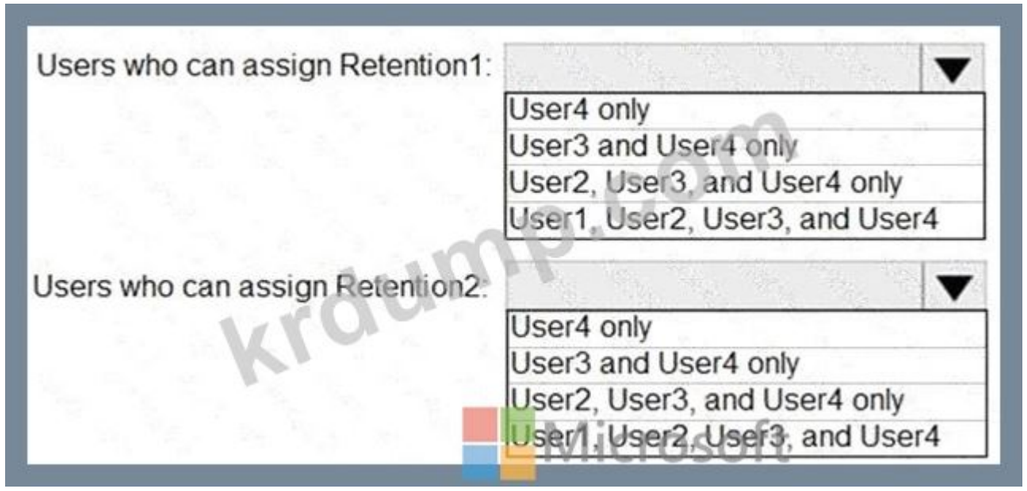


NEW QUESTION: 80

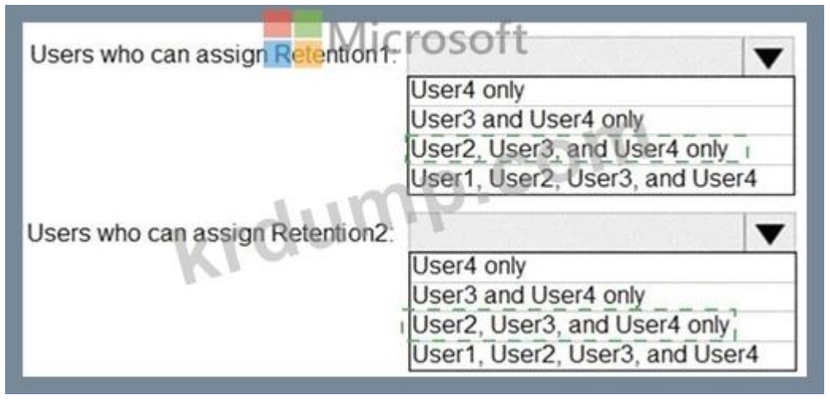
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

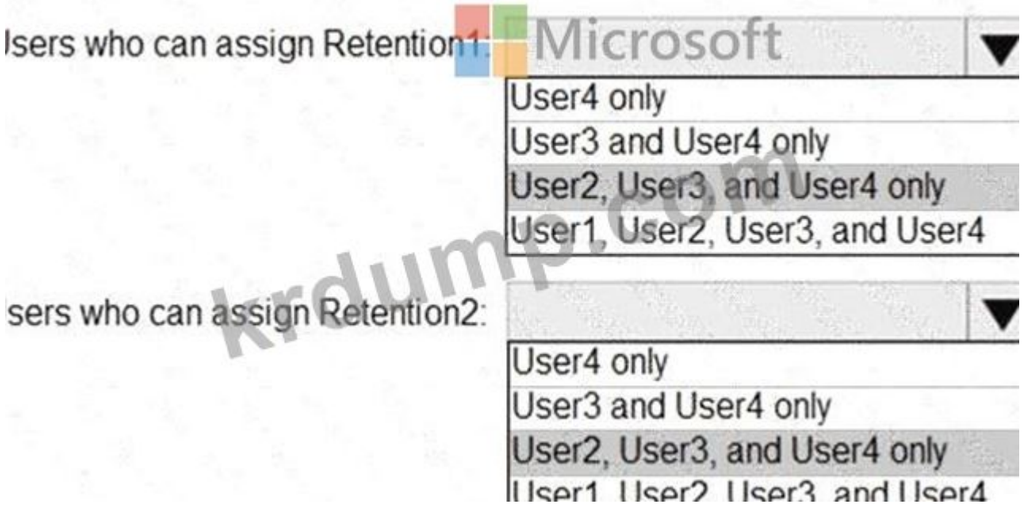
Exchange □□□□ □□□ Retention1□□□ Microsoft Office 365 □□ □□□□ □□□□.
□□ □□□□ □□□□ Microsoft Exchange Online □□ □□□ □□□□. □□ □□□□ Retention2□□ □□ □□□ □□□□ □□□□.
□□ □□□□ Retention1□ Retention2□ □□□□ □□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

NEW QUESTION: 81
Microsoft 365 □□□ □□□□.
DLP(□□□ □□ □□) □□□ □□□□□.
□□□□ □□□□ □□ □□□□ □□□□ DLP □□□ □□□□ □□□ □□□ □□□□□□.
□□□□ DLP □□□ □□□□ □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□
B. □□ □□□
C. □□
D. □□□□ □□□□
Answer: D (LEAVE A REPLY)
A DLP policy can be configured to allow users to override a policy tip and report a false positive.
You can educate your users about DLP policies and help them remain compliant without blocking their work.
For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word.
If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

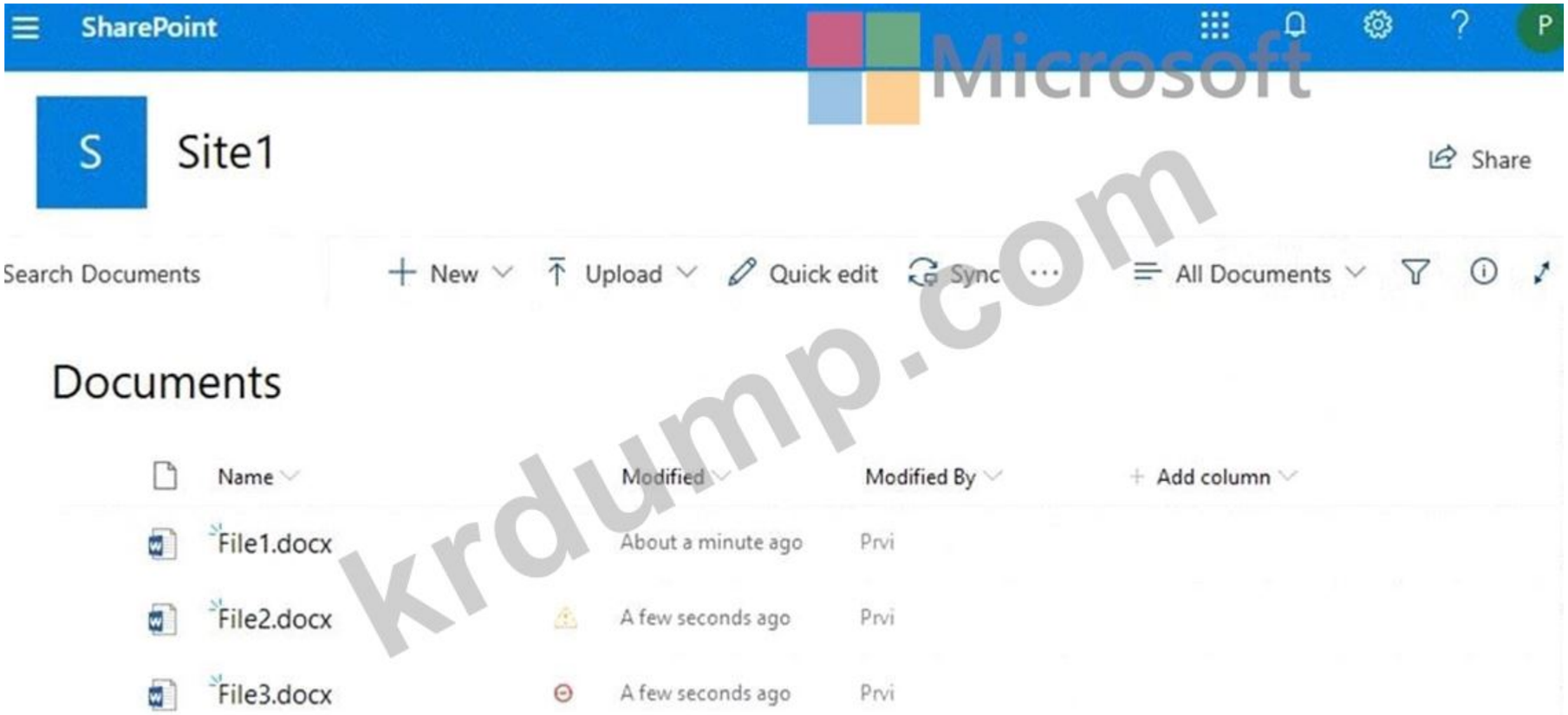
NEW QUESTION: 82
Windows 10 □□□□□ □□□ Microsoft 365 □□□□ □□□□. □□□□□ Microsoft Defender for Endpoint□ □□□□□ □□□□.
Microsoft Defender □□ □□□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□□ PowerShell □□□□□ □□□□ □□□.
□□ □□□□□ □□ □□□ □□□□ □□□?

A. □□□ □□ □□ □□
B. □□ □□ □□
C. □□ □□□□ □□□□□
D. □□□ □□
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365- worldwide

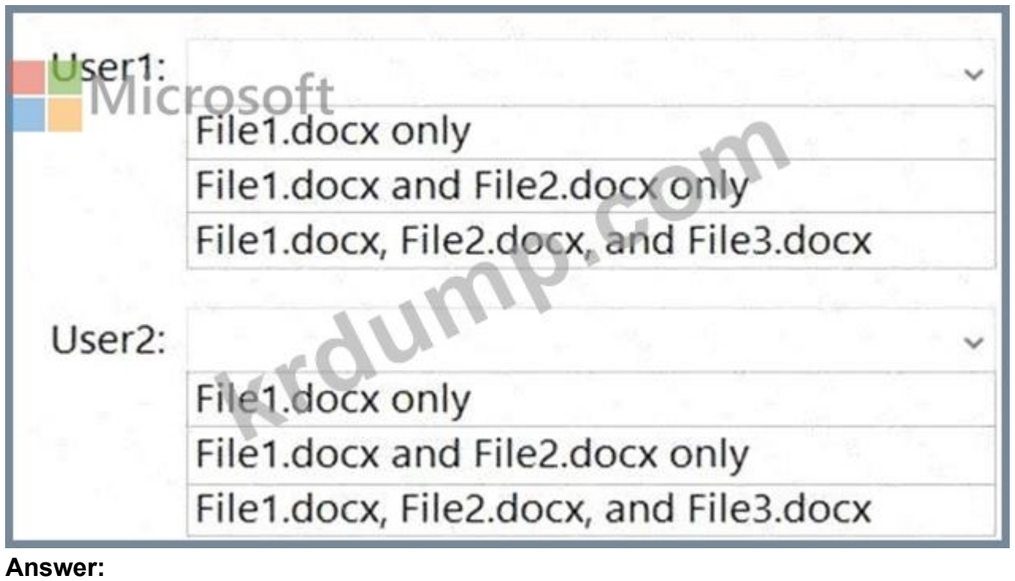
NEW QUESTION: 83
Microsoft 365 □□ □□ □□□□ Site1□□□ Microsoft SharePoint Online □□□□ □□ □□□ □□ □□(DLP) □□□ □□□□□. Site1□□ □□ □□ □□□ □□□ □□□□ □□□□.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

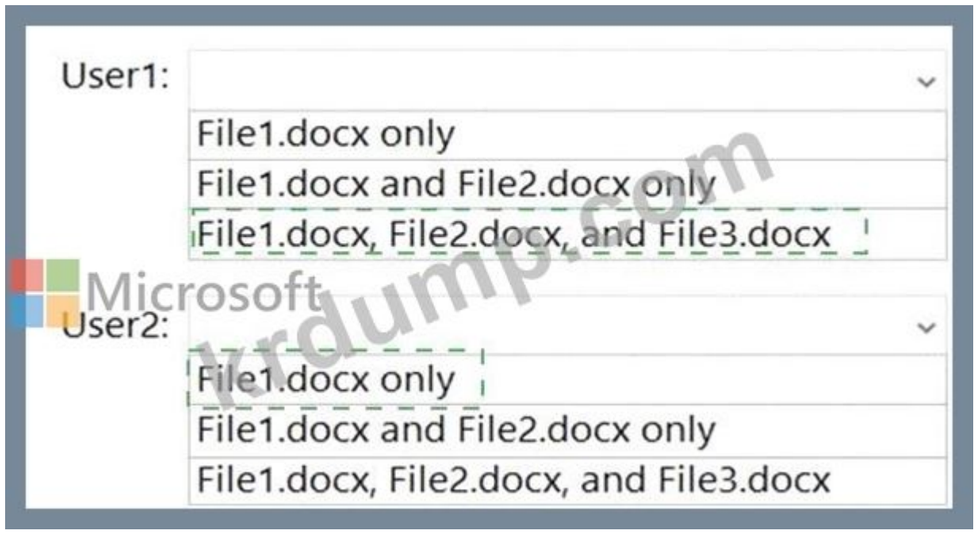
Prvi□ □□□ □□□ □□□ □□□□. (□□ □□ □□□□□.)



User1□ User2□ □□ □□□ □ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



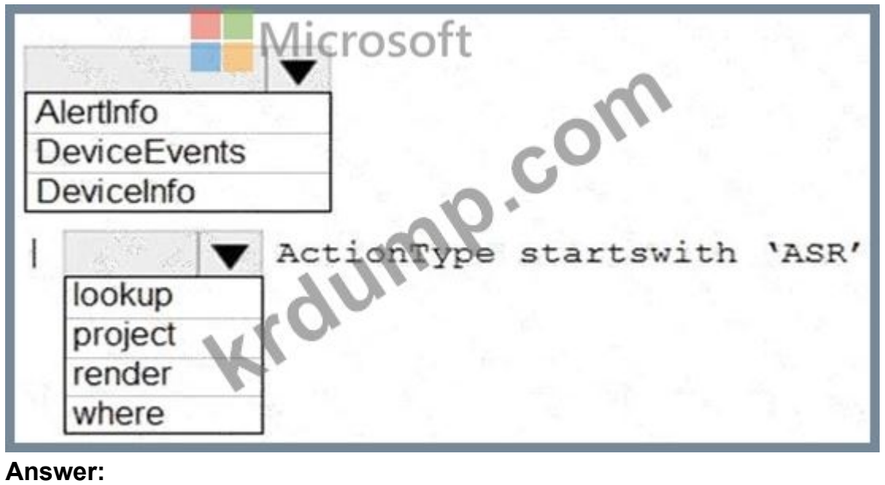
Explanation:

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

NEW QUESTION: 84
Microsoft 365 □□□ □□□□.
□□□ □□□ □□□ □□□□ □□□ □□□□ □□ □□ □□□ □□□ □□□ □□□ □□□ □□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□ □□ □□
B. □□ □□
C. □□ □□
D. □□□ □□ □□(DLP) □□
Answer: C (LEAVE A REPLY)

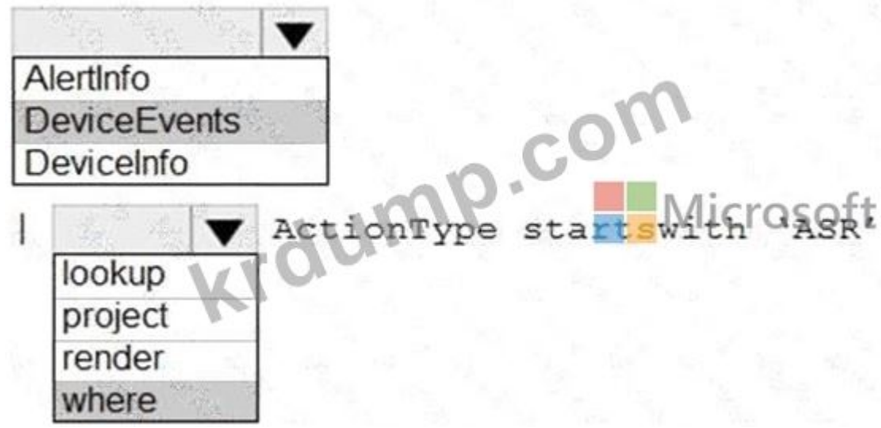
NEW QUESTION: 85
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
□□□□□□ contoso.com□□□ Active Directory □□□□ □□□□ □□□, □ □□□□ Microsoft Azure Active Directory(Azure AD)□ □□□□□ □□□□.
Microsoft System Center Configuration Manager(□□ □□)□ □□□□ Windows 10 □□□ □□□□□.
□□ □□□ □□ □□□□ □□□□□.
□□□□ Device1□□□ □ □□□ □□□□□. Device1□ Configuration Manager □□□□□□ □□□□□.
Microsoft Intune □ Configuration Manager□ □□□□ Device1□ □□□ □ □□□ □□□□ □□□.
□□ □□: □□ □□ □□□□ □□ □□ □□□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)
It looks like the given answer is correct. There is an on-premises Active Directory synced to Azure Active Directory (Azure AD) So the co-management path1 - Auto-enroll existing clients 1. Hybrid Azure AD 2. Client agent setting for hybrid Azure AD-join 3. Configure auto-enrollment of devices to Intune 4. Enable co- management in Configuration Manager https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial- co-manage-client

NEW QUESTION: 86
100□□ Windows 10 □□□ □□□ Microsoft 365 E5 □□□□ □□□□.
Windows 10 □□□ □□ □□ □□(ASR) □□□ □□□ □□□□□.
□□ □□□□ ASR □□□ □□□□ Log Analytics □□ □□□□ □□ □□□□ □□□□□.
□□□ □□□ □□□□ ASR □□□ □□□ □□□.
Kusto □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:



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

NEW QUESTION: 87
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□(MFA)□ □□□□□ □□□.
□□□□ □□ □□ □□□ □□□□ □□□. □□□□ □□□□□ MFA□ □□□□ □□□□ □□□ □□□ MFA□ □□□ □□□□□□ □□□ □□□□□ □□ □□□.
□□□ □□□□ □□?
A. □□
B. Microsoft □□□
C. FID02 □□ □
D. □□□□
E. □□□ OTP
Answer: B (LEAVE A REPLY)

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

□□□ □□□□ □□□□□.
□□□□□ □□ Microsoft Word□□ □□□ □□□ □□□ □ □□□ □□□□□. □□□ □□□ Microsoft 365□ Word□□ □□□ □ □□□□.
□□□□ □□ Word□ □□□ □ □□□ □□□□ □□□ □ □□□ □□□□ □□□.
□□□ □□ □□□?
A. □□□ □□□ □□□□□.
B. □□ □□□ □□ □□
C. Microsoft SharePoint Online □ OneDrive□ □□□ □□ □□□ □□□□ □□□□□□.
D. Azure Information Protection□□ Microsoft 365 Compliance Center□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
□□□□ □□ Microsoft Defender□ □□□□ Microsoft 365 □□□ □□□□.
SharePoint Online □□□□□ □□□□□ □□□□□ □□ □□ □□□ □□□□□.
□□□□□ □□□ SharePoint Online □□□□□ □□□ □□□□□ □ □□□ □□□□□.
□□□□ SharePoint Online □□□□ □□□□ □□□□ □□ □□□□□ □□□□□ □□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□□ □□ □□(DLP) □□
C. □□ □□
D. □□□ □□□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 90
(□□□ □□□□□□ contoso□□ □□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□□ □ □ □□□□.)
com□ fabrikam.com□ □□ □□□ □□ □□□□ □□□□.
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□ □□□□□□ □□ □□□□ Microsoft Entra ID□ □□□□□ □□□. □□□□ □□ □□ □ □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□?)
A. Microsoft Entra □□□□ □□□
B. □□□□□□□ □□□ □□□ □□□
C. Microsoft Entra Connect □□□
D. □□□ □□□□ □□□□□ □□□(AD FS)
Answer: C (LEAVE A REPLY)
The correct answer is Microsoft Entra Connect Sync because it is the only Microsoft-supported solution that meets all of the stated requirements.
1. Support for multiple on-premises AD DS forests
Microsoft Entra Connect Sync is designed to synchronize identities from multiple on-premises Active Directory forests into a single Microsoft Entra tenant. Microsoft documentation explicitly states that when multiple forests are present, they can all be synchronized as long as they are reachable by the same Entra Connect server. A forest trust between contoso.com and fabrikam.com is a supported and common configuration.
2. Ability to sync only a subset of users
Microsoft Entra Connect Sync supports filtering and scoping at multiple levels (domain-based, OU-based, or attribute-based). Microsoft documentation lists pilot deployments and limited user synchronization as a primary use case, allowing administrators to synchronize only selected users from each forest.

3. Support for device objects and hybrid device scenarios
Microsoft Entra Connect Sync supports hybrid device identity , including Microsoft Entra hybrid joined devices. These devices are registered both in on-premises Active Directory and in Microsoft Entra ID, which is required for many Microsoft 365 and Conditional Access scenarios.
4. Device writeback support
Device writeback is a feature that allows device objects from Microsoft Entra ID to be written back into on- premises Active Directory. Microsoft documentation clearly identifies device writeback as a feature of Microsoft Entra Connect Sync .
Important documented behavior:
* Device writeback is supported when device objects and users are correctly located and configured in the same forest.
* Device writeback is not a feature of Cloud Sync or federation services.
Why the other options are incorrect
A). Microsoft Entra Cloud Sync
Cloud Sync is a lightweight provisioning agent and does not provide the full hybrid identity feature set required for this scenario. Microsoft documentation associates advanced device features and device writeback with Microsoft Entra Connect Sync, not Cloud Sync.
B). Microsoft Entra Domain Services
Microsoft Entra Domain Services is a managed domain service used to run legacy, domain-joined workloads in Azure. It does not synchronize on-premises forests into Microsoft Entra ID and is not a replacement for Entra Connect in hybrid identity scenarios.
D). Active Directory Federation Services (AD FS)
AD FS is an authentication and federation service. It does not synchronize users or devices to Microsoft Entra ID and does not support device writeback. Microsoft documentation positions AD FS as an authentication method, not a directory synchronization solution.

NEW QUESTION: 91
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

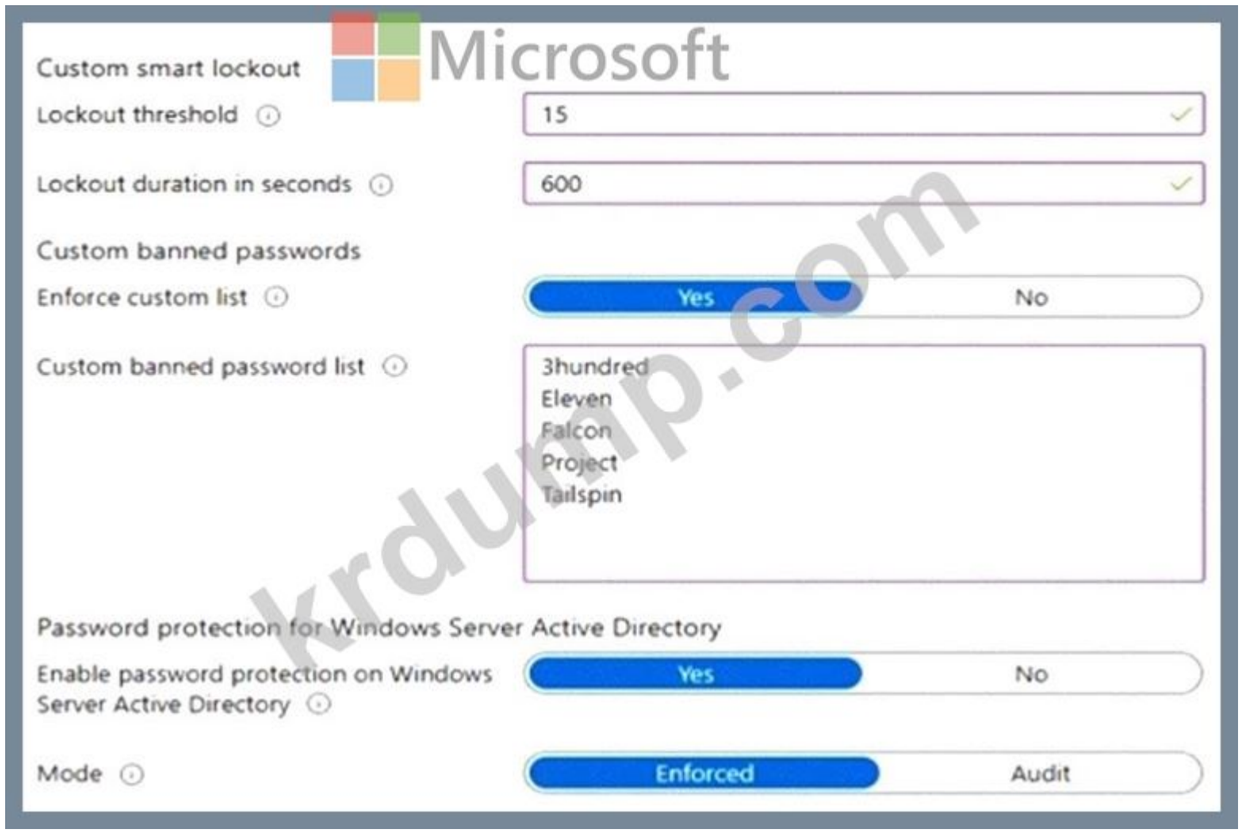
NEW QUESTION: 92
Group1□ Group2□□ □ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.
Group1 □ Group2□ □□□ □□ □□ □□ □□(MFA)□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Group1 □□□ Android □□□□ Microsoft Entra ID□ □□□ □□ MFA□ □□□□□ □□□□ □□□ □□□.
* □□ 2 □□□□ □□ □□□□ □□□□ Microsoft Exchange Online□ □□□□ □□ MFA□ □□□□ □□□.
* □□□ □□□ □□□□□ □□□.
□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 93
Microsoft 365 E5 □□□ □□□□.
□□□ □□□ □□ □□□ Microsoft□□ □□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Microsoft Purview
B. Microsoft □□ □□
C. Azure AD ID □□
D. □□ □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
□□□
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Azure AD □□ □□□ □□ □□□ □□ □□□□□.

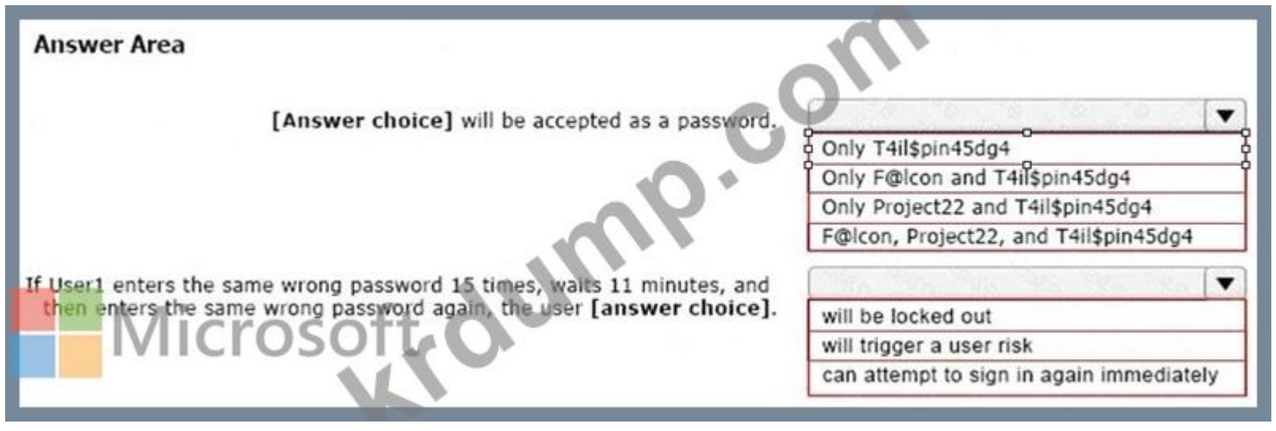


User1□ □□□ □□□□□ □□ □□□□□ □□□□□□□□ □□□□□.

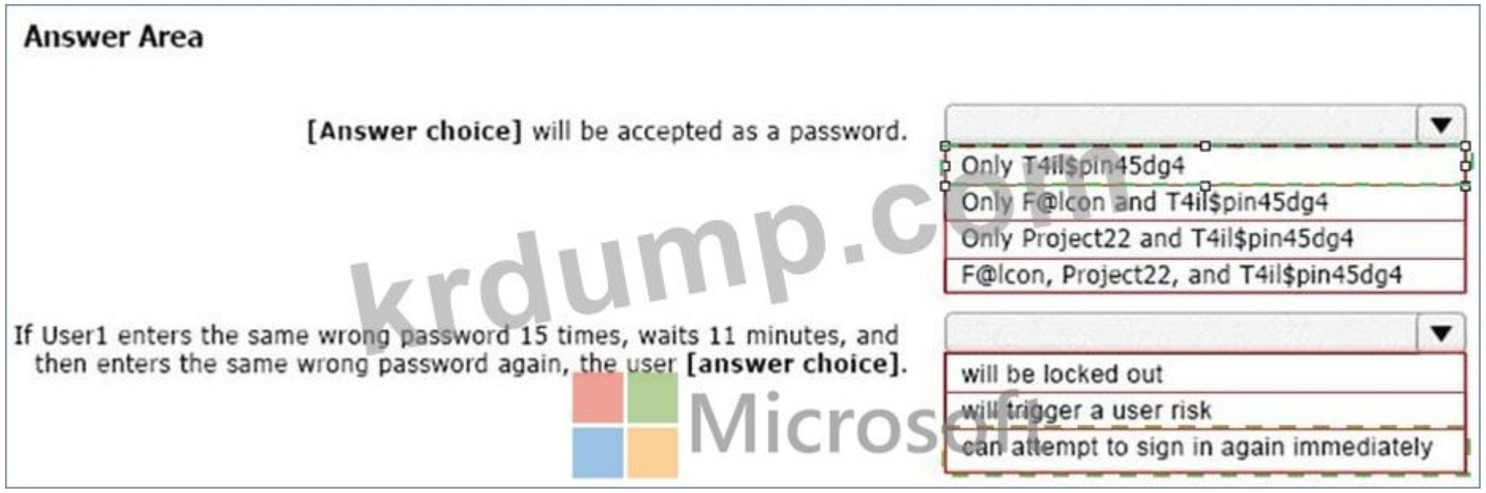
* □□
* □□□□22
* T4il$pin45dg4

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

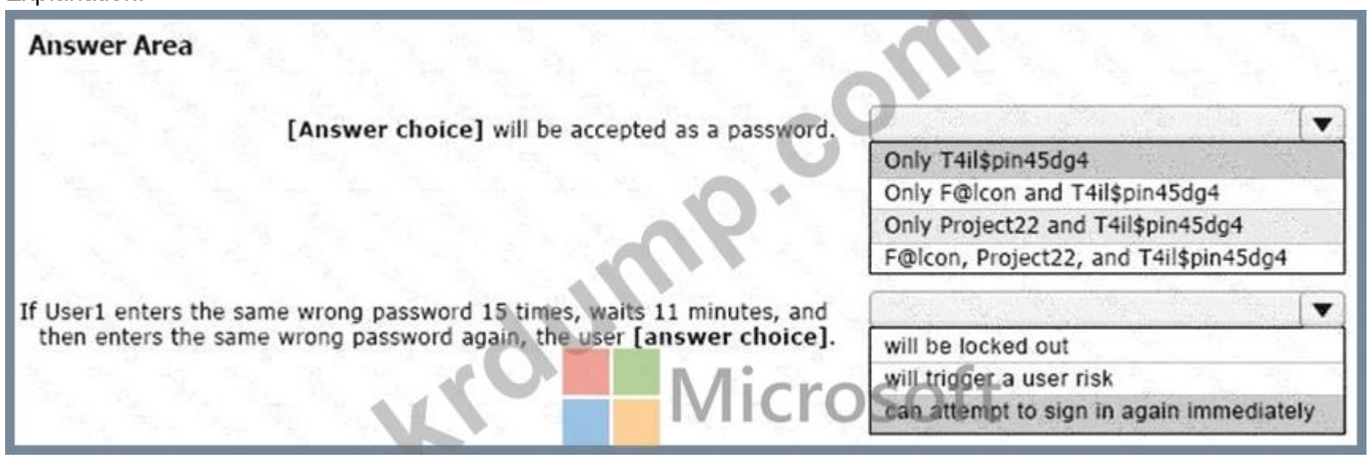
□□□□: □□ □□□ 1□□□□.



Answer:



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: 95

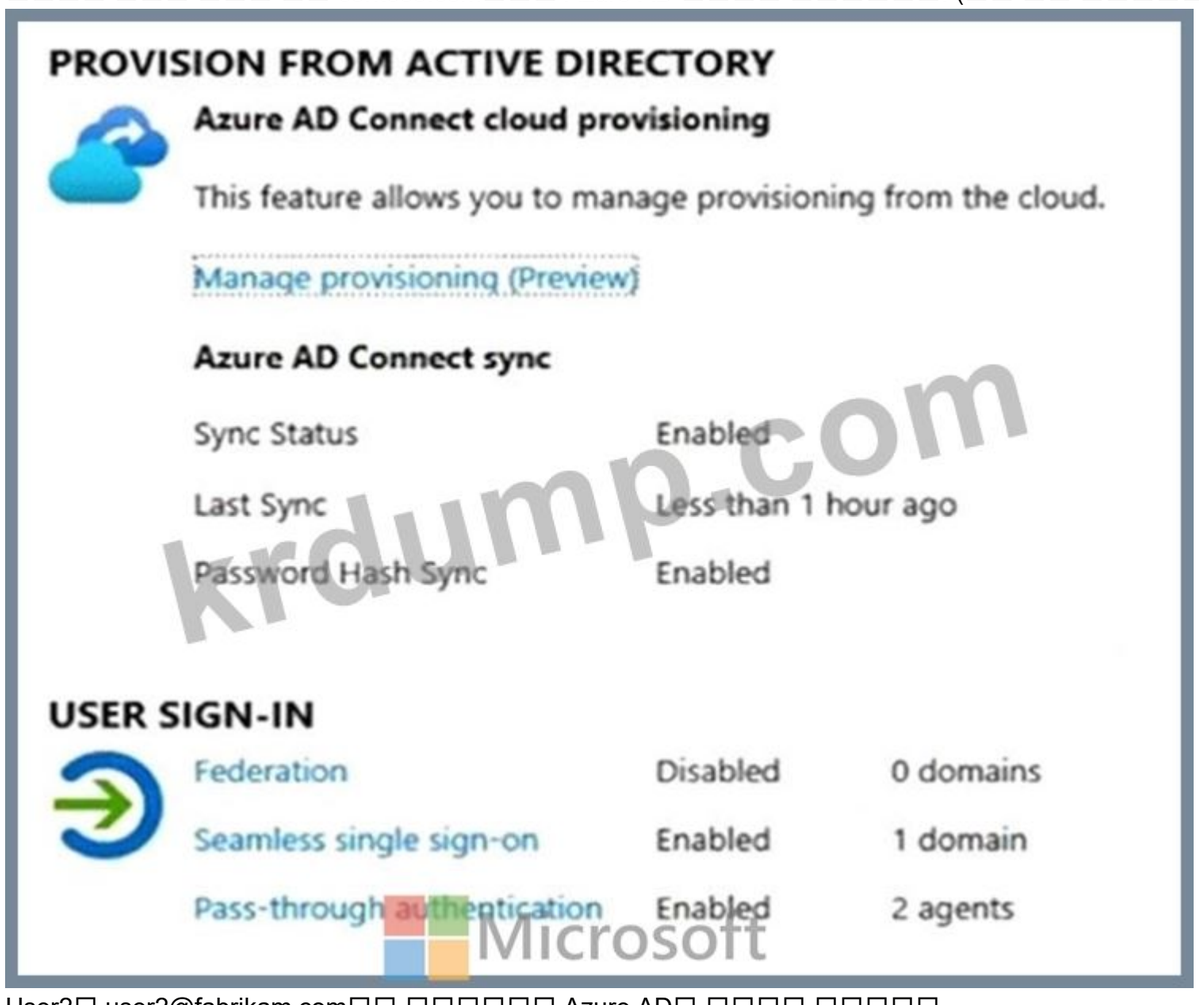
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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



User2□ user2@fabrikam.com□□ □□□□□□ Azure AD□ □□□□ □□□□□.

User2□ Azure AD□ □□□□ □□□□ □ □□□ □□□□ □□□.

□□□: □□□□□ Active Directory □□□□□ User2□ UPN □□□□ @contoso.com□□ □□□□□. User2□□ user2@contoso.com□□ □□□□□□ □□□□□.

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

NEW QUESTION: 96
□□□ □□□□□□ Contoso□□ Active Directory □□□□□ □□□□ □□□□. □□.
Microsoft 365 □□□ □□□□.
□□□□ □□ □□□□ □□□□ □□□□ □□□ □□□□ □□□□□ □□□.
Microsoft 365 □□ □□□□ contoso.com □□□ □□□ □□□□□ □□□□□□.
□□□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Microsoft 365 □□ □□□□ Contoso.Local □□□ □□□ □□□□□.
B. contoso.com□ □□ DNS □□□□ □□□ □□ □□□(MX) □□□□ □□□□□.
C. Active Directory □□□ □ □□□□□ □□ □□□□ UPN □□□□ □□□□□.
D. Active Directory □□□ □ □□□□□□ contoso.com□ UPN □□□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 97
Microsoft 365 E5 □□□ □□□□. □□□□ Site1□□□ Microsoft SharePoint Online □□□□ □□□□ □□□□. Site1□□ □□ □□□ □□□□ □□□□.
* □□.docx
* □□□□.docx
* □□jmportant.docx
Microsoft Defender Cloud □□□ □□ □□□ □□□ □□□ □□ Policy1□□□ □□ □□□ □□□□.

Policy1□ □□ □□□ □□□□□?
A. ImportantFile.docx□
B. File.docx, ImportantFile.docx, Filejmportant.docx
C. Filejmportant.docx□
D. □□.docx□
E. ImportantFile.docx □ Filejmportant.docx□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 98

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

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

□□2□ □□1□ □□□□□.

Group1□ Office 365 Enterprise E3 □□□□□ □□□□□.

Office 365 E3 □□□□□ □ □□ □□□□□?

A. 3

B. 4

C. 2

D. 1

Answer: (SHOW ANSWER)

NEW QUESTION: 99

Windows 10 □□ 2004□ □□ □□□ □ □□□□ □□□□□□.

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

□□□□□ □□□ □□ □□□?

A. □□ □□ □□□□□ □□ □□ □□□□□ □□□□□.

B. □□ □□ □□□□□ 2004□□ □□□ □□□ □□ □□ □□□□□ □□□□□.

C. 2004□□ □□□ □□□ □□ □□ □□□□□ 2004□□ □□□ □□□ □□ □□ □□□□□ □□□□□.

D. 2004□□ □□□ □□□ □□ □□ □□□□□ □□ □□ □□□□□ □□□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 100

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

□□ □□□ □□□ □□□ □□□□□□ Contoso□□ □□□ □□□□□□ □ □□□.

□□ □□□ □□□□□ □□□ □□ □□□?

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

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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 101

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

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

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

□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Name	Role
Admin1	AU1\User Administrator
Admin2	Global Administrator

Answer Area

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

Answer:

Answer Area

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

Explanation:

Admin1 can reset the password of User1: Yes

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

Admin1 can reset the password of User2: No

User2 is a member of both Group1 and Group2. However, User2's job title contains " Executive, " which excludes them from AU1 ' s dynamic membership rule. Therefore, Admin1 cannot reset User2 ' s password.

Admin2 can reset the password of User3: Yes

Admin2 has the Global Administrator role, which grants the ability to reset passwords for any user within the organization, including User3.

NEW QUESTION: 102
□□□ 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: 103
□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□□ Windows 10□ □□□□ 2,000□□ □□□□ □□□□ □□□□.
Microsoft 365 □□□ □□□□□.
□□□□ □□ □□□□ Azure AD Seamless Single Sign-On(Seamless SSO)□ □□□□□.
□□□□ Windows 10 □□□□□ Seamless SSO□ □□□ □ □□□ □□□□ □□□.
□□□ □□ □□□?
A. Azure AD□□ □□□ □□□ □□□ □□□□.
B. Azure AD Connect □□□□ □□□ □□□□□.
C. □□ □□□ □□□□ □□□□ □□ □□□ □□□□□.
D. □□□□ Azure AD□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
Endpoint□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□ □□□□.
Microsoft Defender for Endpoint□□ □□ □□ □□ □□ □□ □□□ □□□.
□□□□ File1.exe□□ □□□ □□□□□□ □□ □□□□ □□□.
A. □□ □□
B. □□ □□ □□□
C. □□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Microsoft 365 E5 □□□ □□□□.
SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.
SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Office 365 Advanced Threat Protection(ATP) □□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Azure Active Directory □□ □□□□ SecAdmin1□□ □□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: (SHOW ANSWER)

NEW QUESTION: 106
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: 107
□□ □□□ Azure ATP □□□ □□□□ □□□?
A. □□ 1
B. □□ 2
C. □□ 3

D. ☐☐ 4
E. ☐☐ 5
Answer: A (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning However, if the case study had required that the DCs can ' t have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.
Topic 2, A. DatumCase Study:
Overview
Existing Environment
This is a case study Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.
Current Infrastructure
A). Datum recently purchased a Microsoft 365 subscription.
All user files are migrated to Microsoft 365.
All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.
Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.
A). Datum uses and processes Personally Identifiable Information (PII).
Problem Statements
Requirements
A). Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.
Business Goals
A). Datum warns to be fully compliant with all the relevant data privacy laws in the regions where it operates.
A). Datum wants to minimize the cost of hardware and software whenever possible.
Technical Requirements
A). Datum identifies the following technical requirements:
Centrally perform log analysis for all offices.
Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
Provide the users in the finance department with access to Service assurance information in Microsoft Office
365.
Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user ' s user account.
A security administrator requires a report that shows which Microsoft 36S users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive US. PII data to other New York office users. Email messages must be monitored to ensure compliance.
Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

NEW QUESTION: 108
□□ □□ □□□ □□ □□□ □□□ Microsoft 365 □□□ □□□□.

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

□□□□ □□ □□ □□□ □□□□ □□□□□.

Name	Members
Group1	User1
Group2	User2, User4

□□□□□□ □□ □□ □□□ □□□ □□□□□.

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

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

Answer Area

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

Answer:

Explanation:

NEW QUESTION: 109

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

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

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

A. Microsoft Entra □□□□□□ □□□□ □□□□□.

B. Microsoft Authenticate □□ □□□□□.

C. □□ □□□ contoso.com□ □□□□□.

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 110

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

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

Microsoft 365 □□□ □□□□.

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

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

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

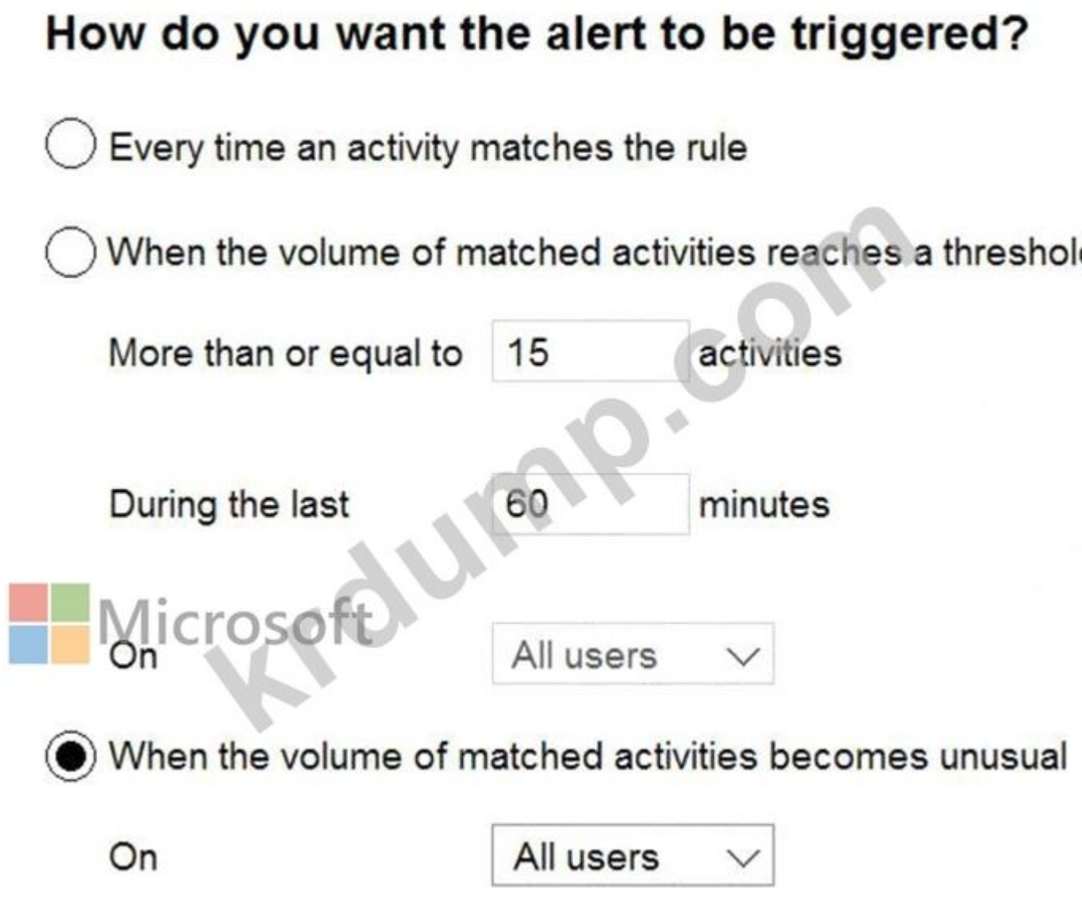
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Windows 10□ □□□□ □□□□ □□□□.
□□□ Windows 10 □□□ □□□□ □□□.
□□ □□: □□ □□□□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

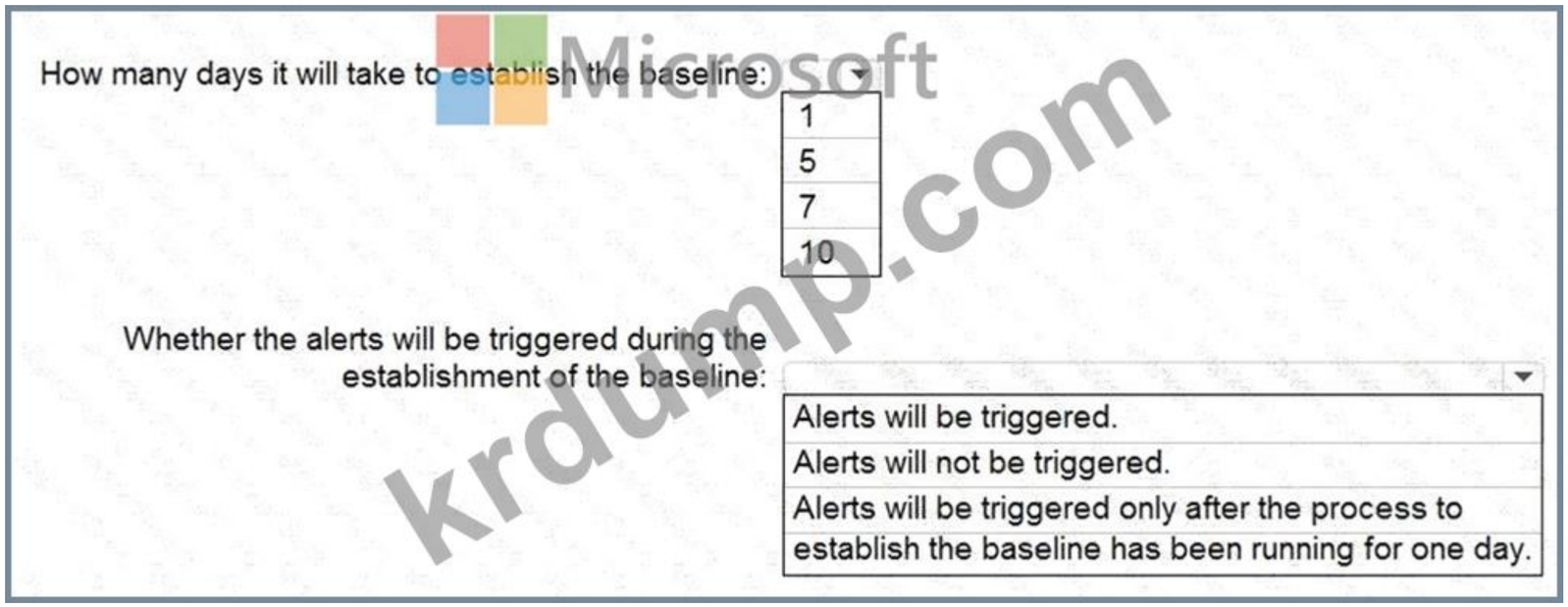
NEW QUESTION: 112
(□□□ 1,000□□ Windows □□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.)
□□□ □□ □□□ □□□□ □□□.
□□ □□□ □□□□ □□□?
A. Microsoft Intune □□ □□
B. Microsoft Purview □□
C. □□□□□□□ □□□ □□
D. Microsoft 365 □□ □□
Answer: C (LEAVE A REPLY)
The correct answer is the Microsoft Defender portal .
Explanation:
* Exposure Score is a security metric provided by Microsoft Defender for Endpoint . It measures an organization's overall security posture by evaluating device configuration, vulnerabilities, and security controls across endpoints.
* Microsoft documentation defines Exposure Score as part of the Microsoft Defender Vulnerability Management experience, which is accessed through the Microsoft Defender portal .
* The Exposure Score helps administrators:
* Understand how vulnerable devices are across the organization
* Track improvements to security posture over time
* Prioritize remediation actions based on risk
* Microsoft explicitly states that Exposure Score is viewed and managed within the Microsoft Defender portal , which serves as the central dashboard for Defender for Endpoint, Defender for Office 365, and related security services.
Why the other options are incorrect

A). the Microsoft Intune admin center
Intune focuses on device management, compliance, and configuration profiles. While it provides device health and compliance reporting, it does not display the Defender Exposure Score.
B). the Microsoft Purview portal
Microsoft Purview is used for data governance, compliance, insider risk, and information protection. It has no functionality related to endpoint exposure scoring.
D). the Microsoft 365 admin center
The Microsoft 365 admin center is designed for tenant-wide administration such as users, licenses, and services. It does not provide detailed endpoint security metrics like Exposure Score.

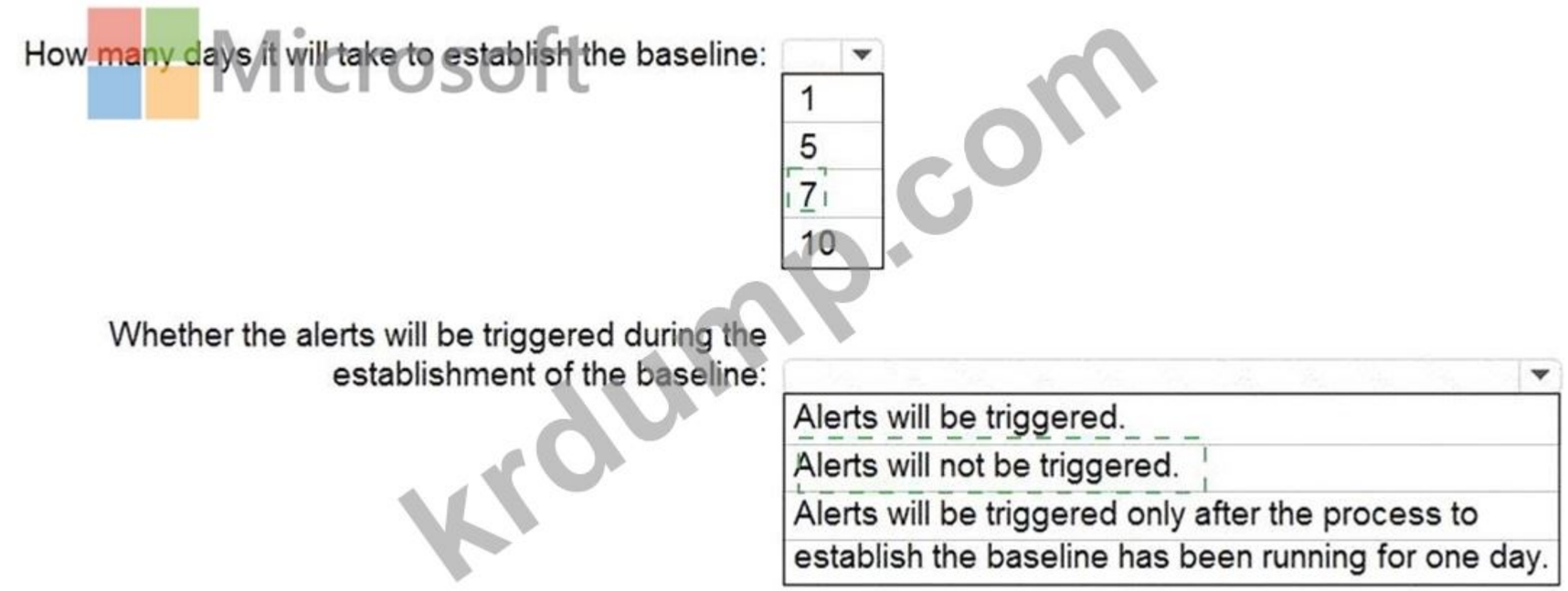
NEW QUESTION: 113
Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□ □□□ □□ □□□ □□□□□.



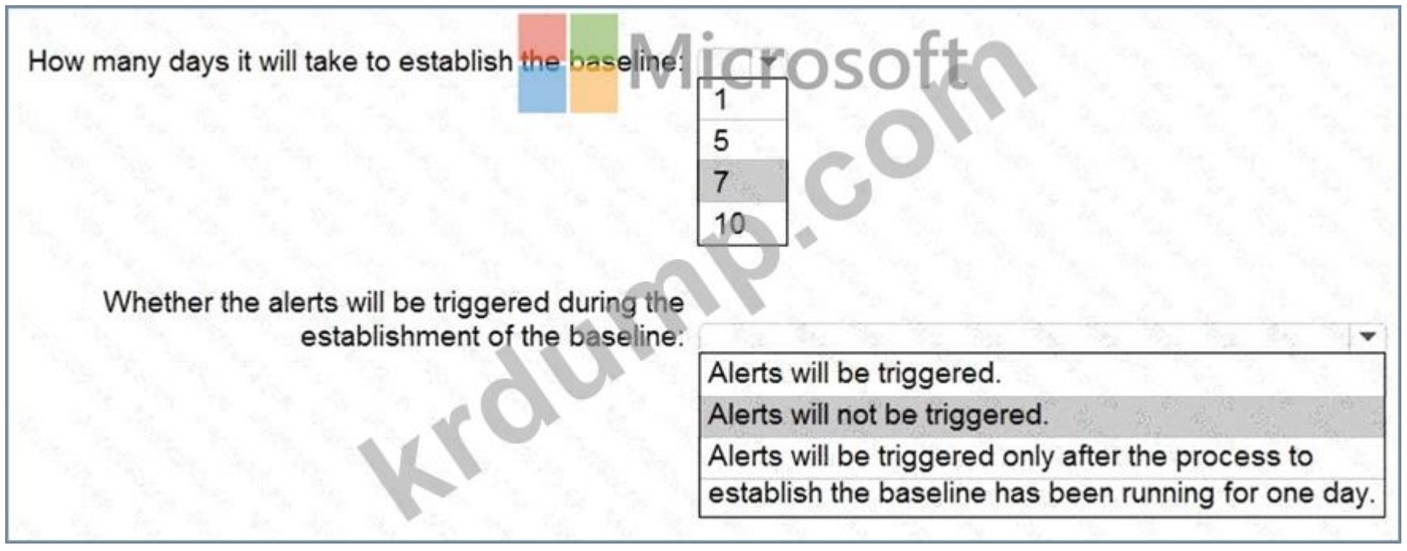
□□ □□□ □□□□ □□□.
* □□□□□ □□□ □□ □□□□ □□□□ □ □□□ □□□□?
* □□□□ □□□□ □□ □□□ □□□□□ □□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



ence:

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

NEW QUESTION: 114

Montreal Users □ Seattle Users OU□ □□ □□□ □□ □□□ □□□□□ Azure AD Connect□ □□□□ □□□.

□□□ □□ □□□?

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

B. PowerShell□□ start-ADSyncSyncCycle cmdlet□ □□□□□.

C. PowerShell□□ Add-ADSyncConnectorAttnbuteinclusion cmdlet□ □□□□□.

D. Microsoft Azure AD Connect □□□□□ □□□□□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 115

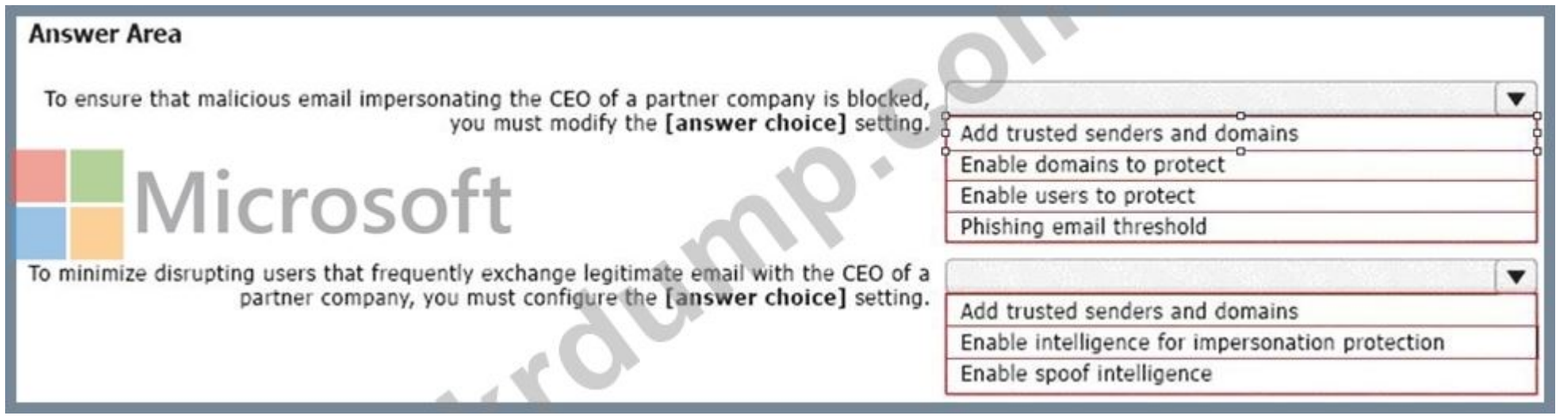
□□□

Microsoft 365 □□□ □□□□.

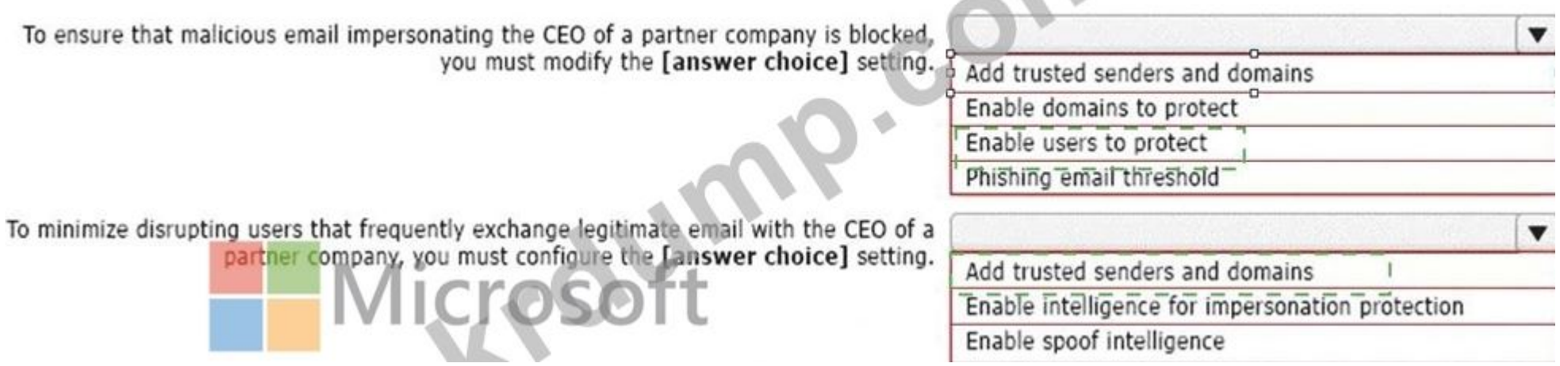
□□ □□□ □□□ □□ □□ □□ □□□ □□□□□.

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

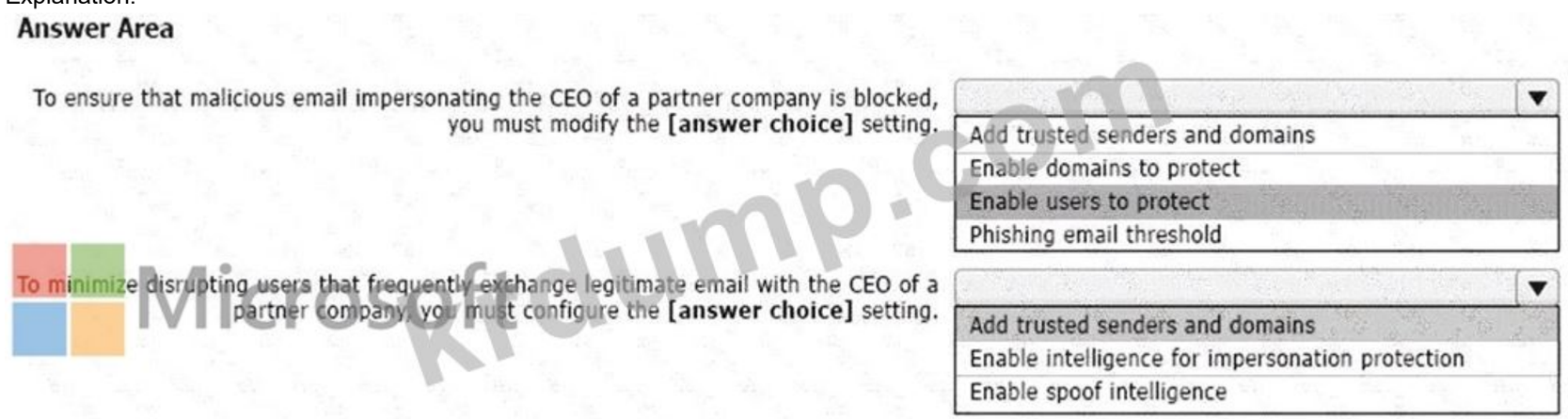
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Box 1: Enable users to protect

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

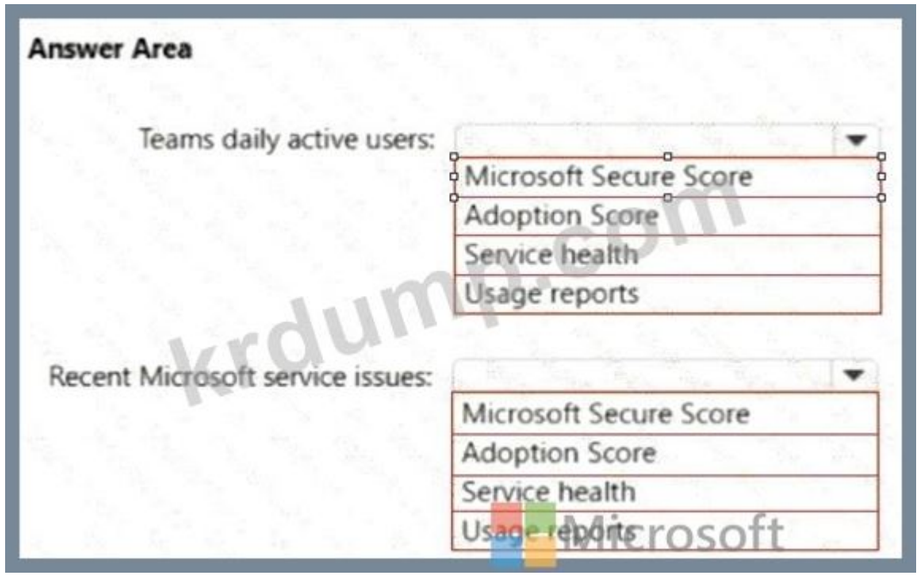
User impersonation protection

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

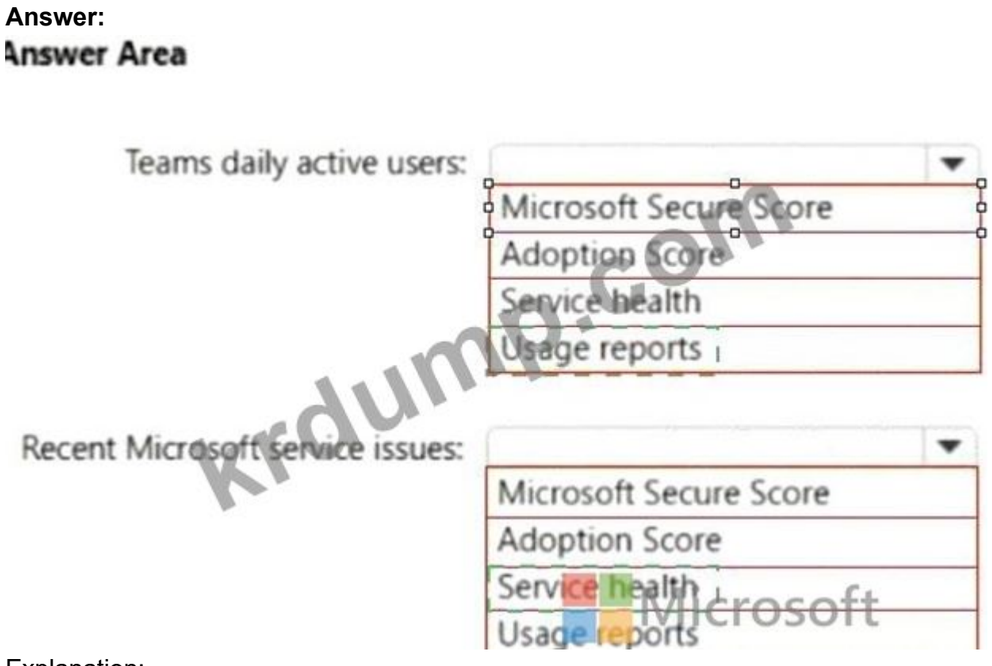
You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).
When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender ' s email address, the action for impersonated users is applied to the message.
Box 2: Add trusted senders and domains
Trusted senders and domains
Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren ' t applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about

NEW QUESTION: 116
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Microsoft 365 E5 □□□ □□□□.
SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.
SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Microsoft Defender for Office 365 □□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Microsoft 365 □□ □□□□ SecAdmin1□□ SharePoint □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: A (LEAVE A REPLY)

NEW QUESTION: 117
□□□
Microsoft 365 □□□ □□□□.
□□ □□□ □□ □□□ □□□□ □□□.
Microsoft Teams□ □□ □□ □□□
□□ Microsoft □□□ □□
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Answer Area

Box 1: Usage reports

The daily active users in Microsoft Teams

Microsoft 365 Reports in the admin center - Microsoft Teams usage activity The brand-new Teams usage report gives you an overview of the usage activity in Teams, including the number of active users, channels and messages so you can quickly see how many users across your organization are using Teams to communicate and collaborate. It also includes other Teams specific activities, such as the number of active guests, meetings, and messages.

Box 2: Service Health

Recent Microsoft service issues

You can view the health of your Microsoft services, including Office on the web, Yammer, Microsoft Dynamics CRM, and mobile device management cloud services, on the Service health page in the Microsoft 365 admin center. If you are experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

Reference:

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

https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health

NEW QUESTION: 118

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

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

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

Answer:

Explanation:

NEW QUESTION: 119

□□□

□□□ □□□□ Microsoft 365 E5 □□□ □□□□.

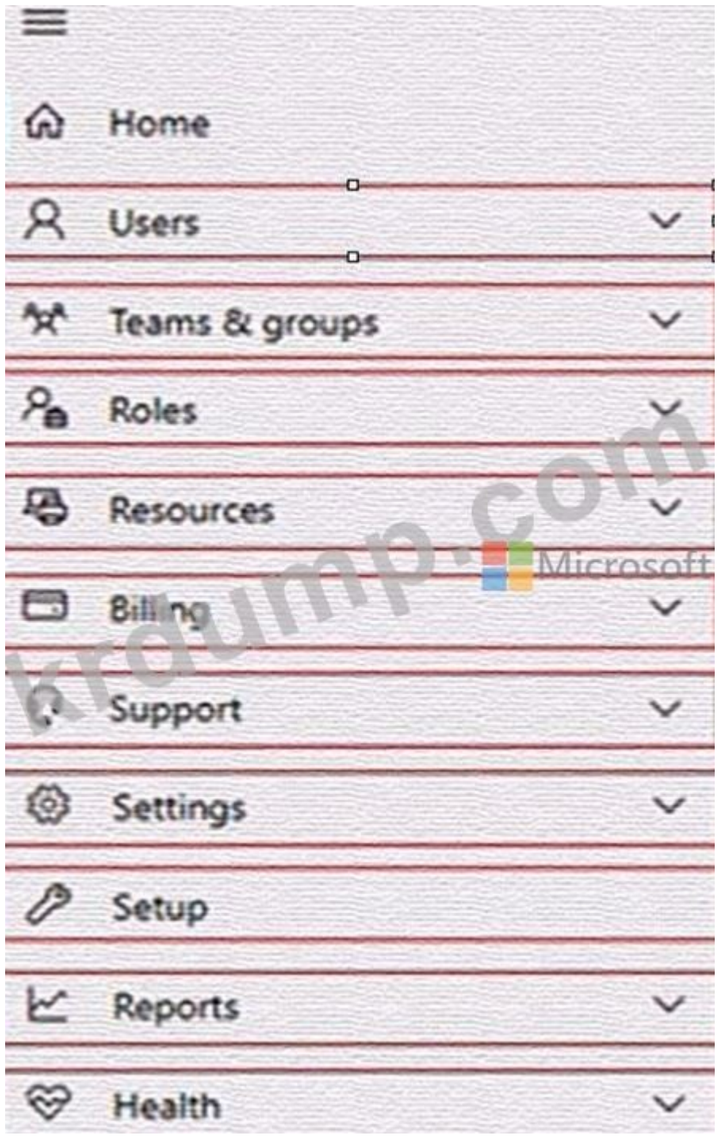
□□ □□□ □□□□ □□□.

□□□ □□ □□□ □□□□□.

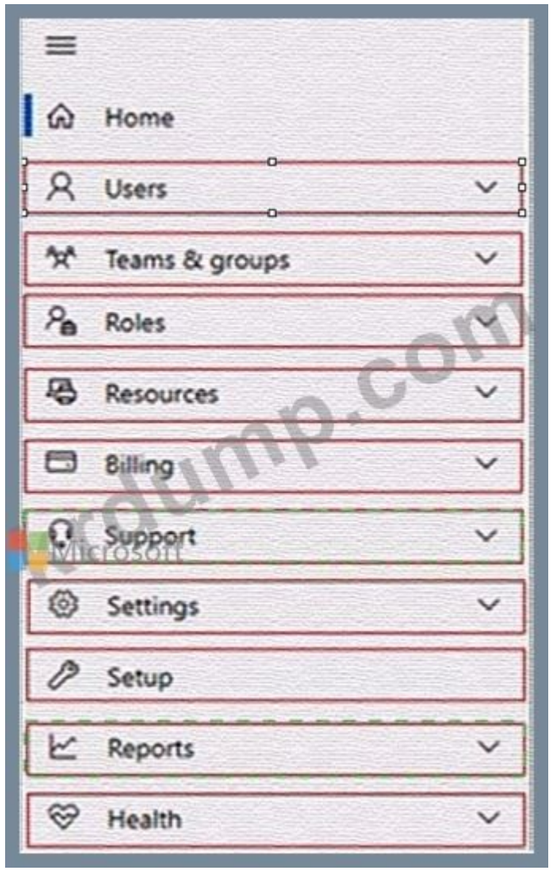
Microsoft□ □□□ □□□ □□□ □□□□.

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

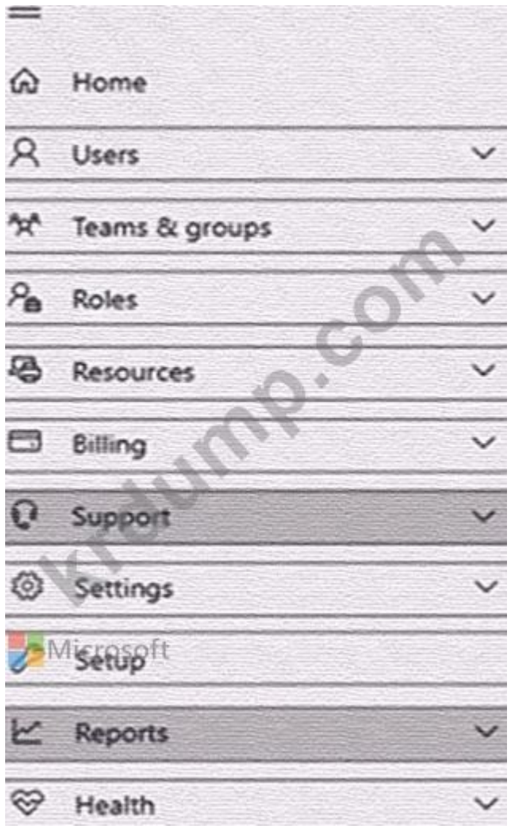
□□□□: □□ □□□ 1□□□□.


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

Answer:



Explanation:



Box 1: Reports

View the Adoption Score of the company.

How to enable Adoption Score

To enable Adoption Score:

Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score Select enable Adoption Score. It can take up to 24 hours for insights to become available.

Box 2: Support

Create a new service request to Microsoft.

Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request.

If you ' re in the admin center, select Support > New service request.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score

https://support.microsoft.com/en-us/topic/contact-microsoft-office-support-fd6bb40e-75b7-6f43-d6f9- c13d10850e77

NEW QUESTION: 120

User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □□ □□□ □□ Policy!□□ □□□□ □□□ □□□□.

* □□ □□□, □□ □ □□□□ □□□□□: User1

* □□ □□□ □□□: 3 - □ □□□

User1□ □□ □□ □□□ □□□ □□□□ □□□□.

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

□□ □□□□ □□ □□□□□□?

A. Mail2, Mail3, Mail4□ □□

B. Mail3 □ Mail4□ □□

C. Mail1, Mail2, Mail3, Mail4

D. Mail4□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 121

Azure AD □□□□ □□□□.

Windows 10 Pro□ □□□□ Azure AD□ □□□ □□□□ 1,000□ □□□□.

Microsoft 365 E3 □□□ □□□□□.

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

□□□ □□ □□□?

A. Microsoft Intune□ □□□□ □□□□□. Edition □□□□□ □ □□ □□ □□□□ □□□□ □□ □□□□ □□□□. Microsoft Endpoint Manager □□ □□□□ □□ □□□□ □□□□ □□□□ □□□□ □ □□□□ □□ □□□□□ □□□□□.

B. Windows □□ □□□□□□ EditionUpgrade □□□ □□ □□□□□ □□□□ □□□ □□□□ Microsoft SharePoint Online □□□□ □□□□□□. □□□□□ SharePoint Online□□ □□□□□ □□□ □ □□□□□ □□□□□.

C. Microsoft Endpoinf Manager □□ □□□□ Windows Autopilot □□ □□□□ □□□□. □□ □□□□ □□□□ □□□□□. □□□□□ □□□□ □□ □□□□ □□□□□ □□ □□□□□ □□□□□.

D. Azure Active Directory □□ □□□□ □□ □□ □□□□ □□ □□ □□□ □□□□. □□□ □□□□□ □□□□ □□□□□ □□□□ □□□□□□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 122

□□□□□□ □□ □□□ □□ Microsoft Entra □□□□ □□□□ □□□□□ Active Directory □□□□ □□□□ □□□□.

Allan Yoo□□ □□□ □□□□□ Active Directory □□□ □□□ Microsoft Entra □□□□ □□□□□□□□. Microsoft 365□□ Allan□ □□□ □□ □□□ □□□ Allan@adatum□□ □□□□ □□ □□ □ □□ □ □□□□.

onmicrosoft.com.

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

□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 123

Project1□ Project2□□ □□ □□ □□ □□□□ □□□□□ □□□ □ □□□ □□□□ □□□.

□□ □□□□□□ □□ □□ □□□ □□□□ □□□?

A. □□□□ □□

B. □□□□ □□ □ □□□ SSO

C. □□□□ □□ □□□ □ □□□ SSO

D. □□□□ □□ □□□

Answer: (SHOW ANSWER)

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

Fabrikam does NOT plan to implement identity federation.

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.

Reference:

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

Topic 5, Litware, IrkLitware, Irk. is a consulting company that has a

main office in Montreal and a branch office in Seattle?

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

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

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

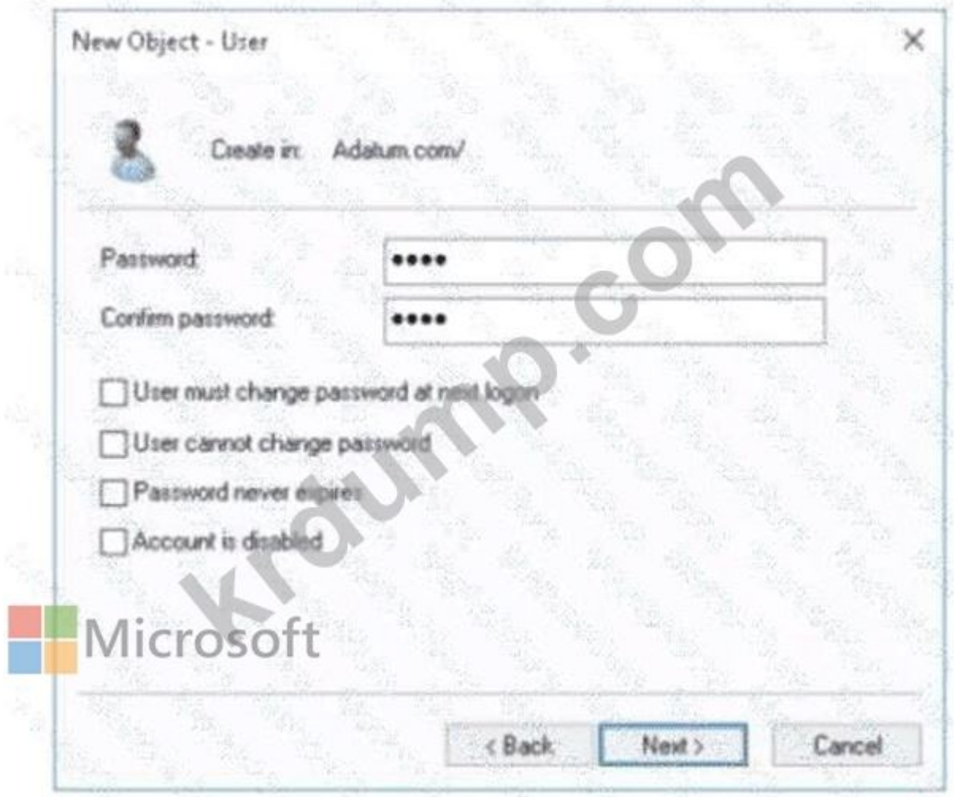
The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.
Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.
The subscription contains a verified DNS domain named litware.com.
Azure AD Connect is installed and has the following configurations:
* Password hash synchronization is enabled.
* Synchronization is enabled for the UtwareAdmins OU only.
Users are assigned the roles shown in the following table.

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

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

* Microsoft 365 incidents and advisories must be reviewed monthly.
* Office 365 service status notifications must be sent to Admin2.
* The principle of least privilege must be used.

NEW QUESTION: 124
□□□ □□□□□□ Azure AD Connect Express □□□ □□□□ Azure AD□ □□□□□ adatum.com□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□ □□ □□ □□□ □□□□□ □□□□.
□□ □□□ □□ User1□□□ □□□□ □□□ □□□□ □□□ Pass□ □□□□□.



Azure AD □□ □□□ □□ □□□ □□ □□□□□.
□□□□ □□
□□□ □□ □□□□ □□ □□ □□□ □□□□□.
□□□□ □□□□ □□ □□ 90
□□□□□ 14□ □□ □□□ □□□□□.
□□
User1□ Azure AD□ □□□□□□□ □□□□□.
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

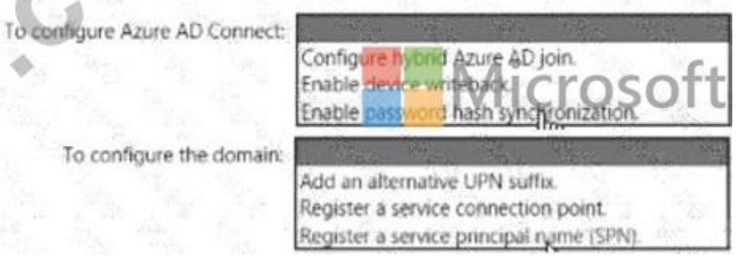
Statements	Yes	No
User1 can sign in to Azure AD.	●	○
User1 can change the password immediately by using the My Apps portal.	○	●
From Azure AD, User1 must change the password every 90 days.	●	○

NEW QUESTION: 125

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

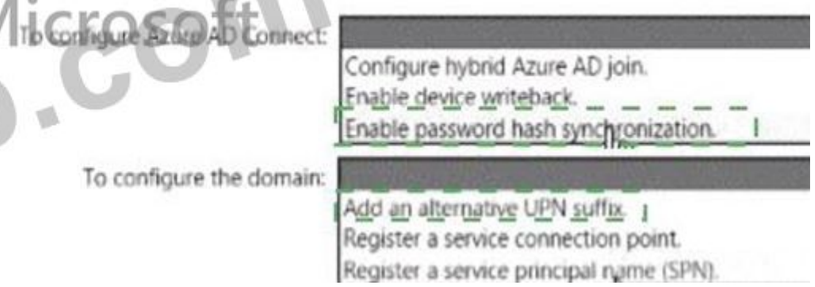
Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□□.
Azure AD Connect□ □□□□ □□□ □□ □ □□ □□□ Azure Directory(Azure AD)□ □□□□□□. □□ □□ □□□□ □□□□□□□.
□□ □□□ □□□ □□□□□.
□□ □□□ □□□□□ Azure AD Connect□ □□□□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



Explanation:

Answer Area

NEW QUESTION: 126

Azure Active Directory(Azure AD) □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □□□□□ Group1□□□ □□□ □□ □□ □□□ □□□□ □□□□□.

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

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

- □□□ □ □□: Group1
- □□□□ □ □□ □□: □□ □□□□ □
* □□ □□:
* □□ □□ □□ □□, □□
* □□ □□□: □□□ □□
□□□□ □□ □□ □□□□ '□'□ □□□□□.
□□ □□ □□□ □□ □□□ □□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

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

Answer:

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

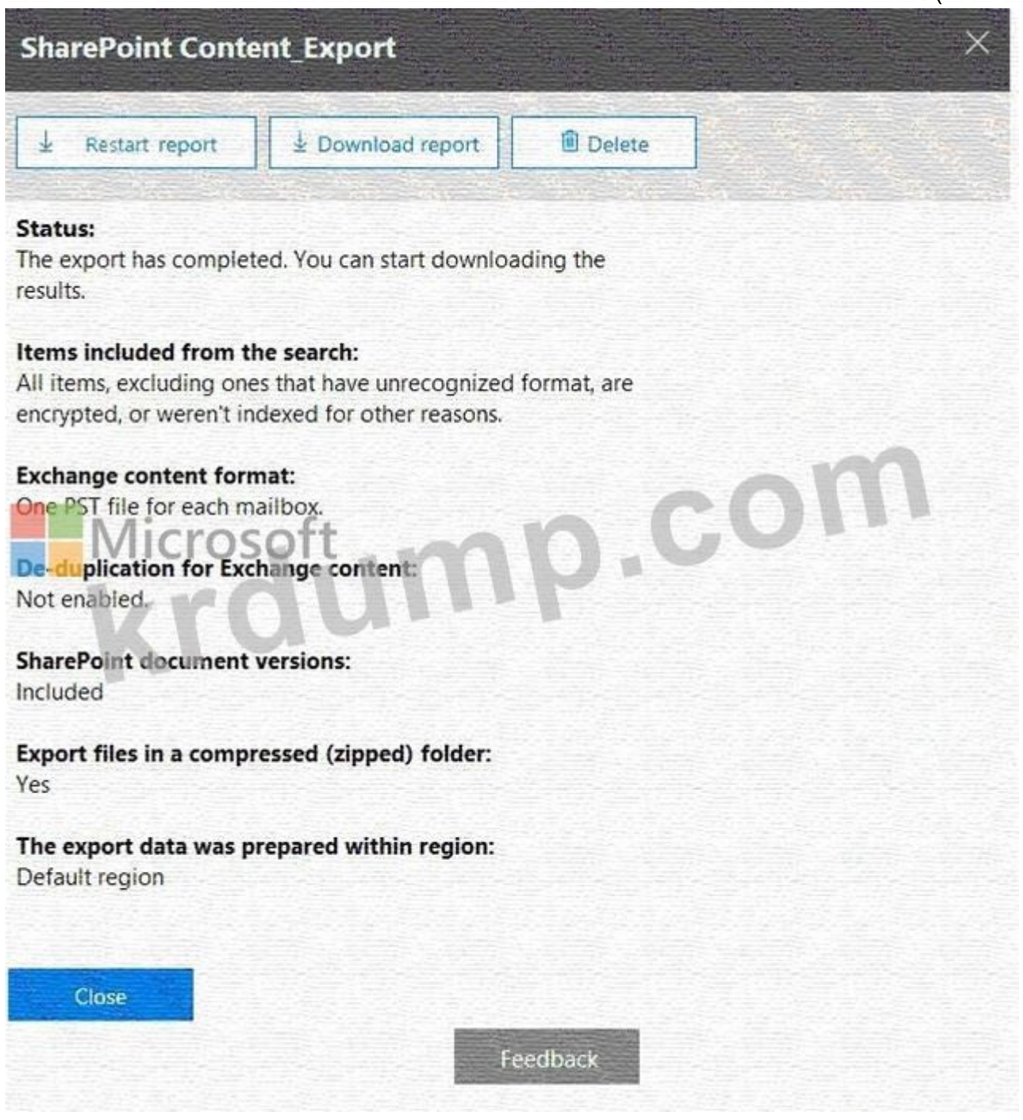
Explanation:

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

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

NEW QUESTION: 127

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



□□□□ □□□□ □□□ □□□□□?

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.

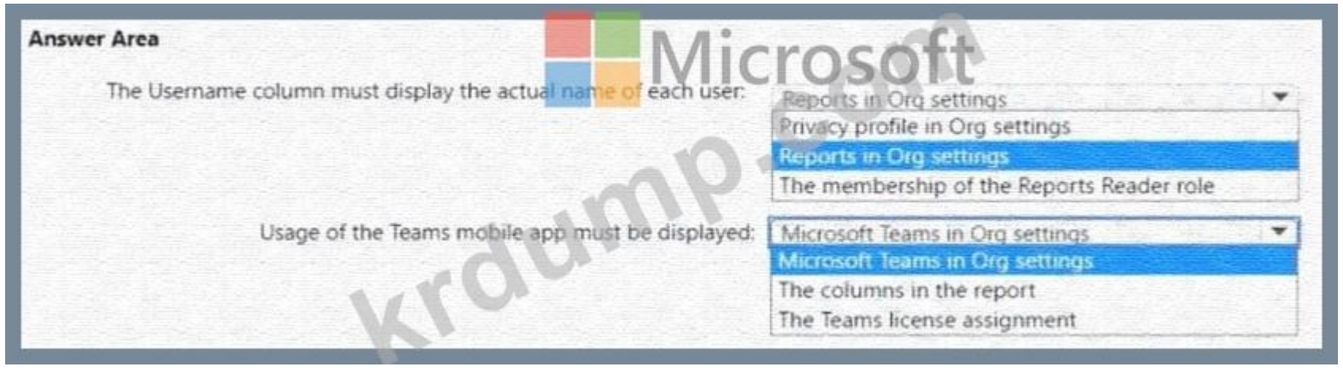
These types of files are considered to be unsupported file types.

Reference:

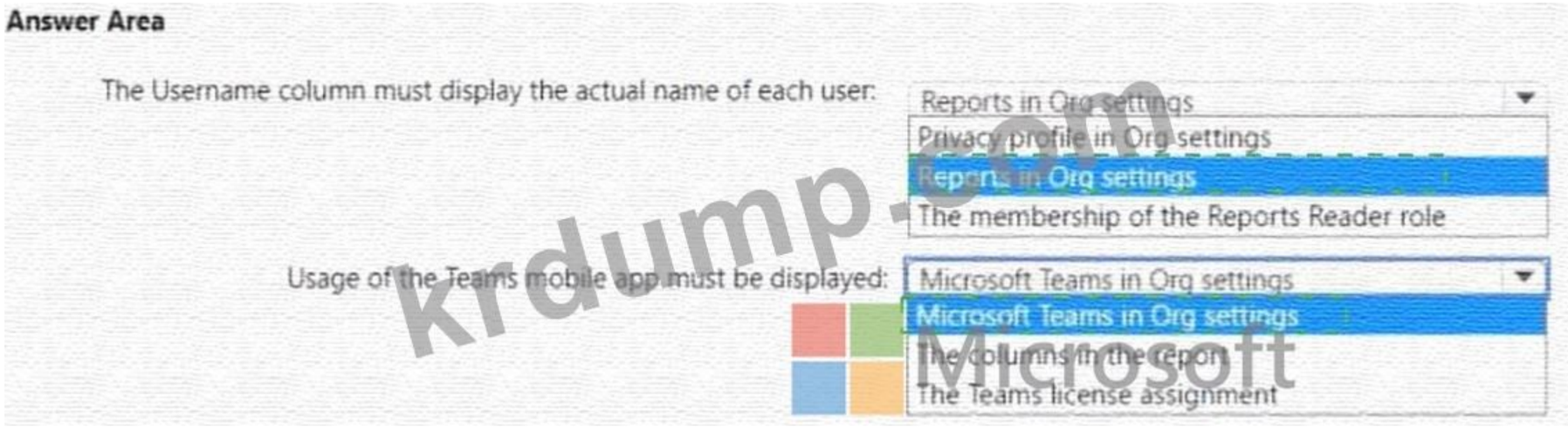
https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide
https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report

NEW QUESTION: 128
Microsoft 365 □□□ □□□□.
Microsoft 365 □□ □□□□ □□ □□□ □□ Microsoft 365 □ □□ □□□□ □□□.

□□□□ □□ □□ □□□ □□□□□ □□□□ □□□.
* □□□ □□ □□□ □ □□□□ □□ □□□ □□□□□ □□□.
* Microsoft Teams □□□ □□ □□□□ □□□□□ □□□.
□ □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□□□ □□□ □□□ □□□□□□. □□: □ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 129
□□□ □□□□ Microsoft E5 □□□□ □□□□.
□□□ ISO/IEC 27001:2013 □□□ □□ □□□ □□□□ □□□.
□□□ □□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□ □□
B. □□ □□□□
C. □□□□□□ □□□
D. □□□ □□ □□(DSR)
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

NEW QUESTION: 130
□□ □□ □□□ □□□□ □□□ Microsoft Entra□ □□□□□ □□□ □□□□.

Name	Description
User1	On-premises directory synchronization service account
User2	Contributor for Microsoft Entra Connect Health
User3	Application Administrator in Microsoft Entra ID

□□ □□□ □□□ □ □□ □□□□ □□□□ □□□.

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

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

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

□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area

Explanation:

NEW QUESTION: 131

□□□ □□□□ Microsoft 365 E5 □□□□ □□□□.

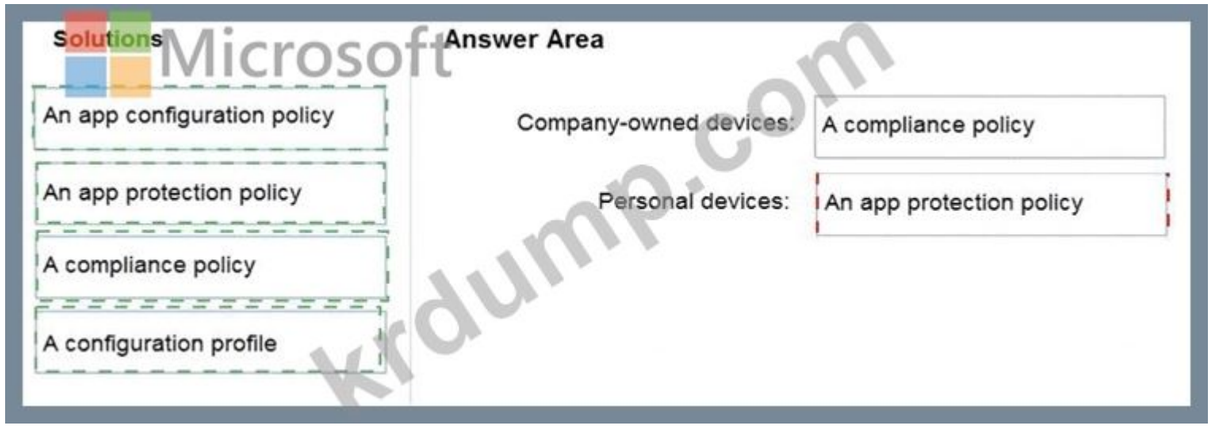
□□□□ □□ □ □□ □□□ Android □□□ □□ □□□□ □□□□ □□□□ □□□□□□. □□ □□□ □□ □□□ □□ □□□ □□ □□□□ Microsoft Exchange Online □□□□ □□□□ □ □□□□.

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

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

□□□□: □□ □□□ 1□□□□.

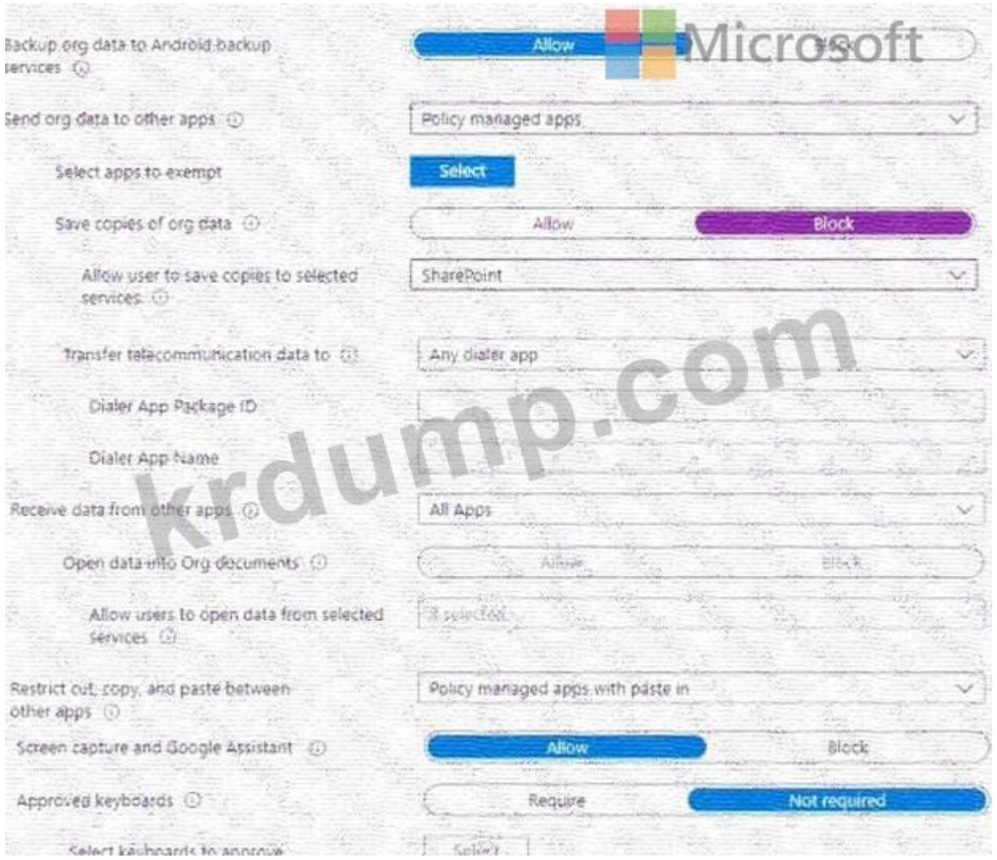
Answer:



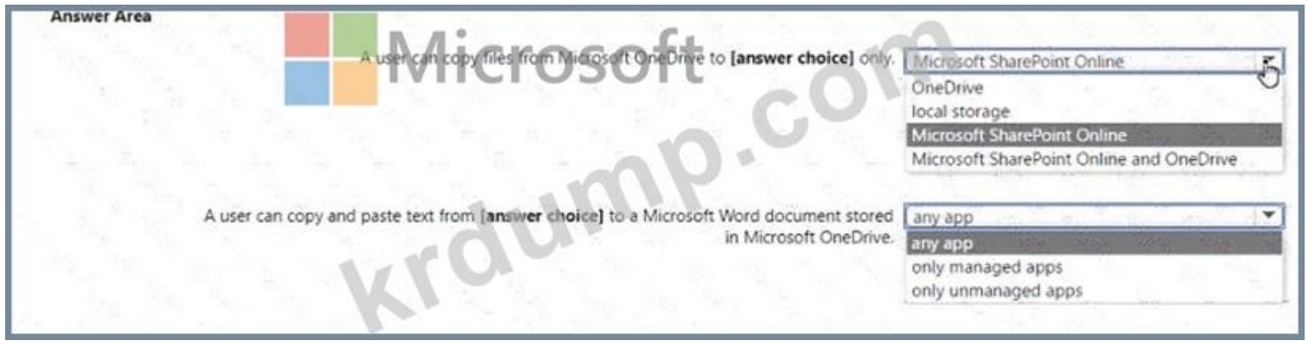
Explanation:

NEW QUESTION: 132
Microsoft 365 E5 □□□ □□ Endpoint Defender for Endpoint□ □□□□ □□□□. Endpoint Defender for Endpoint□ □□ □□ □□□ □□□□□ □□□□ □□□□.
Defender for Endpoint□ □□□□ Device1□□□ □□□ □□□□. Device1□ □□ □□□□ □□ □ □□□ □□□ □□□□ □□□.
Microsoft Defender □□□□ □□□ □□ □□□?
A. □□□□ □□□ □□□□□□.
B. □□ □□□ □□□□□.
C. □□□ □□ □□□ □□□□□.
D. □□1□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 133
Microsoft Intune□ □□□ Android □□ 200□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□ Microsoft □□ □□□□ □□ □□ □□□□□ □□□□ Policy!□□ □□□ Android □ □□ □□□ □□□□.
Policy!□□ □□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□.

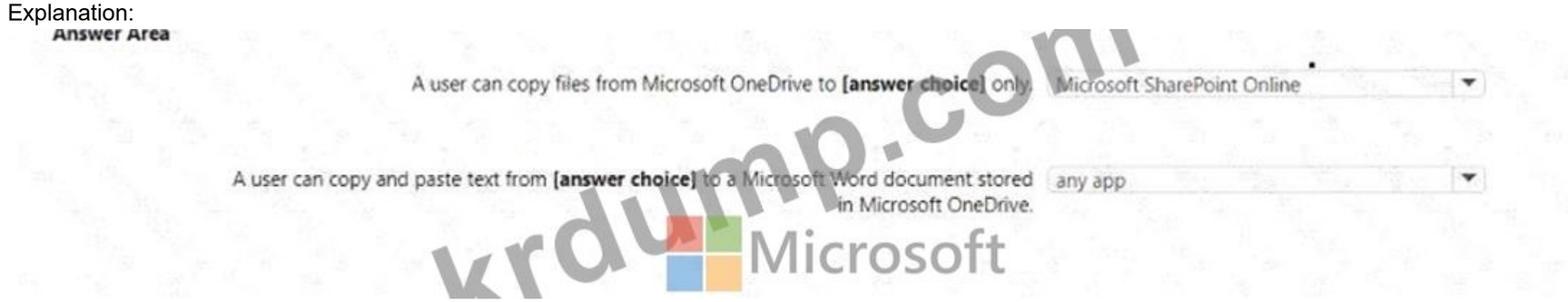

Backup org data to Android backup services
Allow
Block
Send org data to other apps
Policy managed apps
Select apps to exempt
Select
Save copies of org data
Allow
Block
Allow user to save copies to selected services
SharePoint
Transfer telecommunication data to
Any dialer app
Dialer App Package ID
Dialer App Name
Receive data from other apps
All Apps
Open data into Org documents
Allow
Block
Allow users to open data from selected services
Restrict cut, copy, and paste between other apps
Policy managed apps with paste in
Screen capture and Google Assistant
Allow
Block
Approved keyboards
Require
Not required
Select keyboards to approve
Select

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


Answer Area
A user can copy files from Microsoft OneDrive to [answer choice] only.
Microsoft SharePoint Online
OneDrive
local storage
Microsoft SharePoint Online
Microsoft SharePoint Online and OneDrive
A user can copy and paste text from [answer choice] to a Microsoft Word document stored in Microsoft OneDrive.
any app
any app
only managed apps
only unmanaged apps

Answer:

Explanation:



NEW QUESTION: 134

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

60□ □□ □ □□□□ 50□□ □□ □□□ □□□□□□ □□ □□□ □□□ □□□.

□□□ □□□□ □□□?

A. □□ □□

B. □□ □□ □□

C. □□ □□

D. □□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 135

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

Name	Platform
Device1	Windows 11
Device2	Linux
Device3	MacOS

Defender Update □□□ □□□□ □□□□ Endpoint □□ □□□ □□ □□□□□. □□ □□□ □□□ □□□ □ □□□□?

A. Devke1, Device2 □ Devke3

B. Devke1 □ Device3□

C. Device1□

D. Device1 □ Devke2□

Answer: C (LEAVE A REPLY)

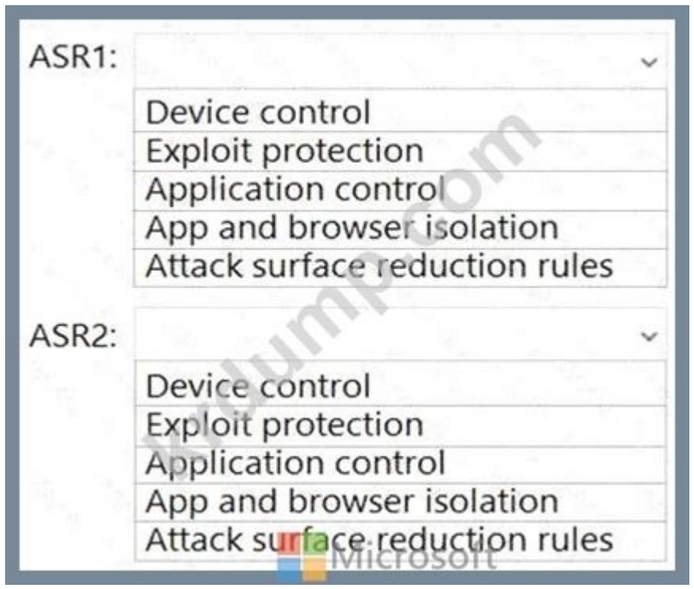
NEW QUESTION: 136

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

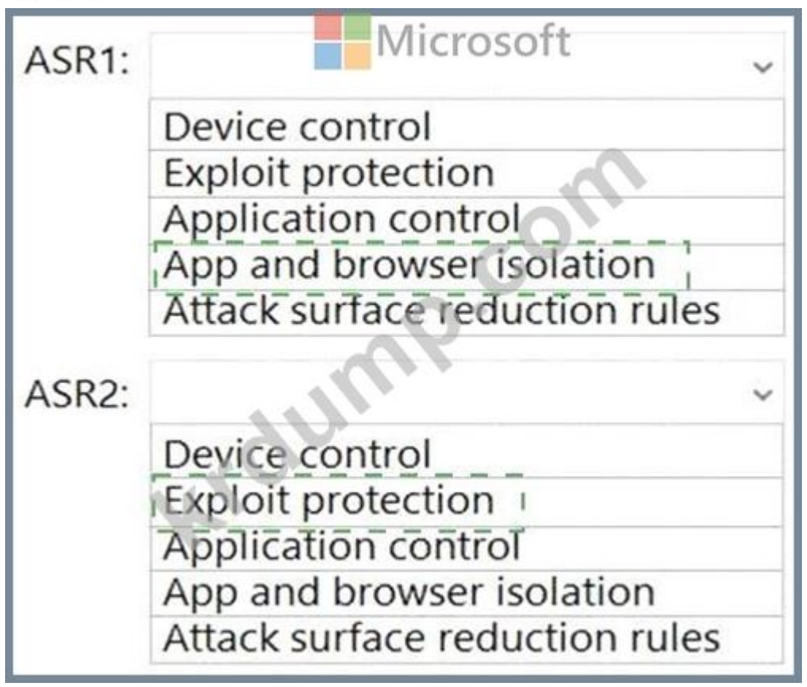
ASR1 □ ASR2□□ □ □□ □□ □□ □□(ASR) □□□ □□ □□□□□. ASR1□ Microsoft Defender Application Guard□ □□□□ □ □□□□□. ASR2□ Microsoft Defender SmartScreen□ □□□□ □ □□□□□.

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

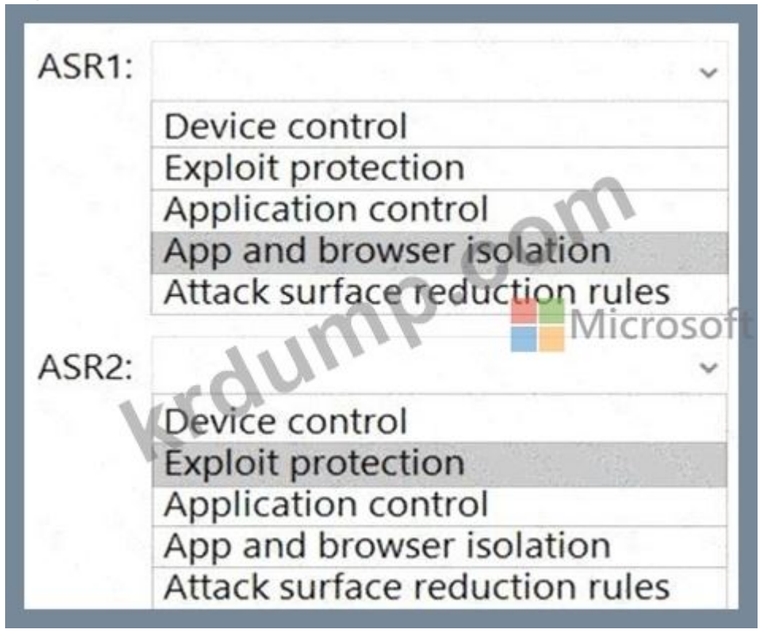
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

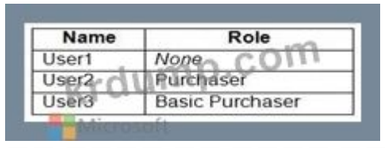


Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy

NEW QUESTION: 137
□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.

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

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



Name	Role
User1	*None*
User2	Purchaser
User3	Basic Purchaser

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

Answer:

Explanation:

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

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

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

□□ □□□ □□□ □□ □□ □□ □□ □□□ □□□□□.
* □□ :
* □□ : Group1
* □□ : Group2
* □□□ : Microsoft Entra ID □□ □□ □□ □□
* □□ □□: □□□□
□□ □□□ □□□ □□□ □□□ □□□ □□□□.
* □□ : Policy1
* □□ :
* □□ : Group1
* □□; □□1
* □□: □□ □□ □□ □□
* □□□ □□□□□□. □□
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□□ □ □□ 1□□□□.

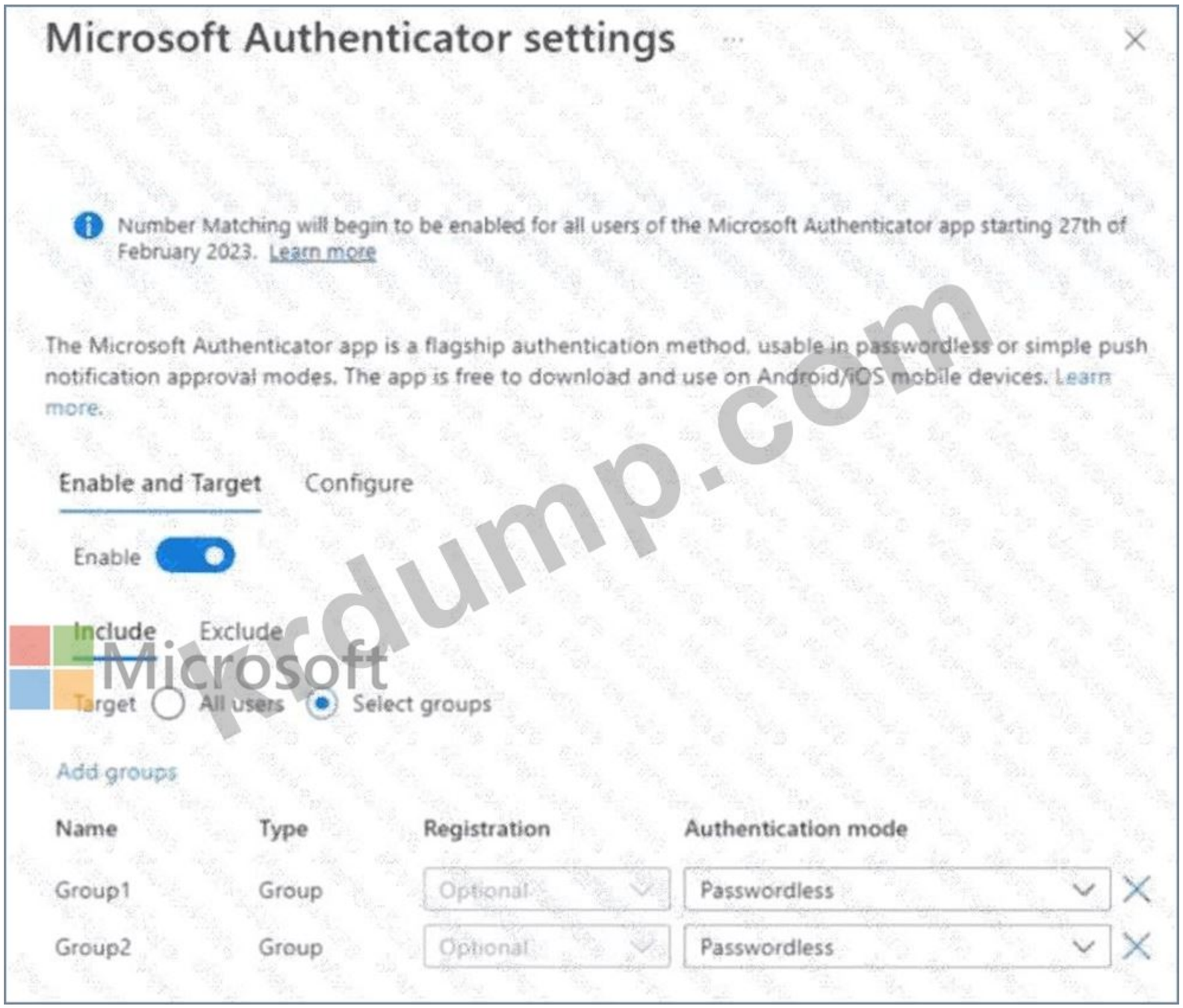
Answer Area

Answer:

Explanation:

User1 will be required to register for MFA on the next sign-in: Yes
User1 is a member of Group1, which is included in the MFA registration policy. Since User1 is not excluded, they will be required to register for MFA on the next sign-in.
User2 will be required to register for MFA on the next sign-in: No
User2 is a member of both Group1 and Group2. Since Group2 is excluded from the MFA registration policy, User2 will not be required to register for MFA.
User3 will be required to register for MFA on the next sign-in: No
User3 is a member of Group2, which is excluded from the MFA registration policy. Therefore, User3 will not be required to register for MFA.

NEW QUESTION: 139
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
□ □□□□ Microsoft Authenticator □□ □□□ Android □□□ □□□ □□□, □□□ □□□□ □□□□□□.
□□ □□□□ □□□ □□ □□□ □□□ □□□ □□□□□.
* □□ : Policy1
* □□
o □□□ □ □□: Group1, Group2
o □□□□ □ □□ □□: □□ □□□□ □
* □□ □□
o □□ □□ □□ □□ □□ □□
* □□ □□□: □□
□□□ □□ Microsoft Authenticator □□□□ Enable □ Target □□□ □□□ □□□ □□ □□□□□. (□□ □□ □□□□□.)


Microsoft Authenticator settings
Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. Learn more
The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. Learn more.
Enable and Target
Configure
Enable
Include
Exclude
Target
All users
Select groups
Add groups
Name
Type
Registration
Authentication mode
Group1
Group
Optional
Passwordless
Group2
Group
Optional
Passwordless

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

Answer:

Explanation:

NEW QUESTION: 140

□□□ □□□□ □□ □□ □□ □□ □□□□ □□□ comoso.onmicrosoft.com□□□ Azure AD □□□□ □□□□.

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

□□ □□ □□□ □□□ □ □□ □□□□ □□□□ □□□.

* User4□ □□□□□ □□□□□□.

* User4□ □□□ □□ □□ □□□□□.

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

□□□□: □□ □□□ 1□□□□.

Answer Area

Reset the password of User4: User1 and User3 only

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

Modify the value for the manager attribute of User4: User3 only

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

Answer:

Explanation:

NEW QUESTION: 141

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

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

Azure AD Connect□ □□□ □□□ □□□□.

□□□□ □□ □□□: □□□□

□□□□ □□: □□□□

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

□□ □□□□ □□□□ □□□?

A. □□

B. □□1 □□□
C. User1□ User2□
D. User1, User2, User3
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn¨

NEW QUESTION: 142
□□□ 5□ □□□ □□□□ □□ □□□□.
□□ □□□□ Microsoft 365 □□□□ □□□□.
□ □□□□ □□ □□□□ □□□□□.
Microsoft Intune□ □□□ □□□□□.
□□ □□ □□□ □□□□ Intune□ □□□□ □□□□ □□□□ □□□□ □□□.
□□ □□□□ □□□ □□□□ □□ □□□□ □□□ □ □□□ □□□.
□□ □□□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□.
□□□ □□□ □□□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. □□ □□□□
B. □□ □□
C. □□ □□□
D. □□□ □□□ □□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

NEW QUESTION: 143
contoso.com□□□ Azure AD □□□□ □□□ Microsoft 365 □□□ □□□□. □□□□□ User1□□□ □□□□ □□□□ □□□□.
Azure AD Identity Protection□ □□□□□□.
User1□ Azure AD Identity Protection□□ □□□□ □□□□ □□□ □□□ □□□ □□□ □ □□□ □□ □□□. □□□□ □□ □□□ □□□ □□□□ □□□.
□□ □□□ User1□ □□□□ □□□?
A. □□ □□
B. □□□ □□□
C. □□□
D. □□□ □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 144
□□□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□□□ □□□ Microsoft Defender for Endpoint□ □□□□□□.
Microsoft Defender □□□□ □□ □□□□□ □□□ □□□ '□□□ □□'□ □□□ □□ □□□□ □□ □ □ □□□□.
□□□□ □□□ □□ □□□ □□ □□□□□ □□□□ □□□□ □□ □□□, □□□ □□ □□□□ □□□ □□□ □ □□□ □□□.

Microsoft Defender □□□□ □□□ □□□□ □□□?

A. □□□□ □□ □□

B. □□ □□ □□

C. □□ □□

D. □□ □□

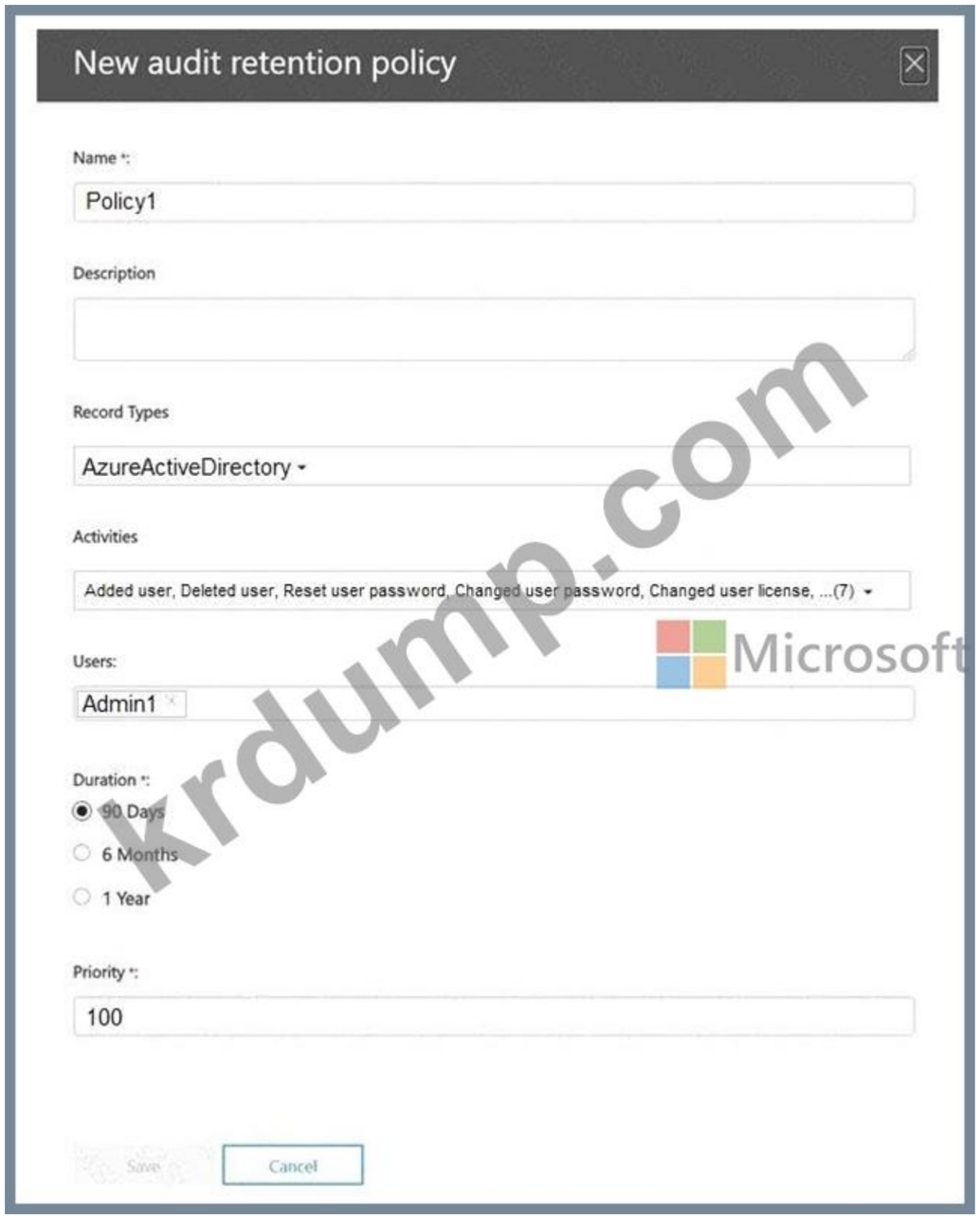
Answer: (SHOW ANSWER)

NEW QUESTION: 145

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

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

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



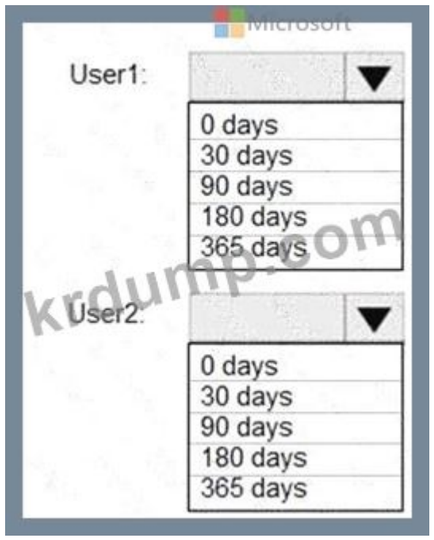
Policy1□ □□□ □□□ □□ □□□ □□□□□.

* Admin1□ User1□□□ □□□□ □□□□□.

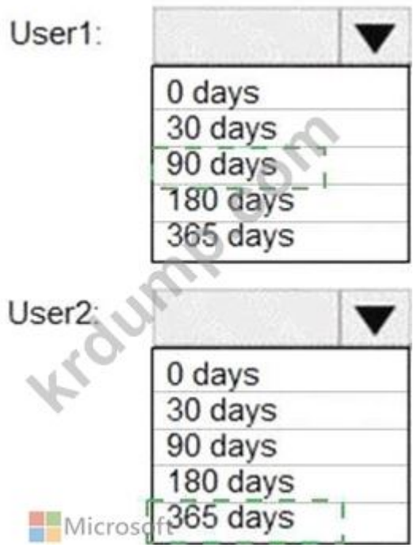
* Admin2□ User2□□ □□□□ □□□□□.

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

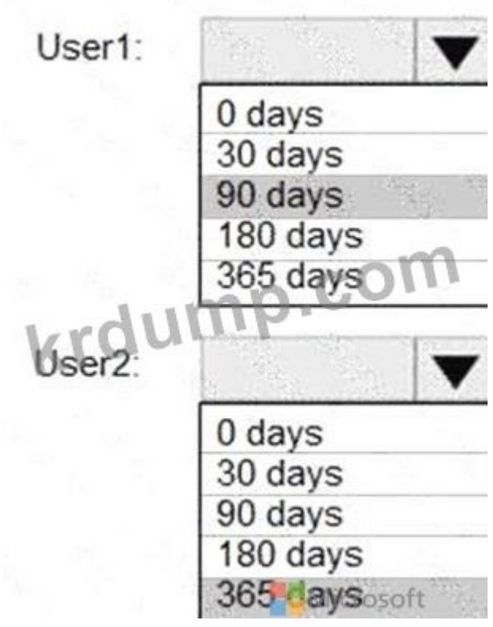
□□□□: □□ □□□ 1□□□□.



Answer:



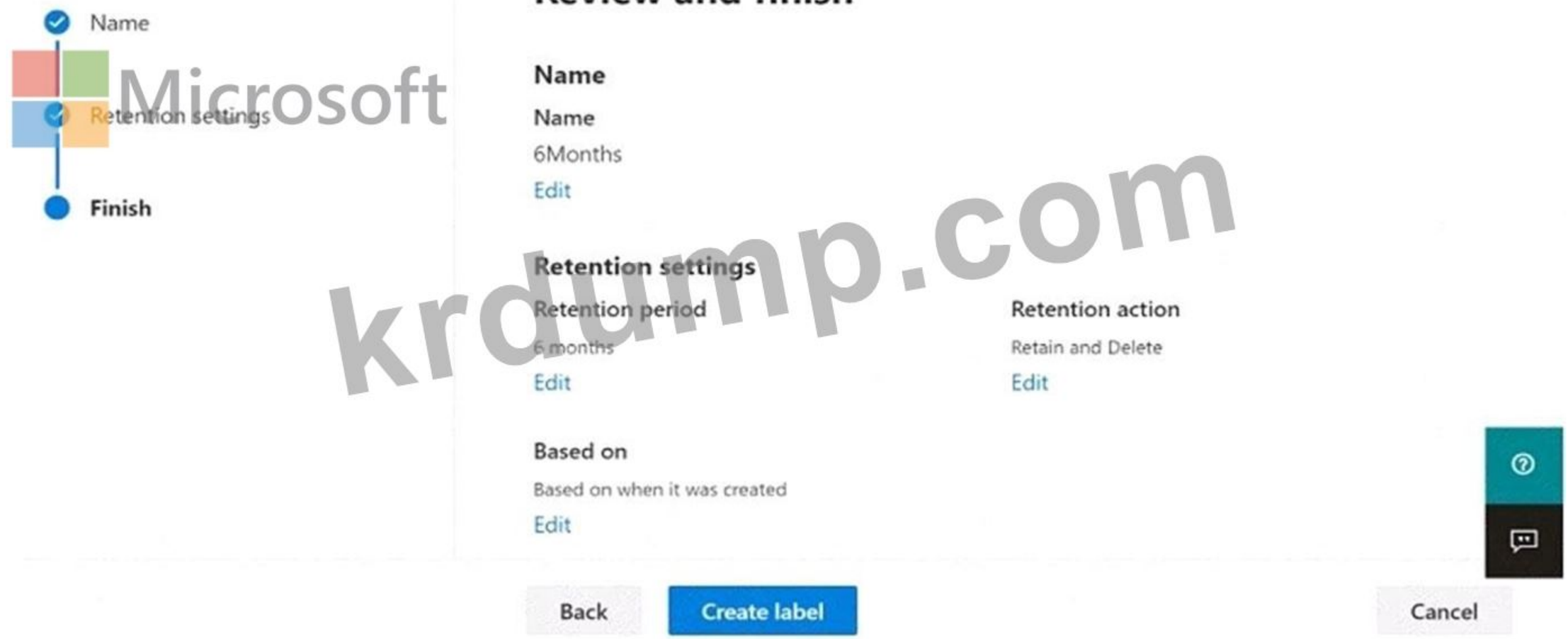
Explanation:



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

NEW QUESTION: 146
Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□□.
Microsoft Endpoint Manager □□ □□□□ □□□□ □□□□□ □□□ □□ □□□ □□, □□ □□ □□□ □□□□□□. □□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□ □ □□□□?
A. 30
B. 10
C. 90
D. 45
Answer: C (LEAVE A REPLY)

NEW QUESTION: 147
□□□
Microsoft 365 □□□□ □□□□.
□□ □□ □□□ □□□ □□ □□ □□□ □□□□. (□□ □□ □□ □□□□□.)



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

□□ □□□ □□ □□ □□ □□□□□.

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

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

Answer Area

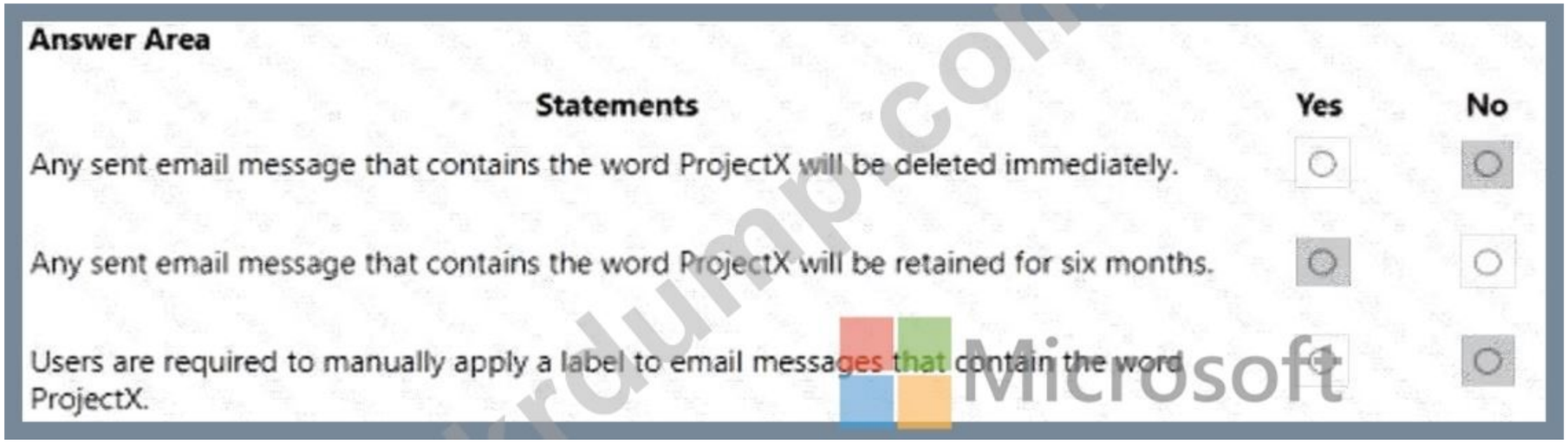
Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	○	○
Any sent email message that contains the word ProjectX will be retained for six months.	○	○
Users are required to manually apply a label to email messages that contain the word ProjectX.	○	○

Answer:

Answer Area

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

Explanation:



Box 1: No
Box 2: Yes
Box 3: No
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

NEW QUESTION: 148
Microsoft 365 E5 □□□□ □□□□.
□□□□□ Microsoft Office 365 □□ □□□ □□□□ □□□ □□□□□ □□□ □□□□ □□□.
□□□ □□□□□ □□□ □□□□ □□□?
A. Microsoft 365 □□ □□
B. Microsoft Purview □□ □□ □□
C. Microsoft Apps □□ □□
D. □□□□ □ □□□ Microsoft Defender
Answer: D (LEAVE A REPLY)

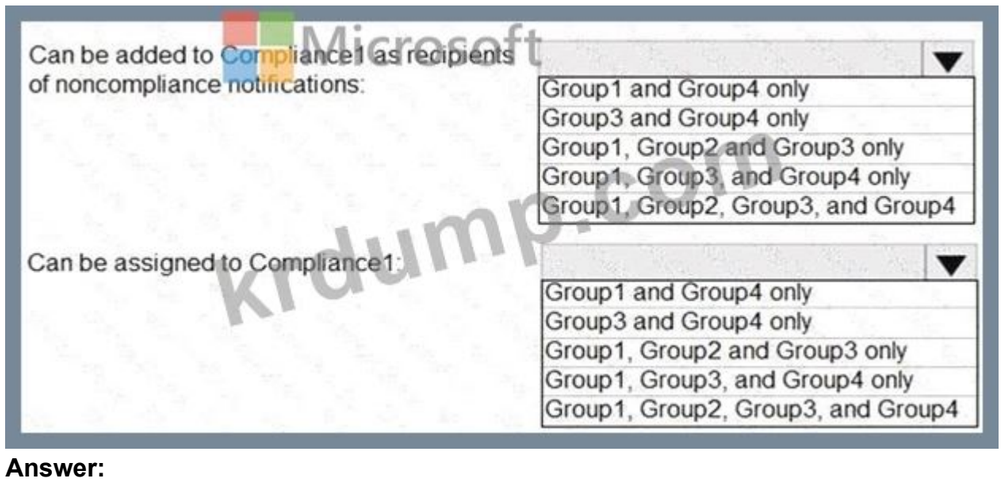
NEW QUESTION: 149
Microsoft Store for Business□ □□□□ □□ User1□□□ □□□□ □□□□ Microsoft 365 □□□□ □□□□. User1□ Microsoft Store for Business□□ □□ □□□ □□□ □ □□□ □□□□ □□□.
* □□□□□ □□□□□ □□□□□.
* Microsoft Store□□ □□ □□□□□.
* □□ □□□ □□ □□ □□□ □□□ □□□□□.
□□□□ □□ □□□ □□□ □□□□ □□□.
User1□□ □□ Microsoft Store for Business □□□ □□□□ □□□?
A. □□□□□
B. Device Guard □□□
C. □□□
D. □□□

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

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

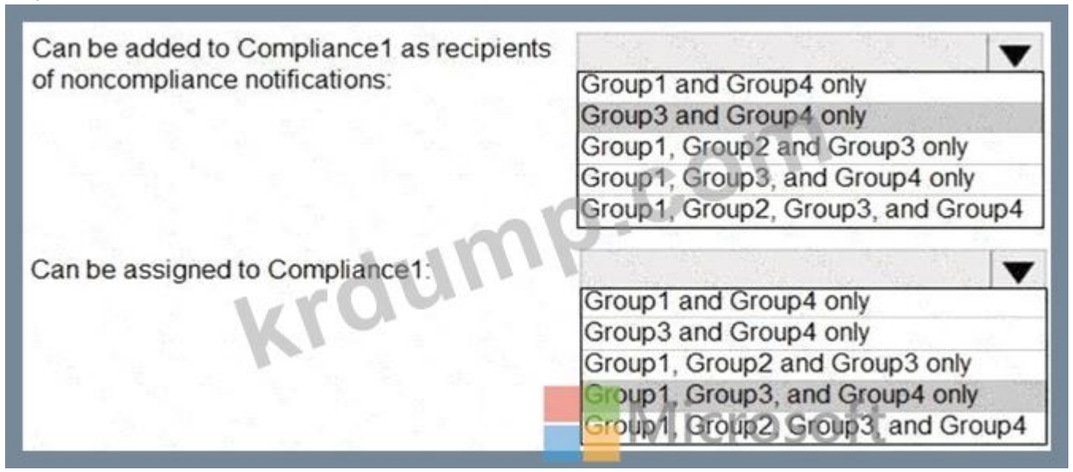
Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

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



Answer:

Explanation:



Reference:

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

NEW QUESTION: 151

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

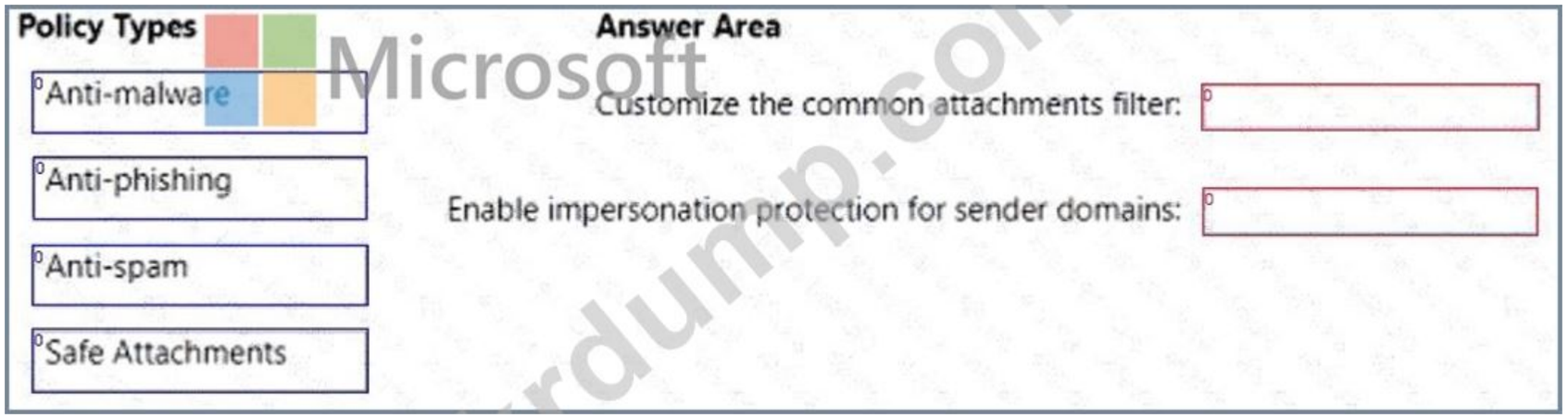
□□ □□ □□□ □□□□□ □□□ □□□□ □□□.

□□□□ □□ □□ □□□ □□□ □□□□□.

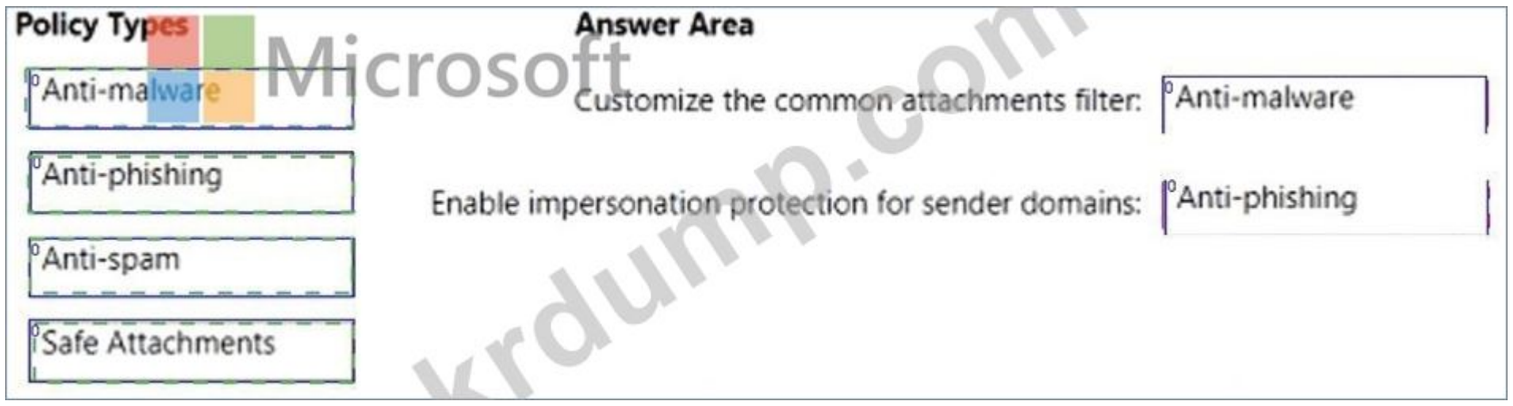
□□□ □□□□ □□ □□ □□□ □□□□□□.

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

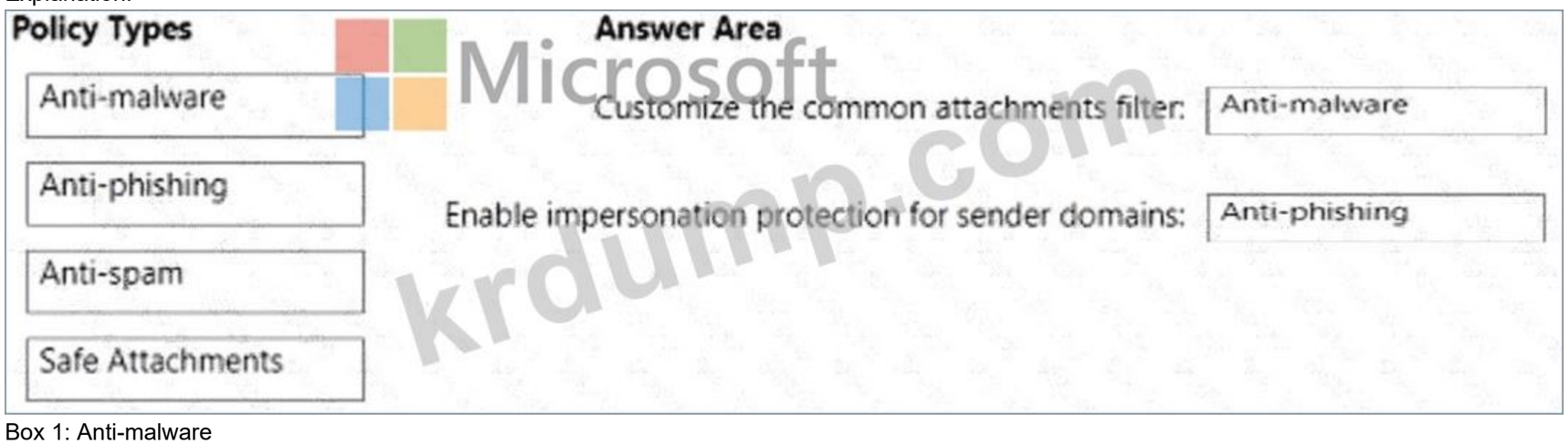
□□□□: □□ □□□ 1□□□□.



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:

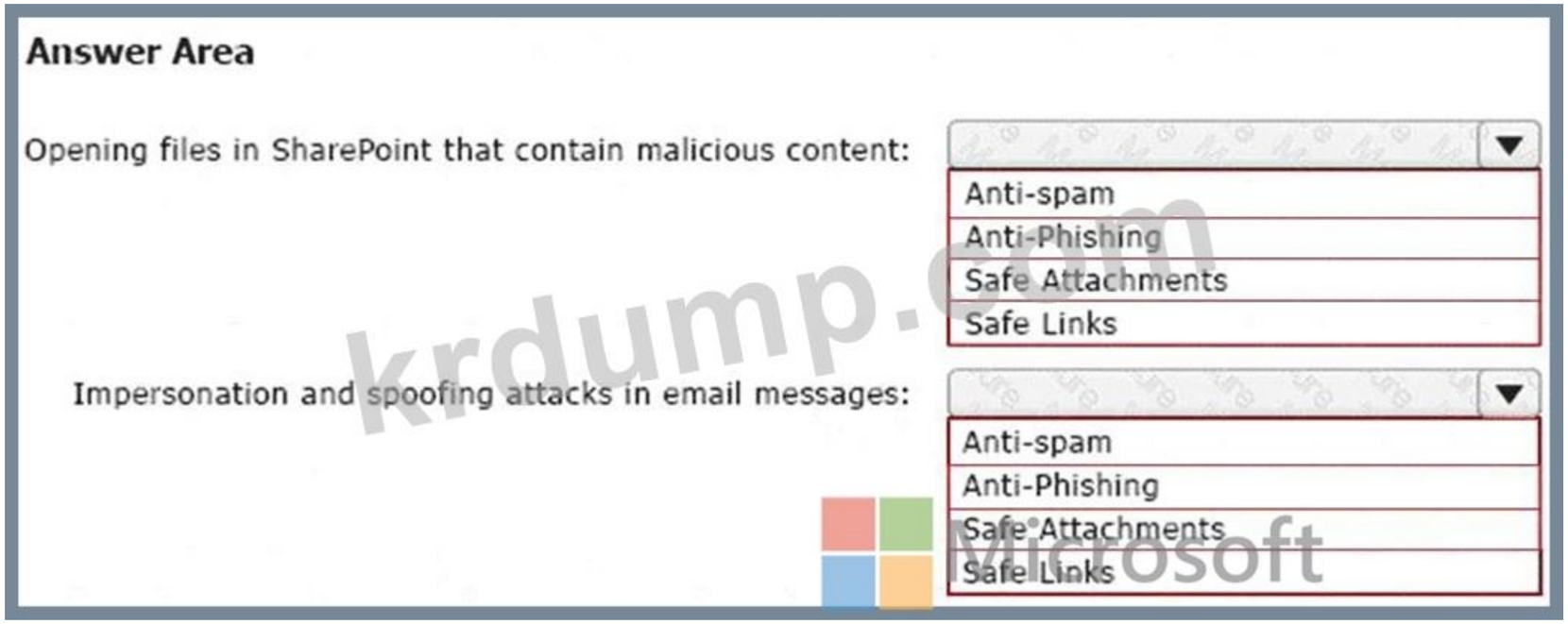
Feature	Anti-phishing policies in EOP	Anti-phishing policies in Defender for Office 365
Automatically created default policy	✓	✓
Create custom policies	✓	✓
Common policy settings*	✓	✓
Spoof settings	✓	✓
First contact safety tip	✓	✓
Impersonation settings		✓
Advanced phishing thresholds		✓

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

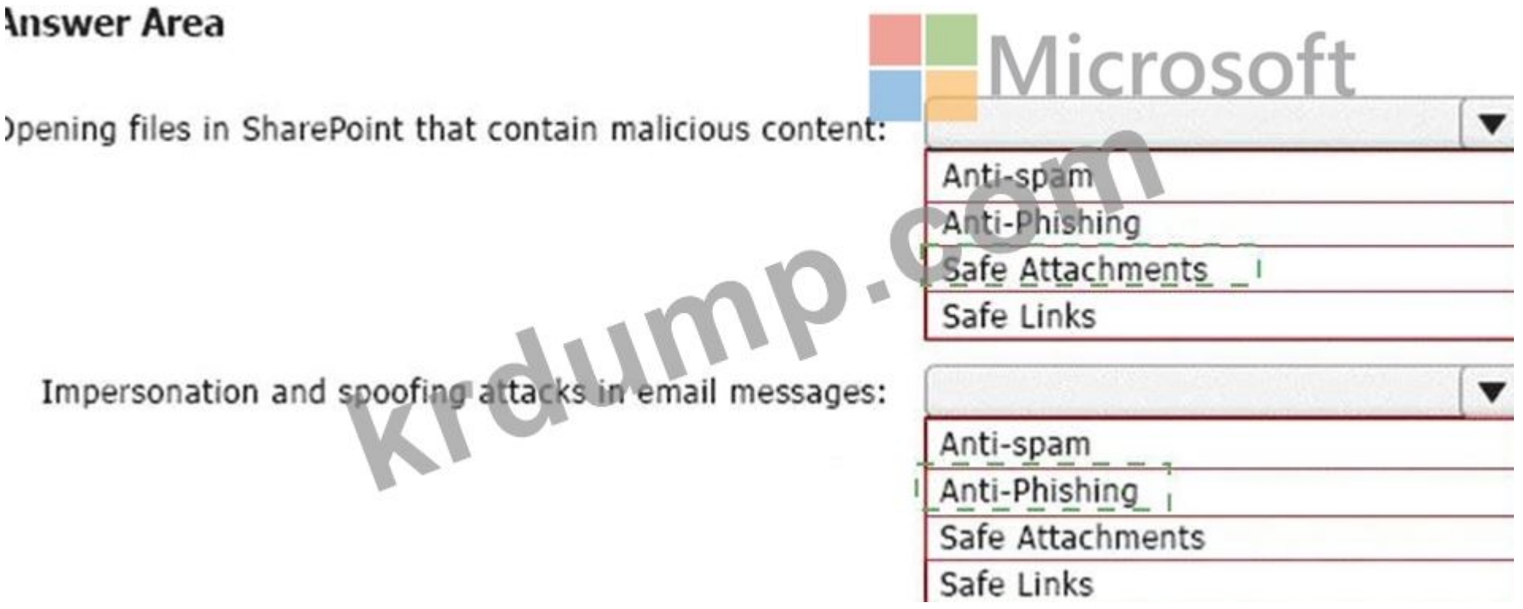
NEW QUESTION: 152
Microsoft 365 □□□□ □□□□.
□□ □□□ □□ □□ Windows 10 □□□ □□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□□ □□□□□.
□□□ □□ □□□ □□□□ □□□□□.
Microsoft Defender Antivirus □□□ □□ □□□ □□□□□□.
□□ □□□ □□□□ □□ □□□ □□□□ □□□□ □□□□□ □□ □□□□ □□□.
□□ □ □□ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. □□ □□
B. □□ □□
C. □□ □□ □□□
D. □□□ □□□ □□
E. □□ □□□
Answer: B,D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION: 153
Microsoft 365 E5 □□□ □□□□. □□□□□ FID02 □□ □□ □□□□□.
FID02 □□ □□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□□ □□□. □□□ □□ □□ □□□ □□ □□□ □□□□ □□□?
A. □□□ □□□ □□ □□ □□□ □□□□□.
B. □□ □□ □□
C. □□ □□ □□
D. □□□ □□□□□ □□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 154
□□□
Microsoft 365 □□□ □□□□.
□□□ □□□ □□ □□ □□ □□□□ □□□□ □□□□.
□□□□ □□□ □□ □□□□□□ □□□ □□ □□□□ □□□□□ □□□.
* □□ □□□□ □□□ Microsoft SharePoint□ □□ □□
* □□□ □□□□□□ □□ □ □□□ □□
Microsoft 365 Defender□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 155
Microsoft J65 E5 □□□ □□□□.
Microsoft Defender for Endpoint□ Microsoft Intune□ □□□□□.
Intune□ □□□ □ □□□ Defender for Endpoint□ □□□□ □□□□□□ □□ □□□.
□□ □□: □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 156
Microsoft 36S E5 □□□ □□□□.
□□ □□ □□□ □□ Microsoft Defender for Endpoint□ □□□ □□□□□ □□□□.

Name	Platform
Device1	Windows 11
Computer2	Windows 11
Device3	Android

□□ □□ □□□ □□ □□□ □□□□.

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

IP □□ □□□□ □□ □□ □□ □□□□□.

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

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

□□: □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 157

□□□ □□□□ Microsoft 365 E5 □□□□ □□□□.

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

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

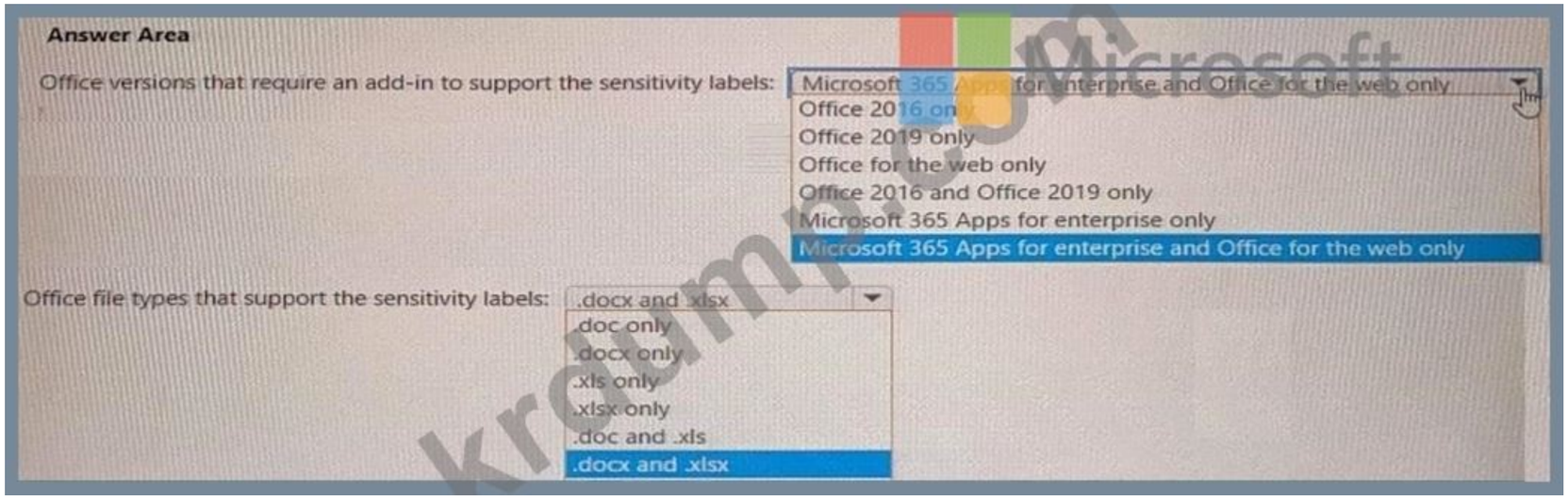
□□ □□□□□ □□□ □□ Office □□ □□□ □□□□□.

* .docx
* .xlsx
* .□□
* □□

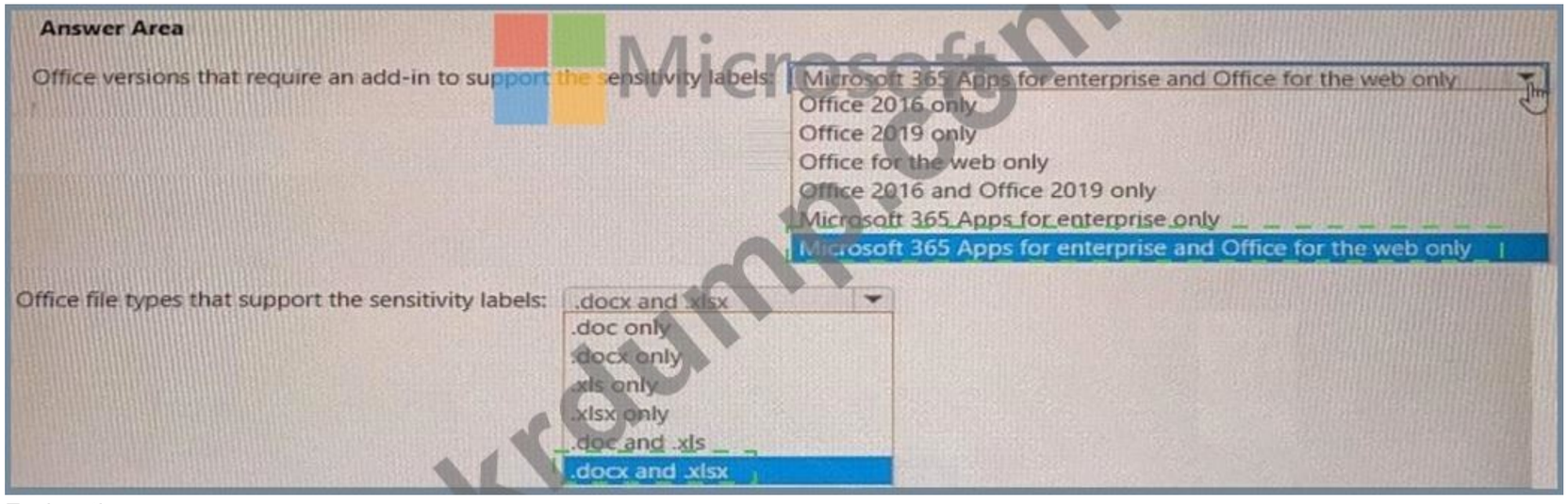
□□□ □□□□ □□□ □□□□□. □□□ □□□□ □□□.

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

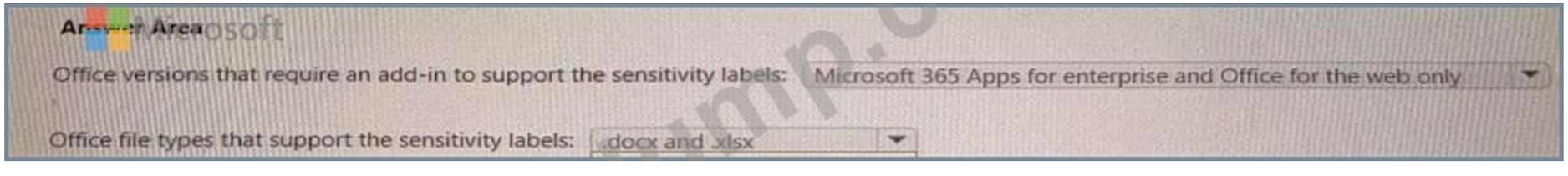
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 158

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

□□□ □□ □□ □□□ □□□□□.

User1□□ □□ □□ □□□ □□□□ □□□: □□ □□□ □□□□ □□□ □□.

□□ □□ □□□ □□ □□□?

A. □□ □□ □□□□□ □□ □□□□ □□□.
B. Azure Active Directory □□ □□□□ □□ □□□ □□ □□□(SSPR)□ □□□□□ □□□□□.
C. Microsoft 365 □□ □□□□ SSPR(□□ □□□ □□ □□□) □□□ □□□□□.
D. Azure Active Directory □□ □□□□ User1□ □□ □□ □□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?
view=o365-worldwide
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure- portal

NEW QUESTION: 159
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.
□□□ □□ □□□ □□□ □□□□□.
User1□ □□ □□□ □□□ □ □□□ □□□□ □□□.
□□□ □□□□□.
□□□ □□□□□.
□□□□ □□□□ □□□□.
□□□ □□□□ □□□□ □□□ □□□□ □□□□□.
□□□□ □□ □□□ □□□ □□□□ □□□.
□□ □□ □□□ User1□ □□□□ □□□?
A. □□□ □□ □□
B. □□ □□ □□ □□□
C. □□ □□ □□ □□□
D. □□ □□ □□ □□□
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365- worldwide

NEW QUESTION: 160
Microsoft 365 E5 □□□ □□□□. DLP1□□□ □□□ □□ □□(DLP) □□□ □□□□.
DLP1□ □□ DLP □□□□ □□□□□ □□ □□□ □□□ □ □□□ □□□□ □□□. DLP1□ □□ □□□ □□□□ □□□?
A. □□□□□ □□□
B. □□
C. □□□□
D. OneDrive □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 161
Microsoft 365 □□□ □□□□.
Exchange □□ □□□□ □□ □□□ □□ Policy1□□□ DLP(□□□ □□ □□) □□□ □□□□.
* □□ □□□□ □□□ □□□□ □□□□□.

* □□ □□ □ □□□□ □□□□□: □□□□ □□□□□□□.
□□ □ □□ □□ □□ □□□□ □□ □□□ □□ Policy2□□ DLP □□□ □□□□.
* □□ □□□ □□□□□: □□□□ □□□□□.
* □□ □□ □ □□□□ □□□□□: □□□□ □□□ □□□□ □□□□ □□□□.
* □□□□ □□□□ □□ □, □□□□ □□ □□□ □□□□ □□ □□ □□□□□ □□□□.
□□□□ □□□□ □□ □ DLP □□□ □□□ □□□□□? □□□□□ □□□ □□□ □□□ □□□□□ □□□ □□□□□. □ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □□□ □□□ □□□ □□□□□ □□□□ □ □ □□□□.
□□□□: □□ □□□ 1□□□□.

Results

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

Answer Area

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

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

Answer:

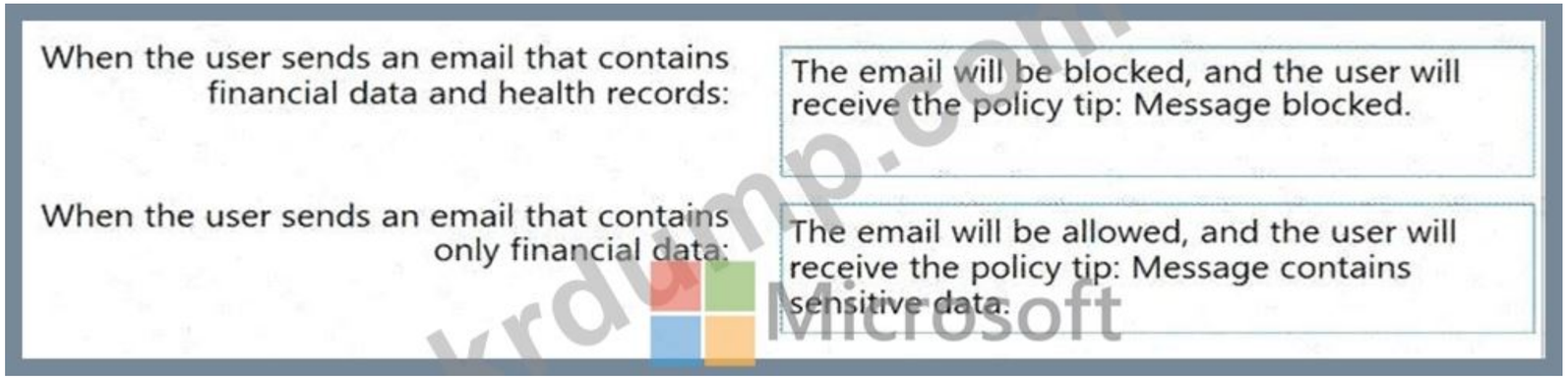
Results

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

Answer Area

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

Explanation:



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

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

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

Reference:

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

NEW QUESTION: 162

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

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

Microsoft Exchange Online □□□ □□□□□.

Microsoft 365 □□□ □□□□.
User1□ 8□□ □□□ □□□ □□□ □□□ □□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. zure AD ID □□
B. Microsoft Entra □□□ ID
C. □□□ □□□
D. Azure AD □□ □□ ID □□(PJM)
Answer: D (LEAVE A REPLY)
Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:
Provide just-in-time privileged access to Azure AD and Azure resources
Assign time-bound access to resources using start and end dates
Require approval to activate privileged roles
Enforce multi-factor authentication to activate any role
Use justification to understand why users activate
Get notifications when privileged roles are activated
Conduct access reviews to ensure users still need roles
Download audit history for internal or external audit
Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

NEW QUESTION: 163
Microsoft 36S E5 □□□ □□□□.
Group1□□□ □□□ □□□ □□□□ □□ Microsoft Defender to Cloud Apps□ □□□□□.
□□ 1□ □□□□ □□□□ □□ □□□ □□□□□□□ □□□□ □ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

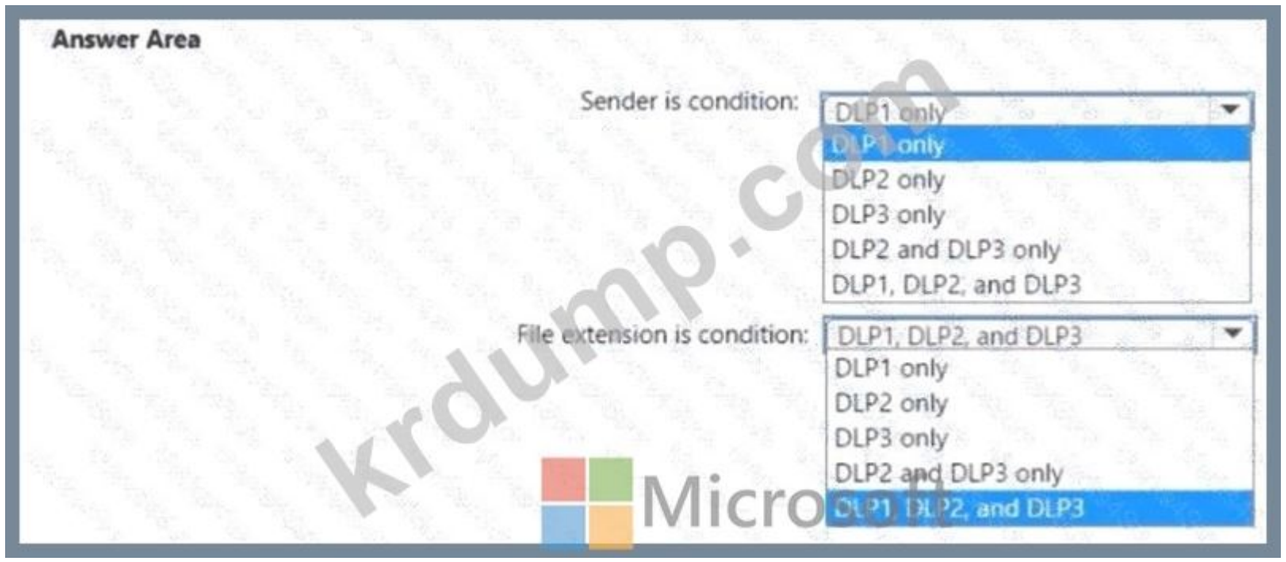
Answer:

Explanation:

NEW QUESTION: 164
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□ □□ □□(DLP) □□□ □□□ □□□□□.

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

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



Answer:

Explanation:

NEW QUESTION: 165

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □ □□ □□ □□□□ □□□ □ □□□, □□ □□□ □□ □□□ □□□□ □□□□.
□□□□□ Active Directory □□□□ □□□□ □□□□.
Azure AD □□□□ □□□□□.
□□ □□□□ □□□□ Azure AD□ □□□□□□ □□□□□.
□□ □□(OU)□ 10□ □□□ □□□ Azure AD□ □□□□□ □□ □□ □□□□□□. □□ □□ □□□ □□□ □□□□□ □□□□□□□□.
Azure AD Connect Health□ □□□□ □□ □□□ □□ □□□□ □□□□□ □□□□□□ □□□□□.
10□□ □□□ □□□ Azure AD□ □□□□□□□ □□□□ □□□.
□□ □□: Azure AD Connect□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

NEW QUESTION: 166
□□ □□□□ □□□ □□□ □□□□□.

□□□□ □□□□ □□ □□□ □□□ □ □□□?

A. Label3, Label4, Label6□

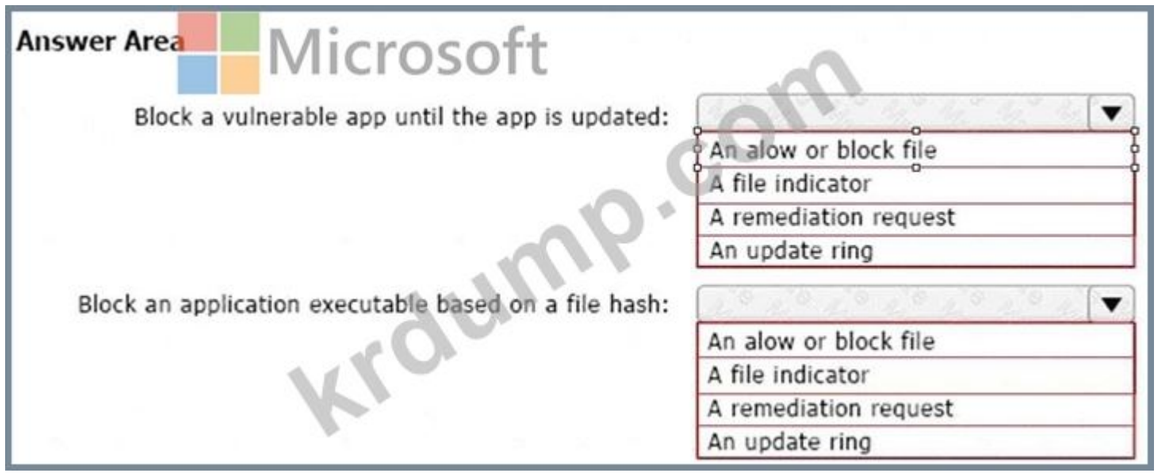
B. □□1, □□2. □□3. □□4. □□5. □□□ □□6

C. Label1, Label2, Label5□

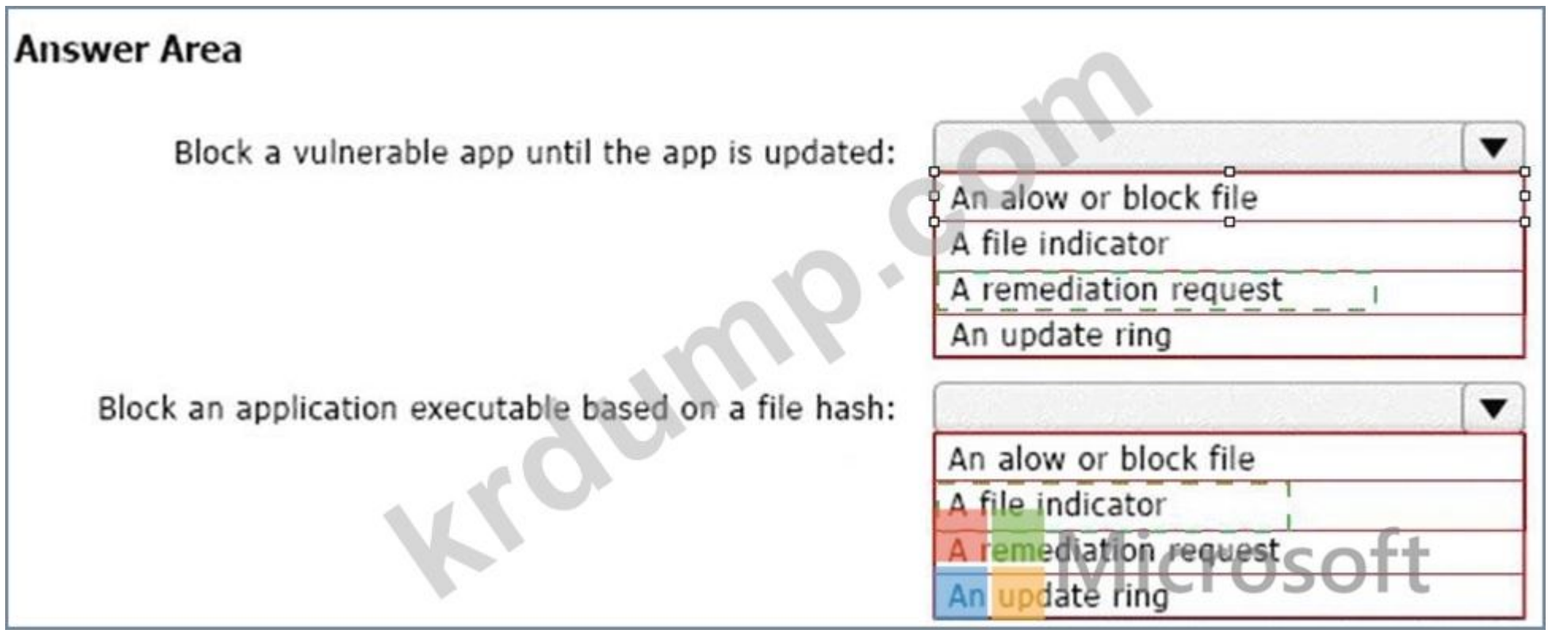
D. Label1, Label3, Label4, Label6□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

NEW QUESTION: 167
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: 168
□□□
Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□ Windows 11 □□□ Microsoft Defender for Endpoint□ □□□□□.
□□ □□ □□□ □□□□□ Defender for Endpoint□ □□□□ □□□.
* □□ □□□□□ □□□ □□□ □□ □□□□□.
* □□ □□□ □□□□ □□□□□□ □□ □□□ □□□□□.
□□□□ □□□ □□□ □□□□□ □□□.
□ □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

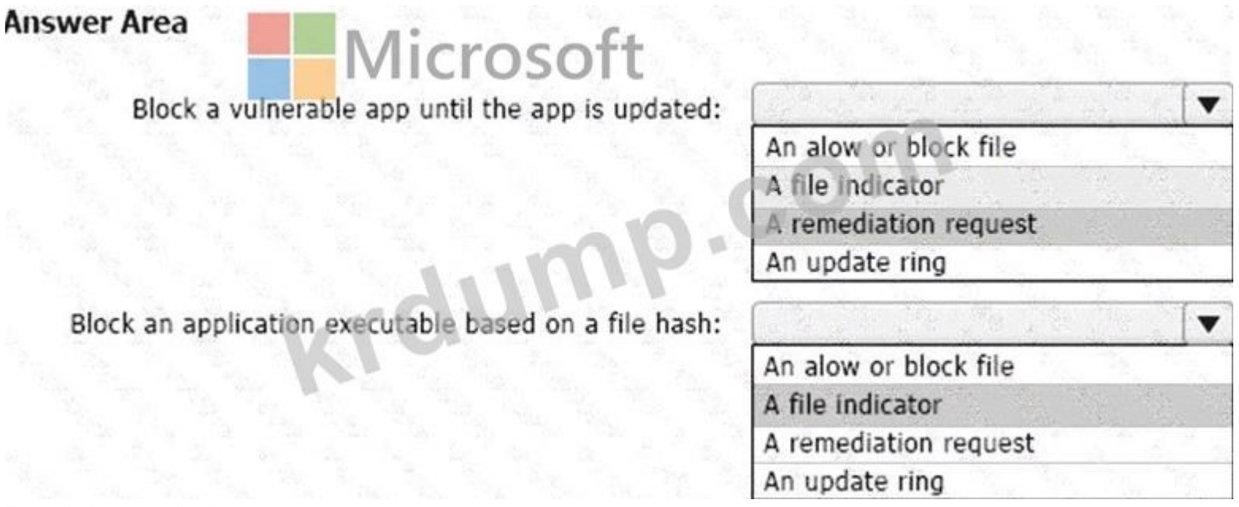


Answer:



Explanation:

Answer Area



Box 1: A remediation request

Block a vulnerable app until the app is updated.

Block vulnerable applications

How to block vulnerable applications

Go to Vulnerability management > Recommendations in the Microsoft 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: 169

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

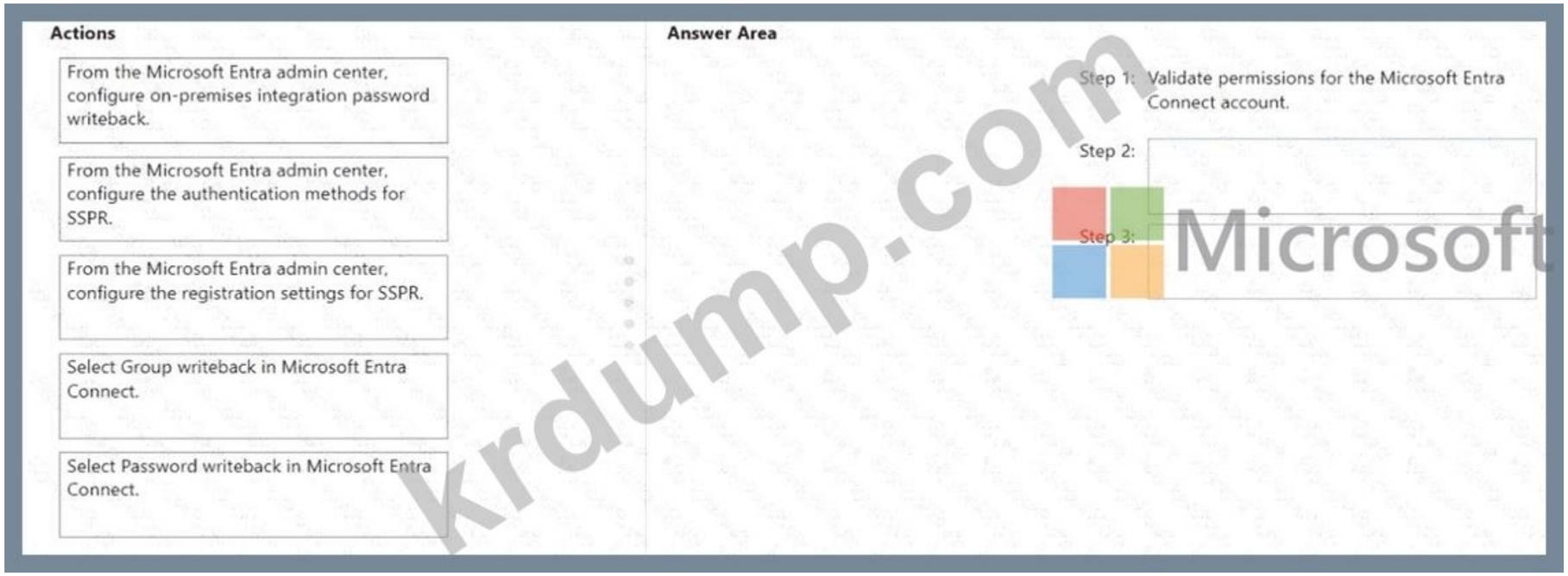
□□ □□□□ Microsoft Entra Connect□ Express Settings□ □□□□ Active Directory Domain Services(AD DS)□□ □□□□ □□□□□□.

□□ □□□ □□□□ □□□(SSPR)□ □□□ □□□□□.

□□□□ □□□□□ □□□□□□ □□□□ □□□□□ AD DS□ □□□□□□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

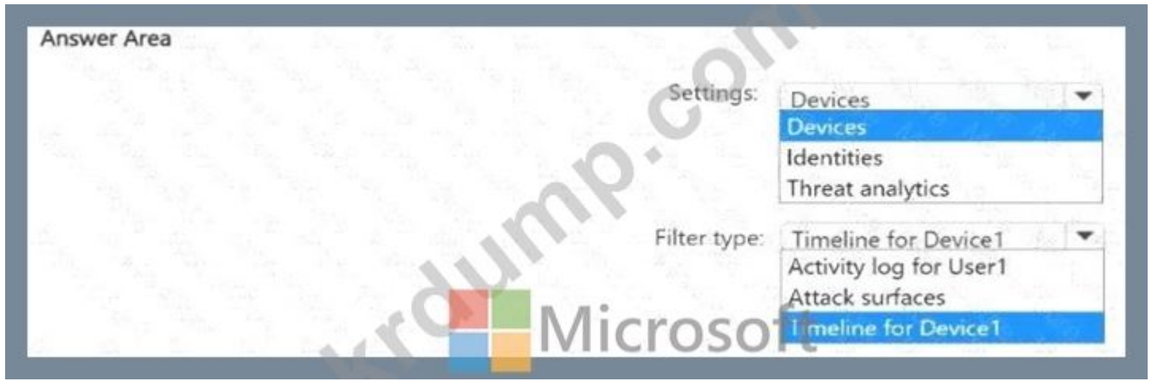
NEW QUESTION: 170
Microsoft 365 E5 □□□□ □□□□.
□□□□□ 1,000□□ □□□ iOS □□□ □□□ □□□□□. □□□ □□□□□□ □□□□□ □□ □□□□□.
□□ □□ □□□ □□□□ Microsoft Intune □□ □□□ □□□□ □□□.
* □□□ □□□□□ □□□□□□
* □□□ □□□ □□□□□□
* □□□ □□ □□□□ □□□□□.
□□□ □□□□ □□□?
A. □□ □□ □□(ADE)
B. BYOD(Bring Your Own Device) □□□ □ □□ □□
C. Apple Configurator □□
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll

NEW QUESTION: 171
2,000□ □□□ □□□ □□□□ □□ Microsoft 365 □□□ □□□□.
□□□□ Microsoft 365 □□□ □□□ □□□□ □□□□ □□ □□□□ 30□□□ □□ □□□□ □□□□ □□□□ □□□.
□□□ □□□□ □□□?

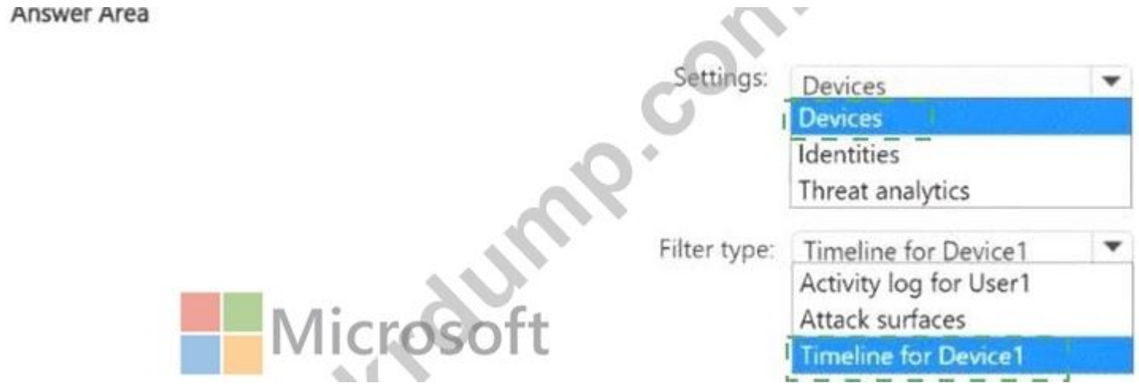
A. □□ □□
B. □□ □□ □□
C. □□□ □□□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 172
User1□□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□□□□ Microsoft 365 □□□ □□□□□□.
Cloud App Security □□ □□□□ □□ □□□ □□□ □□□ □□□□ □ □□□ □□□ User1□□ □□□□□□ □□□□ □□□.
□□ □□: Azure Active Directory □□ □□□□ User1□□ □□ □□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 173
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□. User1□ Microsoft Defender for Endpoint□ □□□□ Device1□□□ Windows 11 □□□ □□□ □□□□.
User1□ Device1□□ □□□ □□□ □□□□□□ □□□□□.
□□□ □□□ □□□□ □□□□□ □□□ □□□□ □□□.
Microsoft Defender □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

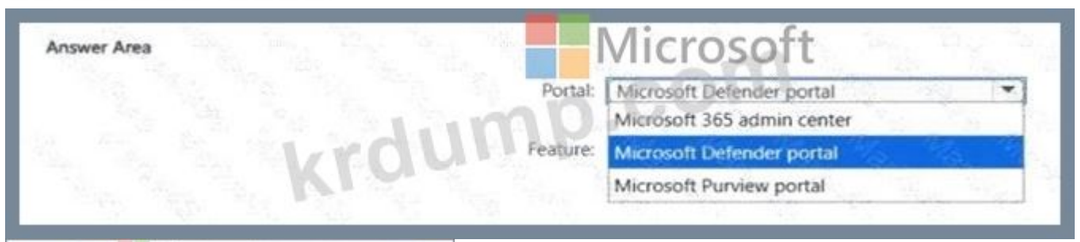
NEW QUESTION: 174

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

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

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

□□: □□ □□□ 1□□□□.



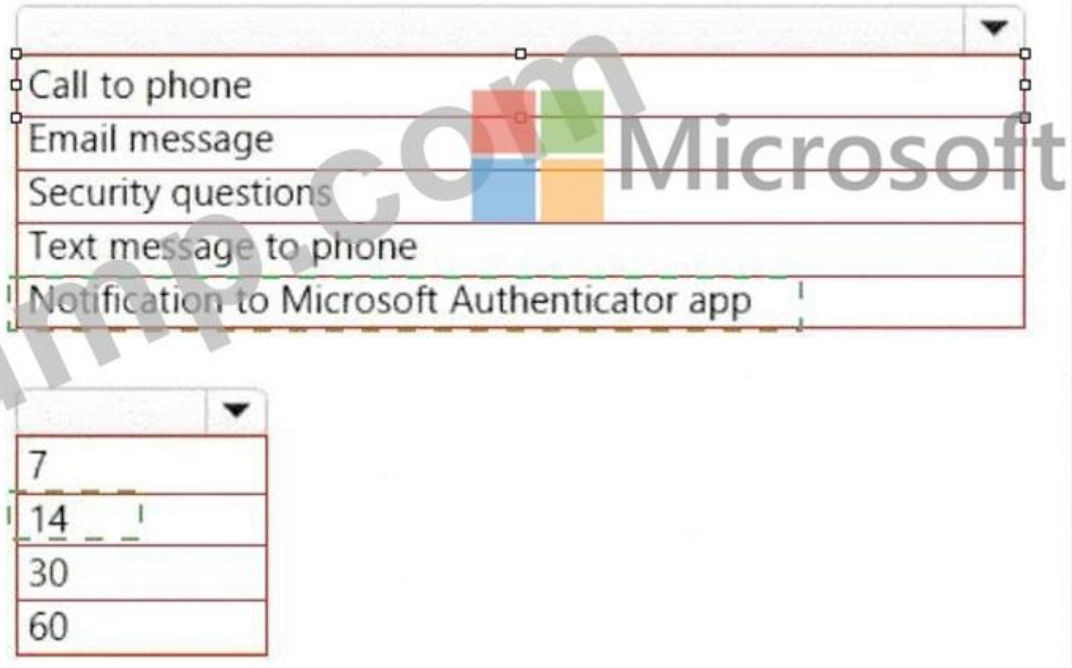
Answer:

Explanation:

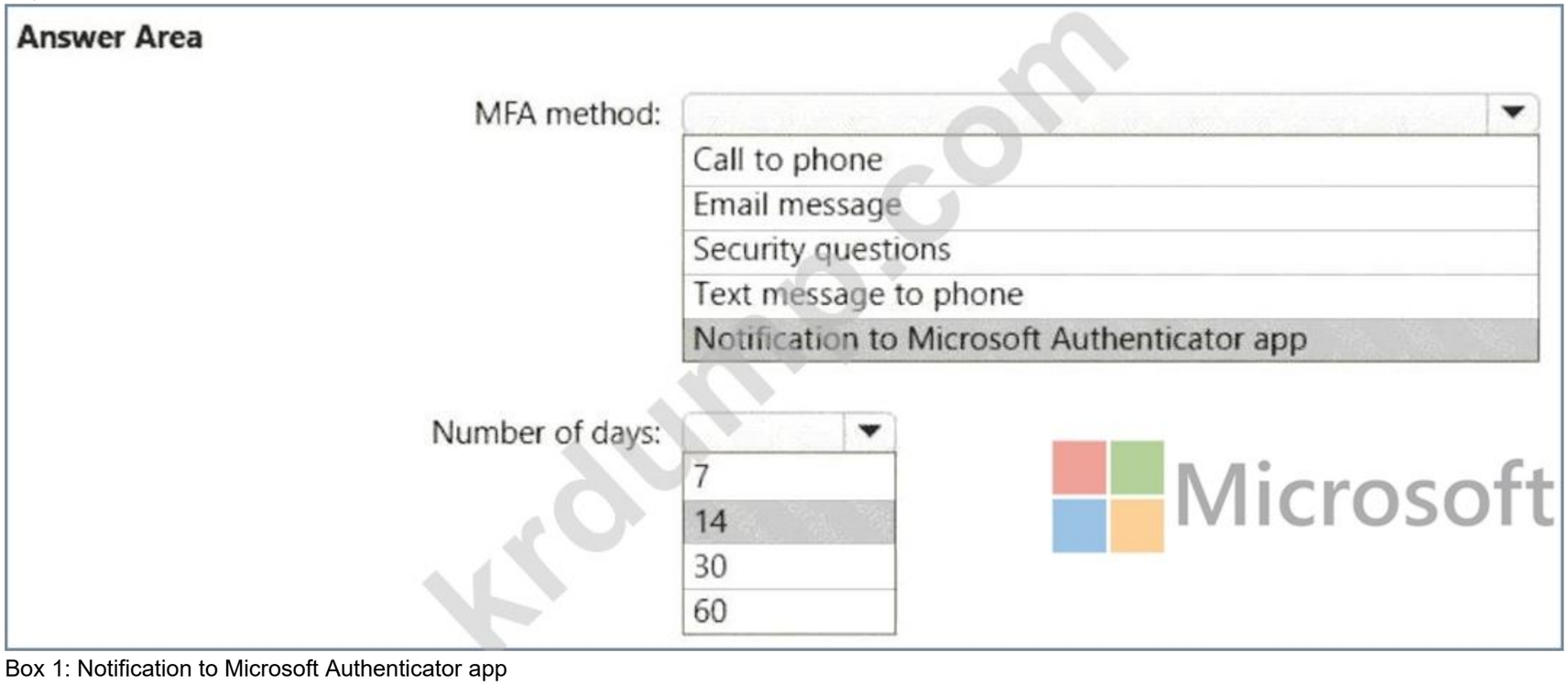
NEW QUESTION: 175
□□□
□□□ Microsoft 365 E5 □□□□ □□□□.
□□ □□□ □□□ □□ □□□□□□□.
□□□□ □□□□ □□□□ □□□□□□.
□□□□ □□ □□ □□ □□(MFA) □□□ □□□ □ □□□, □□□□ MFA□ □□□□ □□ □□□ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Answer Area



Explanation:



Box 1: Notification to Microsoft Authenticator app

Do users have 14 days to register for Azure AD Multi-Factor Authentication?
Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won ' t be able to sign in until MFA registration is completed.
Box 2: 14
Azure AD Identity Protection will prompt your users to register the next time they sign in interactively and they ' ll have 14 days to complete registration. During this 14-day period, they can bypass registration if MFA isn ' t required as a condition, but at the end of the period they ' ll be required to register before they can complete the sign-in process.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/solutions/empower-people-to-work-remotely-secure-sign-in
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection- configure-mfa-policy

NEW QUESTION: 176
Microsoft 365 E5 □□□□ □□□□.
□□ □□□ □□ □□□□ ISO 27001 □□□ □□□□ □□□.
□□□□ □□□ □□ □□□□ □□□.
A. Microsoft J6i □□ □□ □□□□ □□ □□ □□□ □□□□.
B. Microsoft 365 □□ □□□□ □□□ □□□ □□□□□□.
C. □□ □□ □□□□□ □□□ □□□□□.
D. Azure Portal□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

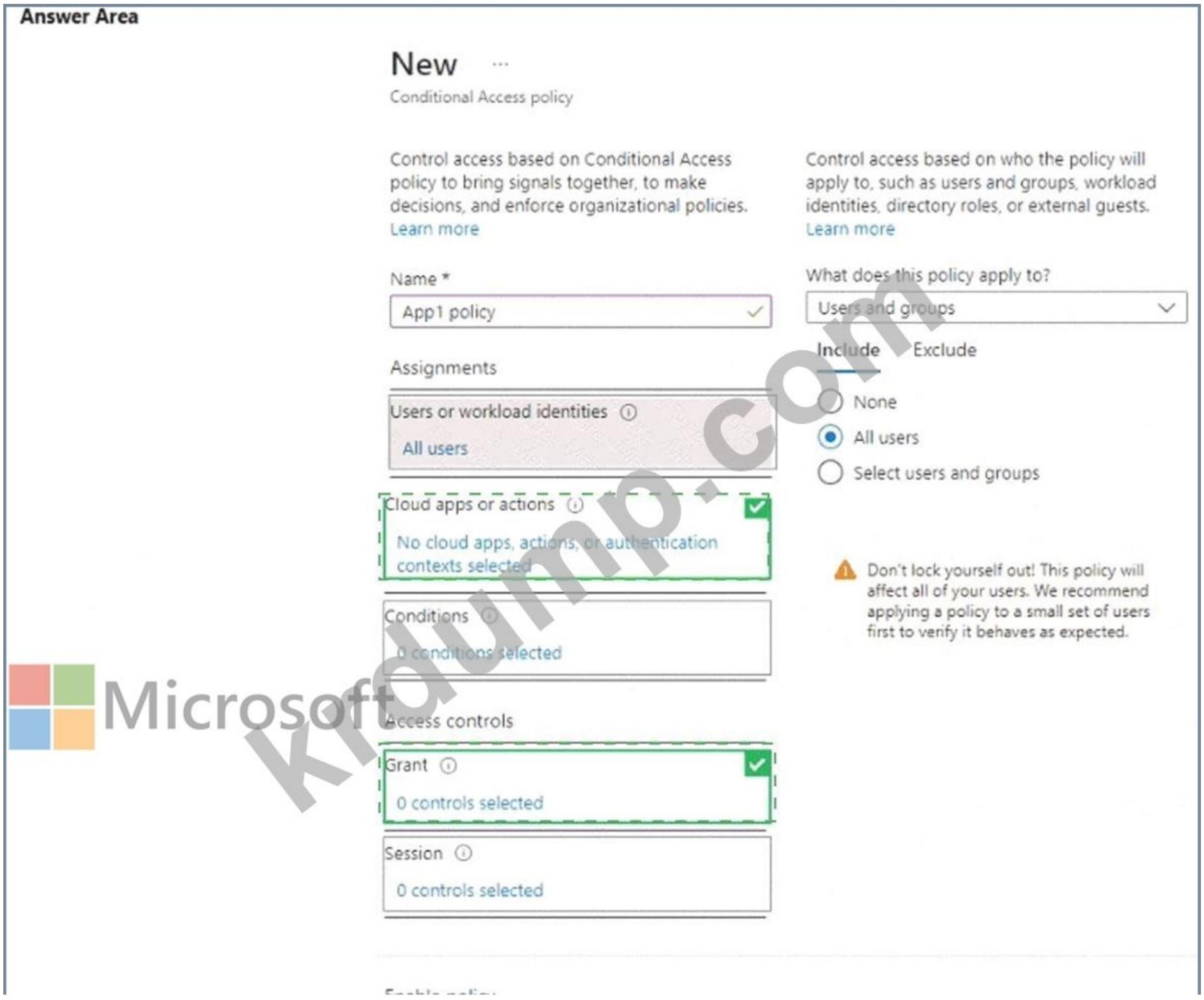
NEW QUESTION: 177
Microsoft 365 E5 □□□ □□□□ □□□ Microsoft Defender for Cloud Apps□ □□□□ □□□□. OAuth □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Microsoft 365□ □□□□ □□ Defender□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 178
Microsoft 365 Enterprise E5 □□□ □□□□.
App1□□□ □□□□ □□ □□ Azure AD □□□□□□ □□□□□□ □□□ □□□□□.
□□□ App1□ □□□ □ □□ □□□ □□□ □□ 2□□ □□□ □□□□□ □□ □□□.
□□□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

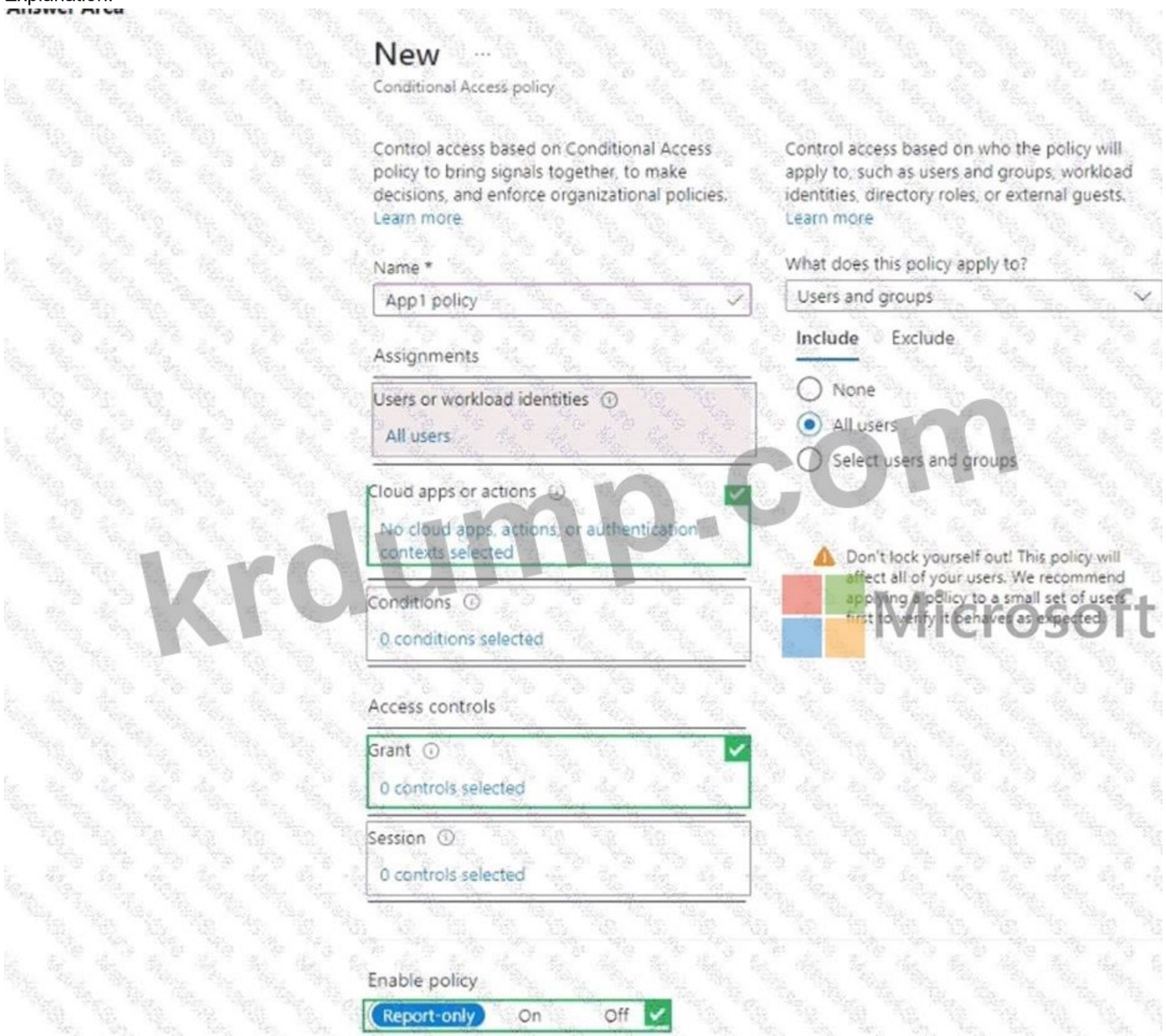
Answer Area

Answer:

Answer Area



Explanation:



NEW QUESTION: 179

□□ □□ □□(MFA) □□□ □□□□ Microsoft 365 □□□ □□□□.
Microsoft Secure Score□ □□□□ □□ □□ □□□□ □□ □□ □□ □□□ □□□□□ □□□ □□ □□□ □□ □□□ □□□□ □□ □□□ □□ □□ □□□□□.
□□□ □□ □□ □□□□ □□□ □□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□□?
A. □□□ □□□□ □□□□□.
B. Microsoft Defender for Identity □□□ □□□□□.
C. □□ □□□ □□□□□.
D. □□□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 180
Microsoft J65 E5 □□□ □□□□.
Microsoft Defender for Endpoint□ Microsoft Intune□ □□□□□.
Intune□ □□□ □ □□□ Defender for Endpoint□ □□□□ □□□□□□ □□ □□□.
□□□: □□ □□□ □□□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 181
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
□□□ □□□□□□ □□□□□ 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: 182

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: 183

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

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

A. □□ 1, □□ 2, □□ 3□
B. □□3□ □□4□
C. □□! □ □□2□

D. □□2□ □□3□

E. □□2, □□3, □□4□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 184

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:

Explanation:

NEW QUESTION: 185

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

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

□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□ □□□ □□□ □□□ □□□ □□□ □□□□.

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

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

□□□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

Explanation:

Answer Area

NEW QUESTION: 186

Microsoft 365 E5 □□□ □□□□.

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

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

□□□: □□ □□ □□□ □□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: (SHOW ANSWER)

NEW QUESTION: 187

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

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

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: 188

□□□

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

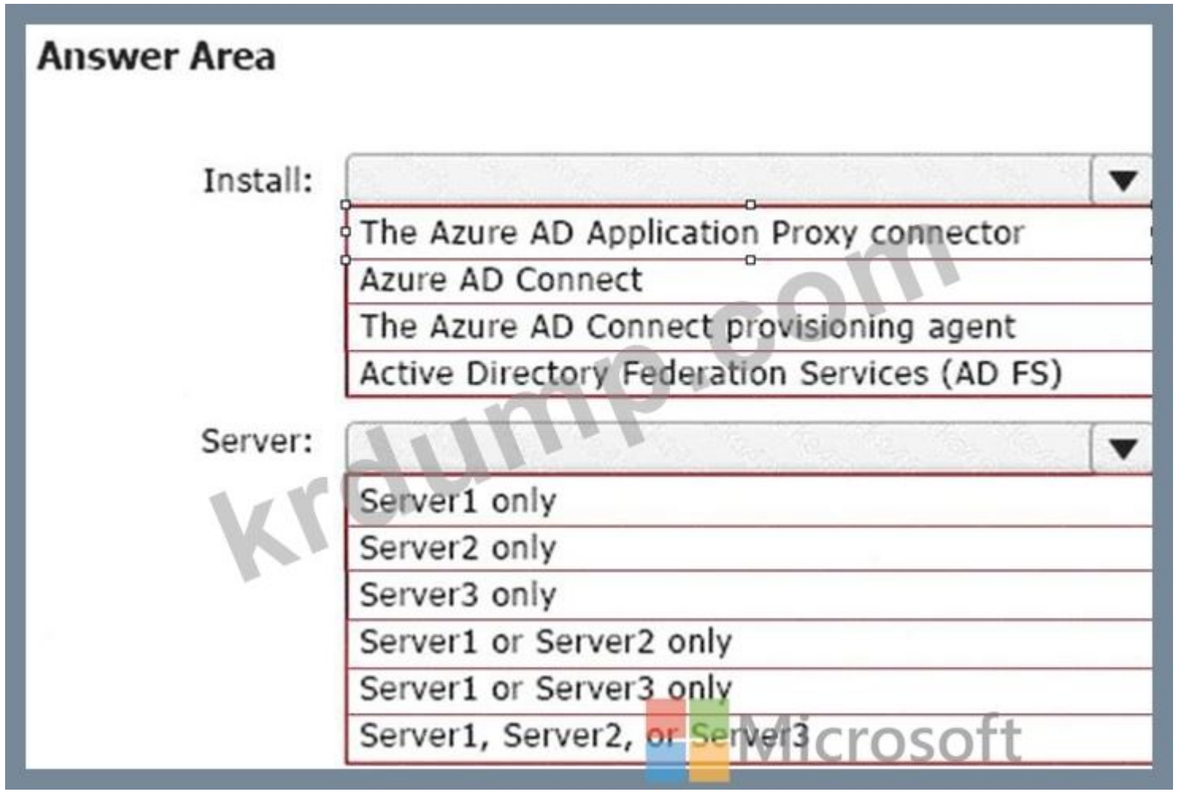
Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

Microsoft 365 E5 □□□ □□□□□.

Azure AD Connect □□□□ □□□□ □□□□ □□□.

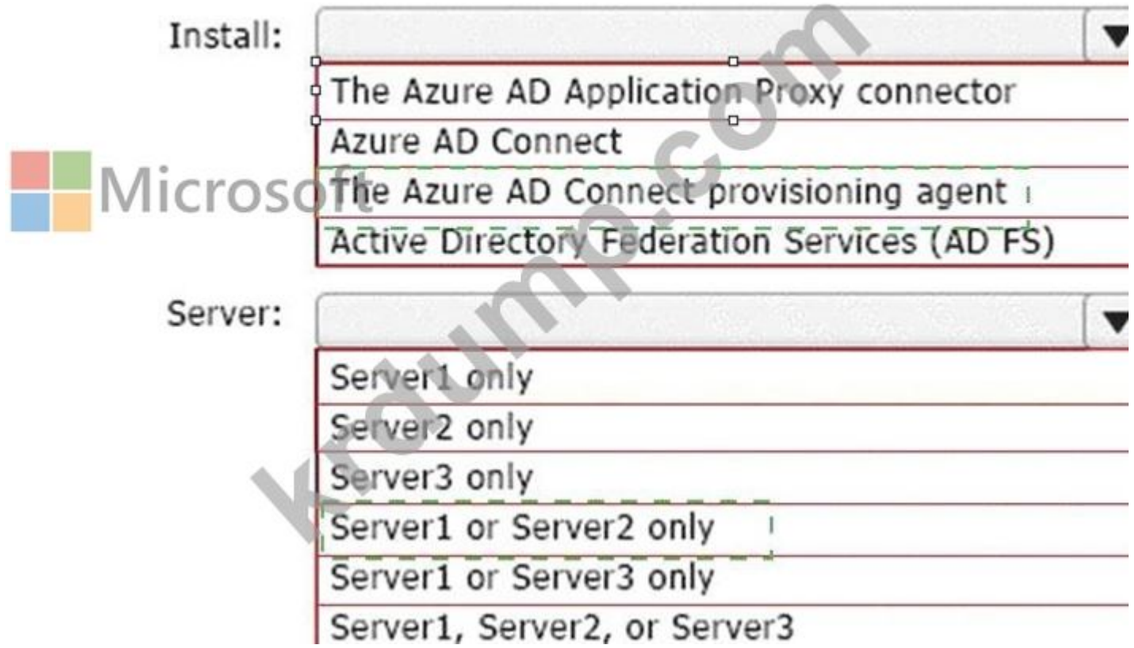
□□ □□□ □□□□ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.



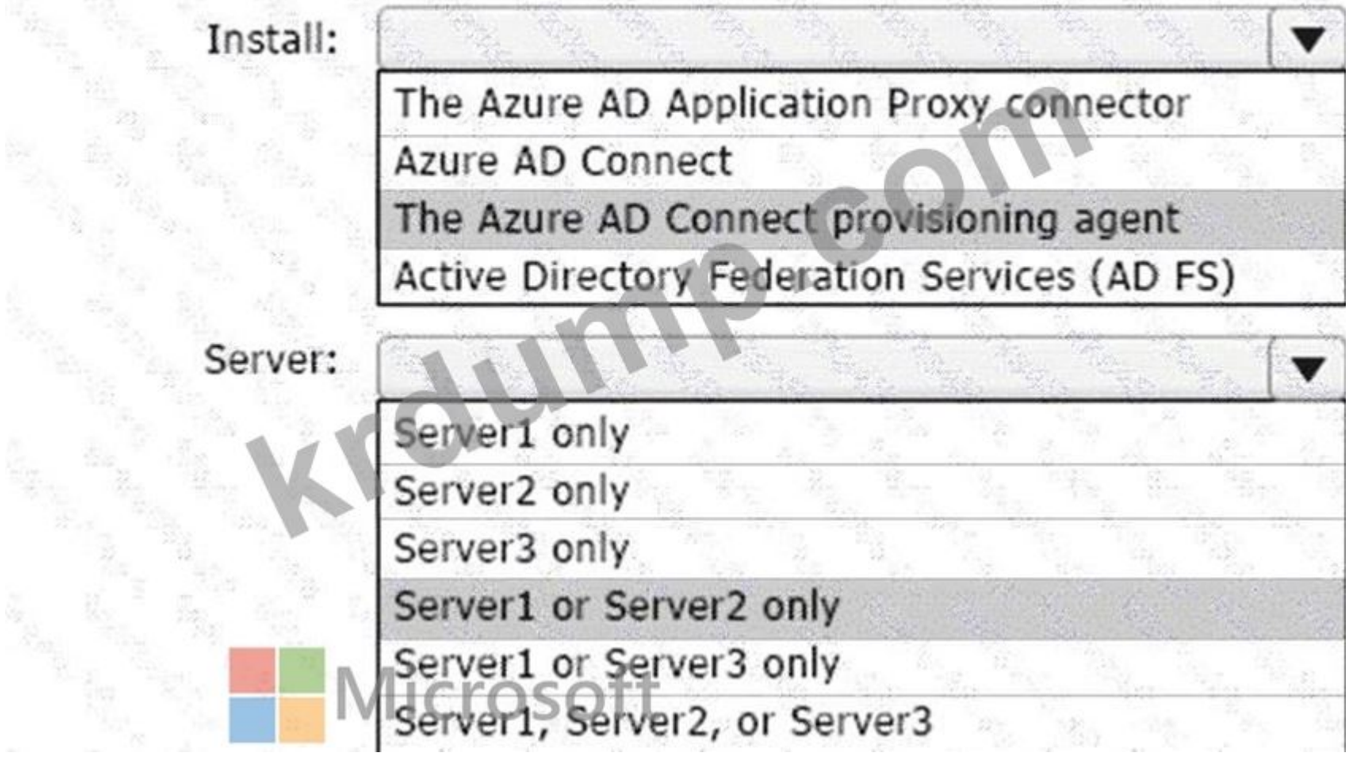
Answer:

Answer Area



Explanation:

Answer Area



Box 1: The Azure AD Connect provisioning agent

Install the Azure AD Connect provisioning agent

How is Azure AD Connect cloud sync different from Azure AD Connect sync?

With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a light- weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.

Box 2: Server1 or Server2 only.

Cloud provisioning agent requirements include:

* An on-premises server for the provisioning agent with Windows 2016 or later.

This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.

Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-install

https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites

NEW QUESTION: 189

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

Platform	Count
Windows 10	50
Android	50
Linux	50

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

A. Microsoft 365 □□ □□□□ □□ □□□ □□□ □□ □□□ □□□□.
B. Microsoft 365 Defender □□□□ □□ □□□ □□□□.
C. Microsoft Endpoint Manager □□ □□□□ □□ □□□ □□□□.
D. Azure Active Directory □□ □□□□ □□ □□ □□□ □□□□.

Answer: (SHOW ANSWER)

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365- worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide

NEW QUESTION: 190

Microsoft 365 E5 □□□ □□□□. □ □□□□ Windows 11 □□□ □□□□ □□□□ □□□□ □□□□.
Microsoft Defender for Endpoint□ □□□ □□□□ □□□□□. □□□ □□□ □□□□ □□ Defender for Endpoint□ □□□□□.
Defender for Endpoint□ □□□ □ □□□ □□ URL□ □□ IP □□□ □□□□□ □□□□ □□□. □□□ □□ □□□?

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 191

Microsoft 365 E5 □□□ □□□□.
□□□□ □□ Microsoft Defender□ □□□□ □□□□.
OAuth □ □□□ □□□ □ □□□ □□□.
□□ □□: Cloud Discovery□ □□□□□.
□□□ □□□ □□□□□?

A. □□□
B. □

Answer: A (LEAVE A REPLY)

NEW QUESTION: 192

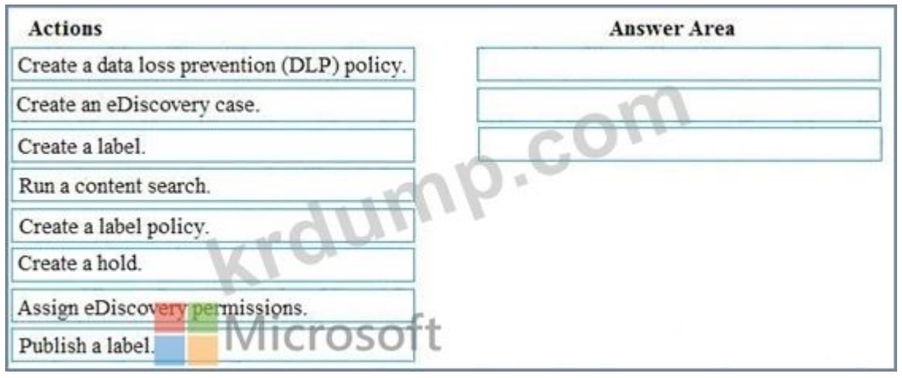
□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□□ □□□□.

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

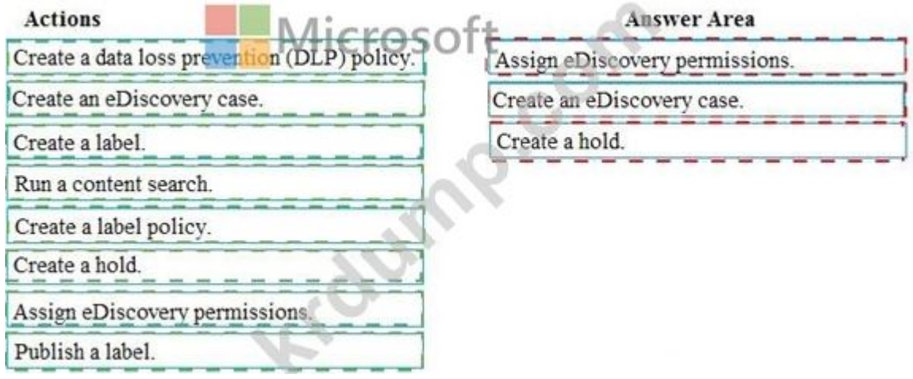
Endpoint □□□ □□□□ □□ □□ □□ □□□ □□□ □□□□□.
Endpoint □□□ □□□□ □□ □□□ □□□□□ □ □□□□?
A. Device1□
B. Device1□ Device2□
C. Device1, Device2, Device3□
D. Device1, Device2, Device4□
E. Device1, Device2, Device3, Device4
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/analytics/overview

NEW QUESTION: 193
Microsoft 365 □□□□ □□□□.
Endpoint Protection □□ □□ □□□□ □□□ □□□□□.
□□□□ □□□□ □□ □□□□ □□□ □ □□□?
A. □□□□□
B. CentOS □□□
C. iOS
D. □□□ 10
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

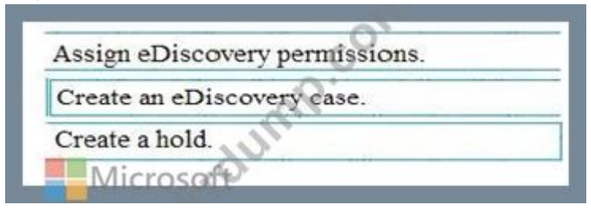
NEW QUESTION: 194
□□□□ □□ □□□ □□□□ □□□.
□□ □ □□ □□ □□ □□□□ □□□□ □□□□ □□ □ □□ □□□ □□□□□? □□□□□ □□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□ □□□ □□□□□.



Answer:



Explanation:



References:

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

NEW QUESTION: 195

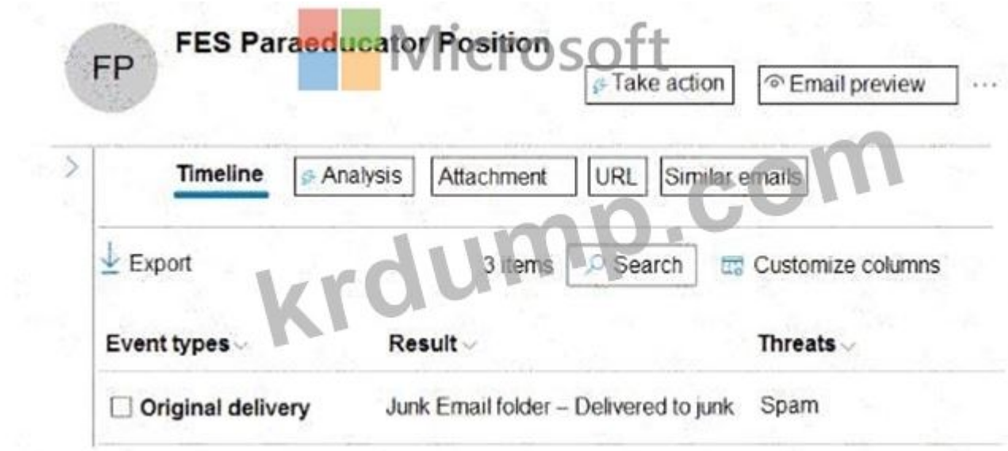
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

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

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

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

□□: □□ □□□ 1□□□□.



Answer:

Explanation:

1. Analysis 2. Take Action

NEW QUESTION: 196

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: 197

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

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

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

Microsoft 365□ □□□□□.

□□□□ □□□□ □□□ □□□□□.

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

* Active Directory□ □□□ □ □□ □□ □□□□ Microsoft 365 □□□□ □□□□□ □□□ □ □□□ □□□.

* □□□ □□□□□ 10□ □□□□□ □□□.

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

□□□ □□□ □□□□□?

A. □

B. □□□

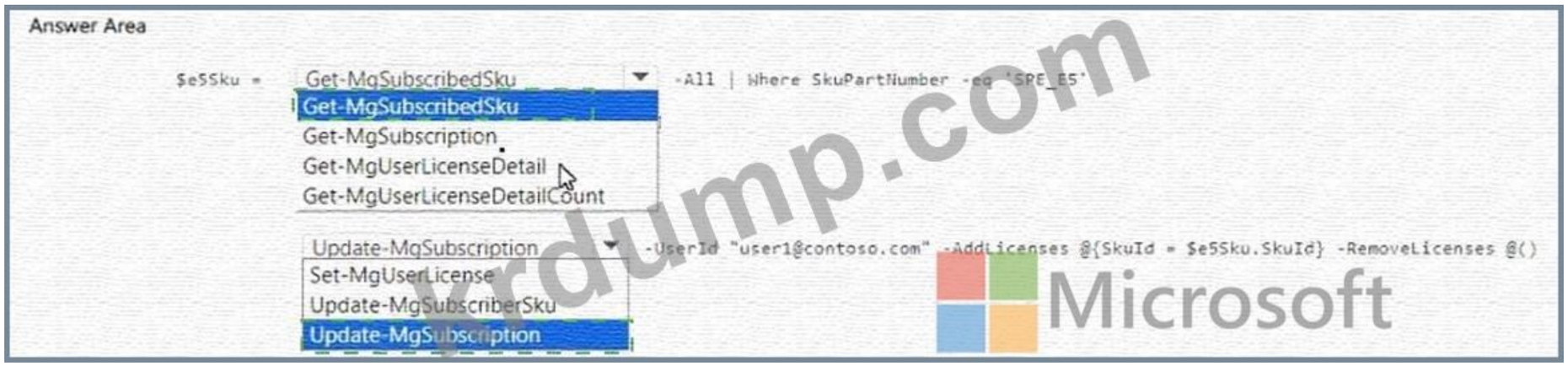
Answer: B (LEAVE A REPLY)

NEW QUESTION: 198

Microsoft 365 E5 □□□ □□□□.

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

Answer:



Explanation:

NEW QUESTION: 199
Microsoft 365 E5 □□□ □□□□.
Microsoft 365 Defender□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□ □□
C. □□□ □□ □□ □□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 200

□□□

Microsoft 365 E5 □□□ □□□□.

Azure AD Privileged Identity Management(PIM)□□ □□ □□□ □□ □□□ □□□ □□□ □□ □□ □□□ □□□□□.

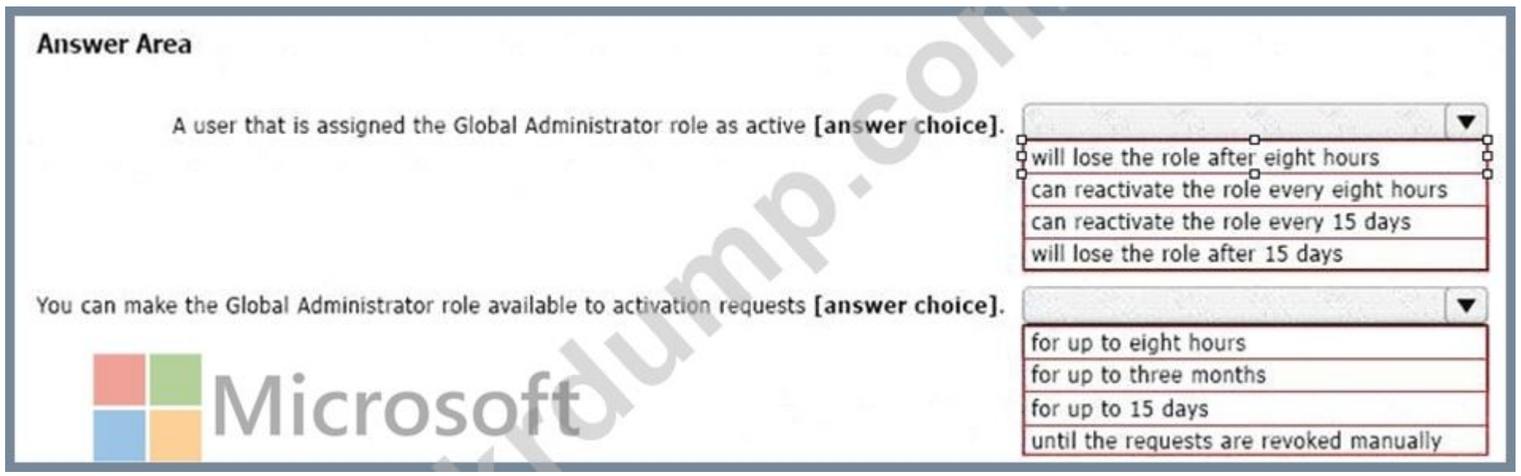
Activation

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

Assignment

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

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



Answer:

Explanation:

Box 1: will lose the role after eight hours

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

NEW QUESTION: 201

Microsoft 365 □□□ □□□□.

□□ □□ □□□ □□ □□□□.

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

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

Azure AU □□□ □□□□ □□ □ □□□□□□ □□□ □□ □□□? □□□□□ □□□ □□□ □□ □□□□□ □□□ □□□□. □ □□□ □ □, □□ □, □□ □□ □□□ □ □□□□. □ □□□ □□ □ □□ □□□ □□□ □□□□□ □□□□ □□□□ □ □□ □□□□.

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 202

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

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

Microsoft 365 E5 □□□ □□□□.

SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.

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

□□ □□: Microsoft Entra □□ □□□□ SecAdmin1□□ □□ □□□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□
Answer: A (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: 203
Microsoft Intune□ □□□ 1,000□□ iOS □□□ □□□□ Microsoft 365 □□□□ □□□□. □□ □□ □□ □□□□ □□□ □□□ □□□□□. Intune□ □□□□ □□□ □□□□□ □□□□ □□ □□□□ □□□. □□ □□□□□ □□□ □□□□ □□□?
A. □□□□□ Microsoft Store
B. Apple Business Manager
C. □□ □□□□ □□□
D. Apple □□□
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios

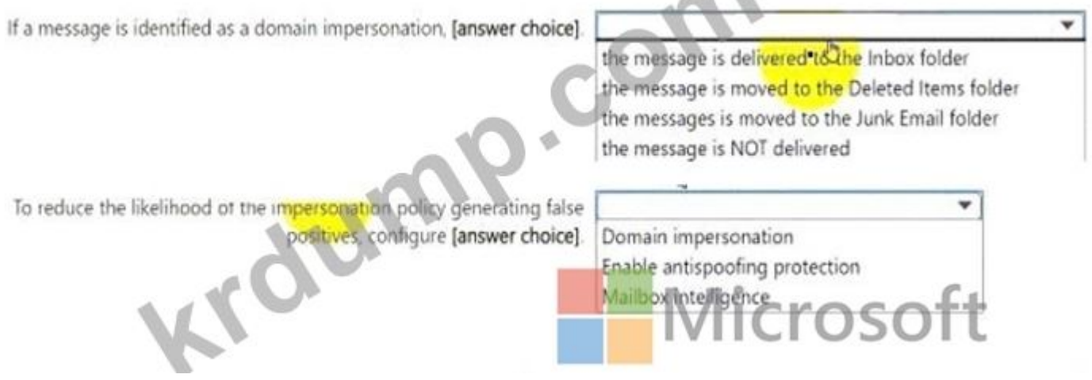
NEW QUESTION: 204
Windows 10 □□□ □□ □□ □□ □□ □□□ □□□□ □□□.
Intune □□ □□□□ □□□ □□□□ □□□?
A. □□ □□ □□
B. □□ □□□□ □□
C. □□ □□ □□□
D. □ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 205
□□ □□ □□□ □□□ □□ □□ □□□ □□□□□.

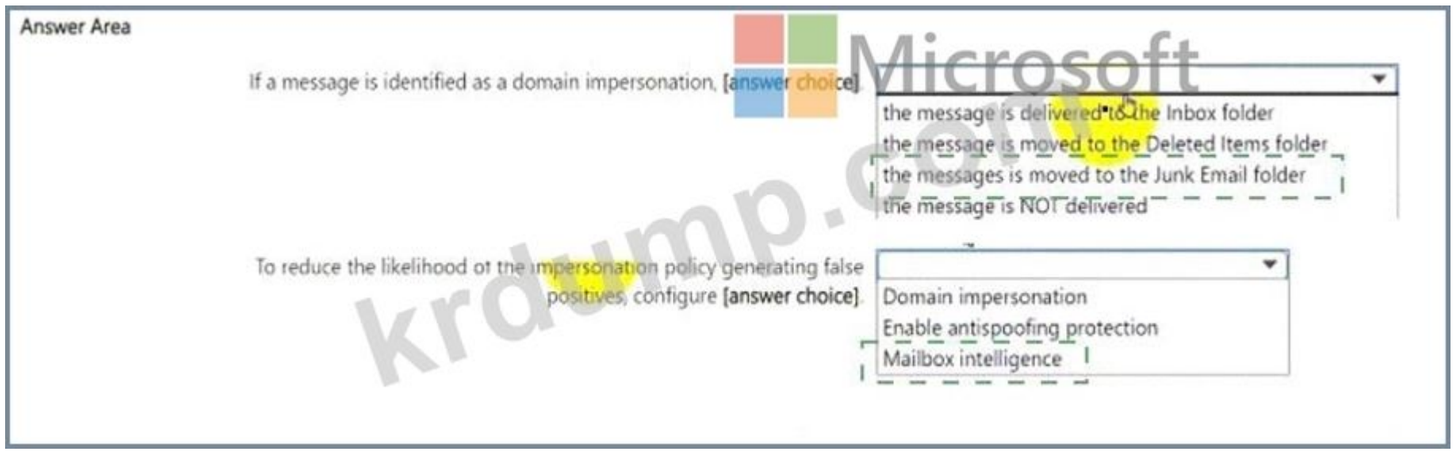
□□□□ □□□ □□□ □□□ □ □□□□ □□□□ □□□□ □□□□□ □□□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area



Answer:



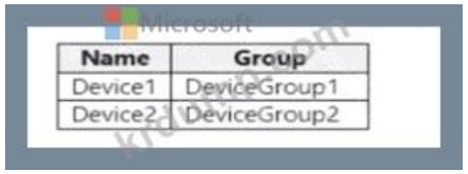
Explanation:

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

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

NEW QUESTION: 206

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



Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

08:00□ □□ □□□ □□ □□□□ □□ □□□ □□□□□.

* □□ : □□!

* □□ □□

o □□ □ □□ 70: □□

o □□ □□ □□: □□(3)

o □□ □□: □□□ □ □□ □□

* □□□: Userl@contoso.com, User2@contoso.com

08:02□ □□ □□□ □□ □□□□ □□ □□□ □□□□□.

* □□ : □□

* □□ □□

o □□ □□□□ □□ □□: □□. □□

o □□ □□ □□: DevtceGroup1, DeviceGroup2

* □□□: Userl@contoso.com

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

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

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

NEW QUESTION: 207

□□□

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

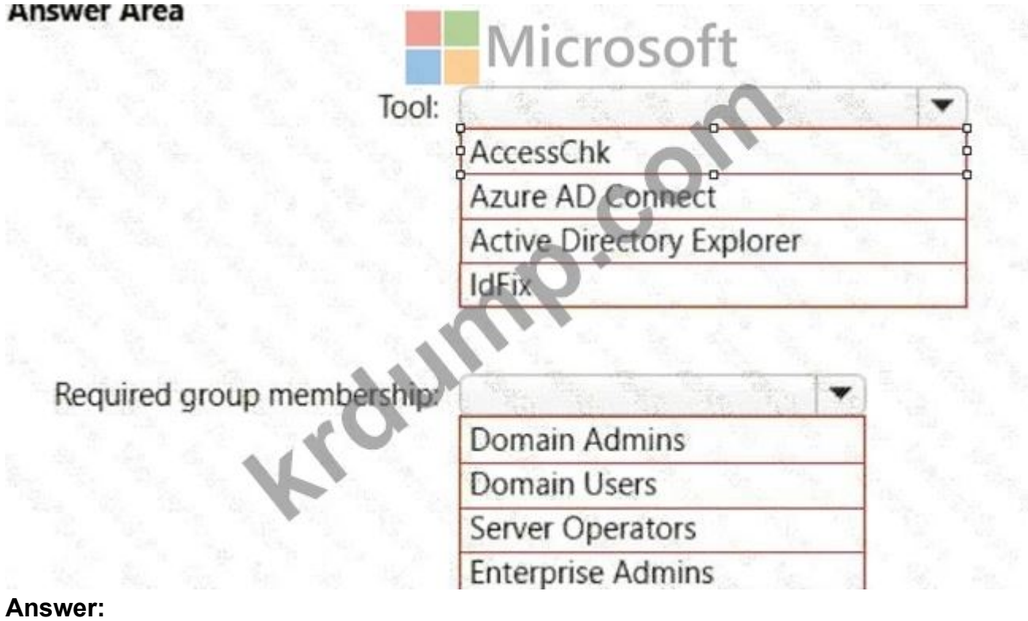
Microsoft 365 E5 □□□ □□□□.

□□□□ □□□□ □□□ □□□□□.

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

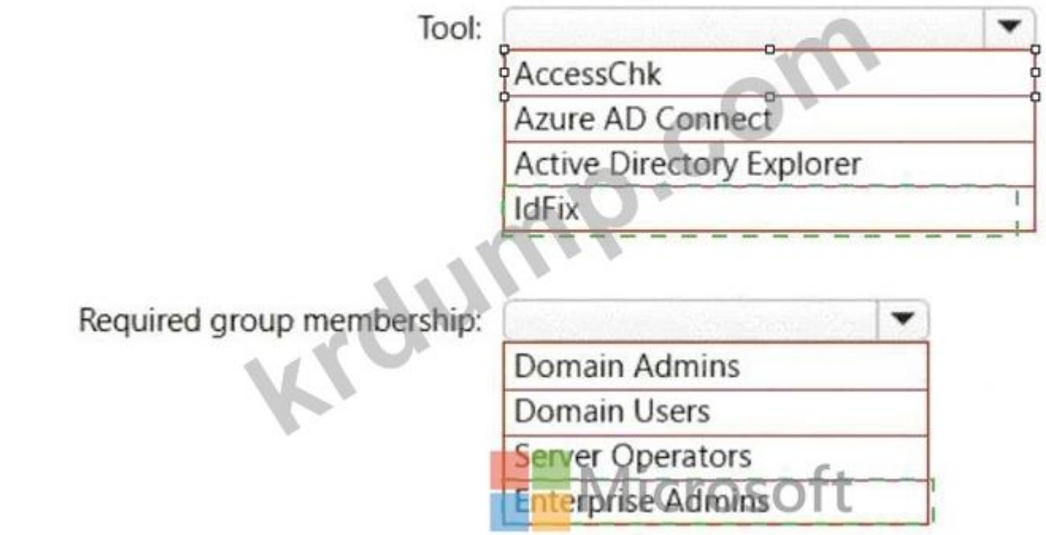
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

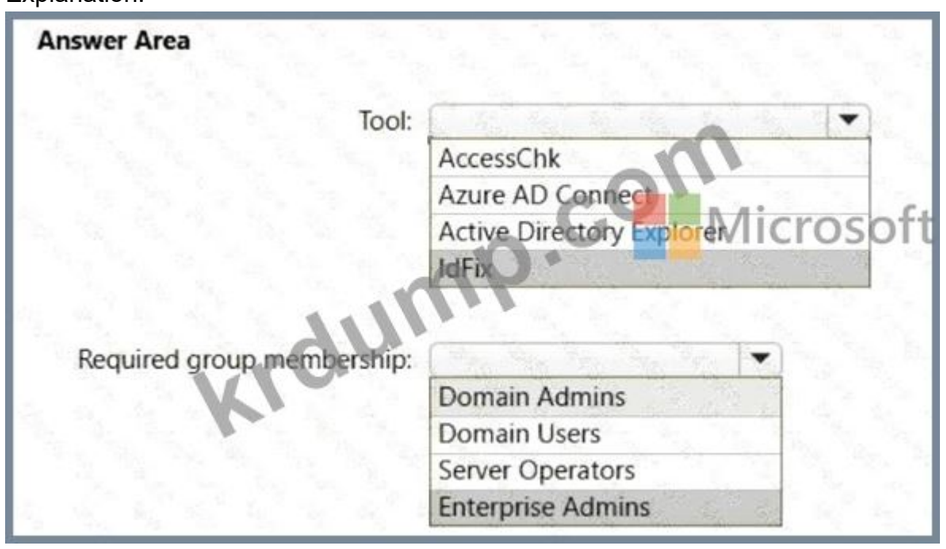


Answer:

Answer Area



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: 208
□□□
□□ □□ □□ □□ □□□□ □□□ 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

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

Microsoft 365 setting: ▼

- Office installation options
- Privileged access
- Release preferences

User: ▼

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

Explanation:

Answer Area

Microsoft 365 setting:

- Office installation options
- Privileged access
- Release preferences

User:

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

NEW QUESTION: 209

Microsoft 365 □□□ □□□□.

□□ □□□ □□□□□ □□□□ □□□□ □□□.

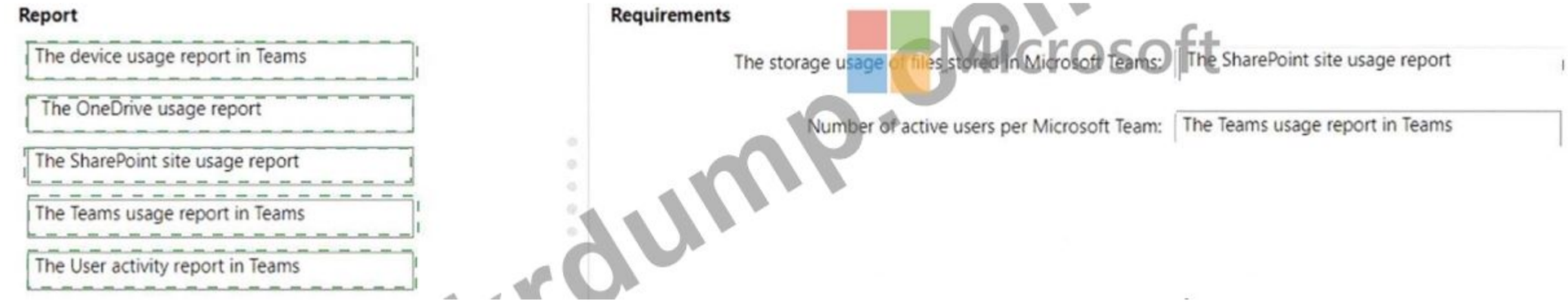
* Microsoft Teams□ □□□ □□□ □□□ □□□

* □□ □□ □□□ □

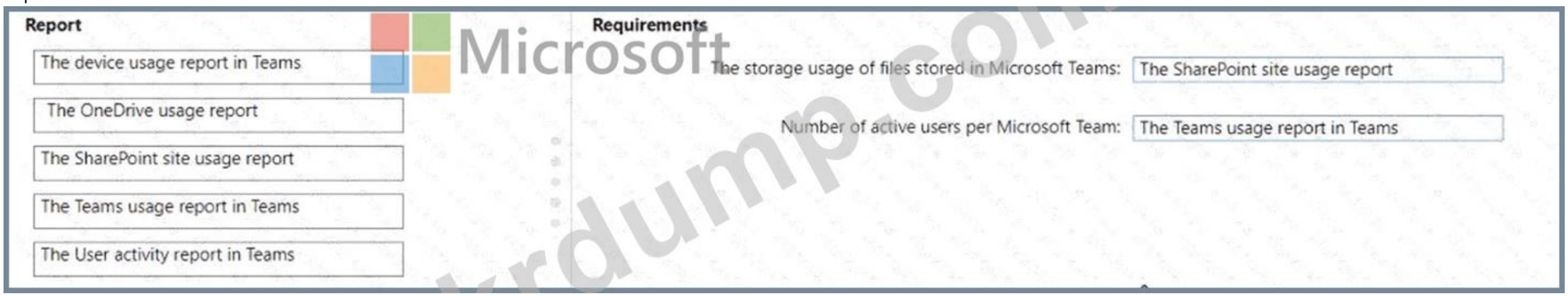
□ □□ □□□ □□ □□ □□□□ □□□□ □□□? □□□□ □□□ □□□□ □□□ □□ □□□□ □□□ □□□□□. □ □□□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □□□ □□□ □□□ □□□□□ □□□□ □ □ □□□□.

Report	Requirements
The device usage report in Teams	The storage usage of files stored in Microsoft Teams:
The OneDrive usage report	Number of active users per Microsoft Team:
The SharePoint site usage report	
The Teams usage report in Teams	
The User activity report in Teams	

Answer:



Explanation:



NEW QUESTION: 210

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

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

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

□□□□ □□□ DNS □□□□ □□□□□.

DNS □□□□ □□□ '□□□ □□□□ □□□□□'□□□.

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

□□ □□□□ □□□□ □□□?

A. □□□1

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

NEW QUESTION: 211
□□□
□□□□□ □+□□□□ Active Directory □□□□ Microsoft 365 □□□ □□□□ □□□□.
□□ □□□□□ □□ □□ □□ □□ □□□□ □□□□ □□□□.

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

□□ □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

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


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

□□ □□ □□ □□ □□□ □ □□□ □□□□□.

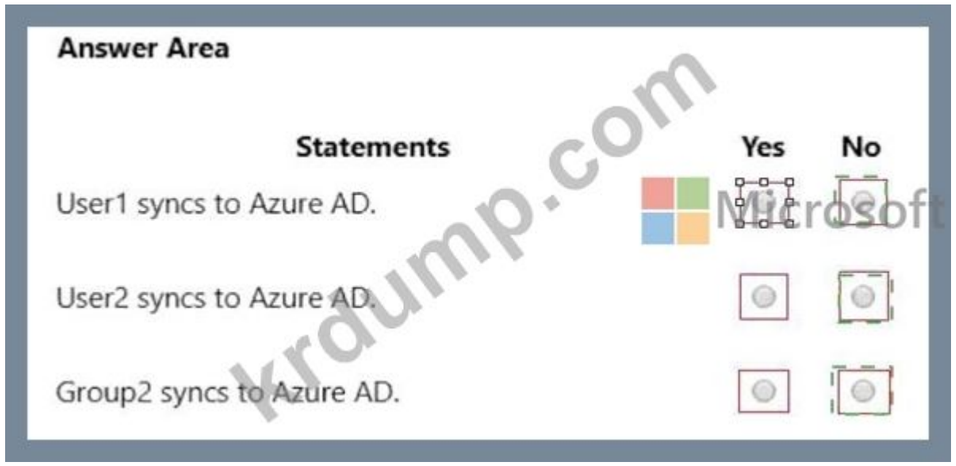
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	☐	☐
User2 syncs to Azure AD.	☐	☐
Group2 syncs to Azure AD.	☐	☐

Answer:



Explanation:

NEW QUESTION: 212

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

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

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

Azure AD □□□□ □□□□□.

□□ □□□□ □□□□ Azure AD□ □□□□□□ □□□□□.

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

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

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

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

A. □

B. □□□

Answer: B (LEAVE A REPLY)

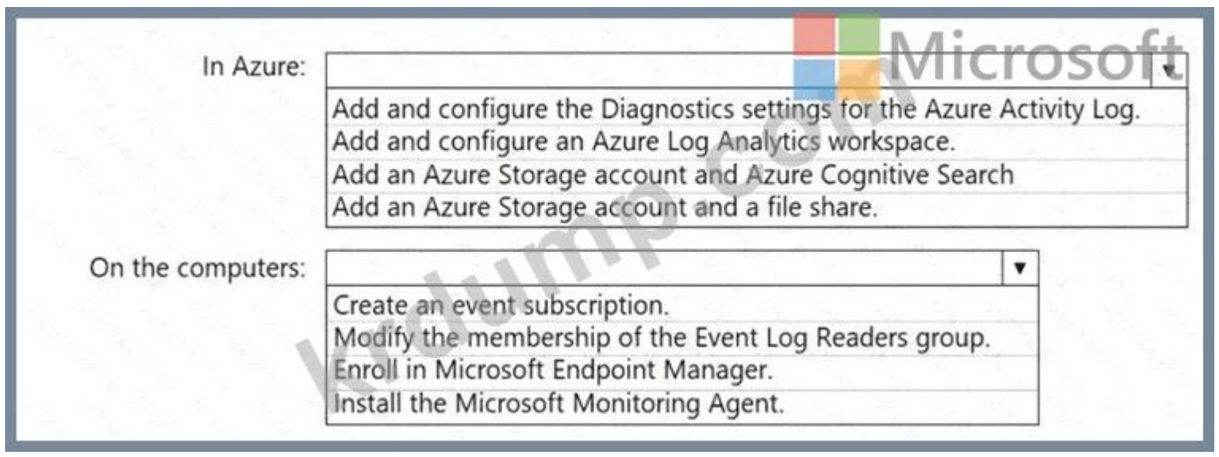
The question states that "all the user account synchronizations completed successfully". Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

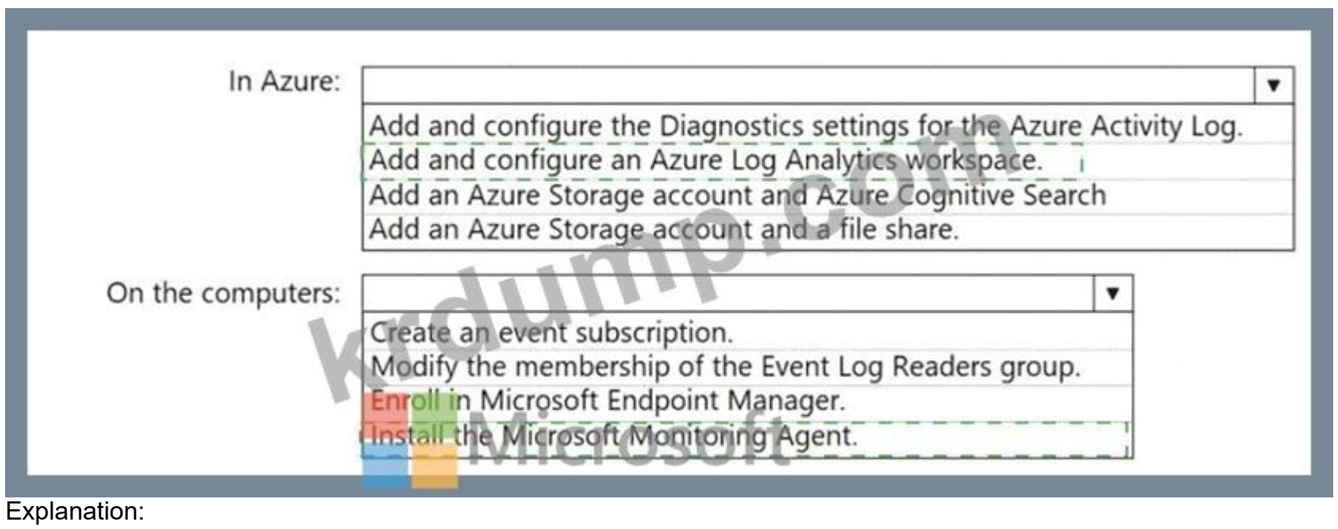
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

NEW QUESTION: 213

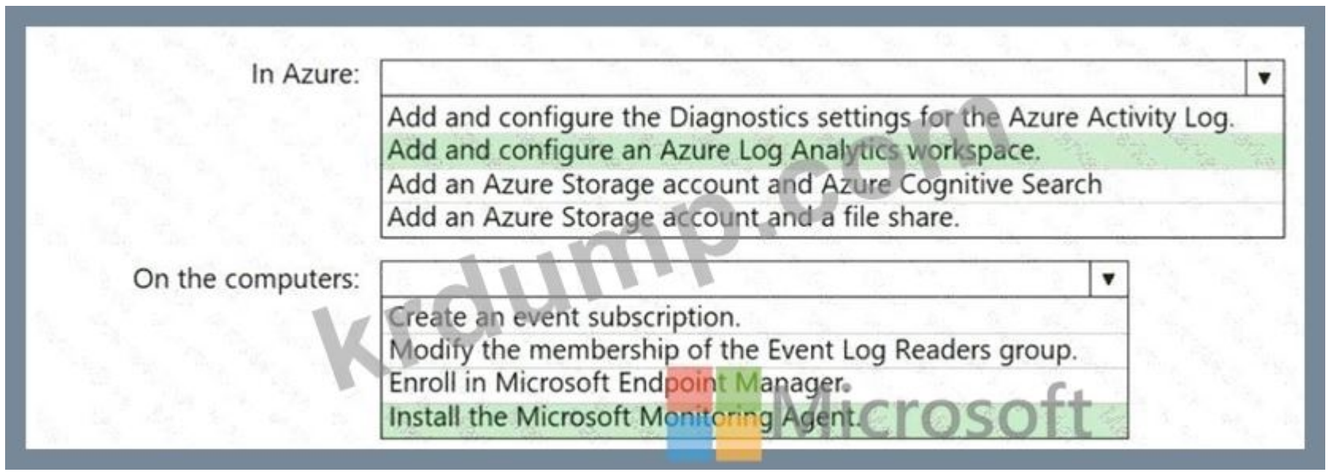
Azure □□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows 10□ □□□□ 50□□ □□□□ □□□□.
□□□□ □□□ □□ □□□□ □□□□ □□□□□□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

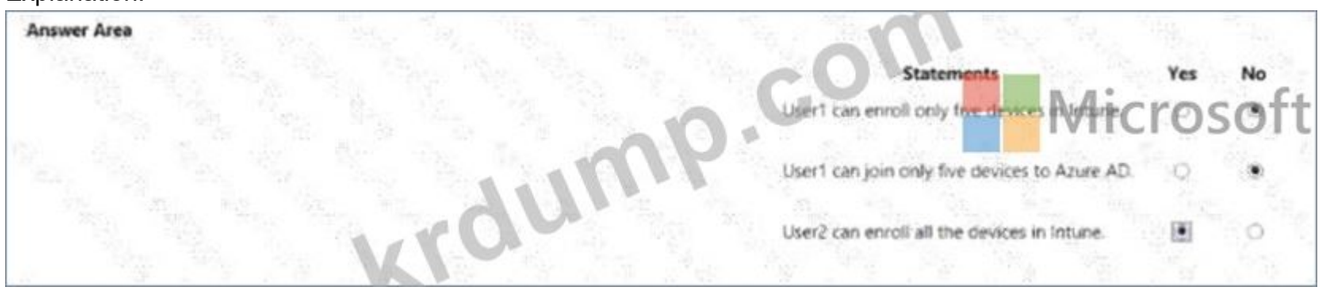
NEW QUESTION: 214
2,500□□ Windows 10 □□□□□ User1□ User2□□ □ □□ □□□□ □□□□ Microsoft 365 E5 □□□□ □□□□. □□□□□ Microsoft Intune□ □□□□ □□□□□.
Microsoft Endpoint Manager□□ □□ □□□ □□ □□ □□□ □□ □□□□□.

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

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

Answer:

Explanation:



NEW QUESTION: 215

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

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

A. □□□

B. □□□□□

C. □□ □□ □□

D. □□ □□ □

Answer: (SHOW ANSWER)

NEW QUESTION: 216

Microsoft 365 E5 □□□ □□□□.

Policy□□ □□□ □□□ □□□ □□□ □□ □□□□□.

□□□□ Azure Portal, Azure PowerShell □□ Azure Command-Line Interlace(CU)□ □□□□□□ □ □ □□ □□ MFA □□ □□□ □□□□□ □□□□ □□□.

Policy1□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 217

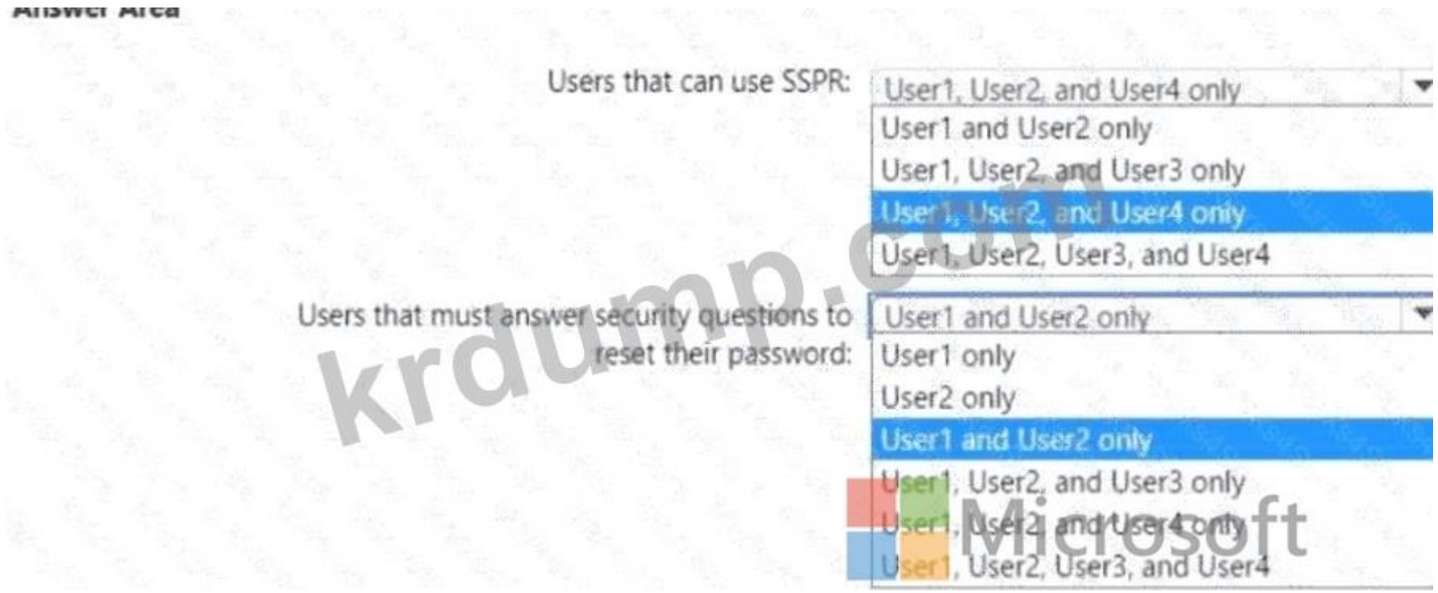
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

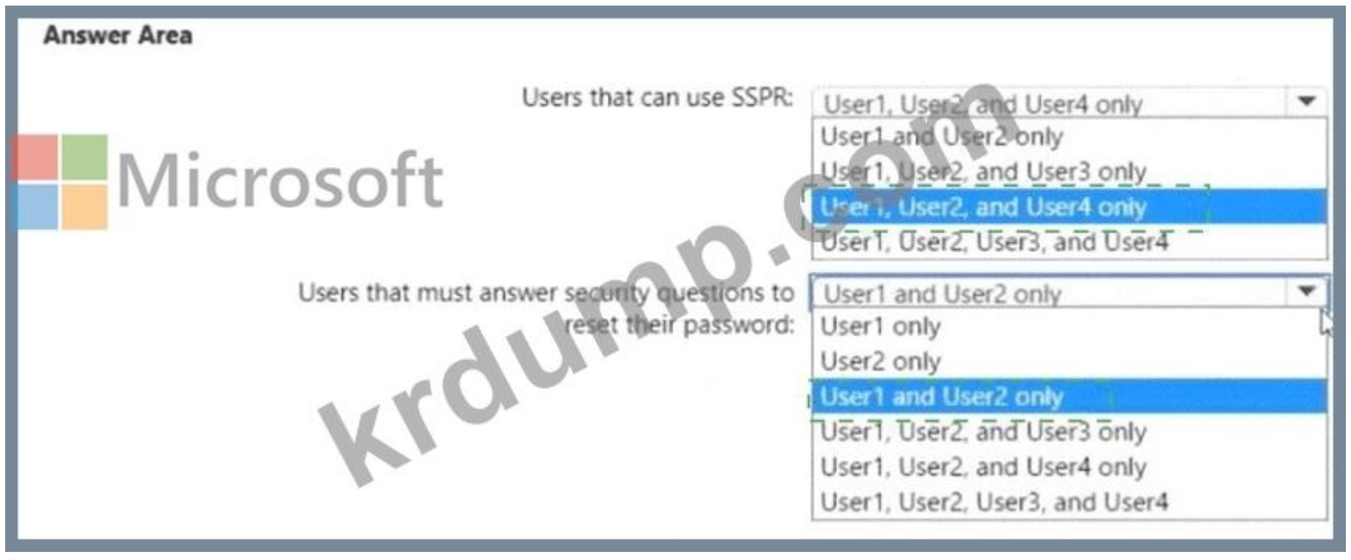
□□1□ □□ □□ □□□ □□□□ □□□(SSPR)□ □□□□□□. SSPR□ □□ □□□ □□ □□□□ □□ □□□ □□□□□.

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

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

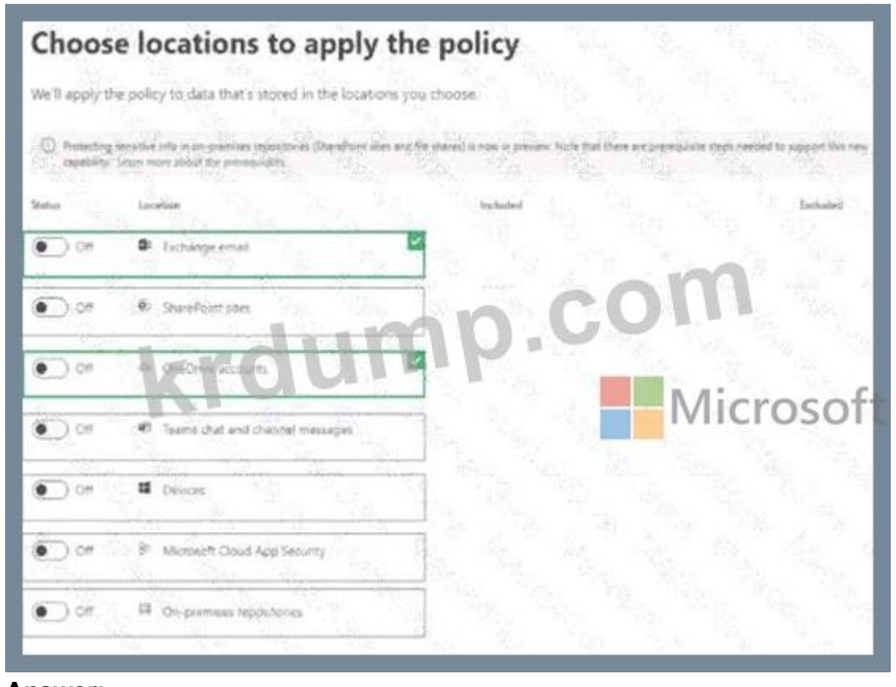
NEW QUESTION: 218

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

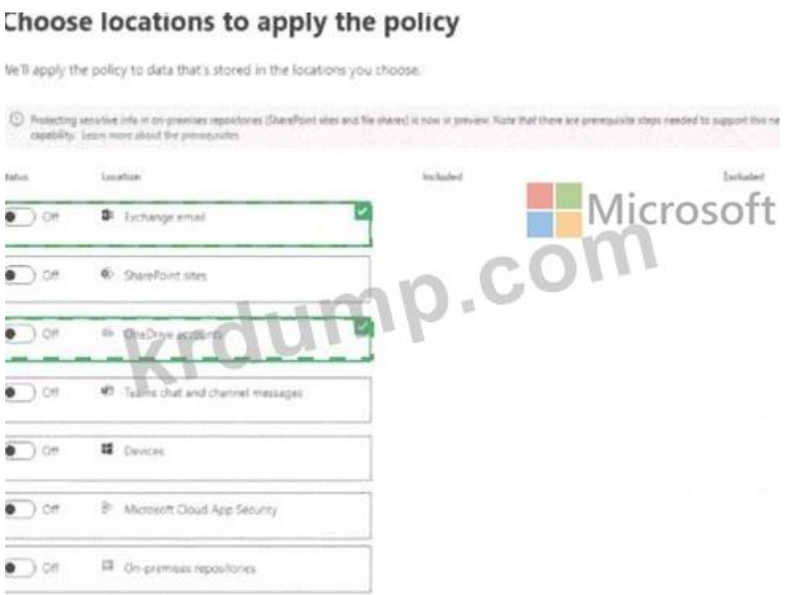
□□ □□□ □□□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□□□□□ □□□□ □□□□.

contoso.com□ Azure AD □□□□ □□□□□□ □□□.
□□□□ □□□□ Azure AD□ □□□□ □ □□□ □□ □□□ □□□□□ □□ □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. □□□□ □□
B. □□□ □□□ □□
C. □□□□ □□□
D. Azure AD ID □□ □□
Answer: A (LEAVE A REPLY)
Reference:
https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

NEW QUESTION: 219
Microsoft 365 E5 □□□□ □□□□.
□□□□ Microsoft Teams□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□□□□ □□□ □□ □□(DLP) □□□ □□□□.
□□□ □□□□ □□ □ □□□ □□□□□? □□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

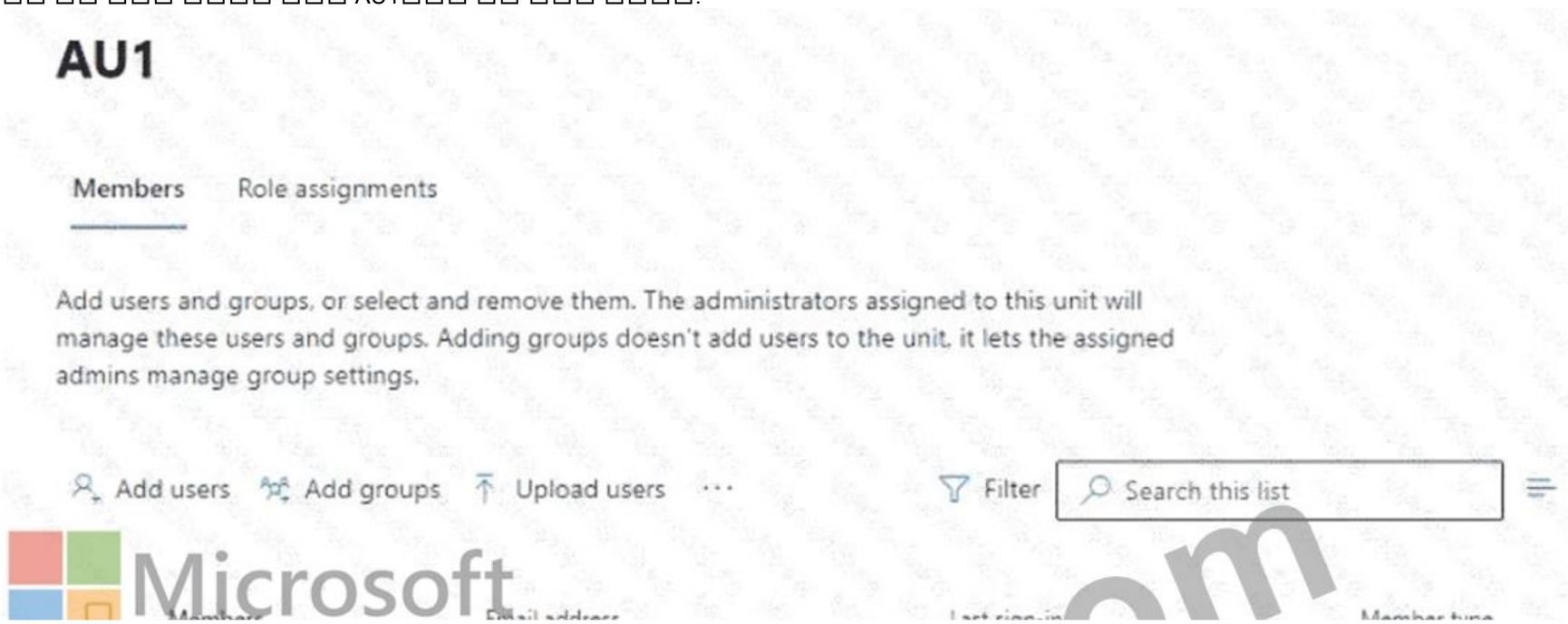


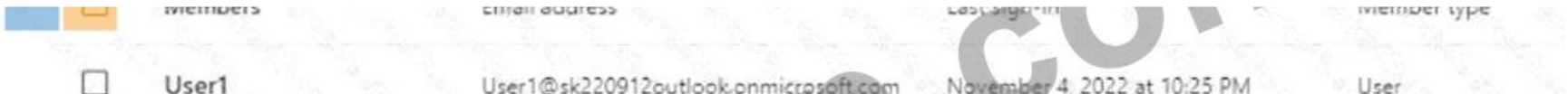
NEW QUESTION: 220

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

Name	Member of
User1	Group1
User2	Group2
User3	None

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





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: 221
□□□ □□ 3□□ □□ 1□□ □□□ □□□□. □□□ □□□ □□□□□.
□ □□□ Microsoft 365 □□□□ □□□□ □□ □□ □□□ □□□ □□□□□.
□□ □□□□ □□□□□□ □□ □□ □□□ □□□□□ □□ Microsoft 365 □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. Microsoft Entra □□□ □□□
B. Microsoft Entra □□ □□
C. Microsoft Intune □□ □□ □□
D. Microsoft Intune □□ □□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 222
contoso.com□□□ □□□□ □□□ Microsoft 365 ES □□□ □□□□. user1@contoso.com□□□ □□□□ □□ □□□ □□ □□ □□□ □□□□ Policy1□□□ □ Microsoft Defender(□□ Office 365 □ □ □□ □□)□ □□□□□.
Policy1□ usei1@fabnkam.com□□□ □□ □□□□□ □□ □□□ □□□□ □□□□□ □□□ □□ □□□□□.

□□□□ □□□□□ □□□□□ □□ □□□.
Policy1□ □□ □□□ □□ □□□?
A. □□ □□□ □□□ □□□ □□□□□.
B. □□□ □□□□ □□□□□.
C. □□□ □□□ □□□□ □□□□□.
D. □□□ □□□□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 223
Microsoft 365 E5 □□□ □□□□.
□□□□□□ □□□□ □□□□□□ □□□□ □□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□□ □□□ □□ KQL□ □□□□□.
* □□ 1□□ □□□ □□□□ □□□□□.
□□□□□ □□□ □□□□ □□□?
A. Microsoft 365 □□ □□
B. □□□□□ □□
C. Azure Monitor □□ □□
D. Microsoft 365 Defender□ □□ □□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 224
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

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

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

□□□ □□ □□ □□□ □□□ □□□□□.

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

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

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

Answer:

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

Explanation:

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

Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service

NEW QUESTION: 225
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
□□□□□ Active Directory □□□□ □□□□ □□□□.
Azure AD □□□□ □□□□□.
□□ □□□□ □□□□ Azure AD□ □□□□□□ □□□□□.
□□ □□(OU)□ 10□ □□□ □□□ Azure AD□ □□□□□ □□ □□ □□□□□□. □□ □□ □□□ □□□ □□□□□ □□□□□□□□.
Azure AD Connect Health□ □□□□ □□ □□□ □□ □□□□ □□□□□ □□□□□□ □□□□□.

10□□ □□□ □□□ Azure AD□ □□□□□□□ □□□□ □□□.
□□ □□: Azure AD Connect□□ Azure AD □□ □□□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

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

Reference:

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

NEW QUESTION: 226

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

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

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

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

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

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

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

Answer Area

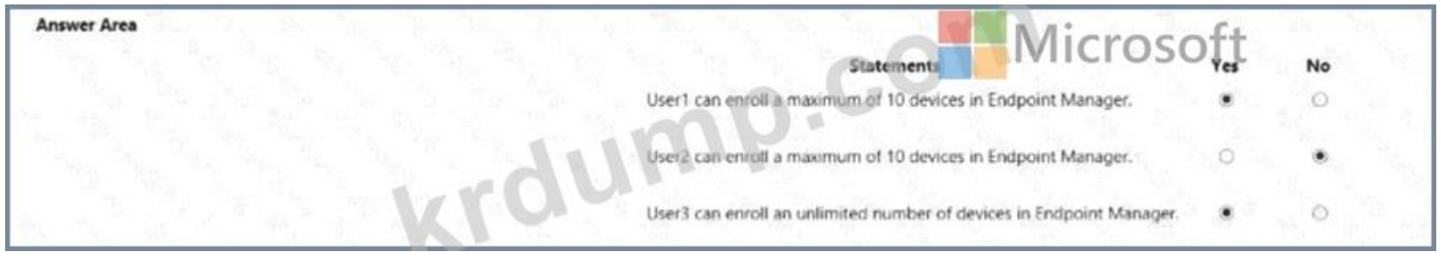
Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User2 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User3 can enroll an unlimited number of devices in Endpoint Manager.	○	○

Answer:

Answer Area

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

Explanation:



NEW QUESTION: 227
□□□ □□ □□□ □□□ □□□ □□□□ Microsoft 365 □□□□ □□□□. □□□ □□ □□ □□□ □□ □□□□□.

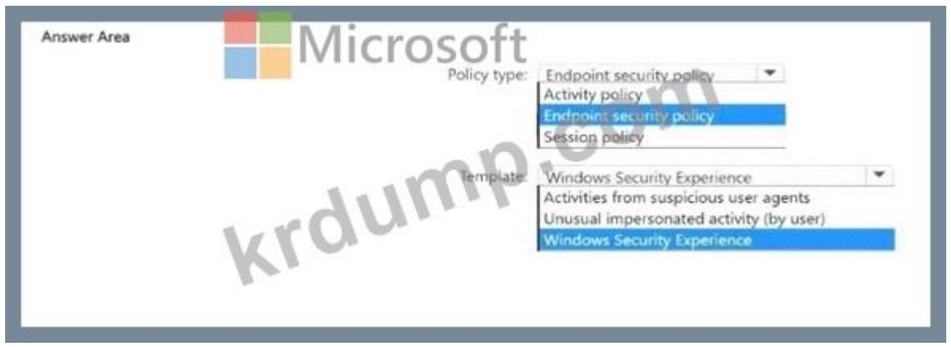
Name	Platform
Device1	MacOS
Device2	Windows 10 Pro for Workstations
Device3	Windows 10 Enterprise
Device4	iOS
Device5	Android

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

NEW QUESTION: 228
□□□ □□ □□□ □□□□□ □□ PII □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□□ □□□□ □□□ □□ □□(DLP) □□
B. □□□ □□□□ □□□ □□□□ □□□□ □□ □ □□ □□ □□ □□
C. □□□ □□□□ □□ □ □□ □□ □□ □□
D. □□□ □□□□ □□□□ □□□ □□ □□(DLP) □□
Answer: (SHOW ANSWER)

NEW QUESTION: 229
Microsoft 365 E5 □□□ □□ Microsoft Defender for Endpoint□ □□□□□. □□□□ Windows 11 □□□ □□□□ □□□□.
□□□ Windows Defender □□ □□□□ □□□□ □□ □□ □□□ □□ □□ □□□ □□□□□ □□ □□□□ □□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□, □□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:

NEW QUESTION: 230

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

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

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

□□□□ □□□□ VDI□□ Microsoft 365□ □□□□□.

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

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

365. □□□□ ID □□□ □□□□ VDI □□□ □□□□ □□□□ □□□.

A. □□□ □ □□ □□

B. □□□ □□□ □□

C. □□ □□ □□

D. Microsoft 365□ ExpressRoute

Answer: A (LEAVE A REPLY)

NEW QUESTION: 231

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

Contoso□ ID □□□□□ □□ Microsoft Defender□ □□□□.

□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□□ □□□□□ Defender□ □□□ □□□□ □□□.

□□□: User4□□ ID □□ □□□ □□ Defender□ □□□□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 232

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

□□ □□□□ □□ □□□□ □□□ □□□□□.

□□ □□□ □□□ □□□□□ □□□□ □□□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.

Answer Area

Windows 10 compliance policy
Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured
Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured
Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-do-date	Require	Not configured
Real-time protection	Require	Not configured

Answer:

Answer Area

Windows 10 compliance policy
Windows 10 and later

Encryption

Encryption of data storage on device	Require	Not configured

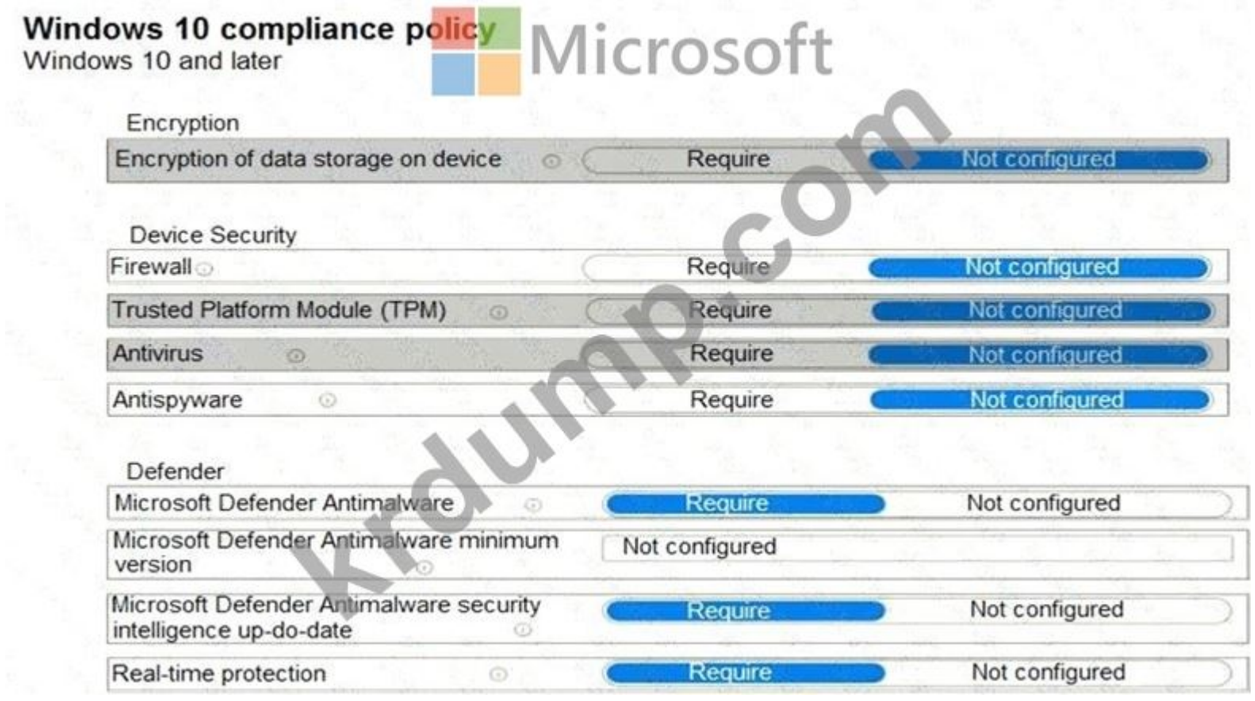
Device Security

Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured

Defender

Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-do-date	Require	Not configured
Real-time protection	Require	Not configured

Explanation:



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

NEW QUESTION: 233

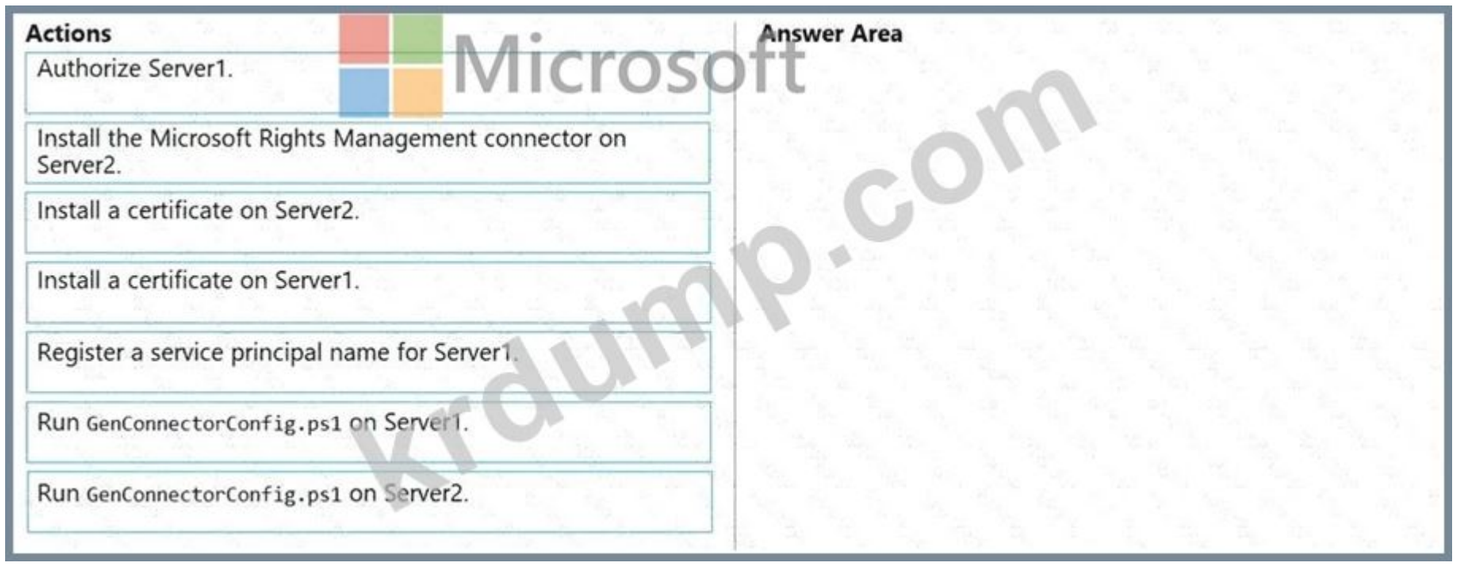
□□□ □□□□□□ Azure Active Directory(Azure AD)□ □□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

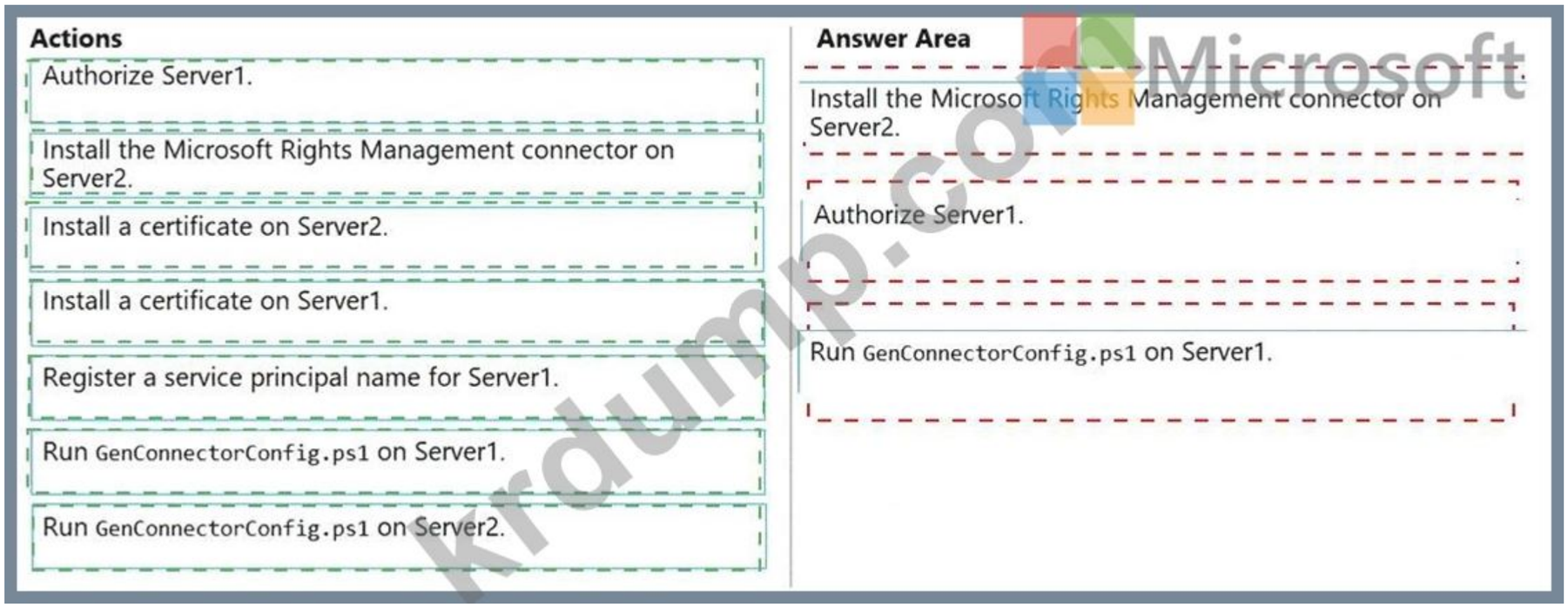
Azure Information Protection□ □□□□□.

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

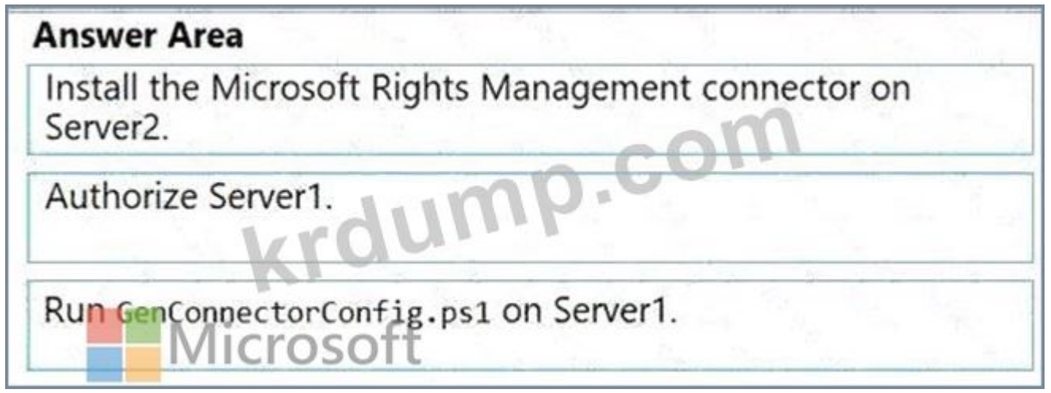
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□□.



Answer:



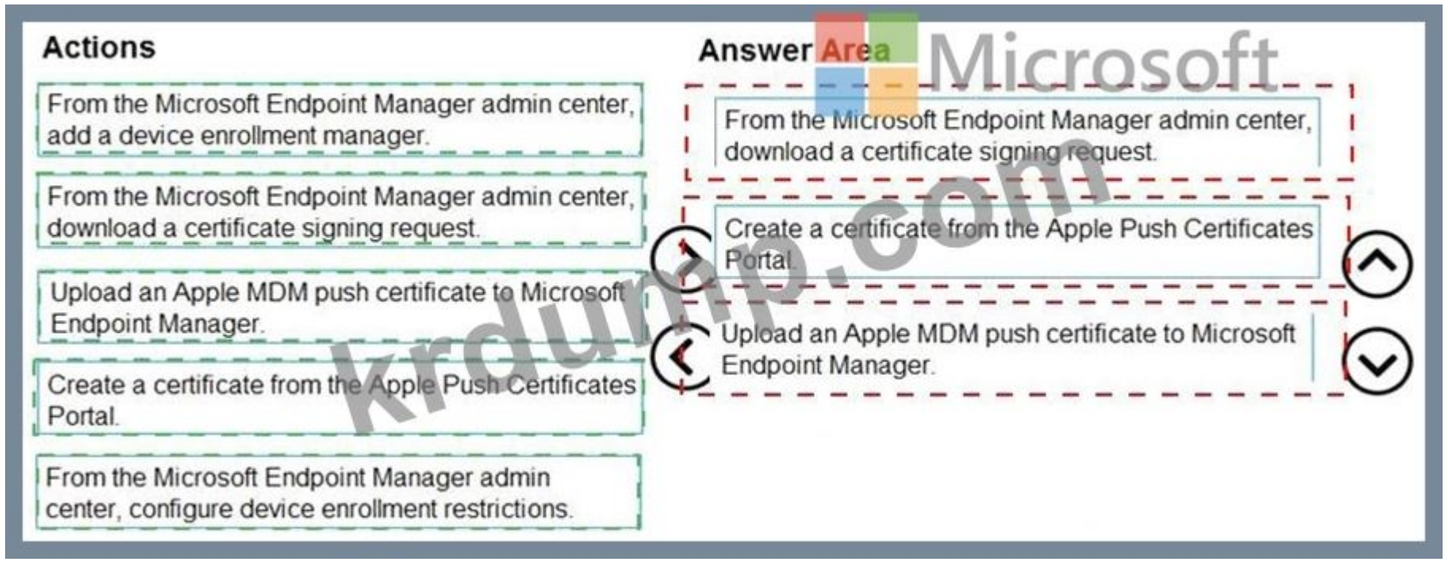
Explanation:



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

NEW QUESTION: 234
Microsoft 365 E5 □□□ □□□□.
□□ □□□□ iOS □□□ □□□□ □□□□.
Microsoft Endpoint Manager□ iOS □□□ □□□□□ □□□.
Microsoft Endpoint Manager□□ iOS/iPadOS □□ □□□□ □□ □ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□□.

Answer:



Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get

NEW QUESTION: 235

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

Name	Type
Label1	Sensitivity
Label2	Retention

□□ □□ □□ □□ □□□ □□□□.

Name	Stored in	Description
File1	Microsoft SharePoint	File document that has Label1 applied
File2	Microsoft Teams channel	File document that has Label2 applied
Mail1	Microsoft Exchange Online	Email message that has Label1 applied
Mail2	Microsoft Exchange Online	Email message that has Label2 applied

□□□ □□□□□ □□ □□□ □ □ □□□?

A. File1, File2, Mail1, Mail2

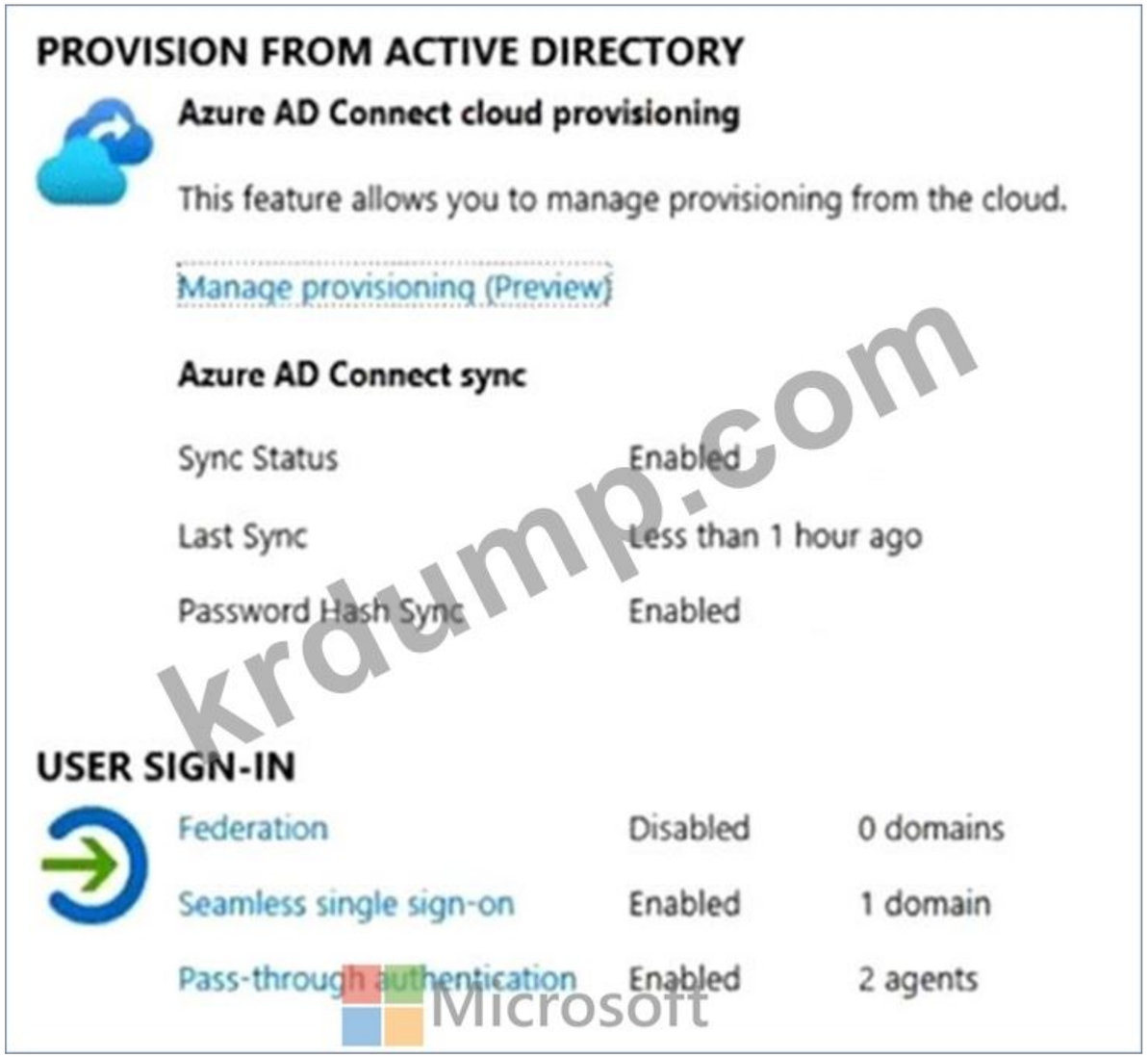
B. File1□ Mail!□
C. File2□ Mail2□
D. File1□ File2□
E. File1□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 236
□□□ □□□□ □□□ □□□□ □□ □□□□.
Microsoft 365 □□□ □□□□.
□□ □□ □□(MFA)□ □□□□ Policy1□□□ □□□ □□□ □□□ □□ □□□□□.
□□□ □□□ □□□□ MFA□□ □□□□ □□□. □□ □□□ □□□□ □□ MFA□ □□□□ □□□.
Policy1□ □□ □□□ □□□□ □□□?
A. IP □□ □□□ □□□ □□□□ □□□ □□□ □□
B. □□□ □□□□□□ VPN □□
C. □□ □□□ □□□□ □□□ □□□ □□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 237
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
□□□ □□□□□□ 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: B (LEAVE A REPLY)
This is not a permissions issue so you do not need to assign the Security Reader role.
The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

NEW QUESTION: 238
Microsoft 365 □□□ □□ Office 365□ Microsoft Defender□ □□□□ □□□□.

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 239
□□□
Site1□□□ Microsoft SharePoint □□□□ DLP1□□□ □□□ □□ □□(DLP) □□□ □□□ Microsoft 365 E5 □□□ □□□□. DLP1□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

Site1□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Matched DLP rule
File1.docx	Rule1, Rule2, Rule3
File2.docx	Rule1, Rule3, Rule4

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

Answer Area

File1.docx:

- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

Answer:

Answer Area

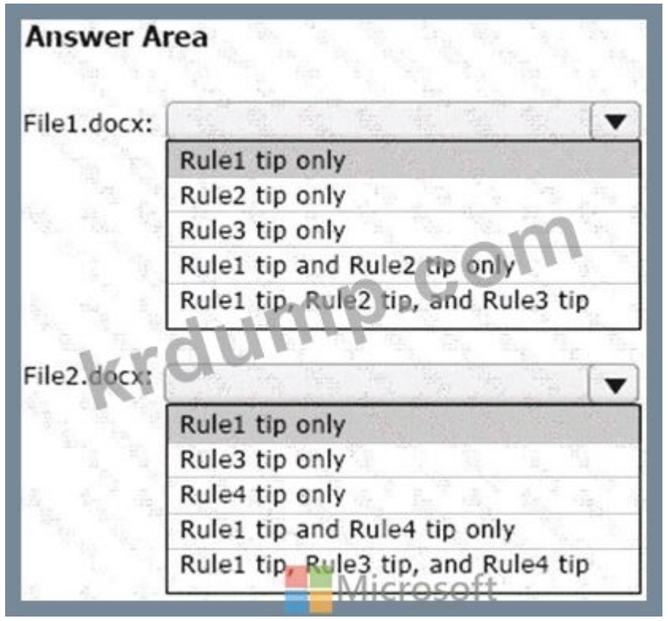
ile1.docx:

- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

ile2.docx:

- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

Explanation:



Box 1: Rule1 tip only

File1 matches Rule1, Rule2, and Rule3.

Rule1 has the highest priority.

Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can ' t have the same priority value.
Box 2: Rule1 tip only
Note: User Override support
The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can ' t be overridden).
It ' s possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.
If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp
https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips

NEW QUESTION: 240
Microsoft 365 Defender□ □□□□ Microsoft 365 □□□ □□□□ □□□□.
□□ □□ □□□ Microsoft□ □□ □□□ □□□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□ □□
C. □□□□□□□ □□ □□
D. □□ □□□
E. □□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 241
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
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: 242
Microsoft 365 E5 □□□ □□□□.
Mailbox1□□□ □□□□ □□□□ □□ □□□ □□□□ □□□ □□□□□.
□□ □□ □□□ □□□□□ Office 365□ Microsoft Defender□ □□□□ □□□.
* Mailbox1□□ □□ □□□□ □□□□□ □□□□ □□□□□.
* □□□ □□ □□ □□ □□□□ □□ □□ □ □□□ □□□ □□□□□.
□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

Answer Area

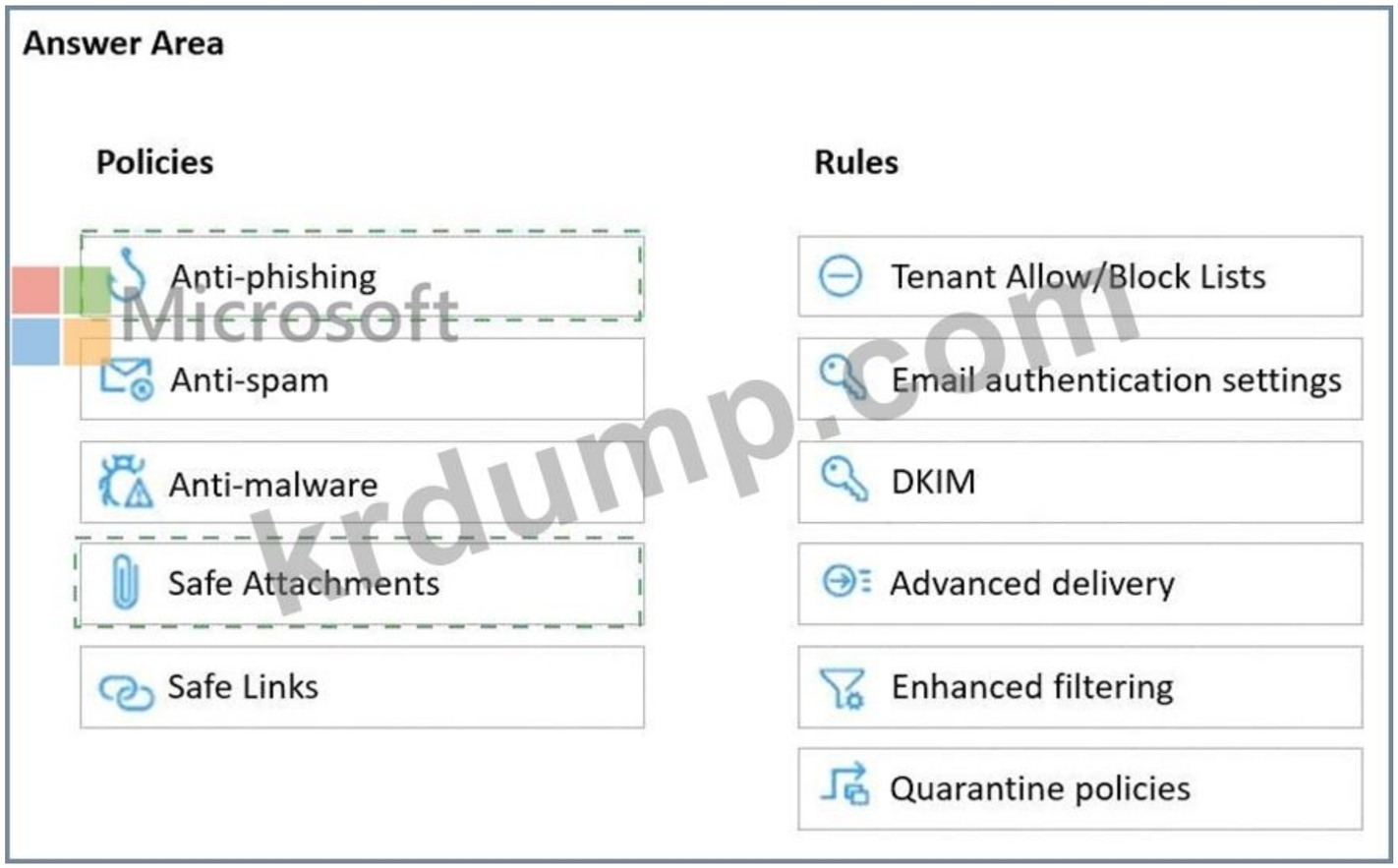
Policies

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

Rules

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

Answer:



Explanation:

Safe Attachments policy: This policy allows you to specify how to handle email attachments that might contain malware. You can create a custom policy for Mailbox1 and set the action to Do not scan attachments.

This will ensure that incoming email is not filtered for Mailbox1. You can also enable the Redirect attachment option to send a copy of the original attachment to another mailbox for analysis1.

Anti-phishing policy: This policy helps you protect your organization from impersonation and spoofing attacks. You can create a default policy for all other mailboxes in the subscription and enable the following features: Impersonation protection, Spoof intelligence, and Domain authentication. These features will help you detect and block emails that try to impersonate your users, domains, or trusted senders2.

NEW QUESTION: 243

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

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

Windows 10□ □□□□ □□□□ □□□□.

□□□ Windows 10 □□□ □□□□ □□□.

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

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

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

NEW QUESTION: 244
□□ □□ □□□ □□□ □□□ Microsoft 365 □□□ □□□□.

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

□□□ □□ □□□ □□□ □ □□□?
A. □□□
B. □□ □ □□□
C. □□ □ □□□□
D. □□, □□□ □ □□□
E. □□, □□□, □□ □ □□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365- worldwide#limitations

NEW QUESTION: 245
Microsoft 365 □□□ □□□□.
□□□ □□ Microsoft Office 365 □□□□□□□□ □□□□ □□□□□□□ □□□ □□□□□.
□□□ □□□□□ □□□□□□□□ □□□□ □□□□ □□□.
□□□ □□□ □ □□ □ □□ □□□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. Microsoft 365 □□ □□□□ □□□ □□ □□□□□ □□□□□.
B. Microsoft 365 □□ □□□□ □□□ □□ □□□□□ □□□□□.
C. Microsoft 365 □□ □□□□ □□ □□□□□ □□□□□.
D. Microsoft 365 □□□ □□□ agg□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
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: 246
Sitel□□□ Microsoft SharePoint □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □□ □□□ □□□□ □□□.
* □□ □□□□ □□□□ SIT1□□□ □□□ □□□ □□ □□□ □□□□.

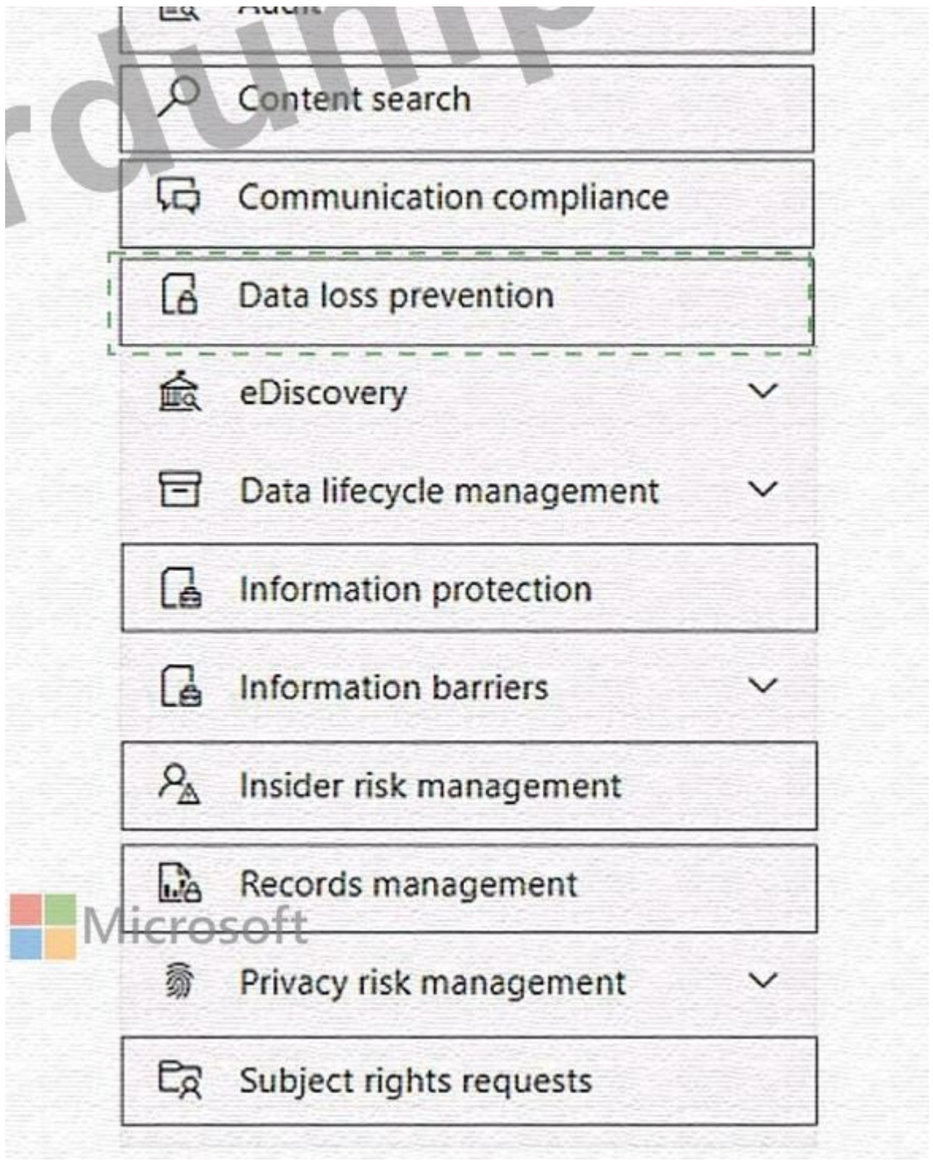
* SIT1□ □□□□ □□ □ □□□ □□□□□ □□□□□.
Microsoft Purview □□ □□ □□□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

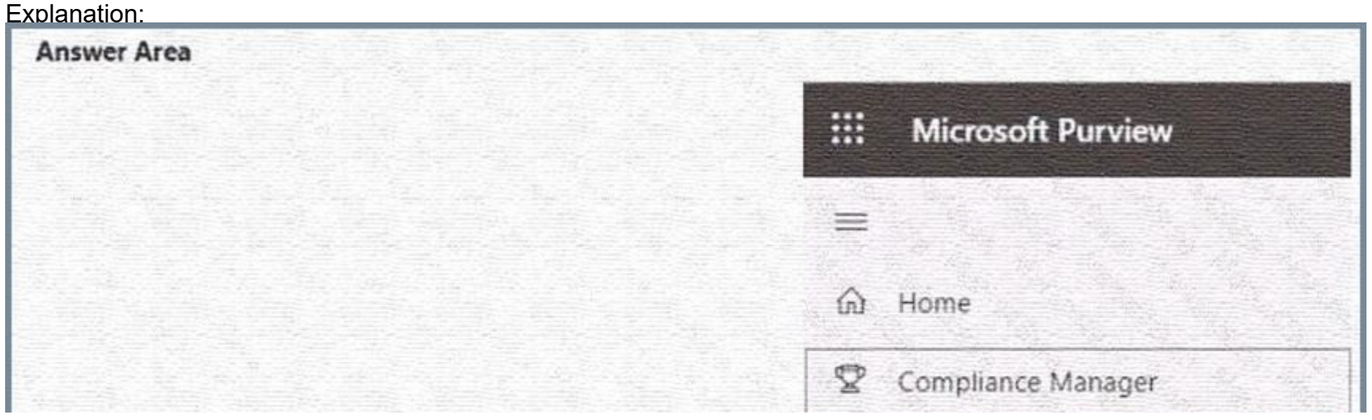

Insider risk management
Records management
Privacy risk management
Subject rights requests

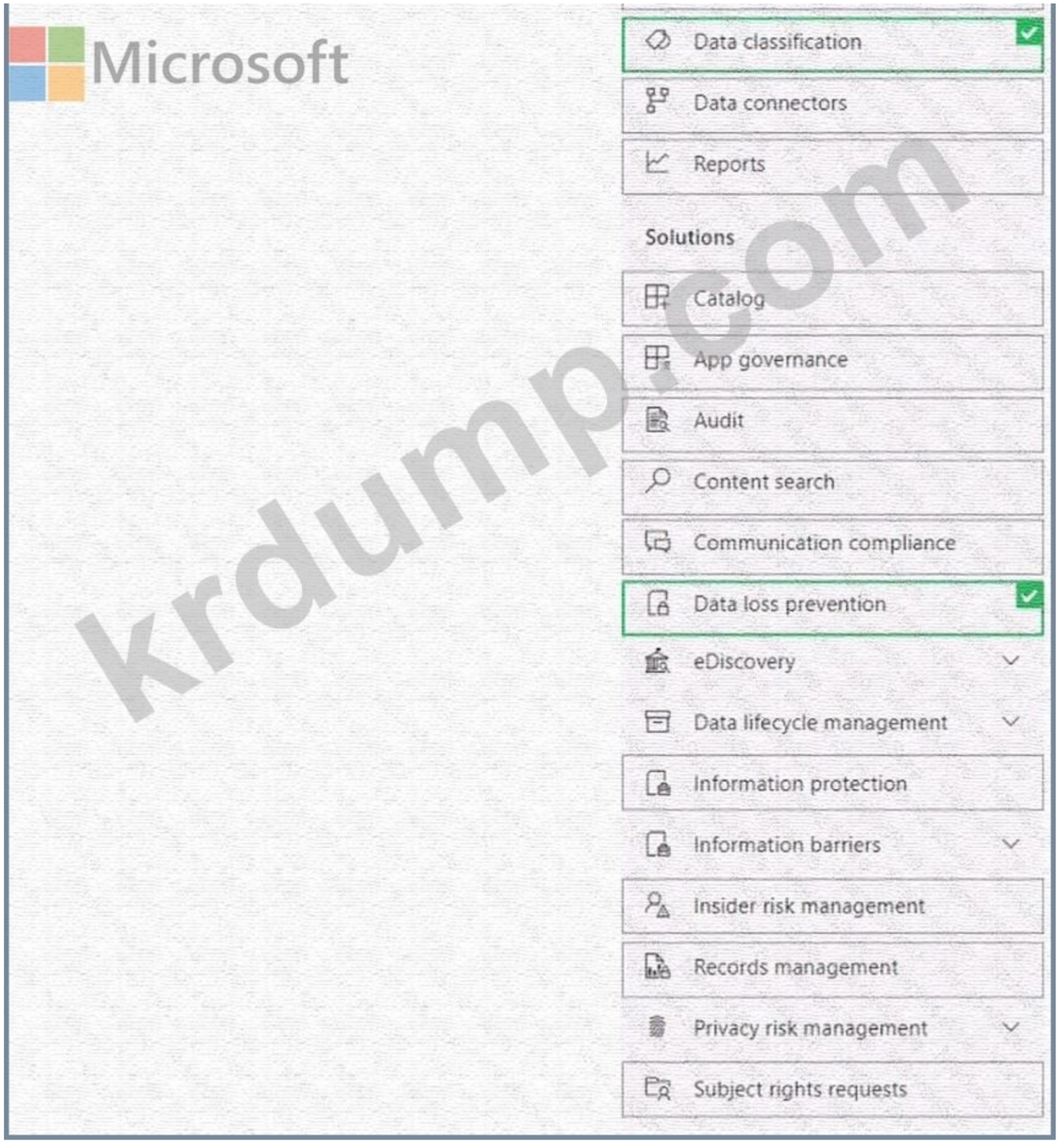
Answer:


Answer Area
Microsoft Purview
Home
Compliance Manager
Data classification
Data connectors
Reports
Solutions
Catalog
App governance



Explanation:





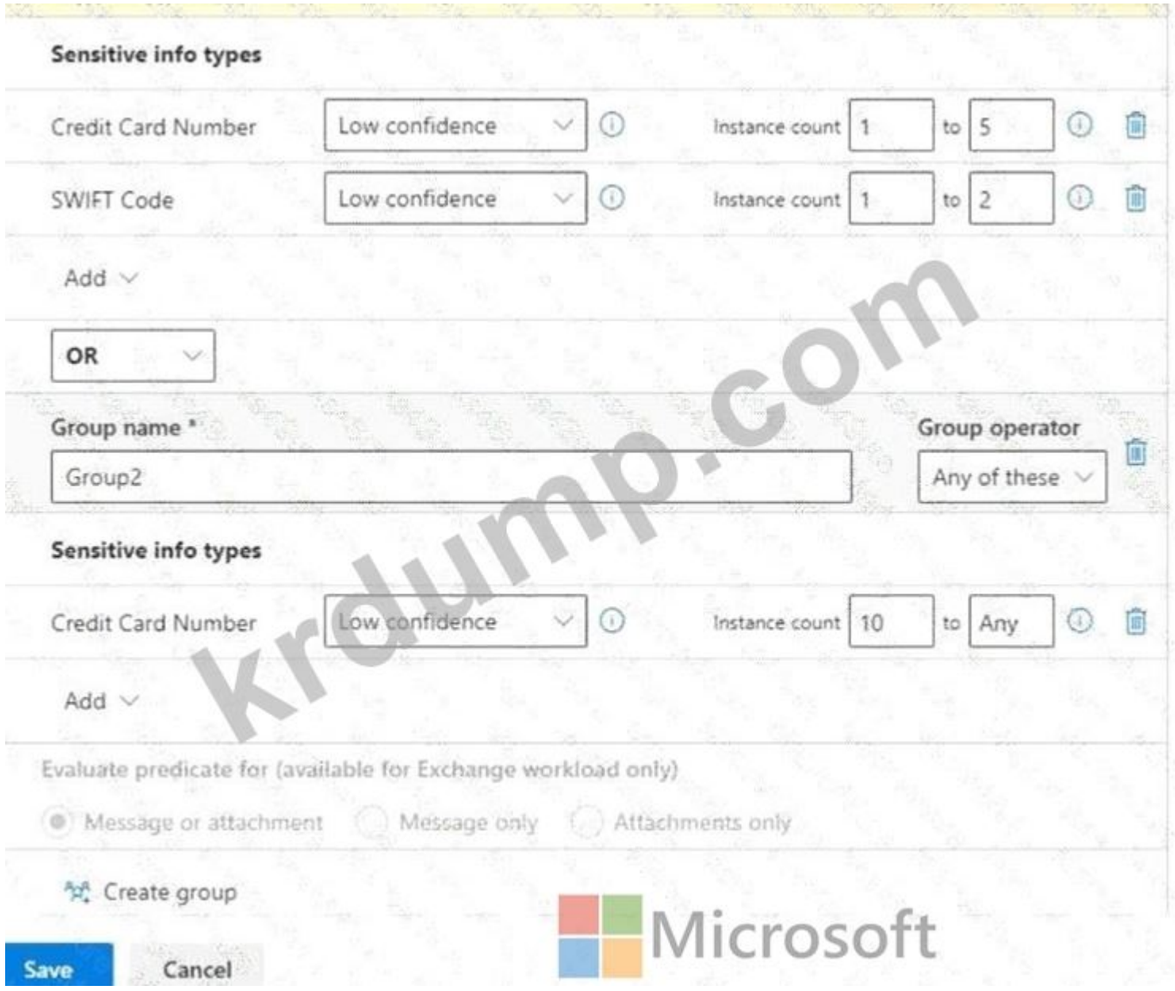
NEW QUESTION: 247

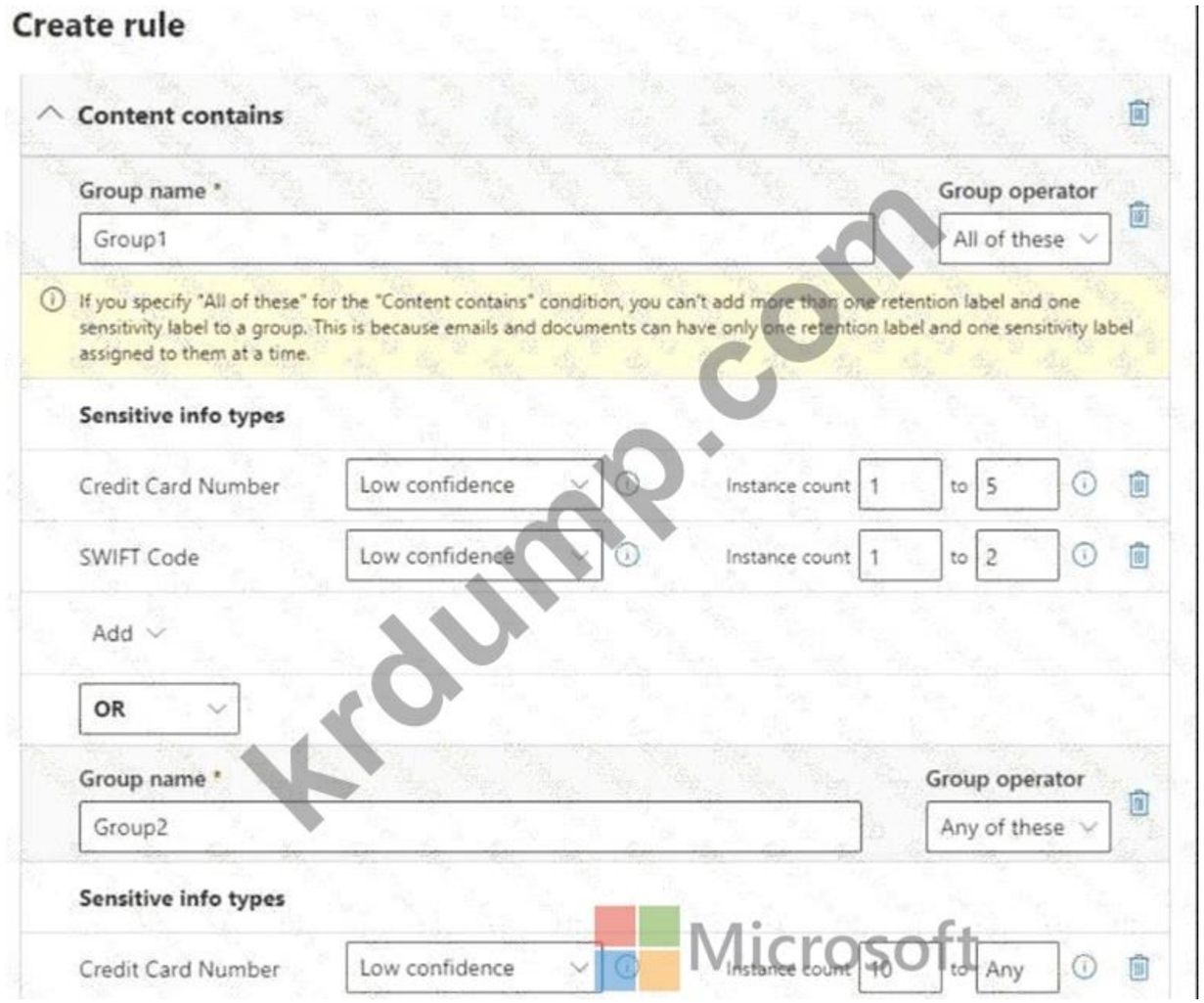
□□□ □□□□ □□ □□ □□□□ □□□□.
Microsoft Intune□ □□ □□□ □□□□ Microsoft 365 E5 □□□□ □□□□. □ □□□□□ □□ □□□□ □□□□.
□□ □□□□ □□ □□□□ □□ □□□ □□□ □ □□□ □□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□ □□□
C. □□ □□□□
D. □□□ □□□ □□
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

NEW QUESTION: 248
□□□ Site1□ Site2□□ □□□ Microsoft SharePoint Online □□□ □ □□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□□ □□ □□ □□ □□ □□□□ □□□ □□□□.

Name	Number of credit card numbers in the document	Number of SWIFT codes in the document	Stored on
Document1	3	3	Site1
Document2	7	2	Site2
Document3	15	0	Site1

) □□□ □□□□□.


Sensitive info types
Credit Card Number
Low confidence
Instance count 1 to 5
SWIFT Code
Low confidence
Instance count 1 to 2
Add
OR
Group name *
Group2
Group operator
Any of these
Sensitive info types
Credit Card Number
Low confidence
Instance count 10 to Any
Add
Evaluate predicate for (available for Exchange workload only)
Message or attachment
Message only
Attachments only
Create group
Save
Cancel


Create rule
Content contains
Group name *
Group1
Group operator
All of these
If you specify "All of these" for the "Content contains" condition, you can't add more than one retention label and one sensitivity label to a group. This is because emails and documents can have only one retention label and one sensitivity label assigned to them at a time.
Sensitive info types
Credit Card Number
Low confidence
Instance count
1
to
5
SWIFT Code
Low confidence
Instance count
1
to
2
Add
OR
Group name *
Group2
Group operator
Any of these
Sensitive info types
Credit Card Number
Low confidence
Instance count
10
to
Any

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

□□: □□ □□□ 1□□□□.


Statements
Yes
No
DLP1 applies to Document1.
DLP1 applies to Document2.
DLP1 applies to Document3.

Answer:

Explanation:

NO

No

Yes

In the Content contains condition, Microsoft Purview DLP lets you combine conditions using logical operators:

* "Any of these" = logical OR
* "All of these" = logical AND

From the exhibit, the rule is effectively:

* Group1 (All of these / AND)
* Credit Card Number: 1 to 5 instances
* SWIFT Code: 1 to 2 instances
* OR
* Group2 (Any of these)
* Credit Card Number: 10 to Any instances

So the rule matches if:

(Credit Card is 1-5 AND SWIFT is 1-2) OR (Credit Card is #10) .

Evaluate each document against the rule

Document1 : Credit Card = 3, SWIFT = 3

* Group1 requires SWIFT 1-2 , but Document1 has 3 # Group1 = false
* Group2 requires Credit Card #10 , but Document1 has 3 # Group2 = false Result: DLP1 does NOT apply # No Document2 : Credit Card = 7, SWIFT = 2
* Group1 requires Credit Card 1-5 , but Document2 has 7 # Group1 = false
* Group2 requires Credit Card #10 , but Document2 has 7 # Group2 = false Result: DLP1 does NOT apply # No Document3 : Credit Card = 15, SWIFT = 0
* Group2 requires Credit Card #10 , and Document3 has 15 # Group2 = true Result: DLP1 DOES apply

Yes

NEW QUESTION: 249

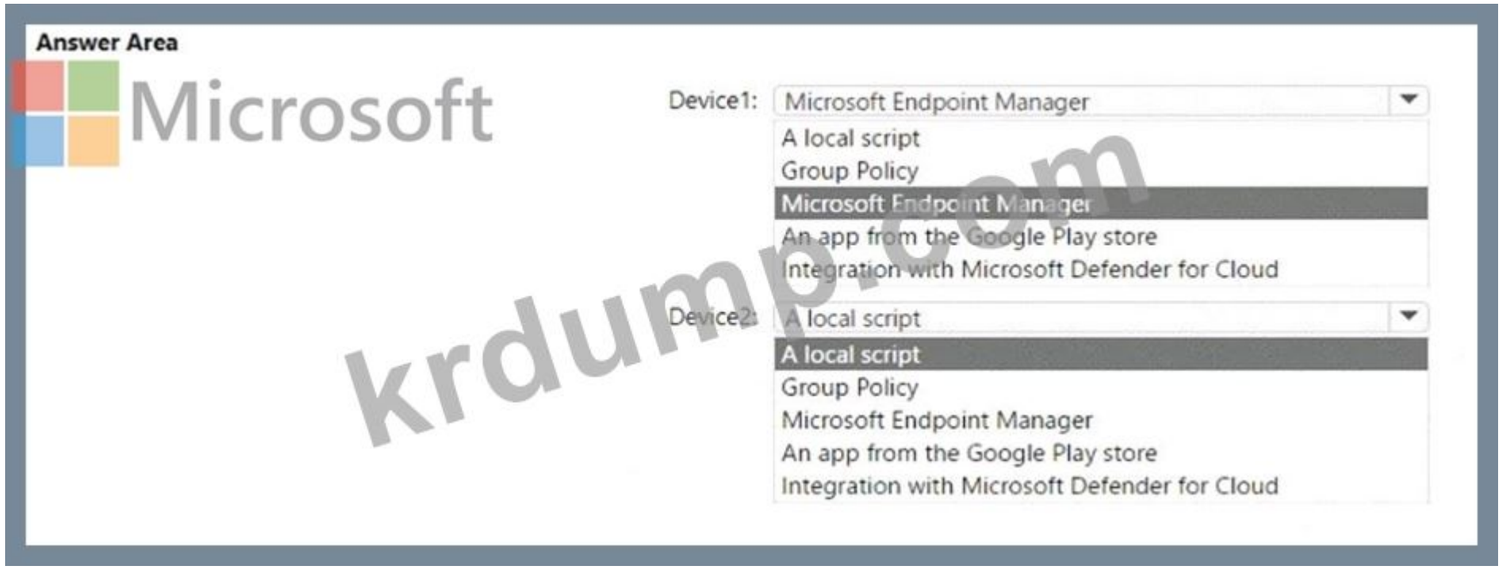
Microsoft Intune□ □□□□ □□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

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

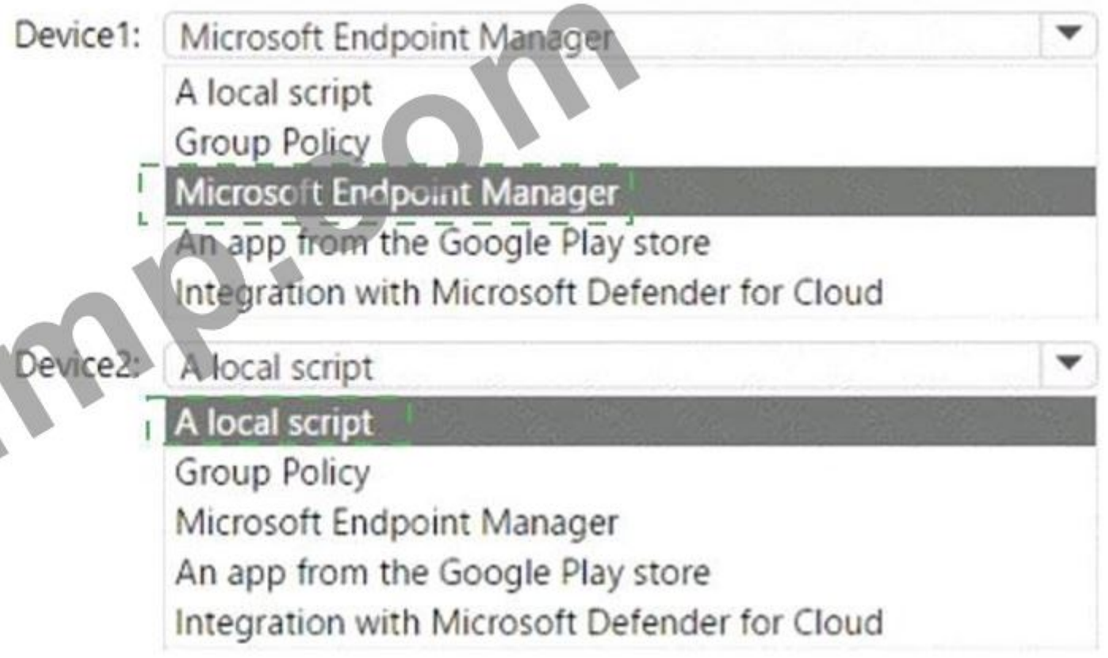
□ □□□ □□□□□ □ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.



Answer:

Answer Area



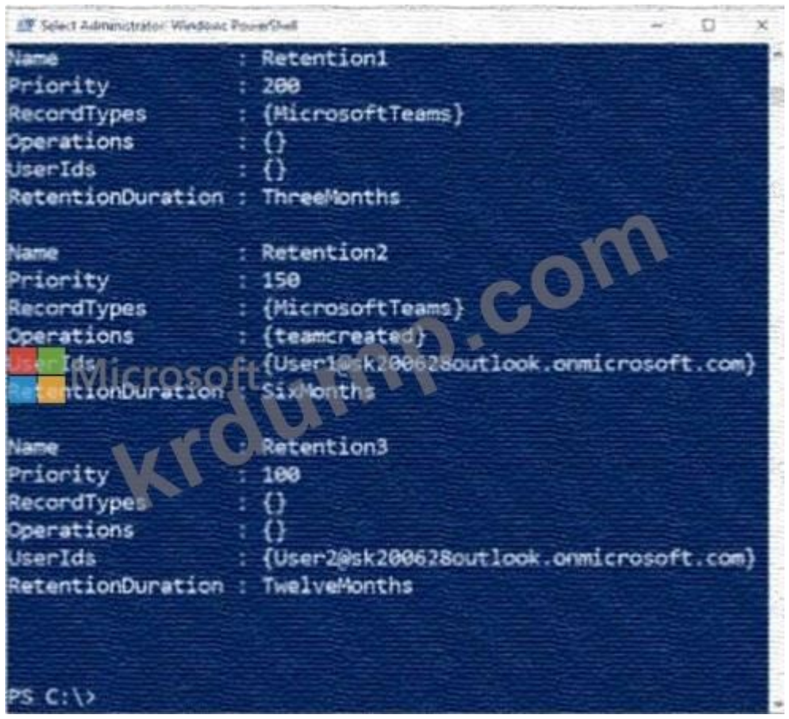
Explanation:

Answer Area

NEW QUESTION: 250
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows Server 2019□ □□□□ □□□ □□□□□ □□□□. □□□□□ □□□□ □□ □□□ Windows Server 2012 R2□ □□.
□ □□□□□ Windows 10□ □□□□ 100□□ □□□□ Windows Server 2012 R2□ □□□□ Server1□□□ □□ □□□ □□□□ □□□□.
Server1□ □□□□ □□□□ □□□□ Windows 10 □□ □□ □□□ □□□ □□□□□.
Server1□ □□ □□ □□ □□(GPMC)□ □□□□□.
Server1□□ □□□□□ Windows □□□□ □□ □□ □□□ □□□□ □□□.
□□ □□: □□□□ □□ □□□ Windows Server 2016□□ □□□□. Windows 10 □□□□□ □□ □□□ □□□□□ Netlogon □□□ □□ □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 251
□□ □□ □□□ □□ □□□ □□ □□□ □□□□ □□□. □□□ □□□□ □□□?
A. □□ □ □□ □□ □□ □□□ □□□ □□ □□(DLP) □□
B. □□ □ □□ □□ □□ □□□ □□ □□
C. Microsoft Cloud App Security□ □□ □□
D. Microsoft Cloud App Security□ □□ □□
Answer: D (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

NEW QUESTION: 252
□□ □□ □□□ □□□ 3□□ □□ □□ □□□ □□ Microsoft 365 ES □□□ □□□□.



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

Answer:

Explanation:

MS-102-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-102-KR □□! DumpTop □ □□ **MS-102-KR** □□ □□□ □□□□□□, DumpTop MS-102-KR □□ □□□ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-102-KR □□□ □□□□□. https://www.dumptop.com/Microsoft/MS-102-KR-dump.html (**572** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)