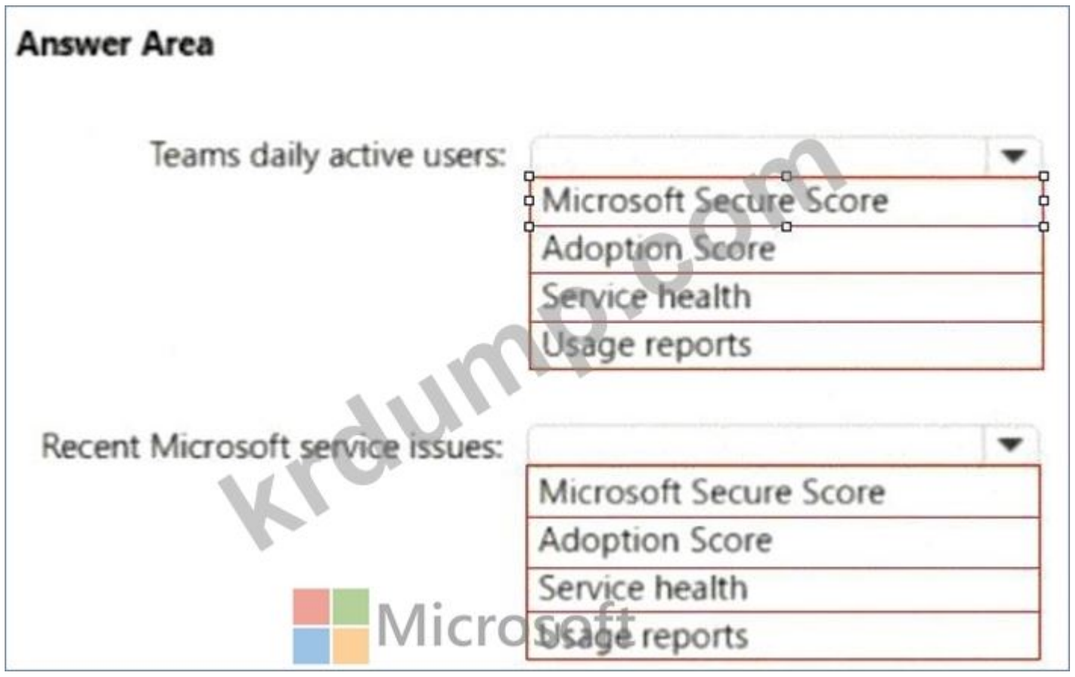
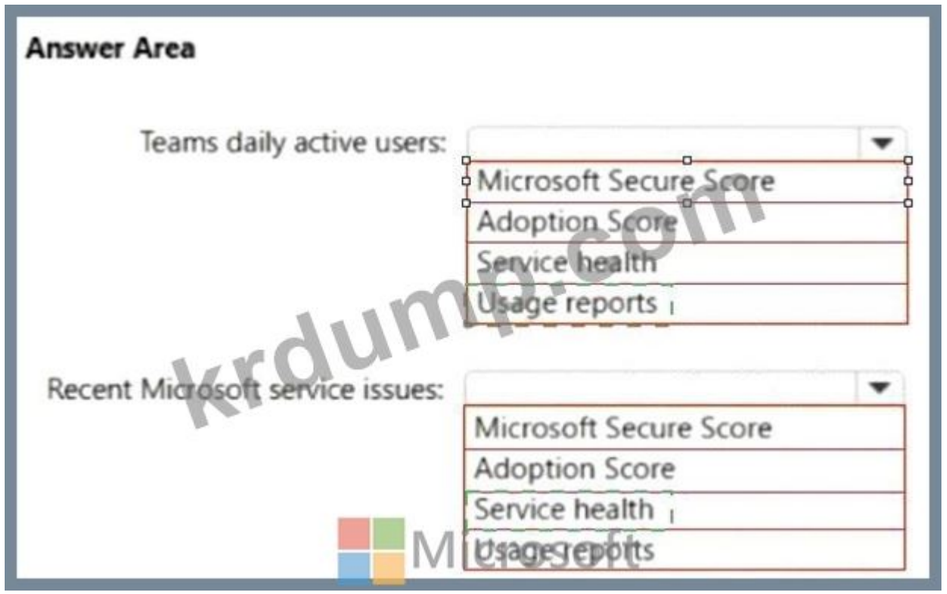
Microsoft.MS-102-KR.v2026-08-24.q284

□□□□:	MS-102-KR
□□□□:	Microsoft 365 Administrator (MS-102 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	284
□□:	v2026-08-24
# □□ □:	136
# □□ □□□:	2840
https://www.krdump.com/Microsoft.MS-102-KR.v2026-08-24.q284.html	

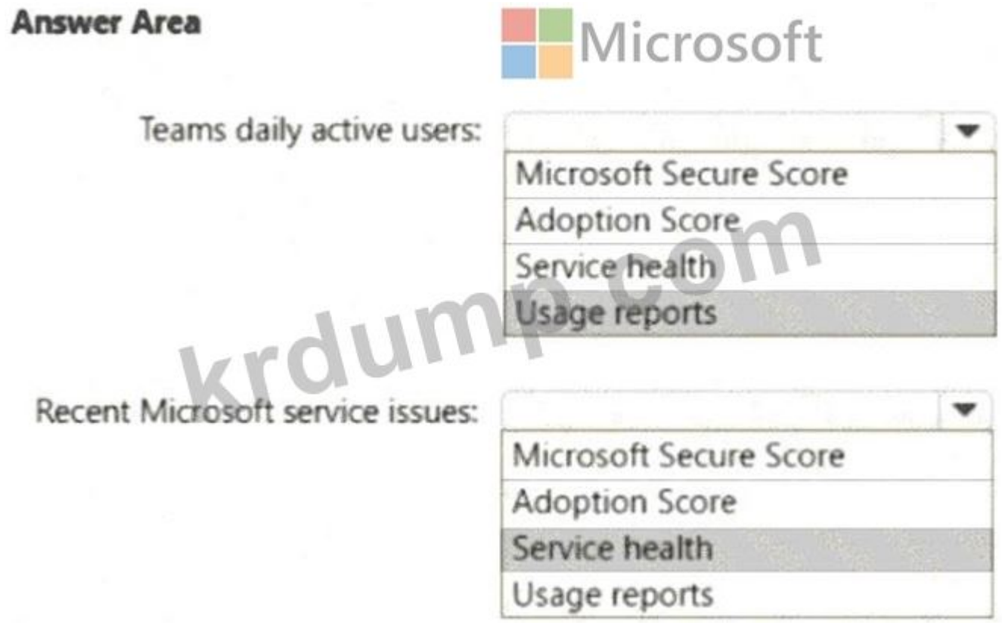
NEW QUESTION: 1
□□□
Microsoft 365 □□□ □□□□.
□□ □□□ □□ □□□ □□□□ □□□.
Microsoft Teams□ □□ □□ □□□
□□ Microsoft □□□ □□
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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: 2
Microsoft Defender for Endpoint□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□□ □□□ □□ □□ □□ □ □□ □□□ □□□ □□□□□.
Device1□□□ □□□ □□□□ □□□□ □□□□ □□□□□.
□ □□□□ □□□ □□ □□□?
A. □□ □□□ □□□□□.
B. Microsoft □□ □□□ - □□□ □□ □□□ □□□□□.
C. □□□ □□□□ □□□□□□ □□□□□.
D. Defender for Endpoint□ Microsoft Intune□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
Office 365□ Microsoft Defender□ □□□□□□?
□□ □□□□□ □□□□ □□□□ □□□□□.
□□□□□□ □□□ □□□□ □□□□□ □□□ □□ □□ □□□ □□□ □□□.
□□□□□ □ □□□□ □□□ □□ □ □□ □□ □□□ □□□□□?
A. 7
B. 30
C. 15
D. 45
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□□□ □□□ □□ □□□ □□□□□ □□□.
□□□ □□□□ □□□?
A. Microsoft Authenticator □
B. Microsoft 365 □□□ □□□ □
C. Intune □□ □□
D. Intune □
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
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: 6
□□□ Microsoft 365 □□□ □□□□ □□□□.
Microsoft Entra □□ □□ □□□□ □□ □□□ □□ □□ □□ □□□□□ □□ Microsoft Authenticator □□□ □□□□□.

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

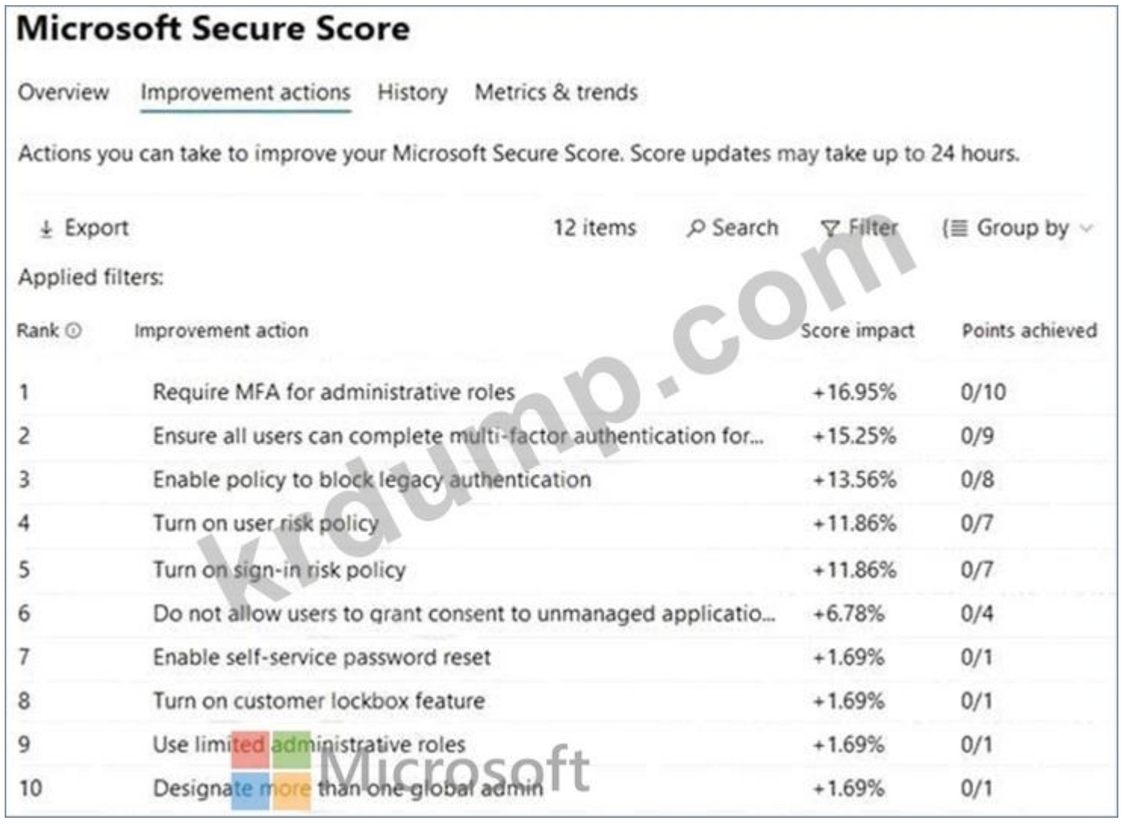
D. □□□□□□□ □□□

Answer: (SHOW ANSWER)

NEW QUESTION: 7

Microsoft 365 E5 □□□□ □□□□ □□□□.

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



Microsoft Secure Score

Overview | Improvement actions | History | Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export | 12 items | Search | Filter | Group by

Applied filters:

Rank	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	+16.95%	0/10
2	Ensure all users can complete multi-factor authentication for...	+15.25%	0/9
3	Enable policy to block legacy authentication	+13.56%	0/8
4	Turn on user risk policy	+11.86%	0/7
5	Turn on sign-in risk policy	+11.86%	0/7
6	Do not allow users to grant consent to unmanaged applicatio...	+6.78%	0/4
7	Enable self-service password reset	+1.69%	0/1
8	Turn on customer lockbox feature	+1.69%	0/1
9	Use limited administrative roles	+1.69%	0/1
10	Designate more than one global admin	+1.69%	0/1

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

□□ □□ □□ □ □□ □□ □□□ □□□ □□□□?

A. □□□ □□□ □□ □□□ □□(MFA)□ □□□□□.

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

C. □□□ □□□ □□□□ □□□ □□□□□□.

D. □□ □□□ □□ □□□ □□□

E. □□□ □□□ □□ □□

Answer: A,B,C (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

NEW QUESTION: 8

□□□ □□□ Microsoft 365□ □□□□ □□□□.
□□□ □□□ □□□ □□ □□□ □□□□ □□□□□.
□□ □□ '□□'□□□ □□□ □□□ □□□ □□□□ □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Microsoft 365 □□ □□ □□□ □□□ □□ □□(DLP) □□
B. Exchange □□ □□□ □□ □□
C. Exchange □□ □□□ □□ □□ □□
D. Microsoft 365 □□ □□□ Dace □□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 9
□□□□□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□□ □□□□ □□□□.
□□□ Microsoft Entra □□□□ □□□□ □□□□.
Microsoft Entra Connect □□□□ □□□□□.
□□□□ □□□□ □□□□□.
□□□ □□□ □□ 'Microsoft Entra Connect Sync□ □□□□ □ □□□□ □□□ □□□ □□□ □□□□.'□□ □□ □□□□ □□□□□□. □□□□ □□□□□ □□□□□ □□ □□, □□□□ □□□ □□□□□ □ □ □□□ □□ □□□□. □□□ □□ □□□?
A. PowerShell□□ set-AosyncScheduler cmdlet□ □□□□□.
B. PowerShell□□ Repair-AAOCloudSyncToolsAccoont cmdlet□ □□□□□.
C. Microsoft Entra □□ □□□□ Microsoft Entra Connect Sync □□□ □□□ □□□□□□□.
D. Active Directory □□□ □ □□□□□ ADSync □□□ □□□ □□□ □□□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 10
□□□□□ □Ł□□□□ Active Directory □□□□ □□□□ □□□□. Microsoft 365 □□□ □□□□.
□□□□ □□□ □□□□ □□□□ □□□ □□□□ □□□□□.
□□ □□□ □□ Microsoft Entra Password □□□ □□□□□.

Active Directory □□□□ □□□ □□ □□□ □□□□ □□□ □□ □□□□□ □□□ □ □□□ □□□ □□□□□□.
□□ □□□□□ □□□ □□□□□ □□ □□□□□ □□ □□□.
□□ □ □□ □□□ □□□ □□□? □□□ □□ □□□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. □□□ □□□□□□ Microsoft Entra Application Proxy □□□□ □□□□□.
B. □□□ □□ □□ □□□□□□ □□□ □□ □□ □□ □□□ □□□□□.

C. □□ □□□ □□□□□□ Microsoft Entra Password Protection DC Agent□ □□□□□.
D. Active Directory□□ □□ □□□ □□□ □□□□□.
E. □□□ □□□□□□ Microsoft Entra Password Protection Proxy□ □□□□□.
F. Windows Server Active Directory□ □□ □□□□ □□ □□□ □□□□□.
Answer: C,E,F (LEAVE A REPLY)

NEW QUESTION: 11
□□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

10□□ □□□ □□□□ □□□ □□ □□ □□□□□ □□□□ □ □□□□□ Microsoft 365 E5 □□□□□ □□□ □□□□□.
□□□□ □□ □□□ □□□□ □□, □□ □□□ □□□□ □□□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:
Answer Area

Explanation:

NEW QUESTION: 12
contoso.com□□□ Microsoft Entra □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Microsoft 365 Business Voice □□ □□ □□□□ 100□□ □□□□□.
Voice□□ □□□ □□□□□ Microsoft 365 Business Voice □□ □□ □□□□□ □□□□ □□□□□ □□ □□□.
□□□ □□ □□□?
A. Microsoft 365 □□ □□□□ □□ □□□ □□□ □□□□□.
B. Microsoft Entra □□ □□□□ □□ □□□ □□□ □□□□□.
C. Microsoft 365 □□ □□□ □□□□ □□□□□ □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □ □ □□□ □□□□.
□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □ □□□□ □□ □□□ □□□□ □□□□.
□□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□. □ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

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

A. □

B. □□□

Answer: B (LEAVE A REPLY)

This is not a permissions issue so you do not need to assign the Security Reader role.

The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

NEW QUESTION: 14

□□□

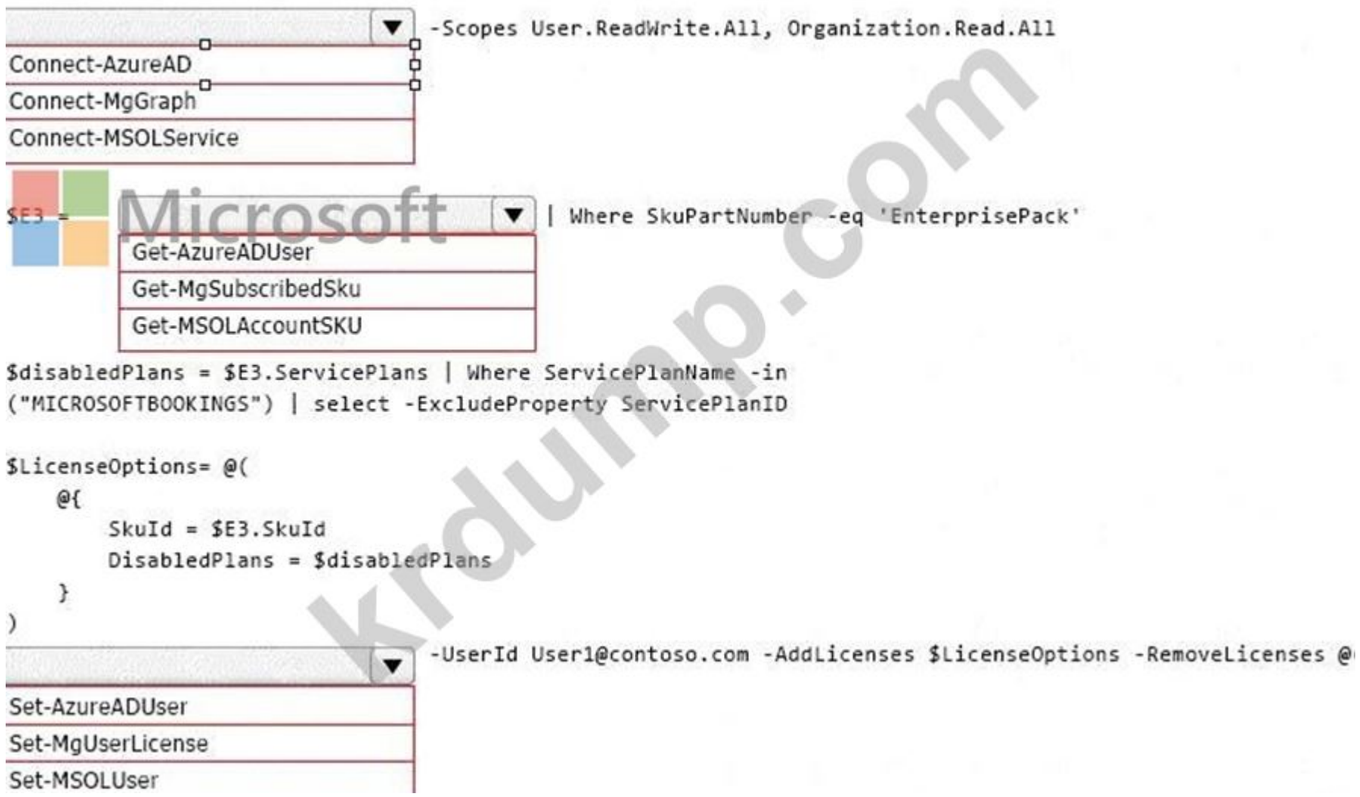
Microsoft 365 □□□ □□□□.

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

PowerShell□ □□□□ User1□ Microsoft Office 365 E3 □□□□□ □□□□ □□□. Microsoft Bookings□ □□□□□□□ □ □□□.

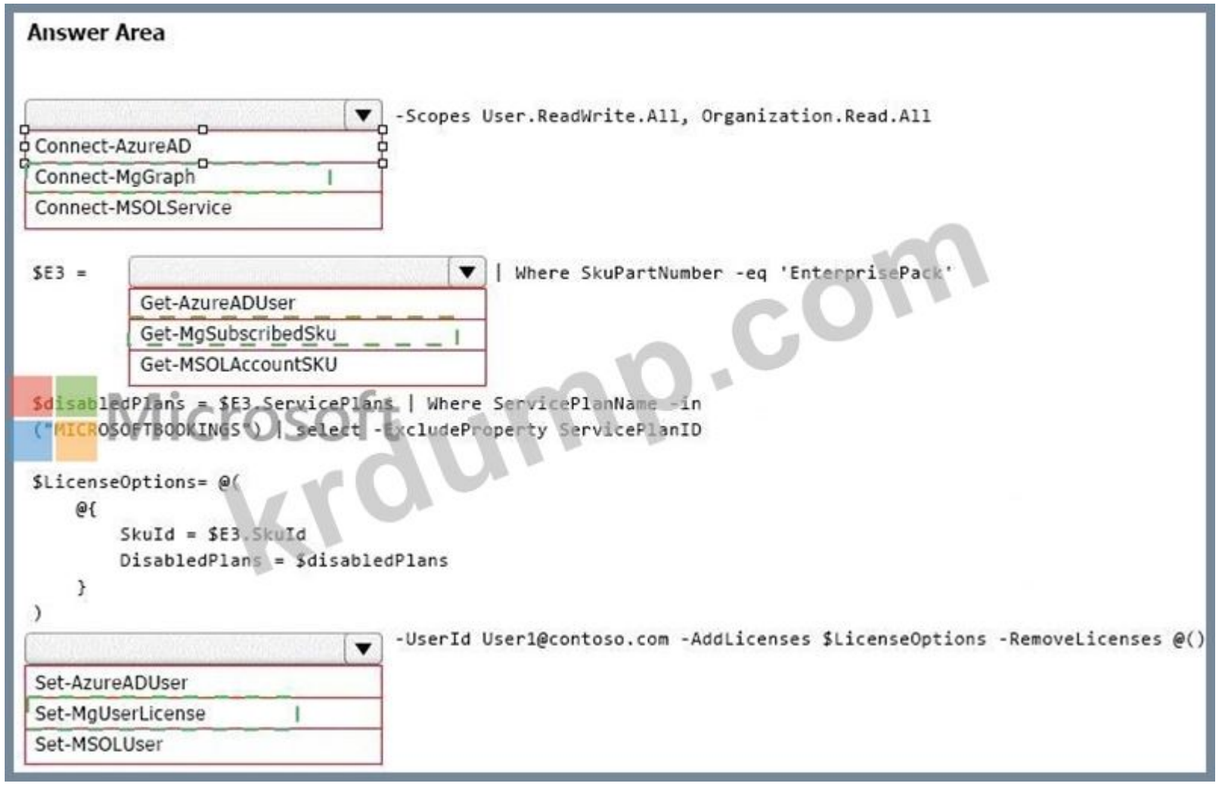
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area



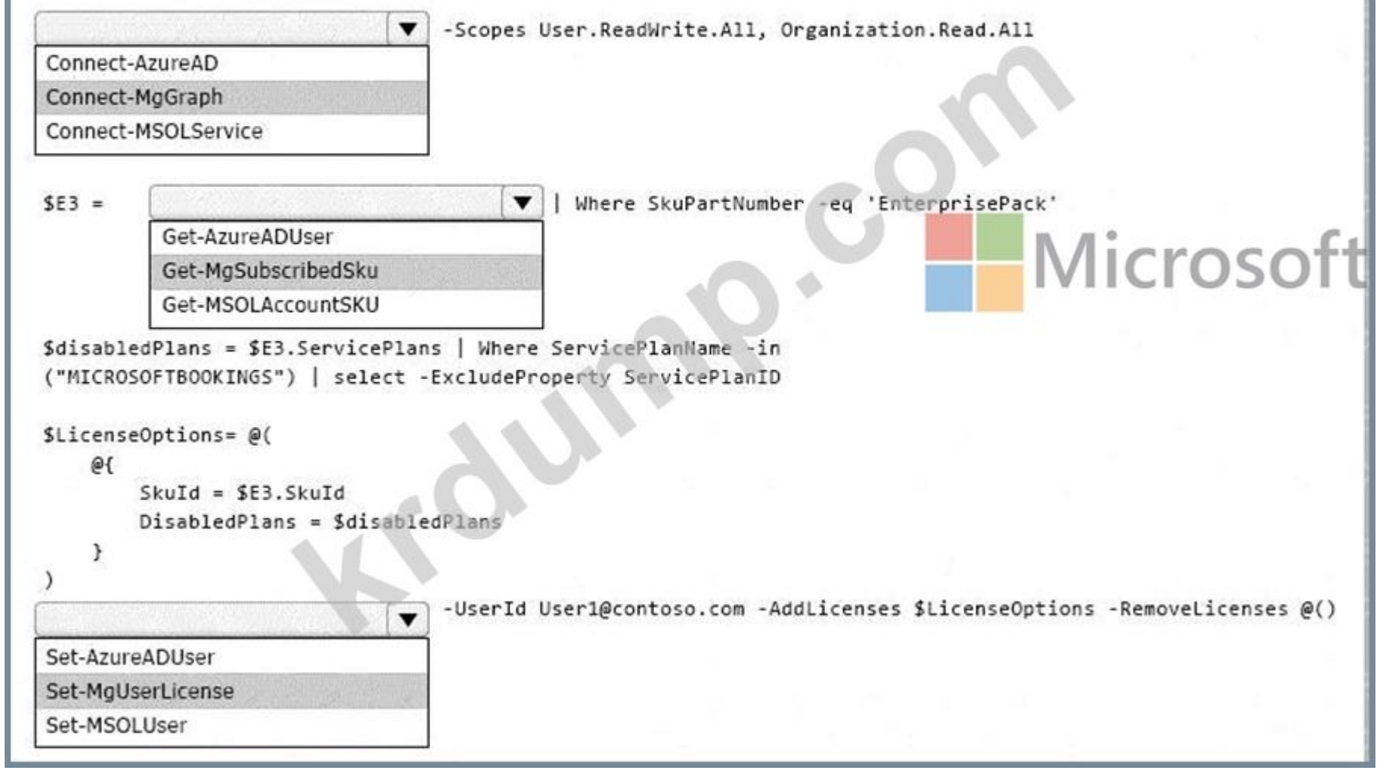
Answer:

Answer Area



Explanation:

Answer Area



Box 1: Connect-MgGraph

Assign Microsoft 365 licenses to user accounts with PowerShell

Use the Microsoft Graph PowerShell SDK

First, connect to your Microsoft 365 tenant.

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the ' Assign license ' Microsoft Graph API reference page.

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All

Box 2: Get-MgSubscribedSku

Run the Get-MgSubscribedSku command to view the available licensing plans and the number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.

Box 3: Set-MgUserLicense

Assigning licenses to user accounts

To assign a license to a user, use the following command in PowerShell.

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

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

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

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

NEW QUESTION: 15

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

Name	Operating system	Tag
Device1	Windows 11	Inventory1
Computer1	Windows 11	Inventory2
Device3	Android	Inventory3

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

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

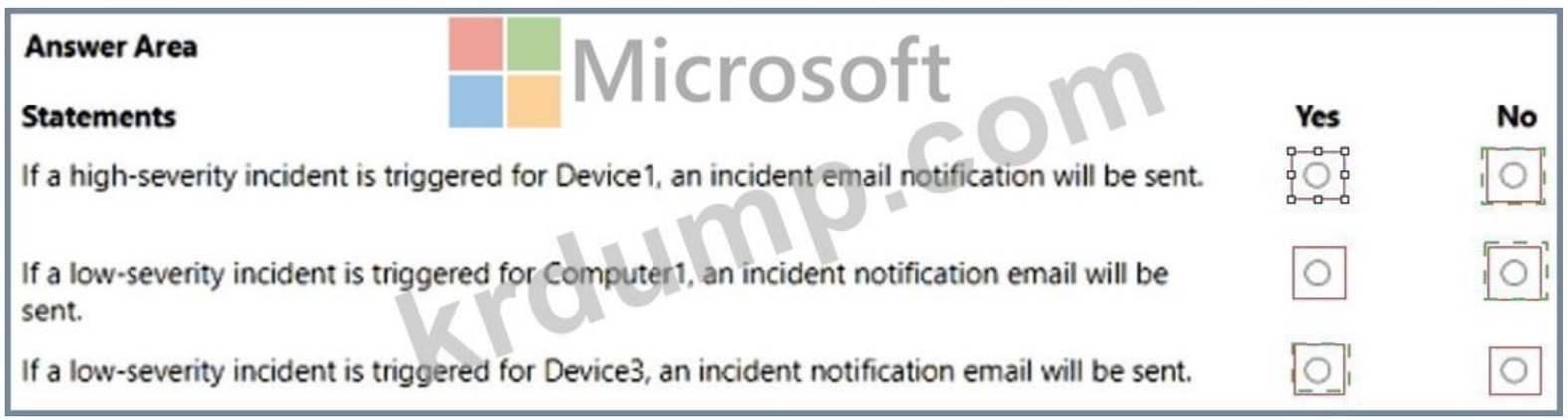
□□ □□ □□□ □□ □□□ □□ □□□ □□ □□□ □□□□□.

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

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

□□: □□ □□□ 1□□□□.

Answer:



Explanation:

Box 1: No

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

However, the Group2 has alert severity low.

Box 2: No

Computer1 does not belong to either Group1 or Group2

Box 3: Yes
Device3 belongs to both Group1 and Group2.
Note: Understanding alert severity
Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.
The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue

NEW QUESTION: 16
Microsoft 365 □□□□ □□□□.
Endpoint Protection □□ □□ □□□□ □□□ □□□□□.
□□□□ □□□□ □□ □□□□ □□□ □ □□□?
A. □□□□□
B. CentOS □□□
C. iOS
D. □□□ 10
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

NEW QUESTION: 17
□□ □□□ □□□□ □□ □□□□ □□□□ □□□?
A. DLP □□□ □□□□□.
B. DLP □□□ □ □□□
C. DLP □□
D. □□ □□□ □ □□□
Answer: C (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

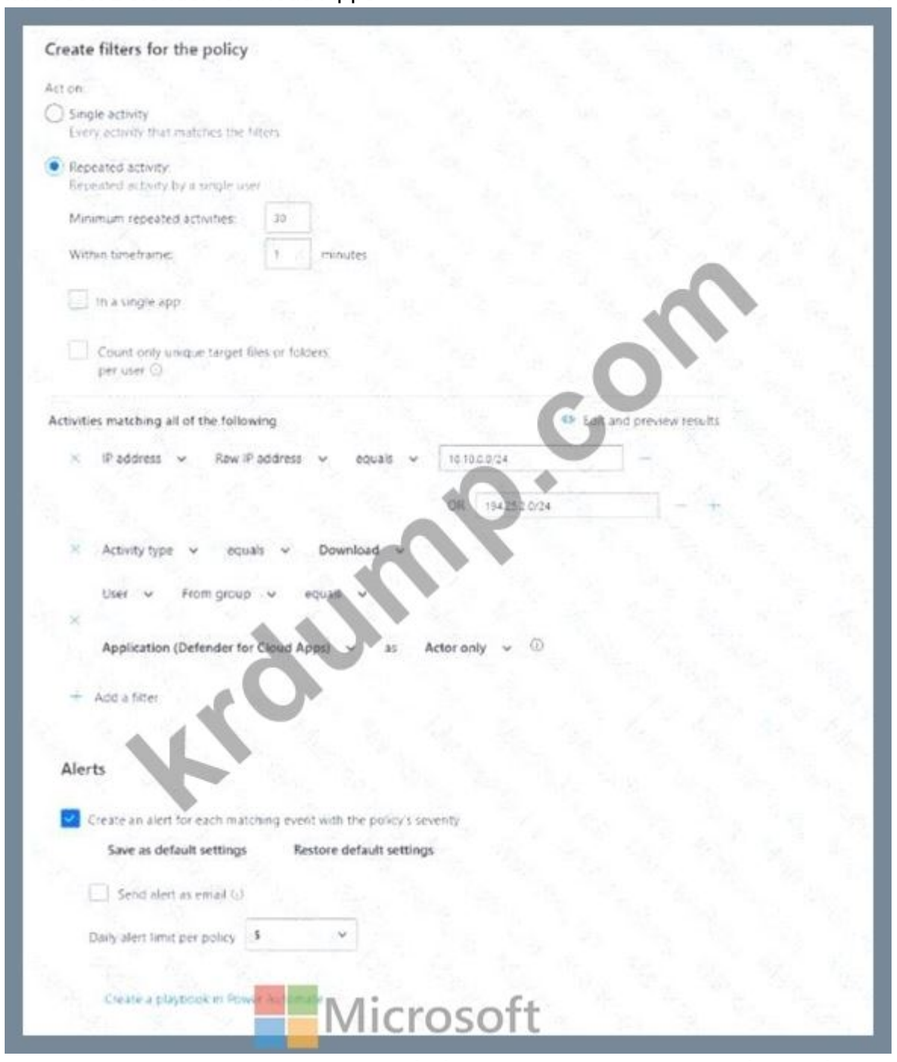
NEW QUESTION: 18
□□□ □□□□, □□□, □□□□ □□□□ □□ □□□□.
□□□ □□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Name	Email address
User1	user1@contoso.com
User2	user2@contoso.com

The offices have the IP addresses shown in the following table.

Office	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

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



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

Answer:

Explanation:

Statement

Answer

At the Montreal office, if User1 downloads 40 files in 45 seconds, an alert will be created.

No

At the Seattle office, if User2 downloads one file per second for two minutes, an alert will be created.

Yes

At the New York City office, if User1 downloads 40 files in 10 seconds, an alert will be created.

No

The policy is a Microsoft Defender for Cloud Apps activity policy configured for Repeated activity by a single user. The threshold is 30 repeated activities within 1 minute, and the activity type is Download.

Microsoft documents that activity policies can be configured for repeated activity, including a minimum activity count and a timeframe, and that activity type filters are used to match app activities such as downloads.

The decisive filter is the Raw IP address condition: 10.10.0.0/24 OR 194.25.2.0/24. Defender for Cloud Apps supports filtering by raw IP address, meaning activities performed from or by those raw IP addresses. For cloud activity, the relevant source address is the externally visible address reported by the cloud app.

Microsoft warns that internal IP addresses audited by connected cloud apps should not be confused with the internal source-network IPs of user devices, because cloud applications are not exposed to those device internal IPs.

Montreal does not match because its public NAT segment is 190.15.1.0/24, not 10.10.0.0/24 or 194.25.2.0/24.

Seattle does match because its public NAT segment is 194.25.2.0/24, and one download per second for two minutes exceeds 30 downloads in one minute. New York does not match because its public NAT segment is 198.35.3.0/24.

NEW QUESTION: 19

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

□□ □□□ □□□ □□□ □□□□□□ "Contoso"□□ □□□ □□□□□□ □ □□□.

□□ □□□ □□□□ □□ □□□ □□ □□□?

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

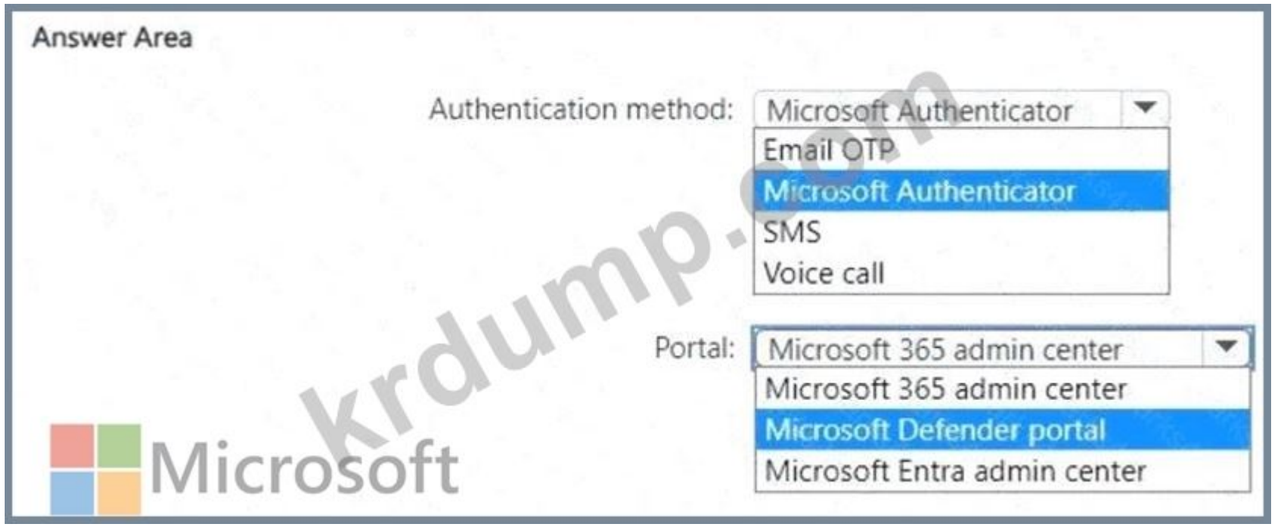
B. Microsoft Entra □□ □□□□ □□ □□ □□□ □□□□□.

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
Microsoft 365 E5 □□□ □□□□.
□□ □□□□ □□ □□□□ □□ □□□ □□□□□ □□□.
□□ □□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:

NEW QUESTION: 21
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: 22
Label1□ Label2□□ □ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □ □□□□ Microsoft Purview□ □□□□ Device1□□□ Windows □□□ □□□□ □□□□. Device1□□ □□ □□ □□ □□ □□□ □□□□ □□□□.

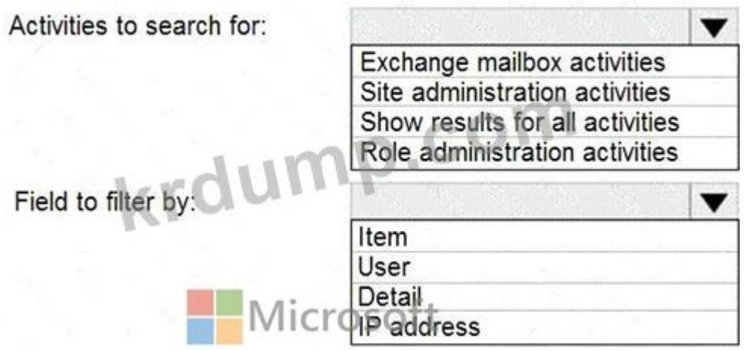
Name	Location	Sensitivity label
File1.docx	C:\Temp\	Label1
File2.docx	C:\Temp\Folder1\	Label2
File3.docx	C:\Temp\Folder2\	Label1

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

Answer:

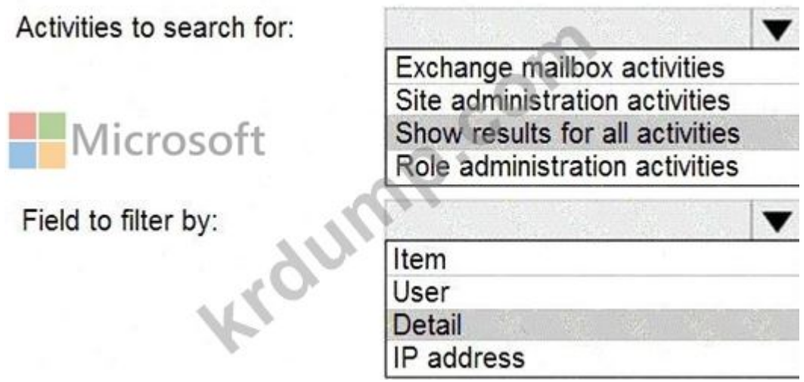
Explanation:

NEW QUESTION: 23
Microsoft 365 □□□ □□□□.
□□□ □□□□□ 51.40.15.0/24□ IP □□ □□□ □□□□□.
Exchange Online □□□□ □□ □□□□□ □□□□□ Role1□□□ □□□ □□□□□□.
□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□.
□□ □□□ □□□□ □□ □□ □□□ □□ □□ □□□ □□□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



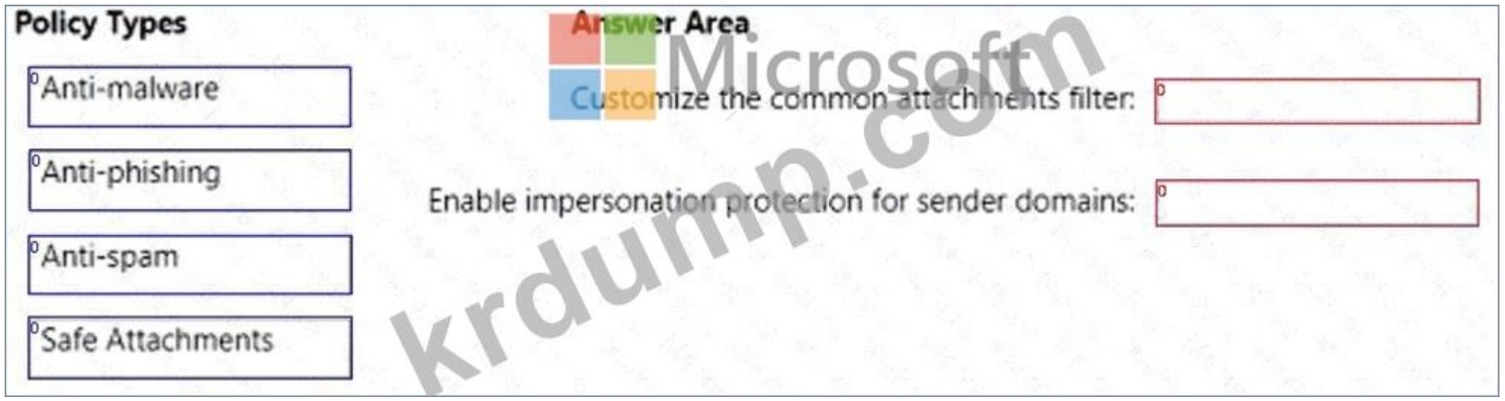
Answer:

Explanation:



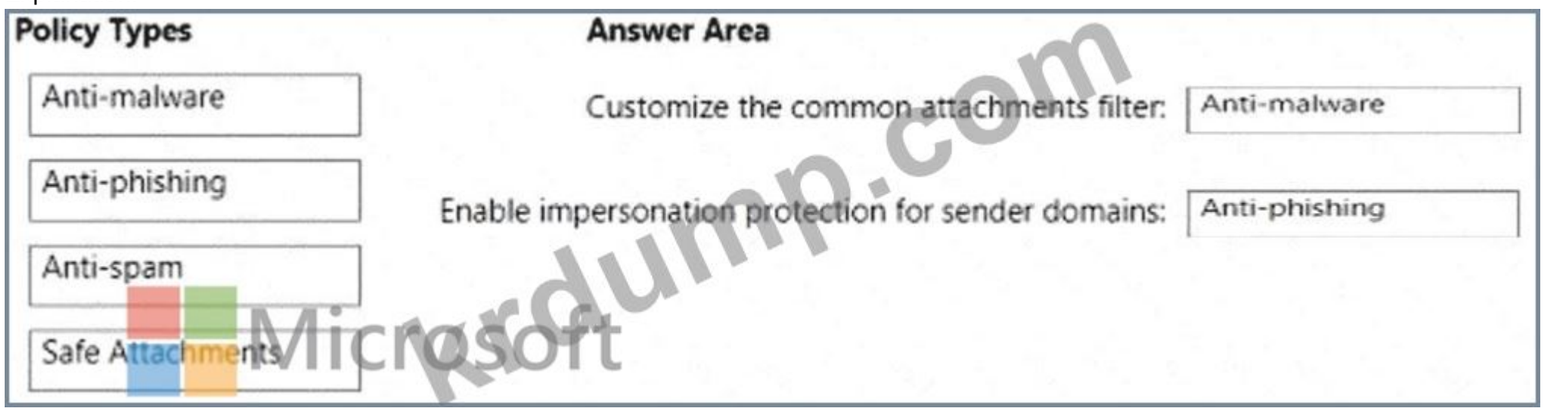
NEW QUESTION: 24
Microsoft 365 E5 □□□□ □□□□.
□□□□ □□□ □□□ □□□ □□□□□ □□□ □ □□ □□□ □□□□□□ □□□□ □□□.
□□ □□□ □□□□ □□□?
A. □□ □□
B. □□ □□ □□
C. □□ □□□ □□
D. □□□ □□ □□
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

NEW QUESTION: 25
Office 365□ Microsoft Defender□ □□□□ Microsoft 365 □□□ □□□□.
□□ □□ □□□ □□□□□ □□□ □□□□ □□□.
□□□□ □□ □□ □□□ □□□ □□□□□.
□□□ □□□□ □□ □□ □□□ □□□□□□.
□ □□ □□□ □□ □□ □□□ □□□ □□□□ □□□? □□□□ □□□ □□ □□□ □□□ □□ □□□□ □□□ □□□□□. □ □□ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □ □□ □□□ □□□ □□□□□ □□□□ □ □ □□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Explanation:



Box 1: Anti-malware

Customize the common attachments filter.

See step 5 below.

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

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

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

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

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

NEW QUESTION: 26
□□□ contoso.com□□□ □□□ Microsoft Entra □□□□ □□□□ □□□, □□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

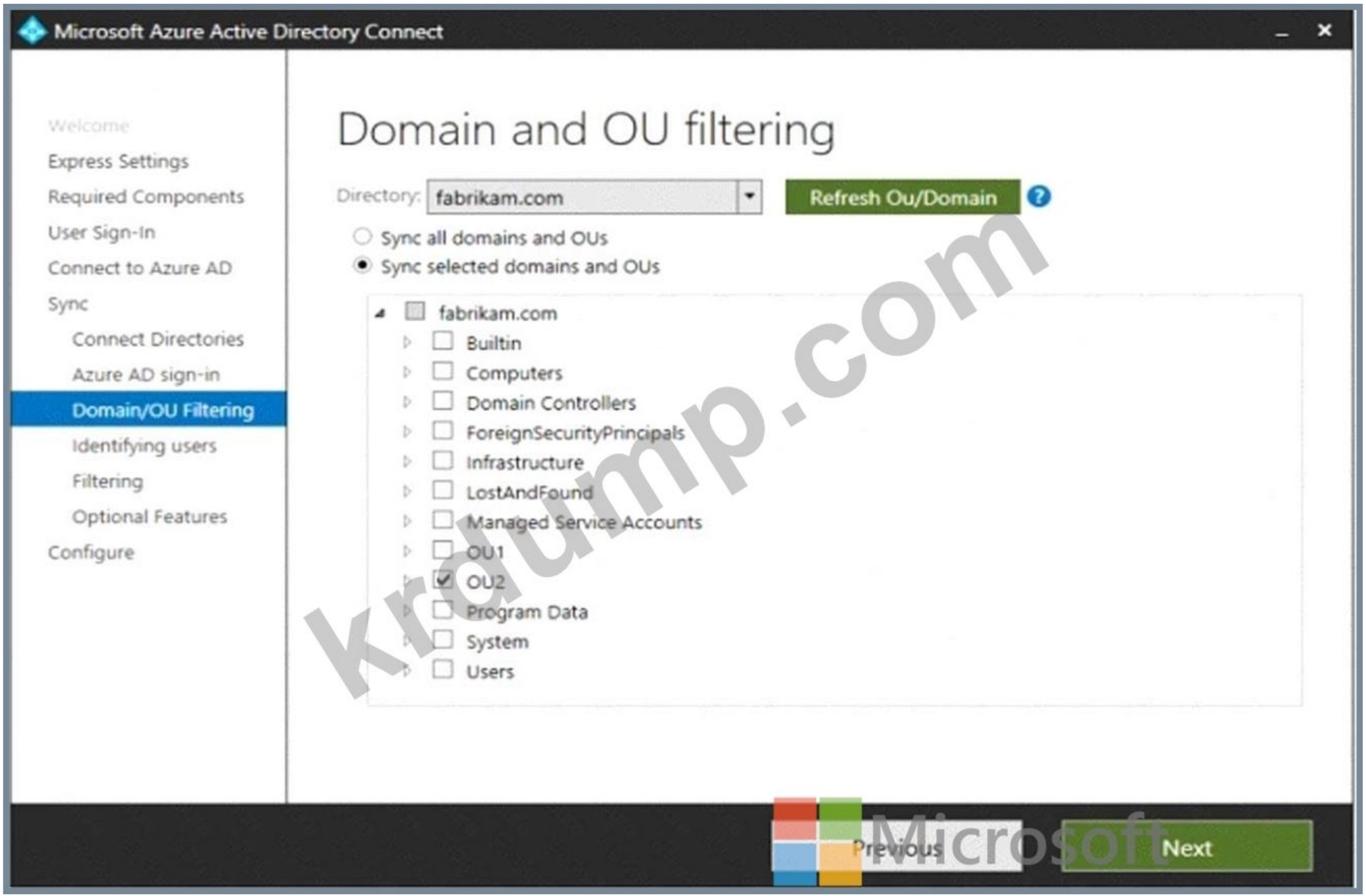
NEW QUESTION: 27
□□□
□□□□□□ fabrikam.com□□□ Active Directory □□□□ □□□□. □ □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

□ □□□ □□□□ □□ □□ □□ □□□□.

Group	Members
Group1	User1
Group2	User2, User3, Group1

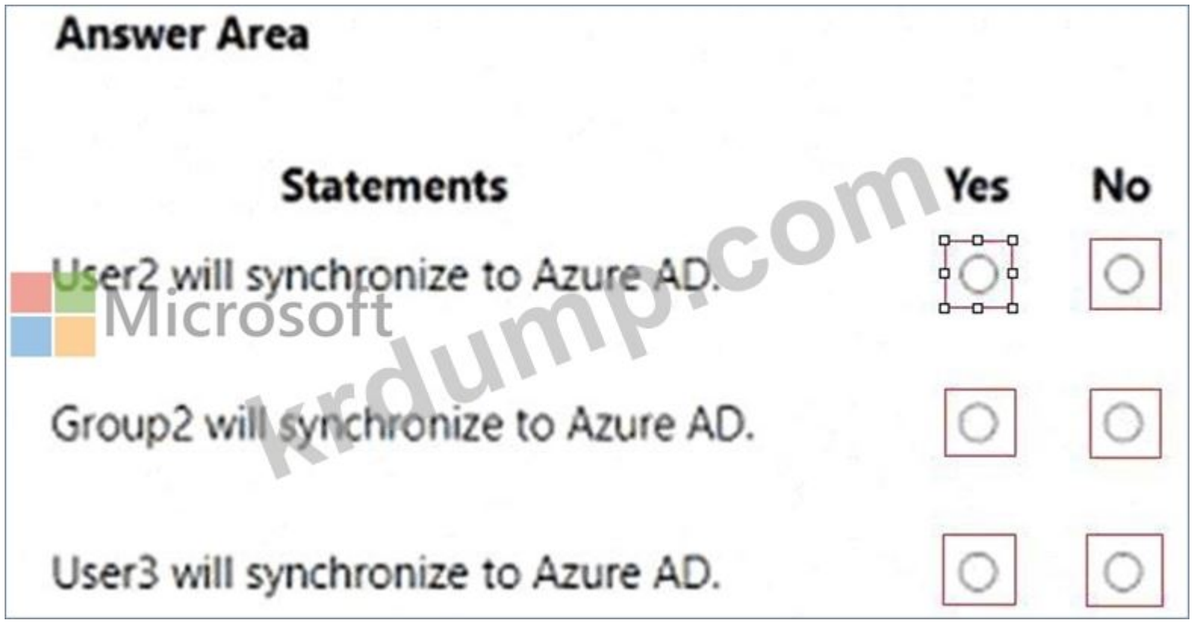
fabrikam.com□ Microsoft Entra □□□ □□ □□□□ □□□□ □□□□.
Microsoft Entra Connect Sync□□ □□□/OU □□□ □□□ □□□□ □□□ □□□ □□□□ □□□ □ □□□□.
/OU □□□ □□ (□□□/OU □□□ □□ □□□□□.)



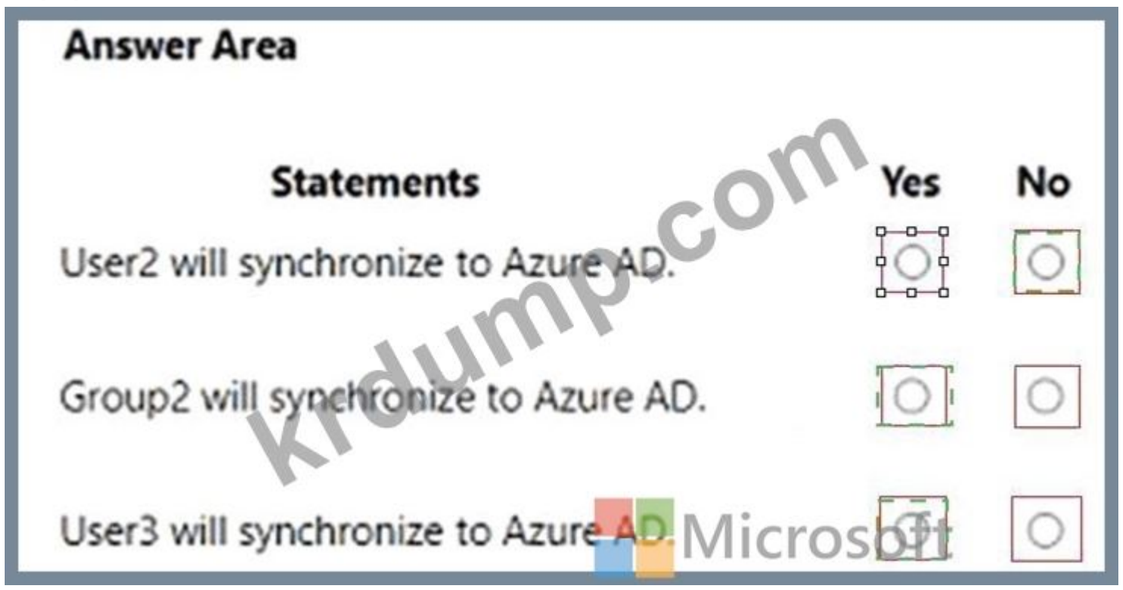
Microsoft Entra Connect Sync□□ □□□ □□□ □□□□ □□□ □□□ □□□ □□□□□□. (□□□ □□ □□□□□□.)


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

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



Answer:



Explanation:

Box 1: No

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

User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Microsoft Entra ID.

Box 2: Yes

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

Box 3: Yes

User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Microsoft Entra ID.

Reference:

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

NEW QUESTION: 28

□□ Microsoft 365 E5 □□□□ Label1□ Label2□□ □□□ □□□ □□□□ □ □ □□□□.

□□□□ Microsoft Purview□ □□□ Device1□□□ Windows □□□ □□□□ □□□□. Device1□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name

Location

Sensitivity label

File1.docx

C:\Temp\

Label1

File2.docx

C:\Temp\Folder1\

Label2

File3.docx

C:\Temp\Folder2\

Label1

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

* □□: □□: □□ □□□ □ □□

* □□: □□□□ □□□ □□ Label1□ □□□□ □□□□.

* □□: □□□□□ □□□ □□□□□ □□□□□.
* □□: □□
□□□ □□ □□ □□□□ C:\Temp\ □□□ □□ □□ □□ □□□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

Answer:

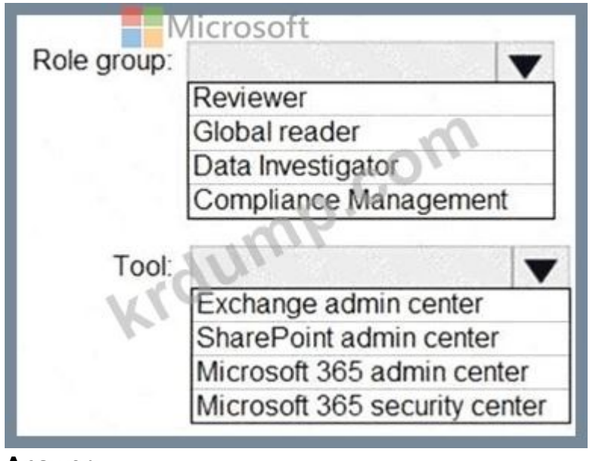
Explanation:
A user on Device1 can print File1.docx.
Yes
A user on Device1 can print File2.docx.
Yes
A user on Device1 can print File3.docx.
No
The DLP rule blocks printing only when the file is subject to Endpoint DLP enforcement and the content matches the configured condition: sensitivity label Label1. Microsoft Purview Endpoint DLP can enforce protective actions on onboarded devices, and Microsoft lists Print as an auditable and restrictable endpoint activity for protected files.
The path exclusion is the deciding detail. Microsoft states that file path exclusions turn off DLP monitoring, alerts, and policy enforcement for files in excluded locations. For Windows file path syntax, a path ending with a backslash, such as C:\Temp\, excludes only files directly under that specified folder. A path ending with * excludes files within subfolders, while a path without trailing \ or * excludes both the folder and all subfolders.
Therefore, File1.docx can be printed because it has Label1 but is directly under C:\Temp\, so DLP enforcement does not apply. File2.docx can be printed because it is in a subfolder and not excluded, but it has Label2, so it does not match the Label1 blocking condition. File3.docx cannot be printed because it is in a subfolder, is not excluded by C:\Temp\, and has Label1, so the print action is blocked.

NEW QUESTION: 29
□□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft 365 □□□ □□□□.
□□□□ □□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□□□□ Active Directory □□ □□□ □□□ □□□□ □□□.
* □□□□ Microsoft Entra Self-Service Password Reset(SSPR)□ □□□ □ □□□ □□□.
□□□ □□□□ □□□?
A. □□□□ □□ □□□
B. □□□□ □□
C. Microsoft Entra ID □□

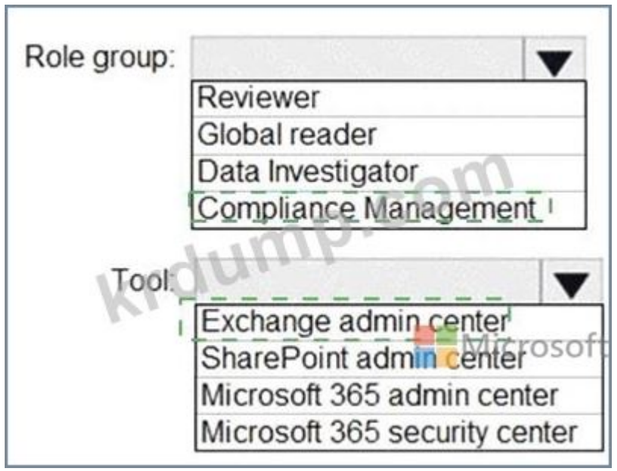
D. Microsoft Entra Seamless Single Sign-On(Microsoft Entra Seamless SSO)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
□□□□ □□ Microsoft Defender□ □□□□ Microsoft 365 □□□ □□□□.
SharePoint Online □□□□□ □□□□□ □□□□□ □□ □□ □□□ □□□□□.
□□□□□ □□□ SharePoint Online □□□□□ □□□ □□□□□ □ □□□ □□□□□.
□□□□ SharePoint Online □□□□ □□□□ □□□□ □□ □□□□□ □□□□□ □□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□□ □□□ □□
C. □□□ □□ □□(DLP) □□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 31
User2□ □□ □□□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
User2□ □□ □□ □□□ □□□□ □□, □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

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

Topic 4, FabrikamOverview

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment

Active Directory Environment

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

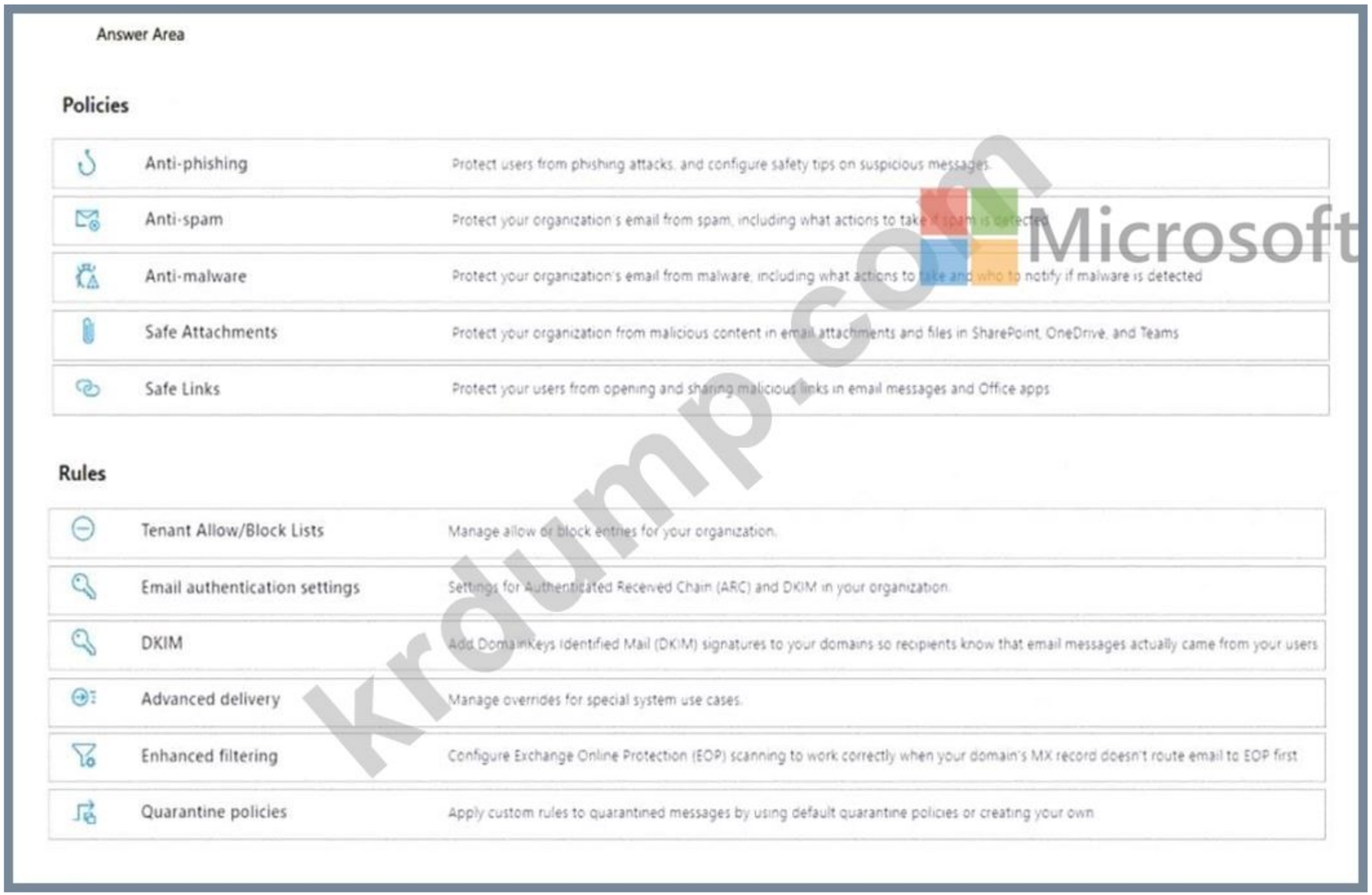
Fabrikam does NOT plan to implement identity federation.

Network Infrastructure

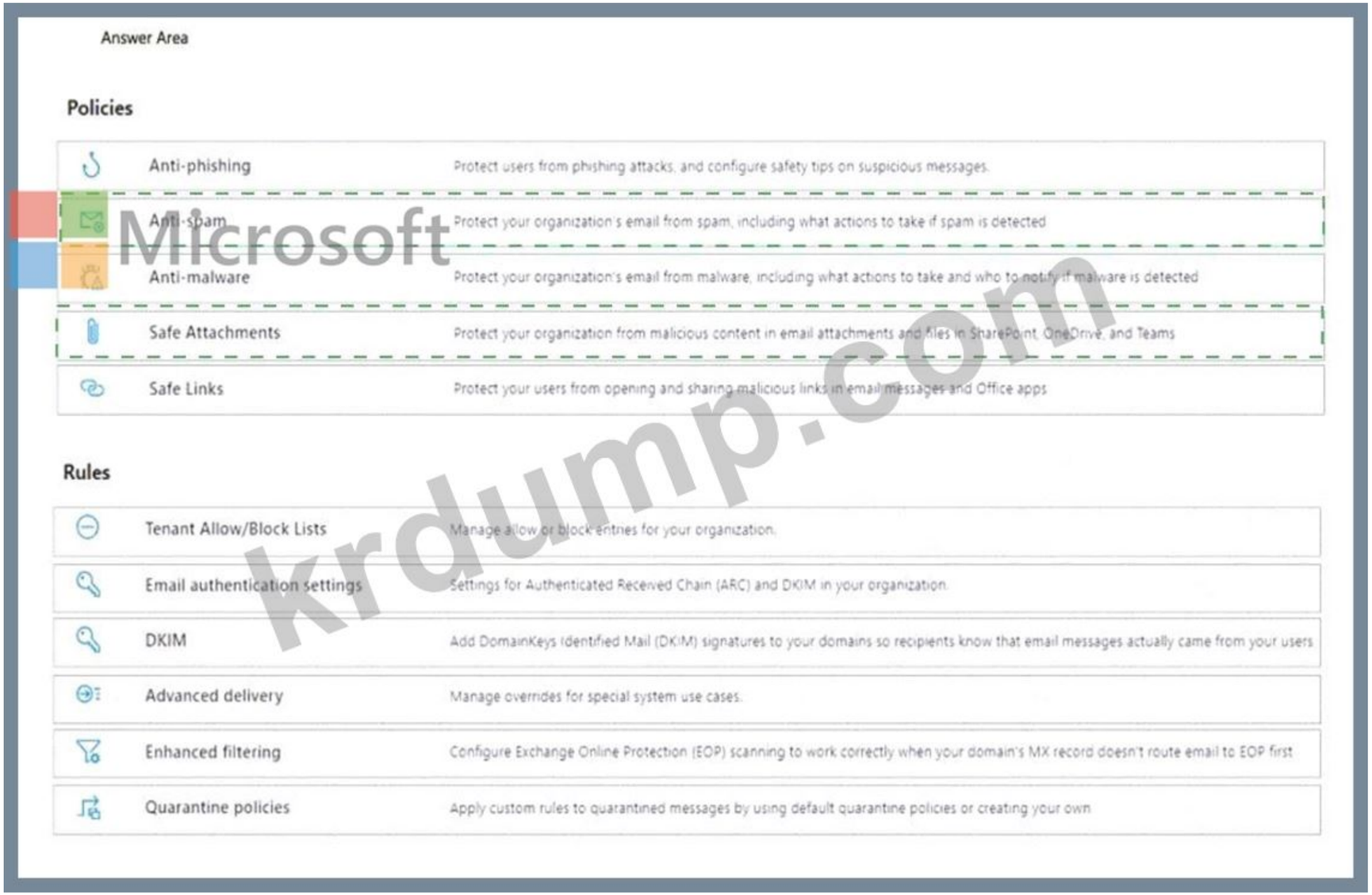
Each office has a high-speed connection to the Internet.
Each office contains two domain controllers. All domain controllers are configured as DNS servers.
The public zone for fabrikam.com is managed by an external DNS server.
All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.
All shared company documents are stored on a Microsoft SharePoint Server farm.
Requirements
Planned Changes
Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
Fabrikam plans to implement two pilot projects:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.
Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.
Technical Requirements
Fabrikam identifies the following technical requirements:
All users must be able to exchange email messages successfully during Project1 by using their current email address.
Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.
Application Requirements
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online.
App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.
Security Requirements
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

NEW QUESTION: 32
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□□ Microsoft 365□ □□ □□ □□□ □□□□ □□□.
* User 1□□□ □□□□ □□□ 30□□ □□ □□□ □□□□ □□□ □□□□ □□□□□.

* □□ □□□ □□□□ □□ □□□ □□□ □□□□□.
Microsoft Defender for Office 365□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Limit a user named User 1 from sending more than 30 email messages per day: Anti-spam policy The anti-spam policy in Microsoft Defender for Office 365 allows you to configure outbound spam settings, including limiting the number of email messages a user can send per day. This helps prevent spam and potential email abuse within the organization.

Prevent the delivery of a specific file based on the file hash: Safe Attachments policy The Safe Attachments policy in Microsoft Defender for Office 365 can be configured to block or quarantine emails with attachments that match specific file hashes. This ensures that potentially malicious files are not delivered to users' inboxes.

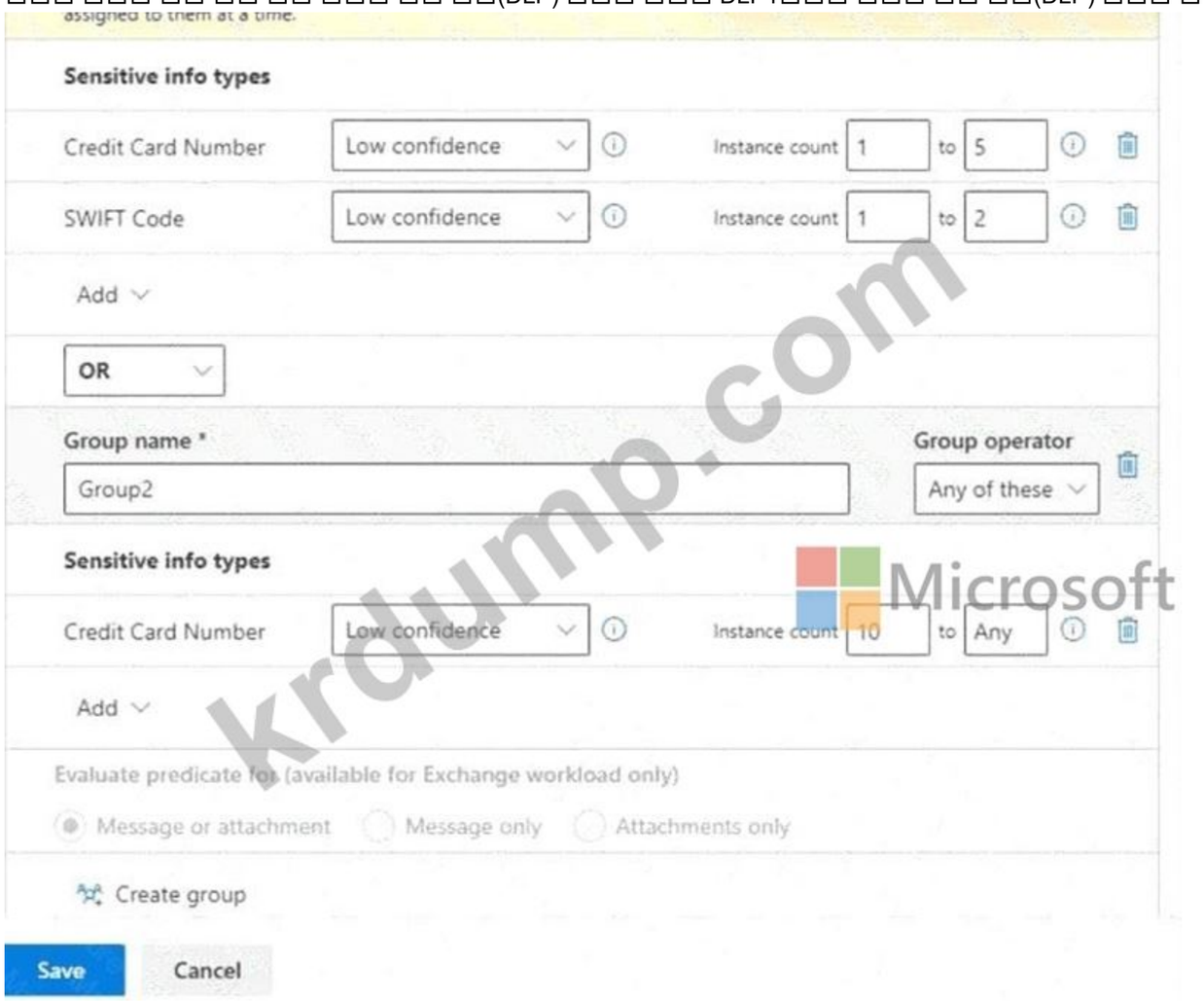
NEW QUESTION: 33

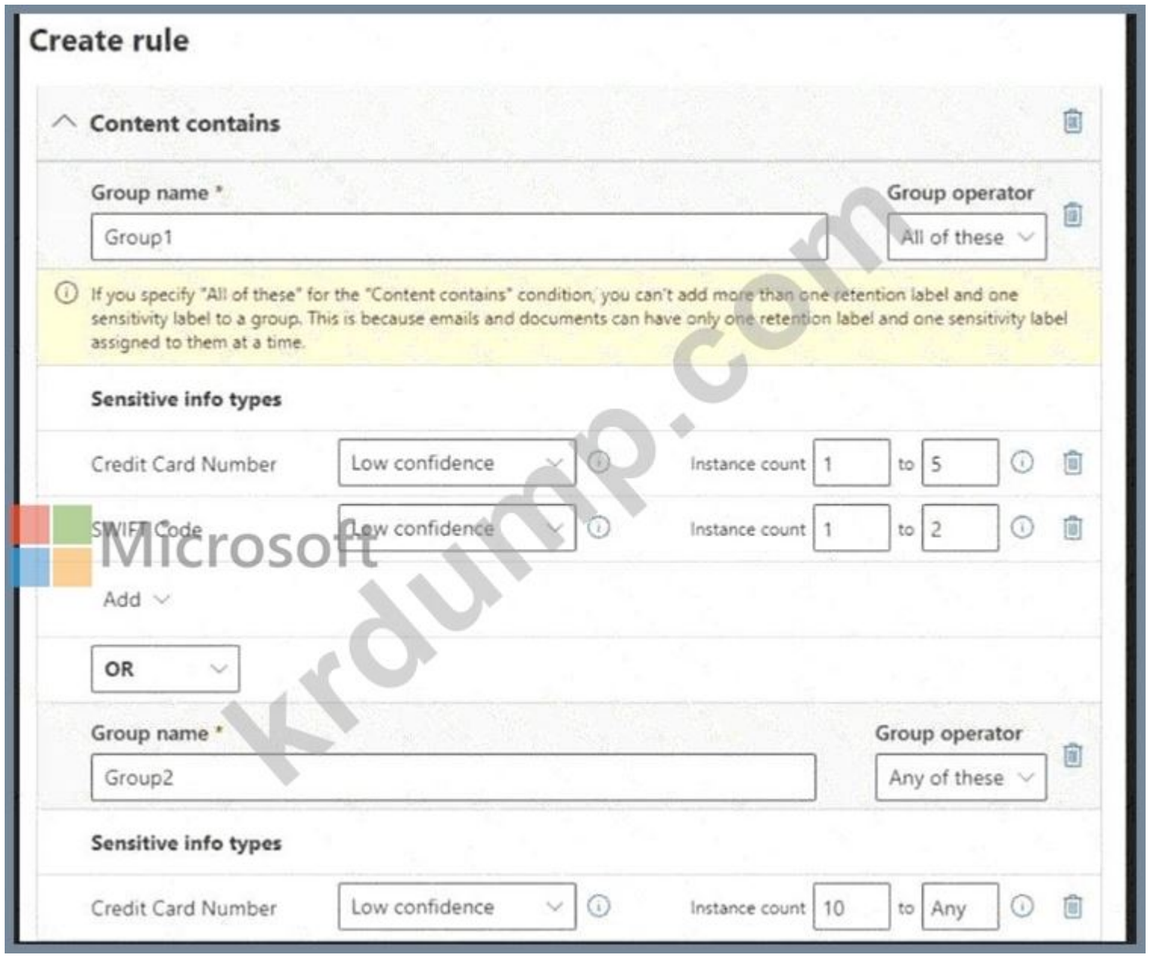
□□□ Site1□ Site2□□ □□□ Microsoft SharePoint Online □□□ □ □□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

□□□ □□ □□ □□ □□ □□□□ □□□ □□□□.

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

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




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: 34

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

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

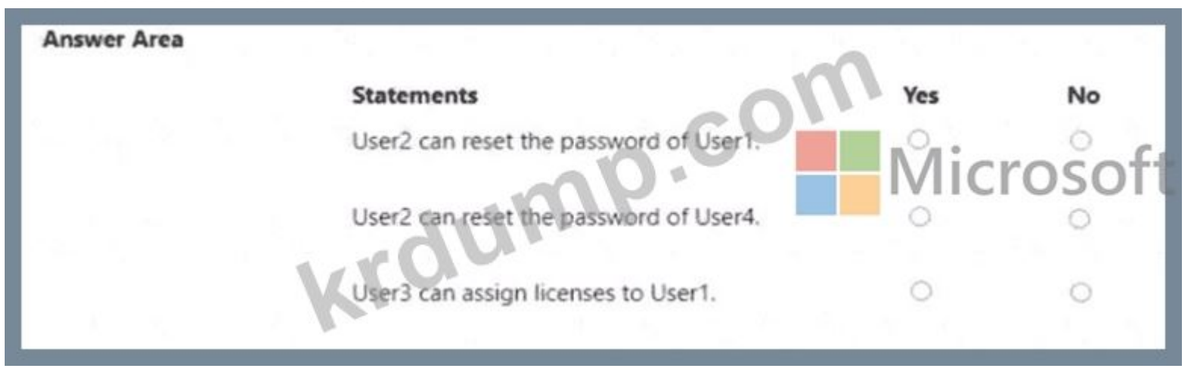
□□□□ □□ □□ □□□ □□□□ □□□□□.

Name	Members
Group1	User1
Group2	User2, User4

□□□□□□ □□ □□ □□□ □□□ □□□□□.

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

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



Answer:

Explanation:

NEW QUESTION: 35
Microsoft □ SharePoint Online□ □□ □□□ □□□ □□□ □□□□ Microsoft 365 E5 □□□□ □□□□.
Microsoft 365 □□□ □□ □□ □□□ □□□ □□□□□ □□□.
□□ cmdlet□ □□□□ □□□?
A. □□□□ □□
B. □□□□□□ □□
C. Execute-AzureAdLebelSync
D. □□□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 36
□□□ Microsoft 365 □□□ □□□□ □□□□.
□□ □□□ □□ Microsoft □□ □□□ 60□□□, □□ □□□ □□□ 75□□□□.
□□□ □ □□ □□□□ □□□□ □□□□□ □□□ □□(MFA)□ □□□□ □□□ □□□ □□□ □□□□ □□□.
□ □□□ □□□ □□ □□□ □□□□?
A. □□ □□□ □□□□ □□ □□ □□□ □□□□□.
B. □□ □□□ □□ □□ □□□ □□□□□.
C. □□ □□□ □□ □□ □□□ □□□□ □□□□.
D. □□ □□□ □□□□ □□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The correct exam selection is D. The Secure Score will increase, and the achievable score will decrease.
Microsoft Secure Score measures security posture, and Microsoft states that a higher score indicates that more recommended security actions have been taken. Microsoft also states that points are awarded for configuring recommended security features, and Conditional Access/MFA-related controls are part of the Microsoft 365 security posture model.
When you implement a Conditional Access policy requiring MFA from untrusted devices, you are applying a control that strengthens identity protection. That increases the current Secure Score because the tenant has completed or partially completed a recommended security action. The "achievable score" represents the remaining score opportunity available from your current licenses and risk posture. After you complete an improvement action, the remaining achievable gap is reduced, so the achievable score decreases in the exam's scoring logic. Microsoft's Secure Score documentation confirms that completed actions grant points and that Secure Score views include current score, current license score, planned score, and achievable score.

NEW QUESTION: 37
Site!□□□ 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: 38
□□□ □□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

NEW QUESTION: 39
Microsoft Entra ID □□□□ □□□ 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: 40
Microsoft 365 □□□□ □□□□.
Microsoft Defender XDR□ □□□□ □□□□□ □□□□ □□□□□ □□□ □□□□□. Microsoft Defender □□□ □□□□ □□□□ □□ Microsoft □□□ □□□ □□□□□?
A. Azure □ □□□□□□ □□□
B. □□□ □□
C. Microsoft Defender for Cloud
D. Microsoft Defender for Identity
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
Microsoft Intune □ Microsoft Purview□ □□□□ Microsoft 365 E5 □□□ □□□□. □ □□□□ Microsoft Defender for Endpoint□ □□□ □□□ □□□□ □□□□.
□□□ □ □□ □□□□□ □□□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□□ □□□. □ □□□ □□ □□□ □□□□□ □□□.
□□ Microsoft Purview □□□□ □□□□ □□□?
A. AI□ □□□ □□ □□ □□(DSPM for AI)
B. □□□□□□ □□ □□
C. □□□ □□ □□
D. □□ □□
Answer: C (LEAVE A REPLY)
The correct answer is Data Loss Prevention because the requirement is to stop sensitive data from being pasted into untrusted websites from managed endpoint devices. Microsoft Purview Endpoint DLP extends DLP monitoring and enforcement to Windows and macOS devices and can enforce protective actions on sensitive items when users attempt risky activities. Microsoft states that Endpoint DLP makes endpoint activity visible in Activity Explorer and allows administrators to enforce protective actions through DLP policies.
Microsoft also provides a specific Endpoint DLP scenario to restrict users from pasting sensitive content into browser-based applications . That scenario evaluates content at the moment it is pasted and controls sensitive information in real time, regardless of the source. The endpoint DLP settings include browser and domain restrictions for sensitive data, including controls that help prevent leakage by restricting paste actions into browsers.
DSPM for AI can surface AI-related data security insights and recommendations, but it is not the direct enforcement solution for blocking paste actions to untrusted websites. Communication Compliance reviews risky communications, and Information Barriers restrict collaboration between groups. Neither is designed to enforce endpoint copy/paste protection. References/topics: Microsoft Purview Data Loss Prevention, Endpoint DLP, browser and domain restrictions, sensitive content paste protection.

NEW QUESTION: 42
Azure □□□ Microsoft 365 E5 □□□ □□□□.
Microsoft Defender XDR□ □□□ □ □□ □□□□□ □□□□.
Azure□□ □□□□□ IP □□□ □□□ □□□□□ □□ □□□ □□□□□□ □□□.
□□□ □□□□□□ □ □□□ □□□□ □□, Azure□ Microsoft Defender XDR□ □□□□ □ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 43

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

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

□□□ □□□□□□ □□□□□ 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: A (LEAVE A REPLY)

NEW QUESTION: 44

□□□ □□ □□□ □□□□□ DLP □□□ □□□□ □□□.

□□ □□□ □□□□ □□□?

A. □□□ □□ □□

B. Insider □□ □□ □□

C. □□□ □□

D. □□□ □□□

Answer: A (LEAVE A REPLY)

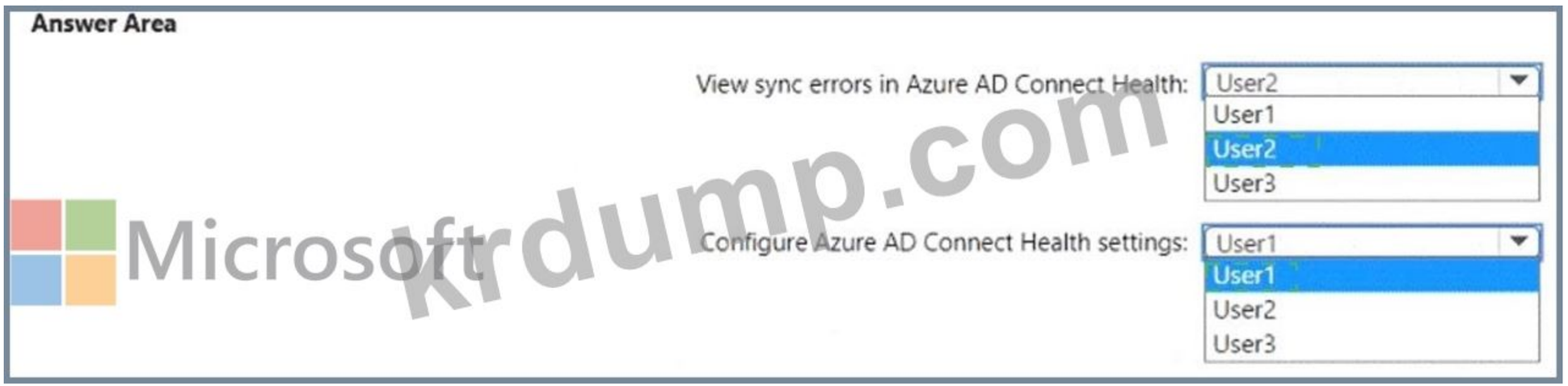
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

NEW QUESTION: 45
□□□ □□ □□ □□□ □□□□ □□□□ Microsoft Entra ID□ □□□□□ □□ □□□ □□□□ □□□□.

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

□□ □□□ □□□ □ □□ □□□□ □□□□ □□□.
* Microsoft Entra Connect Health□□ □□□ □□□ □□□□□.
* Microsoft Entra Connect □□ □□□ □□□□□.
□ □□□ □□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer:



Explanation:

Answer Area

View sync errors in Azure AD Connect Health: User2

Configure Azure AD Connect Health settings: User1

Microsoft

NEW QUESTION: 46
Microsoft Entra ID Protection □□ □□ □□□□ □□□□□□.
□□ □□ □□□ □□□□ □□□□□.

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

□□ □□□□□ □□ □□ □□□□ □□□□ □□ □□□?
A. □□□2, □□□3, □□□4□ □□
B. □□□1, □□□2, □□□3, □□□4
C. □□□2 □ □□□3□ □□
D. □□□ 3 □□
E. □□□1 □ □□□3□ □□
Answer: E (LEAVE A REPLY)
By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or Security Administrators will automatically be added to the recipients list.

NEW QUESTION: 47
Microsoft 365 E5 □□□□ □□□□.
□□ □□□ □□ □□□□ ISO 27001 □□□ □□□□ □□□.
□□□□ □□□ □□ □□□□ □□□.
A. □□ □□ □□□□□ □□□ □□□□□.

B. Microsoft 365 □□ □□□□ □□□ □□□ □□□□□□.
C. Microsoft J6i □□ □□ □□□□ □□ □□ □□□ □□□□.
D. Azure Portal□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

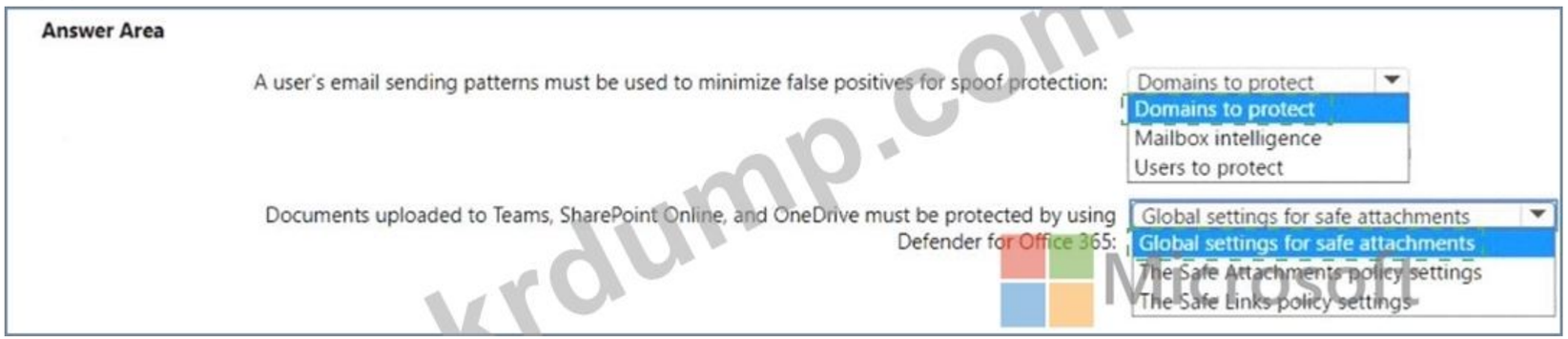
NEW QUESTION: 48
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□□ Office 365□ Microsoft Defender□ □□□□ □□□.
* □□□□ □□□ □□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□□ □□□.
* Microsoft Teams, SharePoint Online □ OneDrive□ □□□□ □□□ Defender for Office 365□ □□□□ □□□□ □□□.
□ □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□□□ □□□ □□□ □□□□□□. □□: □ □□□ □□□ 1□□□□.

Answer Area

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

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365: Global settings for safe attachments
- Global settings for safe attachments
- The Safe Attachments policy settings
- The Safe Links policy settings

Answer:



Explanation:

Answer Area

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

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

NEW QUESTION: 49

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

Platform	Count
Windows 10	50
Android	50
Linux	50

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

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

NEW QUESTION: 50
SharePoint □□□□ □□ □□ □□□ □□□□ □□□. □□□ □□ □□□? □□□□ □□□ □□□ □□□ □□□□□□. □□: □ □□□ 1□□□□.

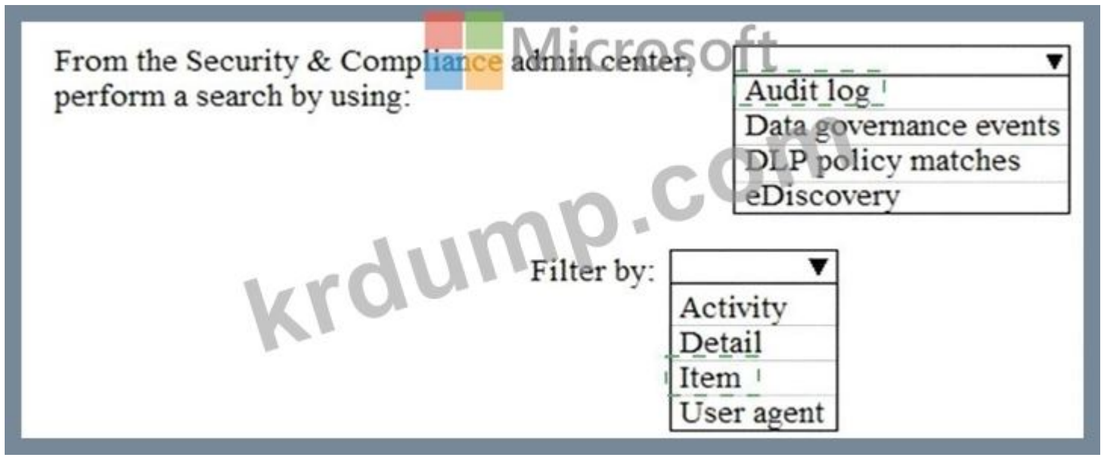
From the Security & Compliance admin center, perform a search by using:

- Audit log
- Data governance events
- DLP policy matches
- eDiscovery

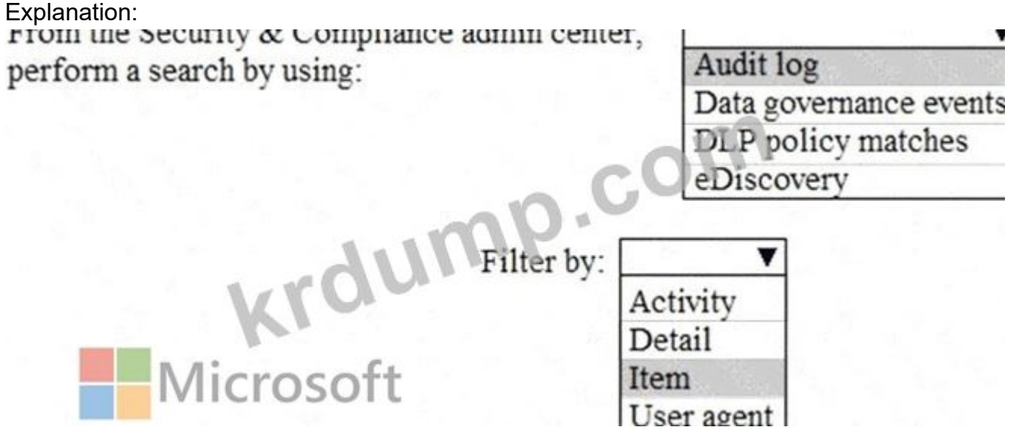
Filter by:

- Activity
- Detail
- Item
- User agent

Answer:



Explanation:



References:

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

NEW QUESTION: 51

□□ □□ □□□ □□□□ □□□ 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□□□□.

Can add apps to the private store:

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

Can assign apps from Microsoft Store for Business:

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

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: 52
Project1□ Project2□□ □□ □□ □□ □□□□ □□□□□ □□□ □ □□□ □□□□ □□□.
□□ □□□□□□ □□ □□ □□□ □□□□ □□□?
A. □□□□ □□
B. □□□□ □□ □ □□□ SSO
C. □□□□ □□ □□□ □ □□□ SSO
D. □□□□ □□ □□□
Answer: C (LEAVE A REPLY)
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
Fabrikam does NOT plan to implement identity federation.

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

NEW QUESTION: 53
□□□ Microsoft 365 Enterprise E5 □□□ □□□□ □□□□.
Microsoft Entra ID □□□□□□ □□□□□□ □□□ App1□□□ □□□□ □□ □□ □□□□□.
App1□ □□□ □□□ □ □□ □□□ □□□ □□ 2□□ □□□ □□□□□ □□ □□□.
□□□□ □□ □ □□ □□□ □□□□ □□□? □□□ □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

New ...

Conditional Access policy

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

Name *

App1 policy

Assignments

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

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

What does this policy apply to?

Users and groups

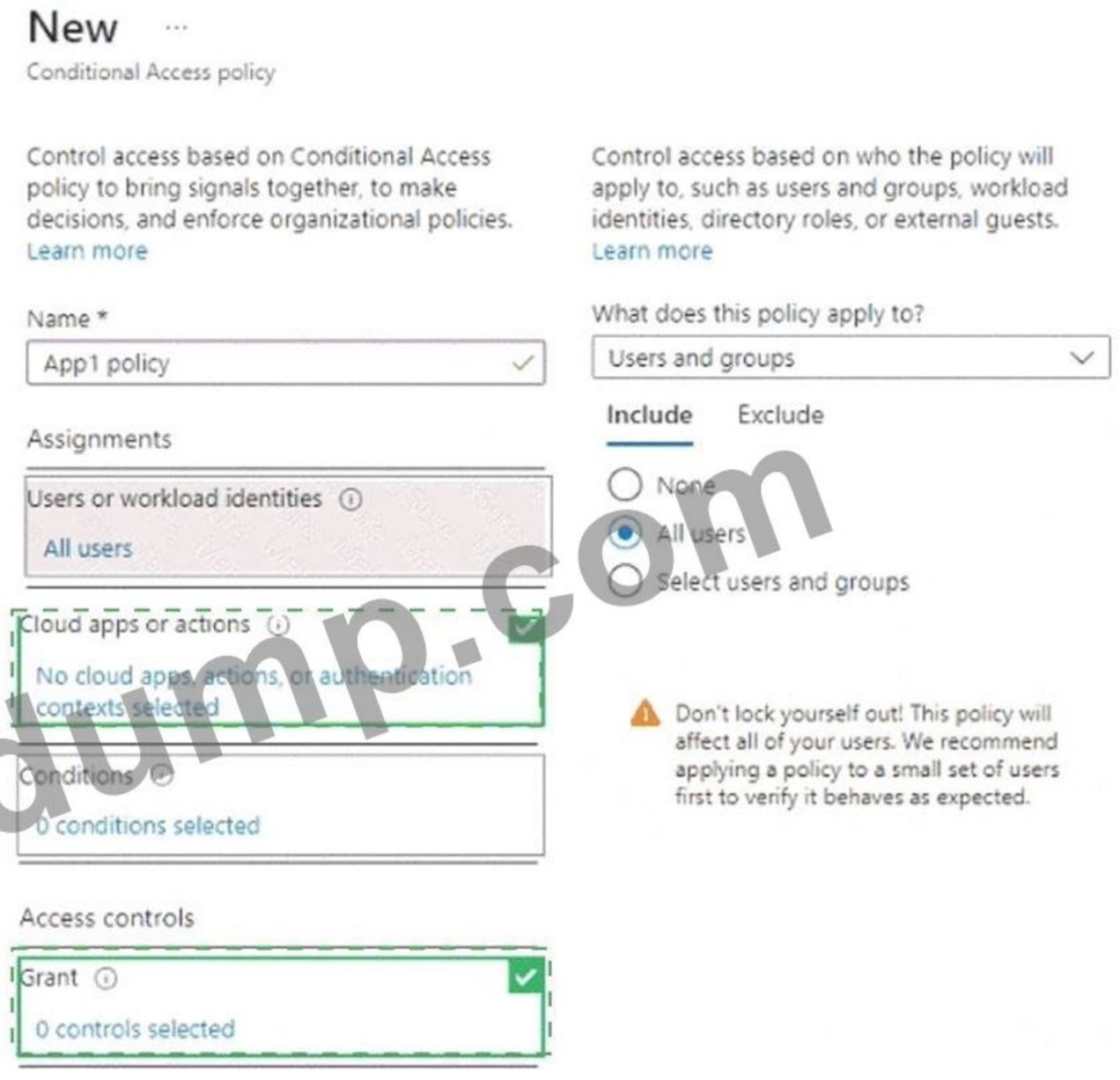
Include Exclude

- None
- All users
- Select users and groups

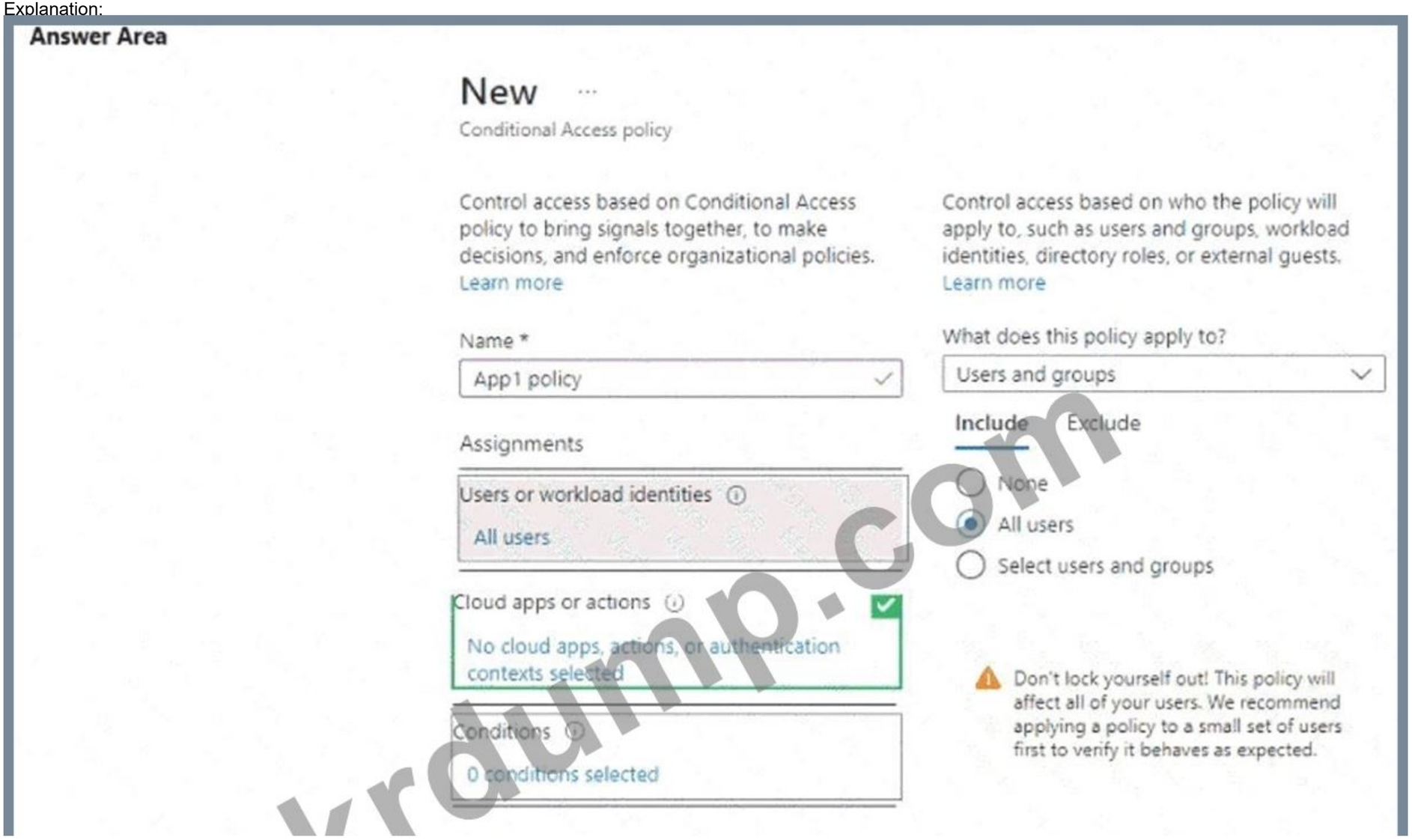
Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

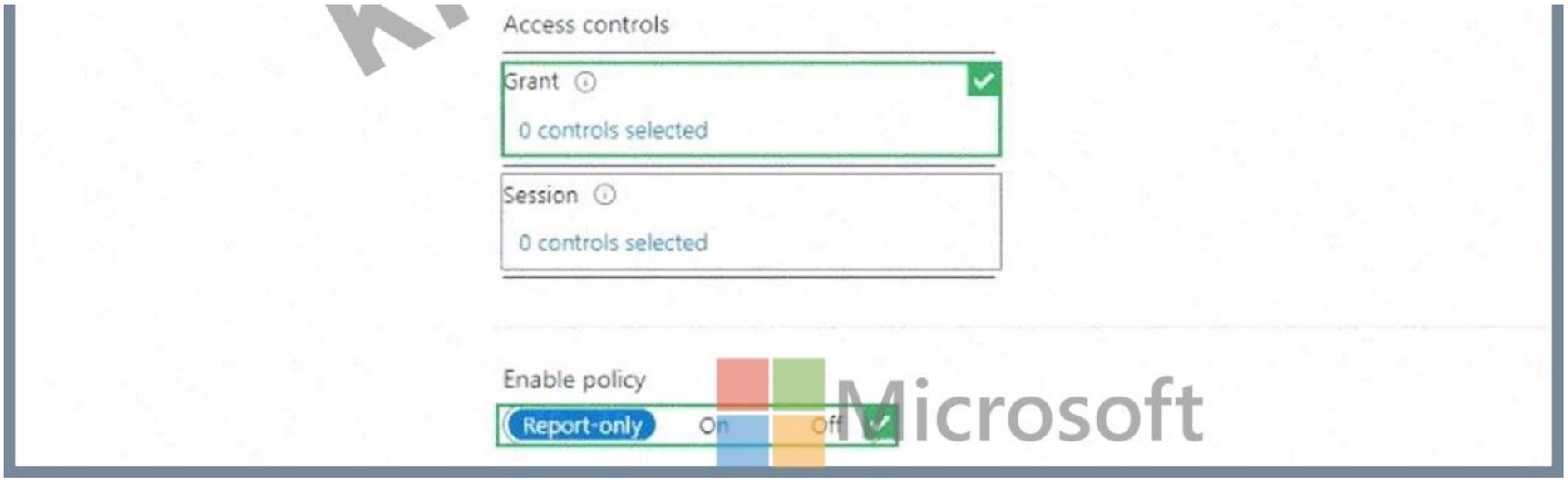
Answer:

Answer Area



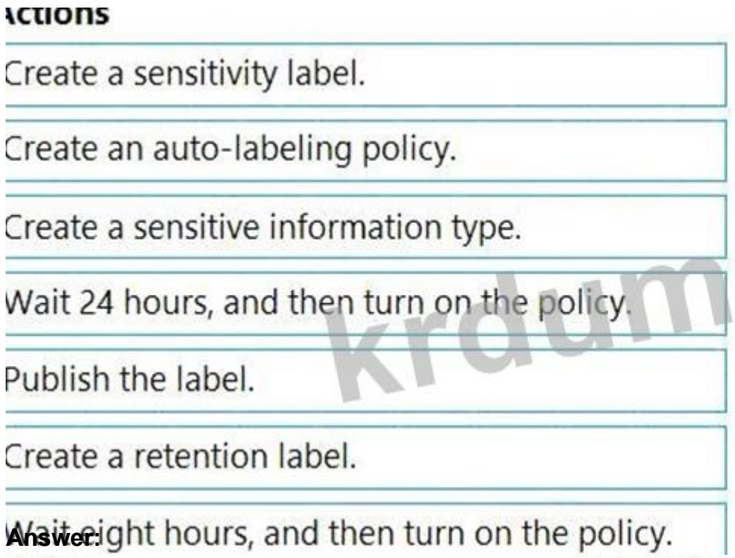
Explanation:



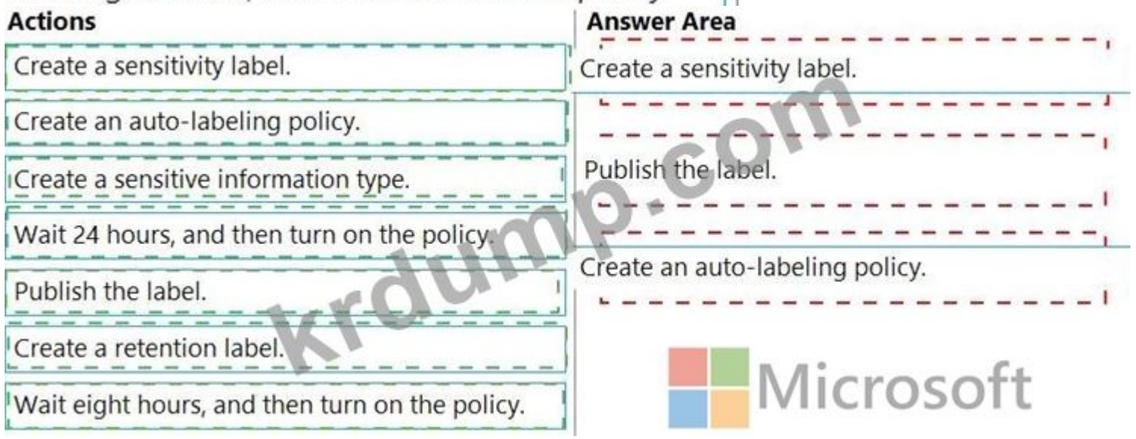


NEW QUESTION: 54
□□□ Microsoft 365 E5 □□□□ □□□□.
Microsoft Exchange Online □□□ □□ □□□ □□□□ □□□□□ □□ □□□ □□□□□ □□□.
□□ □□ □□□ □□ □□□?
A. □□□ □□□□□□.
B. Microsoft 365 □□ □□□ □□□□□□.
C. □□□ □□ □□ □□□ □□□□□.
D. □□□□□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Microsoft Purview auditing solutions provide an 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: 55
Site1□□□ Microsoft SharePoint Online □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Site1□□ □□□□ □□□ □□□ □□□ □□□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□□.



Answer:



Explanation:

Reference:

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

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

NEW QUESTION: 56

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

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

□□□ □□□□ □□□?

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

NEW QUESTION: 57
Microsoft 365 E5 □□□ □□□□. □□□□□ FID02 □□ □□ □□□□□.
FID02 □□ □□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□□ □□□. □□□ □□ □□ □□□ □□ □□□ □□□□ □□□?
A. □□ □□ □□
B. □□□ □□□ □□ □□ □□□ □□□□□.
C. □□□ □□□□□ □□ □□□□□.
D. □□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 58
□□□ □□□□ □□□ □□□□ □□ □□□□.
Microsoft 365 □□□ □□□□.
□□ □□ □□(MFA)□ □□□□ Policy1□□□ □□□ □□□ □□□ □□ □□□□□.
□□□ □□□ □□□□ MFA□□ □□□□ □□□. □□ □□□ □□□□ □□ MFA□ □□□□ □□□.
Policy1□ □□ □□□ □□□□ □□□?
A. IP □□ □□□ □□□ □□□□ □□□ □□□ □□
B. □□ □□□ □□□□ □□□ □□□ □□
C. □□□ □□□□□□ VPN □□
D. □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
□□ □□□ □□ Microsoft Defender XDR □□□ □□□ □□□□.

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

Answer Area

Answer:

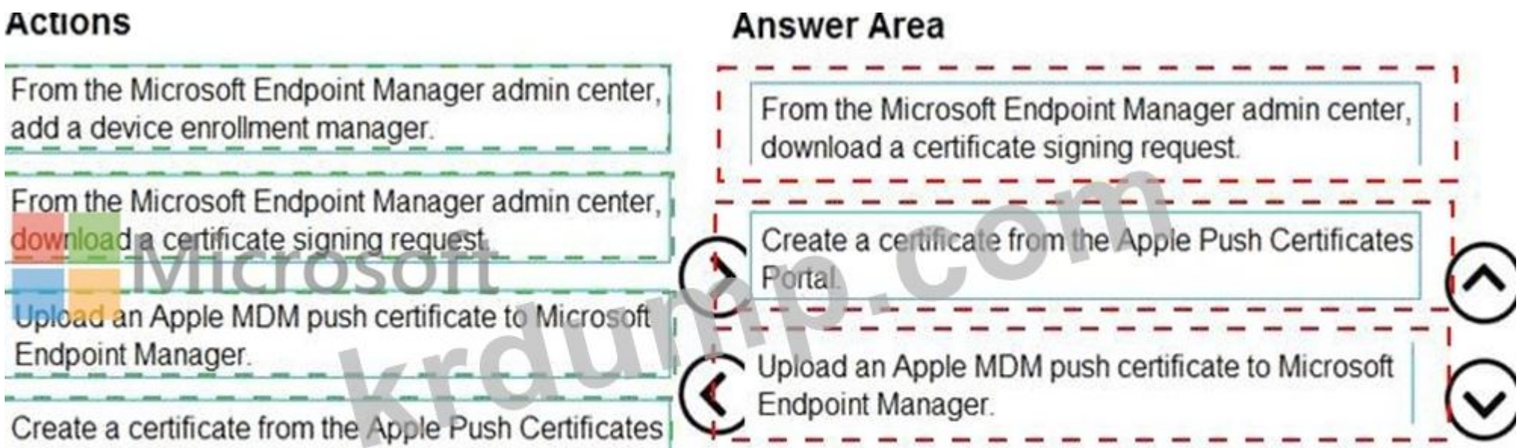
Explanation:

NEW QUESTION: 60
Microsoft 365 □□□ □□□□.
□□ □□□□ Microsoft SharePoint □□□ □□□ □□□□ □□ □□□□□□.

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

NEW QUESTION: 61
Microsoft 365 E5 □□□ □□□□.
□□ □□□□ iOS □□□ □□□□ □□□□.
Microsoft Endpoint Manager□ iOS □□□ □□□□□ □□□.
Microsoft Endpoint Manager□□ iOS/iPadOS □□ □□□□ □□ □ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□□.

Answer:



Explanation:

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Create a certificate from the Apple Push Certificates Portal.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Reference:

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

NEW QUESTION: 62

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

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

Microsoft Defender Vulnerability Management□□ □□ □□ □□ □□□ □□□□ Microsoft Edge(Chromium)□ □□ □□□□ □□□□□□□ □□ □□□ □□□□□□.

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

□□□ □□ □□□?

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

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

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

D. Microsoft Intune □□ □□□□ Windows Autopatch□ □□□□□.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 63

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

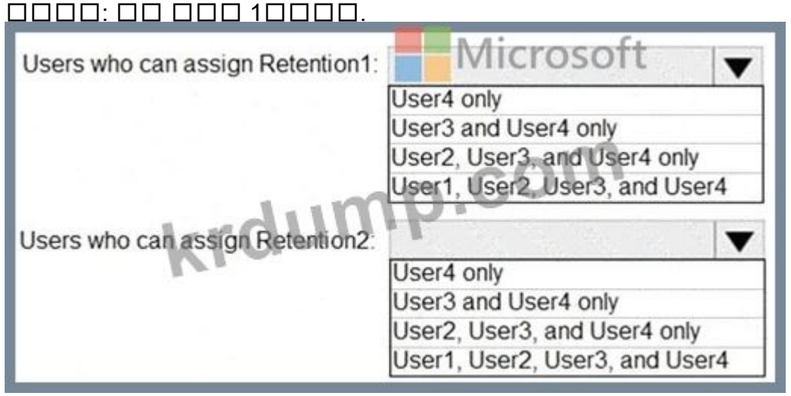
Name	Mailbox size
User1	5 MB
User2	15 MB
User3	25 MB
User4	55 MB

Exchange □□□□ □□□ Retention1□□□ Microsoft Office 365 □□ □□□□ □□□□.

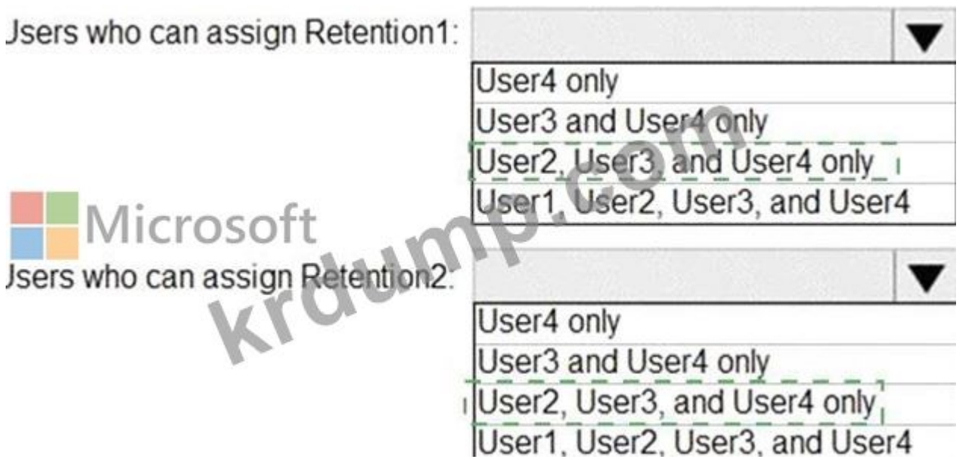
□□ □□□□ □□□□ Microsoft Exchange Online □□ □□□ □□□□. □□ □□□□ Retention2□□ □□ □□□ □□□□ □□□□.

□□ □□□□ Retention1□ Retention2□ □□□□ □□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

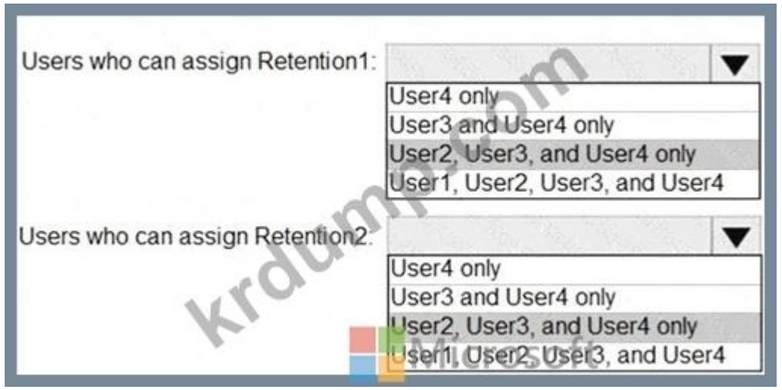
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

NEW QUESTION: 64
□□□
contoso.com□□□ □□□ Microsoft Entra □□□□ □□□, □□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

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

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

□□□ □□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□ □□ □□□□ ID □□: □□ □□□
□□□□ □ □□ □□ □□: App1
□□: □□ □□□ □ □□ □□□ □□□□□
□□ □□ □□: □□□ □□ □□
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Box 1: Yes

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

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

Box 2: Yes.

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

Box 3: No.

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

/24

Reference:

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

NEW QUESTION: 65

Microsoft 365 IS □□□ □□ Microsoft Defender for Cloud Apps□ □□□□□. Microsoft Entra 10□□ App1□□□ □□□□ □□ □□□□□. Appl□ □□ □□□ □□□ □□□□ □□□. □□ □□□ □□ □□□?

A. □□□□ □□ Defender□ □□ □□ □ □□□ □□(SIEM) □□□□□ □□□□□.

B. App1□ □□ □ □□□ □□□□□.

C. □□□□ □□ Defender□ □ □□□□ □□□□□.

D. App1□ □□□ □□□ AppControl□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 66

□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Admin1□□□ □□□ □□□□ □□□□□.

Admin1□ Microsoft Defender □□□□ □□□□□ □□ □□□ □ □ □□□ □□ □□□. □ □□□□ □□ □□ □□□ □□□ □□□.

Admin1□□ □□ Microsoft Entra □□□ □□□□ □□□?

A. □□ □□□

B. □□ □□□

C. □□□□ □□ □□□

D. □□□ □□

E. □□ □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Policy□□ □□□ □□□ □□□ □□□ □□ □□□□□.
□□□□ Azure □□□ □□□□ □ □□ □□ MFA □□ □□□ □□□□□ □□ □□□. Azure PowerShell □□ Azure □□□ □□□□□(CLI)□ □□□ □ □□□□.
Policy1□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 68
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Compliance Manager □□□ □□□□□ User1□ □□□□□ □□□.
□□ □□: Microsoft 365 □□ □□ □□□□ User1□ □□ □□ □□□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□

Answer: A (LEAVE A REPLY)
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security
/permissions-in-the-security-and-compliance-center.md

NEW QUESTION: 69
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □ □ □□□ □□□□.
□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □ □□□□ □□ □□□ □□□□ □□□□.
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
SecAdmin1□□□ □□□□ □ □□ □□□ □□□ □□□□□.
SecAdmin1□ Microsoft Teams, SharePoint □ OneDrive□ □□ Office 365 □□ □□ □□(ATP) □□ □ □□□ □□□ □ □□□ □□ □□□.
□□ □□: Microsoft Entra ID □□ □□□□ SecAdmin1□□ Teams □□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
You need to assign the Security Administrator role.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365- worldwide

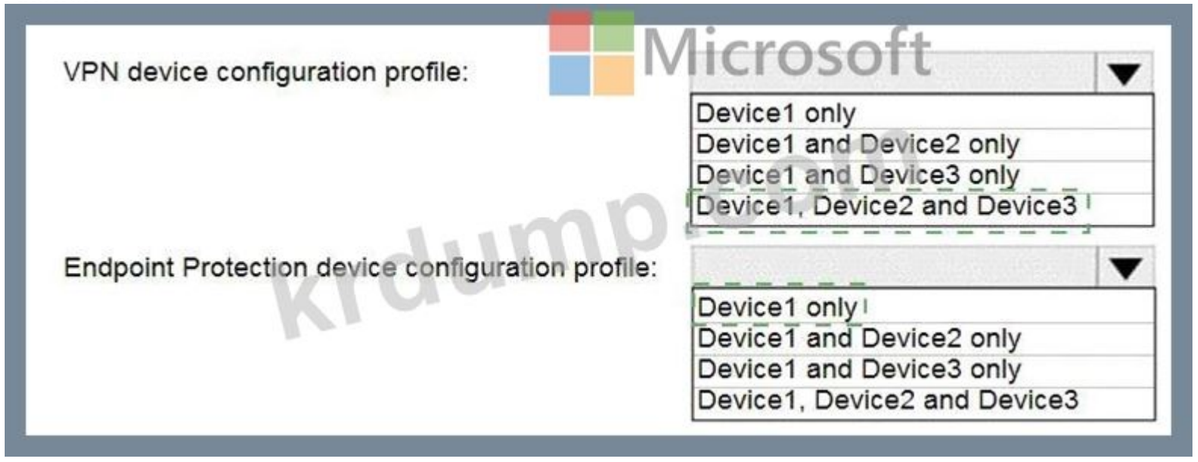
NEW QUESTION: 70
Microsoft Intune□ □□□ □□□□□ □□□□ Microsoft 365 □□□□ □□□□. □□□□□ □□ □□ □□□ □□ □□□□□.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

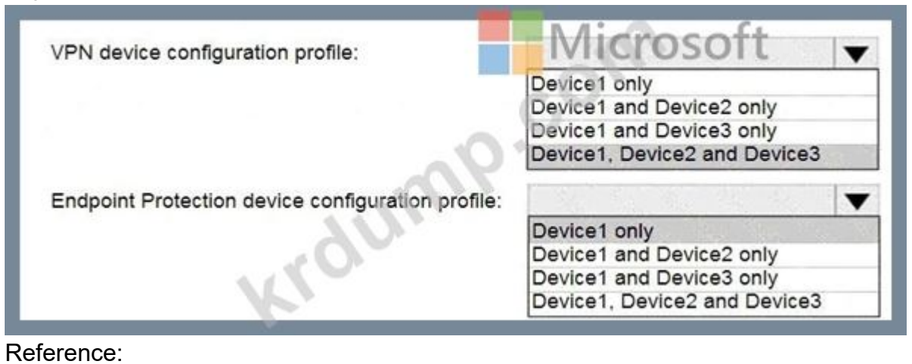
Microsoft Endpoint Manager□□ □□□ □□ □□ □□ □□□ □□□ □□□□□.
* VPN □□ □□ □□□□ □□□□ VPN □□□ □□□□□.
* Endpoint Protection □□ □□ □□□□ □□□□ □□ □□□ □□□□□.
□□□ □□ □□□ □□□□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer:



Explanation:



Reference:

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

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

NEW QUESTION: 71
Office 365□ Microsoft Defender□ □□□□ Microsoft 365 □□□ □□□ Mailbox1□□□ □□□□ □□□□.
Mailbox1□ □□□□ □□□□□ □□ □□□ □□□□ □□□□ □□□ □□□□□.
Defender for Office 365□ Mailbox1□ □□□ □□ □□ □□□□ □□ □□□ □□□ □□□ □□□ □□ □□□.
□□□ □□ □□□?
A. Mailbox1□ □□ □□□ □□□□□.
B. Mailbox1□ □□ □□ □□□ □□□□□.
C. Mailbox!□ SecOps □□□□□ □□□□□.
D. □□ □□ □□□ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 72
Microsoft 365 □□□□ □ □□ □□□ □□ □□□□ □□□.
□□ □□□□ □□□ □□□ □□□ □ □□□, □□□□ □□ □□□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

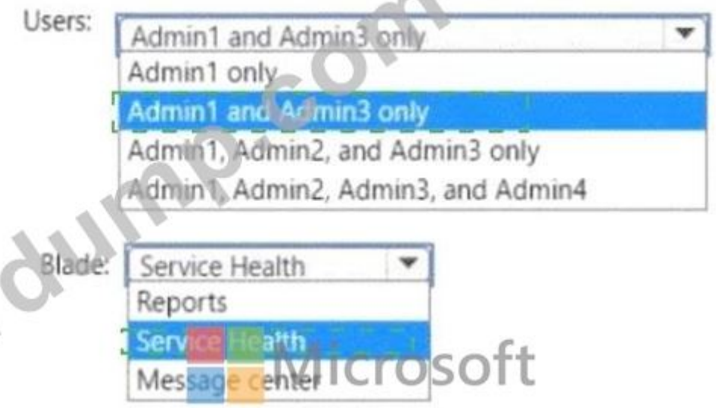
Answer Area

Users:
- Admin1 and Admin3 only
- Admin1 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Blade:
- Service Health
- Reports
- Service Health
- Message center

Answer:

Answer Area



Explanation:

NEW QUESTION: 73

□□□

□□□ □□□□ Microsoft 365 E5 □□□ □□□□.

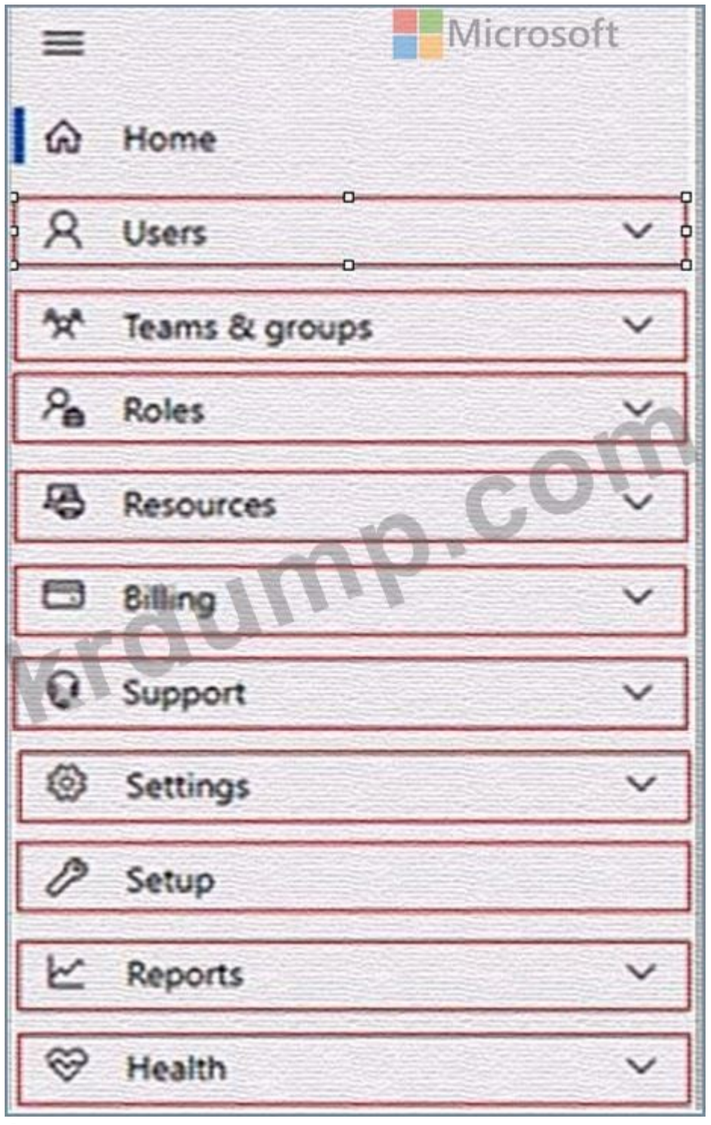
□□ □□□ □□□□ □□□.

□□□ □□ □□□ □□□□□.

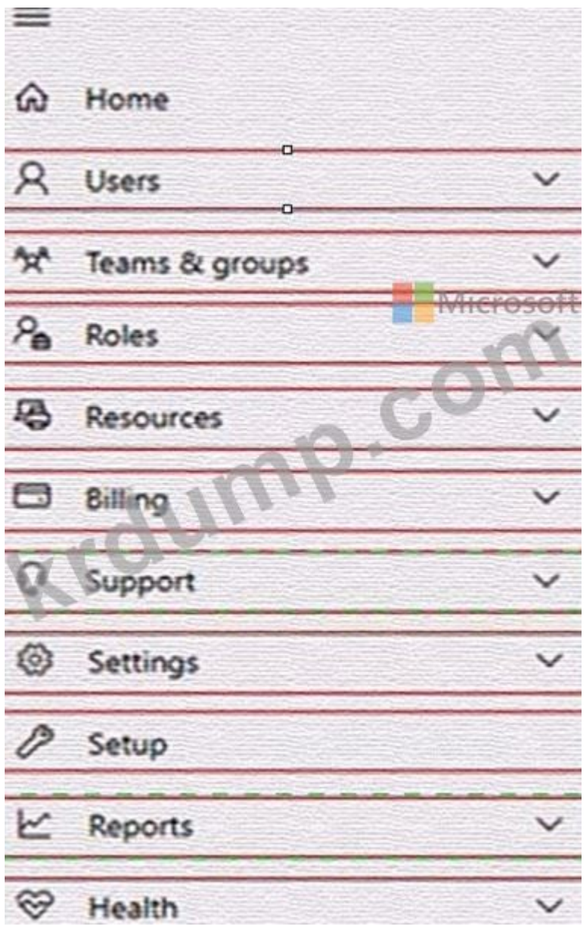
Microsoft□ □□□ □□□ □□□ □□□□.

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

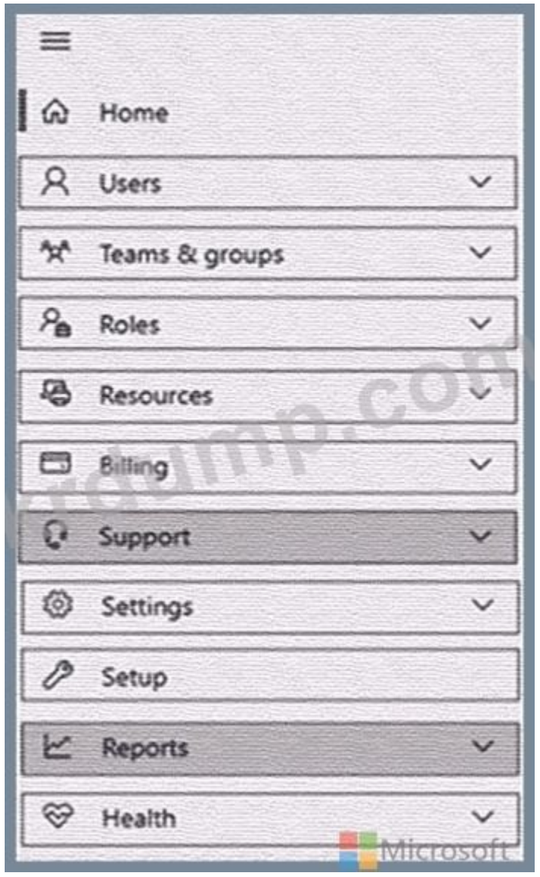
□□□□: □□ □□□ 1□□□□.


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

Answer:



Explanation:



Box 1: Reports

View the Adoption Score of the company.

How to enable Adoption Score

To enable Adoption Score:

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

Box 2: Support

Create a new service request to Microsoft.

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

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

Reference:

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

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

NEW QUESTION: 74

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

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

Microsoft 365 E5 □□□ □□□□.
SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.
SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Microsoft Defender for Office 365 □□ □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: Microsoft Entra □□ □□□□ SecAdmin1□□ □□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)
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: 75
Microsoft Intune□ □□□□ Microsoft 365 E5 □□□ □□□□. □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1□ Device1□ □□□□□□.
□□ □□ □□ Microsoft 365 □ Windows 10 □□ □ □□□ Intune□ □□□□□.
□□□□□ □ □□ □□□ □□□□□.

Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

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

Answer:

Explanation:

NEW QUESTION: 76

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

□□ □□□ □□ Policy1□□□ □□□ □□□□□ □□ □□ □□□ □□□□.

Policy1□ User1□ □□□□□.
User1□ 24□□ □□ □□ □ □□ □□ □□□ □□□ □□ □□□□□?

A. 720
B. 1000
C. 30
D. 1030

Answer: (SHOW ANSWER)

NEW QUESTION: 77

Microsoft 365 E5 □□□ □□□□.

□□ □□ □□□ □□□□ □□□□.

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

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

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

A. Admin1□

B. Admin1 □ Admin2□

C. Admin2□

D. Admin1 □ Admin3□

E. □□□1, □□□2, □□□3

Answer: D (LEAVE A REPLY)

NEW QUESTION: 78

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

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

□□□□ □□□□ □□□ □□□□□□.

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

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

□ □□□ □□□ □□ □□□□ □□□.

□□□ □□ □□□?

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

B. idfix.exe□ □□□ □□ □□□ □□□□□.

C. Windows PowerShell□□ start-AdSyncSyncCycle -PolicyType Delta □□□ □□□□□.

D. idfix.exe□ □□□ □□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Microsoft Entra ID. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Microsoft Entra ID.

Reference:

https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for-synch-with-idfix

NEW QUESTION: 79

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

A. Microsoft Endpoint Manager □□ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□□.
B. Microsoft Endpoint Manager □□ □□□□ □ □□ □□□ □□□□.
C. Microsoft 365 □□ □□□□ □□ □□□ □□□□□.
D. Microsoft 365 □□ □□□□ □□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Reference:
https://systemcenterdudes.com/intune-company-portal-customization/
Q

NEW QUESTION: 80
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Windows 10□ □□□□ □□□□ □□□□.
□□□ Windows 10 □□□ □□□□ □□□.
□□ □□: □□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

NEW QUESTION: 81
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 □□□ □□□□.

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

□□ □□□ □□□ □□□ □□ □□□□.

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

□□ □□□ □□ □□□ □□□ □□□ □□□□.
* □□□ □□ □□ ID:
o □□: □□ 1
o □□: □□2
* □□□□ □ □□ □□: □□ □□□□ □□ □□□□□.

* □□ :
o □□: □□ □□
o □□ □□: □□□□
* □□ □□: □□ □□, □□ □□ □□ □□
User1□ □□ □□ □□(MFA) □□ □□□ □□□ □□□□.
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	○	○
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	○	○
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	○	○
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	○	○
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	○	○

Explanation:

Answer Area

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	●	○
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	○	●
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	●	○

NEW QUESTION: 82

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

Name	Member of
User1	Group1
User2	Group2
User3	Group3

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

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

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

Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (default)	Device2	Group2

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

□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

Explanation:

NEW QUESTION: 83

□□□ □□□□ Microsoft 365 E5 □□□□ □□□□.

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

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

□□ □□□□□ □□□ □□ Office □□ □□□ □□□□□.

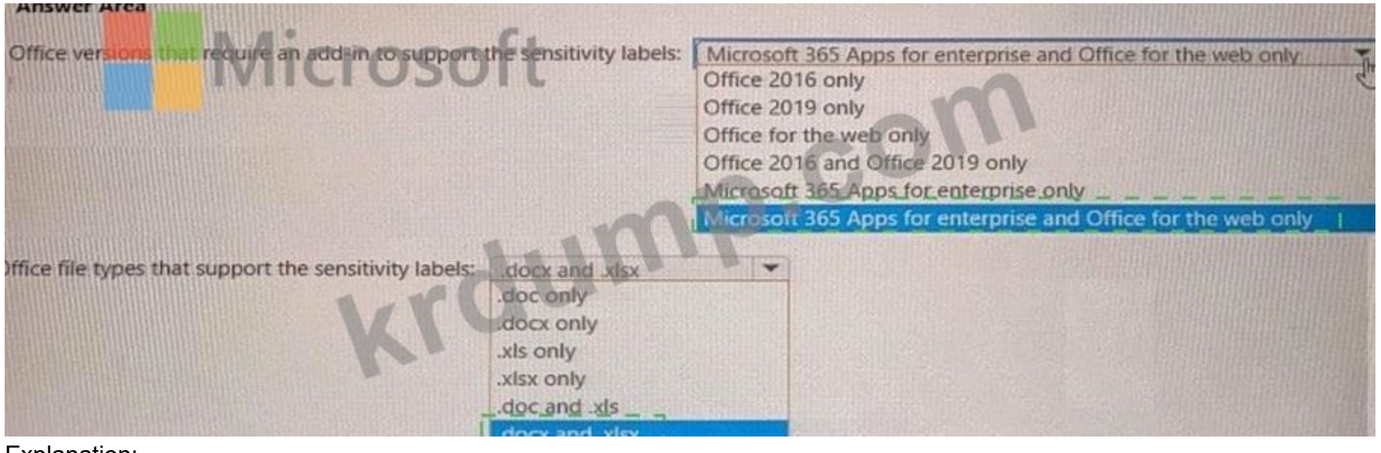
* .docx
* .xlsx
* .□□
* □□

□□□ □□□□ □□□ □□□□□. □□□ □□□□ □□□.

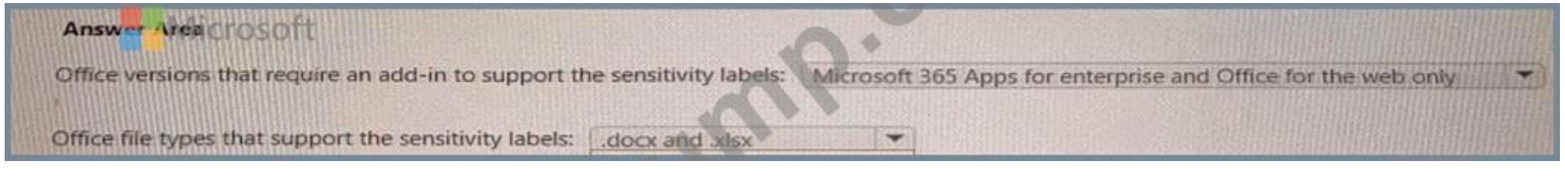
* □□□ □□□□ □□□□ □□ □□ □□□ □□□ Office □□□ □□□□□?
* □□□ □□□ □□□□ □□ □□□ □□□□□?

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

Answer:



Explanation:



NEW QUESTION: 84

□□□

Microsoft 365 E5 □□□ □□□□.

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

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

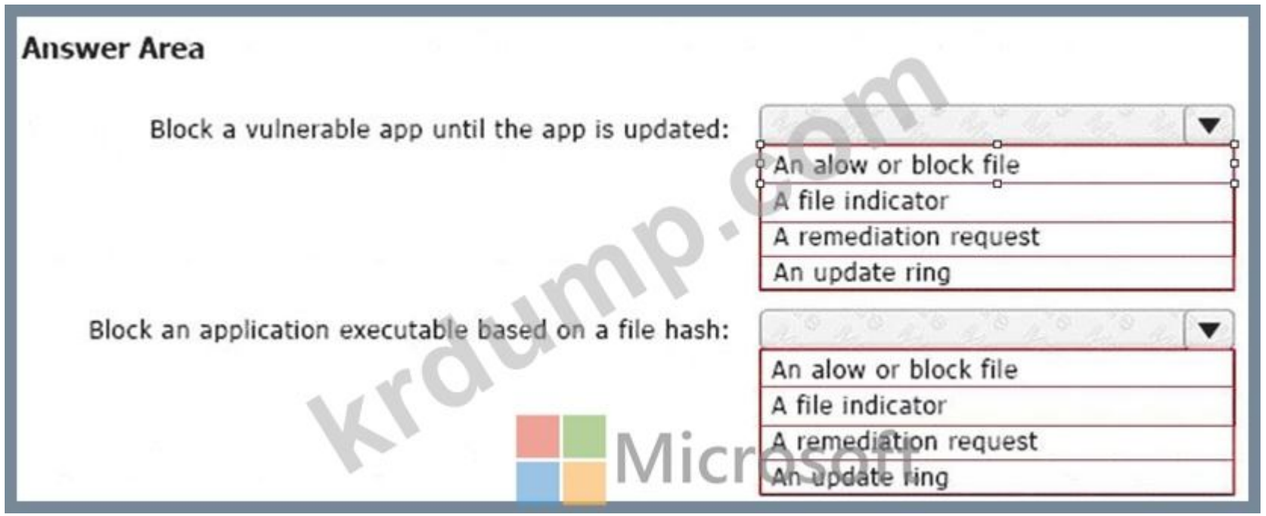
* □□ □□□□□ □□□ □□□ □□ □□□□□.

* □□ □□□ □□□□ □□□□□□ □□ □□□ □□□□□.

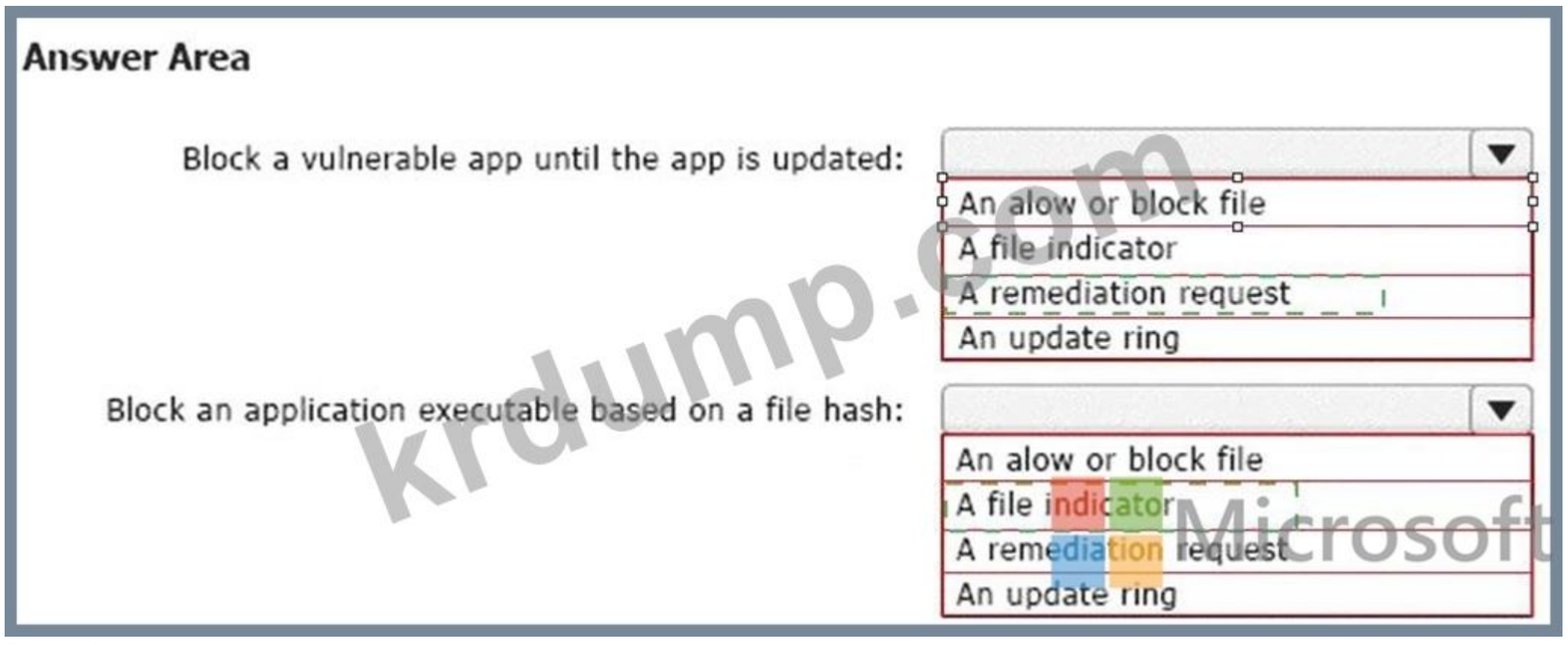
□□□□ □□□ □□□ □□□□□ □□□.

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

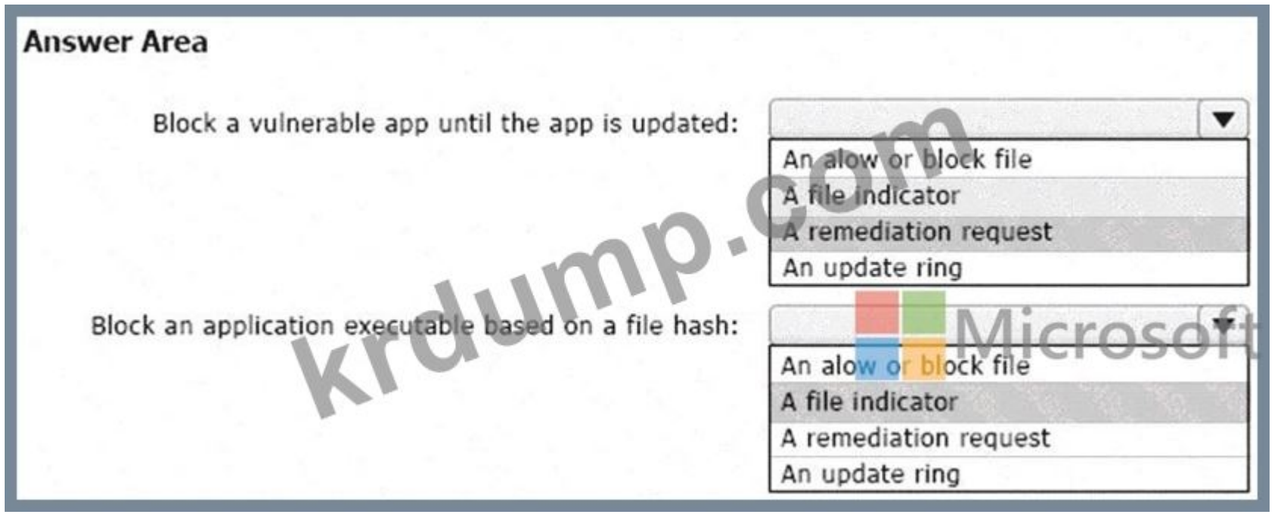
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Box 1: A remediation request

Block a vulnerable app until the app is updated.

Block vulnerable applications

How to block vulnerable applications

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

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

Select Request remediation.

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

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

Pick a Remediation due date and select Next.

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

Review the selections you made and Submit request. On the final page you can choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.

Box 2: A file indicator

Block an application executable based on a file hash.

While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.

The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

Reference:

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

NEW QUESTION: 85

Microsoft J65 E5 □□□ □□□□.

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

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

□□□: □□ □□□ □□□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 86
(□□□ □□□□□□ 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: 87

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

A. Microsoft Entra Connect □□□□□ □□□□□ □□□ □□□□□.
B. PowerShell□□ Start-ADSyncSyncCycle cmdlet□ □□□□□.
C. PowerShell□□ Add-ADSyncConnectorAttributeInclusion cmdlet□ □□□□□.
D. Microsoft Entra Connect □□□□□ □□□ □□ □□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)

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

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

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

Policy Types

- App configuration policy
- App protection policy
- Compliance policy
- Conditional Access policy

Answer Area

Device1:
Device2:
Device3:

Answer:

Explanation:

NEW QUESTION: 89

Microsoft 365 E5 □□□□ □□□□.

□□□□ □□ □□□ □□□□ □□□□□.

□□□□□□□ □

□□□□□□□ □□□□□

□□□□□□□ □□□□□ □□□

□□□□□□□ □□□□□ □□□

Microsoft 365 □□□□ 2□ □□ □□□□ □□□.

□□□ □ □□ □□ □□□ □□□□ □□□?

A. 1

B. 2

C. 3

D. 4

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 90

□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Microsoft Entra□□ □□□ □□□ □□□ □□ □□ □□ ID □□(PIM)□ □□□□□ □□□. □□□□ □□ 6□□ □□□□ □□□ □□□ □□ □□ □□□ □ □ □□□ □□ □□□. □ □□□ □□□ □□□□ □□□?

A. □□ □□□ □□ □□□ '□'□ □□□□□.

B. □□ □□ □□ □□ □□□ '□'□ □□

C. □□ □□□ □□□□ □□□□□.

D. □□ □□□ □□□□ □□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 91

□□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□. □ □□□□□ Windows Server□ □□□□ Server1□□□ □□□ □□□□. □ □□□□□ □□ □□ □□ □□ □□□□ □□□□ □□□□.

Name	DistinguishedName	UserPrincipalName	Email address
User1	CN=User1,OU=Department1,DC=Contoso,DC=LOCAL	user1@contoso.com	user1@contoso.com
User2	CN=User2,OU=Team1,OU=Department2,DC=Contoso,DC=LOCAL	user2@contoso.local	user2@contoso.local
User3	CN=User3,OU=Department2,DC=Contoso,DC=LOCAL	user3@contoso.com	user3@contoso.com

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

Answer Area

Statements	Yes	No
User1 syncs with user1@contoso.com.	○	○
User2 syncs with user2@contoso.com.	○	○
User3 is created as a new user in Microsoft 365.	○	○

Answer:

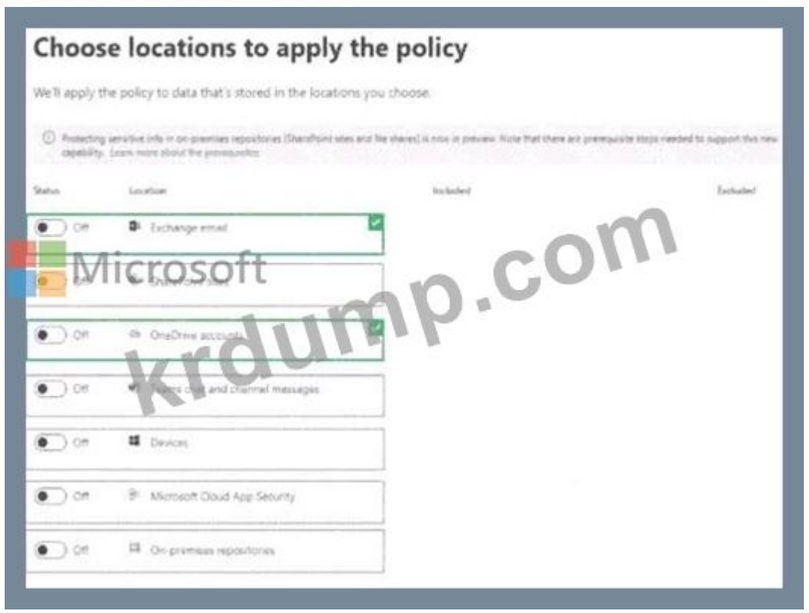
Explanation:

Answer Area

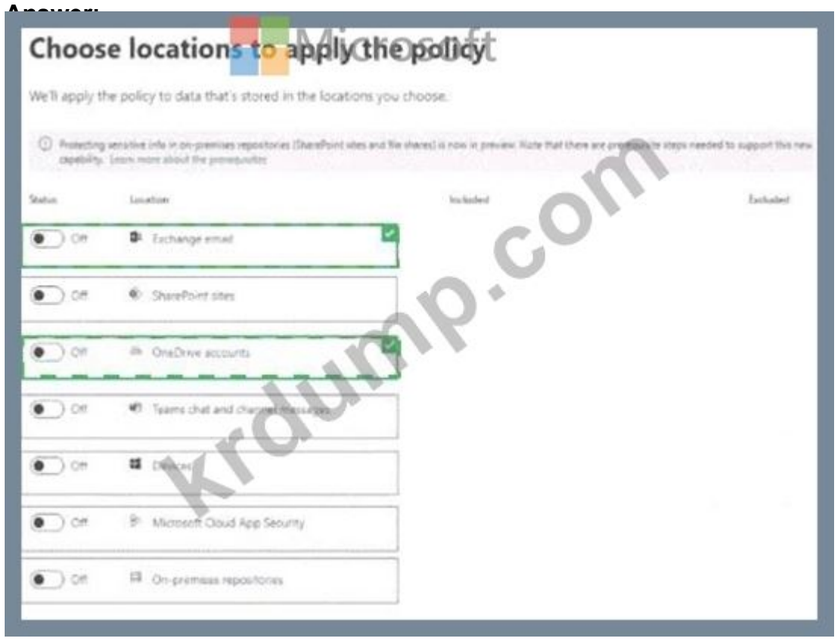
Statements	Yes	No
User1 syncs with user1@contoso.com.	●	○
User2 syncs with user2@contoso.com.	○	●
User3 is created as a new user in Microsoft 365.	■	○

NEW QUESTION: 92

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



Answer:



NEW QUESTION: 93
□□□□□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□. □ □□□□□ 500□□ Windows 11 □□□ □□□□.

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

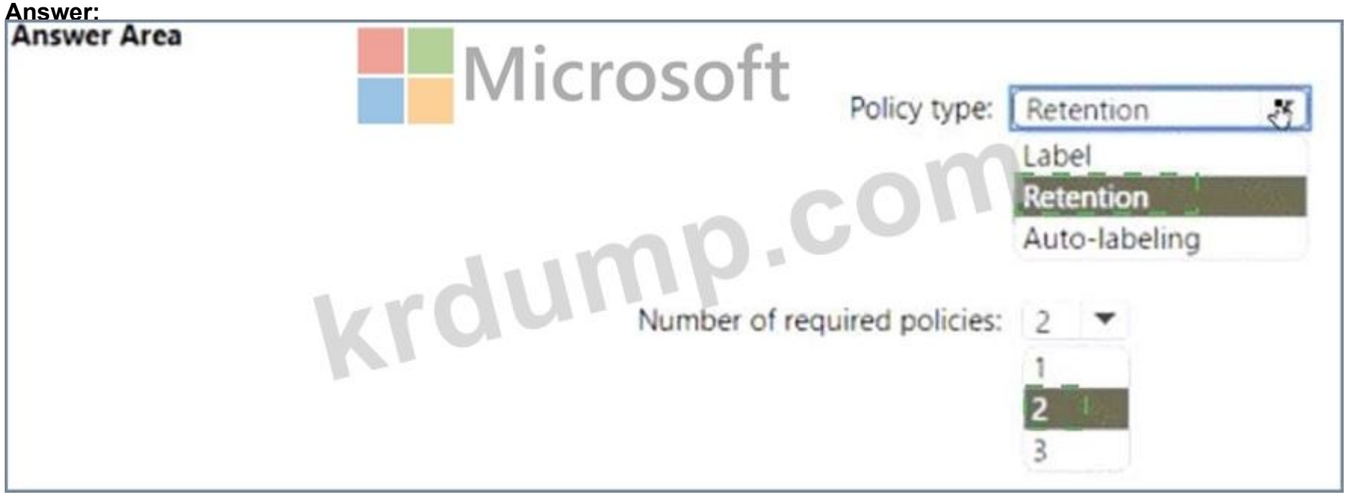
NEW QUESTION: 94
Microsoft 365 E5 □□□ □□□□.
□□□ □□□ □□□ □□□□□□□ Microsoft Defender for Cloud Apps□ □□□□ □□□. □□□ □□ □□□?
A. □□□ □□ □□□ □□□□□□.
B. □□ □□□ □□□□.
C. Microsoft 365□ □ □□□□ □□□□.
D. □□□ □□□ □□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 95
□□□□□□ Active Directory □□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□□□□ □□□ □□□□□ □□□ □□□ □□□ □□□□ □□□□□.
□□□□ □□□□ □□□□□ □□□ □□□□□□.
□□□□ □□ □□□ □□□□□.
* □□□□□□□□□
* □□□□□
□□□□ □□□□ □□□□□ □□□□□□ □□□□ □□□.
□□□ □□□□ □□ □□ □□ □□ □□□ □□□□?
A. □□□□□ Azure □□□ □□□ IP □□ □□□ □□□□□ □□□ □□□□□.
B. □□□□ □□□□ Microsoft Entra Connect Sync □□□ □□□ □□□□□.
C. Microsoft Entra Connect□□ □□□ □□ □□□ □□ □□□ □□□□□.
D. □□□□□ □□□□ □□□□□ □□□ □□□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 96
□□□ □□ □□□ □□□□□ □□ □□□□ □□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□, □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:



Explanation:

NEW QUESTION: 97
Microsoft 365 □□□ □□□□. User1□□□ □□□□ □□□□.
Used□ □□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□ □□□.

User1□□ □□ □□□ □□□□ □□□?

A. Microsoft Entra ID □□ □□□ □□ □□ □□□ IDE□□□.

B. Exchange □□ □□□ □□ □□ □□ □□□□□.

C. Microsoft 365 □□ □□ □□□ eDiscovery Manager □□□.

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 98

□□ □□ □□□ □□□□ □□□ 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:

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: 99

□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

□□□(FID02)□ □□□ □□ □□□□ □□□□ □□ □□□ □□□ □□□□□. □□ □□□□ □ □□□(FID02)□ FIDO Alliance □□□□□ □□□□ □□ □□□□□ □□ □□□. □□ □□□ □□□□□ □□□?

A. □ □□ □□

B. □□ □□

C. □□ □ □□

D. □□ □□□ □□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 100

□□□

Microsoft 365 E5 □□□ □□□□.

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

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

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

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

□□□□: □□ □□□ 1□□□□.

Answer Area

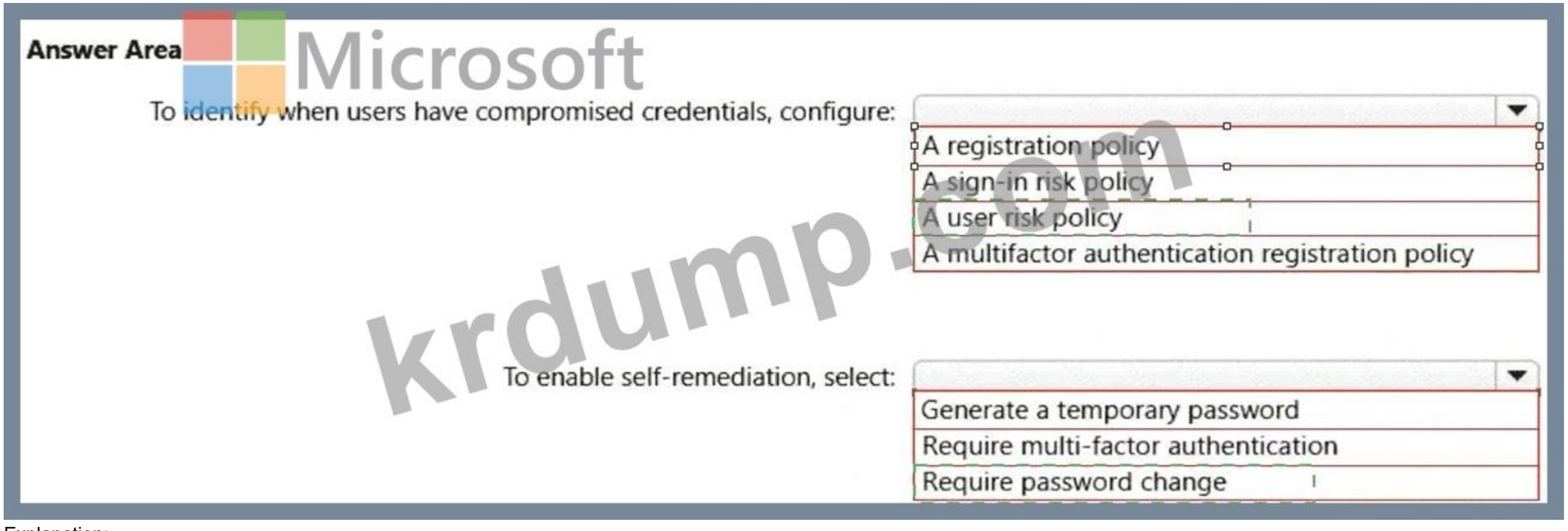
To identify when users have compromised credentials, configure:

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

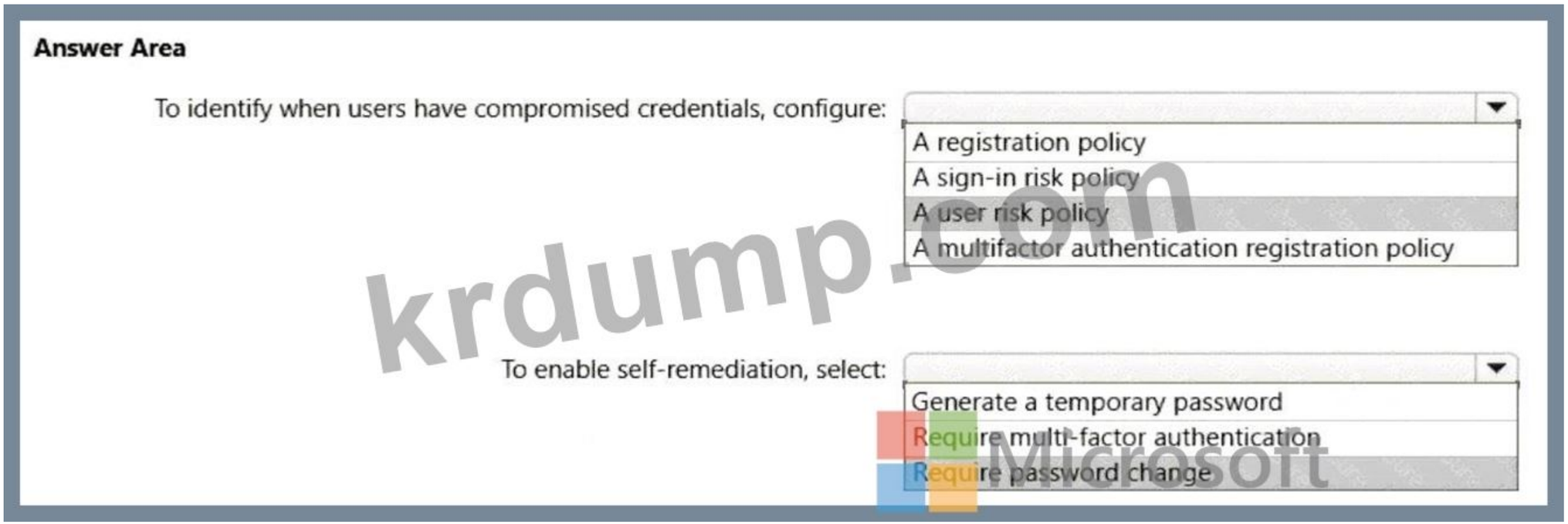
To enable self-remediation, select:

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

Answer:



Explanation:



Box 1: A user risk policy

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

User risk-based Conditional Access policy

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

Block access

Allow access but require a secure password change.

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

Box 2: Require password change

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

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

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

NEW QUESTION: 101

□□□

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

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

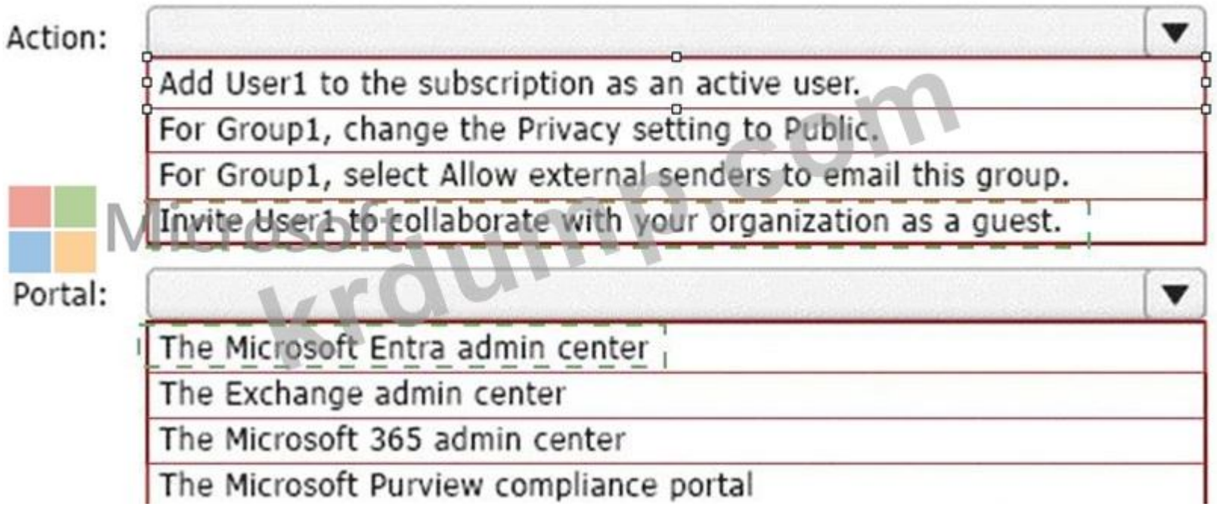
User1□ Group1□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.

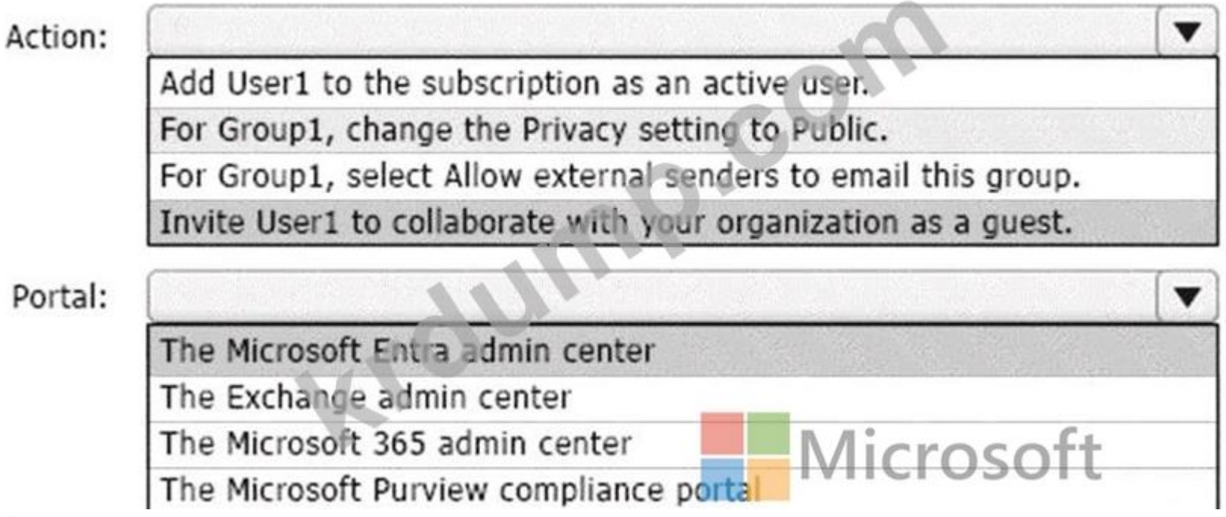
Answer:

Answer Area



Explanation:

Answer Area



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

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

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

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

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

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

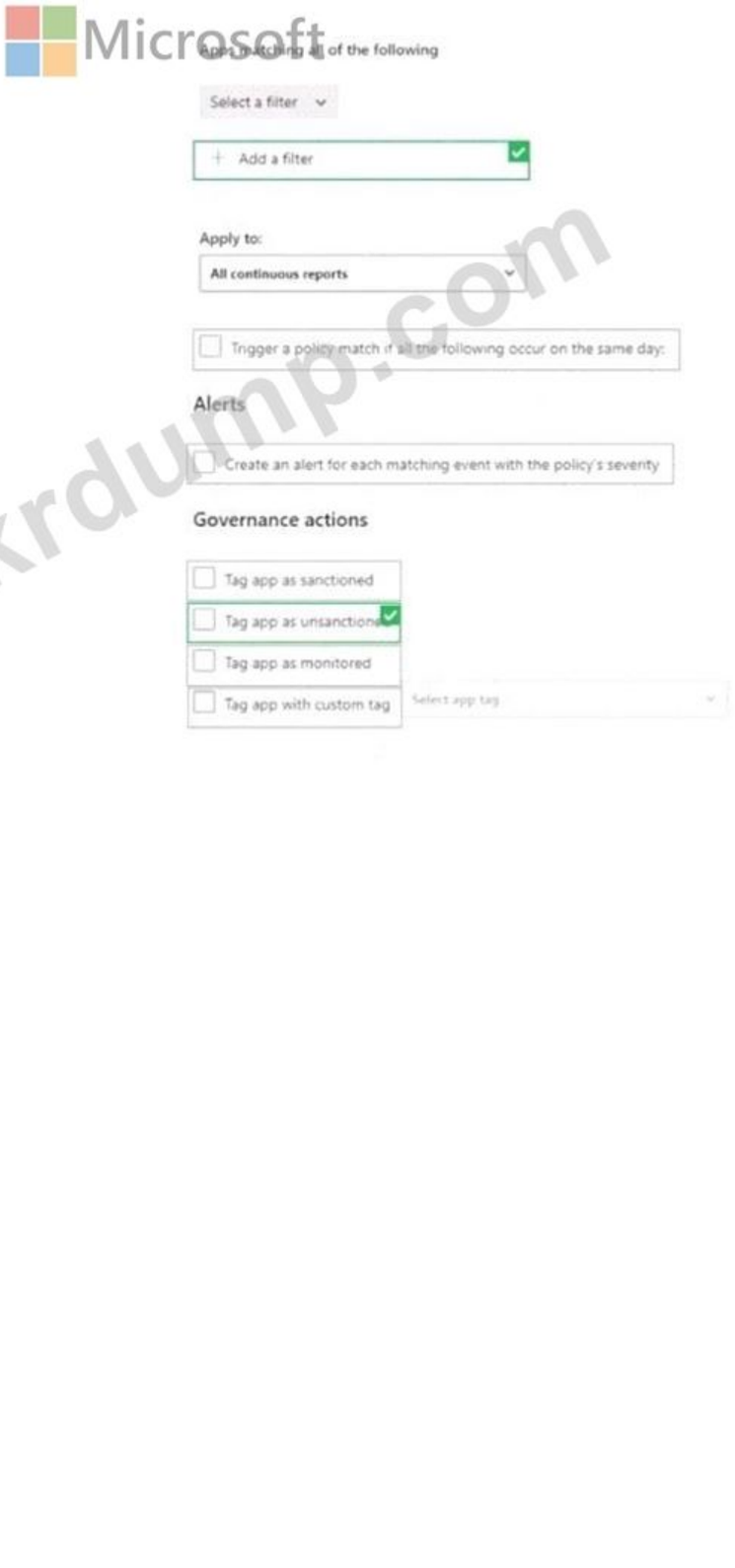
they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the "Invite user" option.
Box 2: The Microsoft Entra admin center
Microsoft Entra admin center unites Microsoft Entra ID with family of identity and access products Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Microsoft Entra ID (Microsoft Entra ID) and Microsoft Entra Permissions Management, formerly known as CloudKnox.
Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Microsoft Entra admin center (aad.portal.azure.com).
Reference:
https://stefanos.cloud/kb/how-to-manage-microsoft-365-guest-users
https://m365admin.handsontek.net/microsoft-entra-admin-center-unites-azure-ad-with-family-of-identity-and-access-products

NEW QUESTION: 102
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows Server 2019□ □□□□ □□□ □□□□□ □□□□. □□□□□ □□□□ □□ □□□ Windows Server 2012 R2□□□.
□ □□□□□ Windows 10□ □□□□ 100□□ □□□□ Windows Server 2012 R2□ □□□□ Server1□□□ □□ □□□ □□□□ □□□□.
Server1□ □□□□ □□□□ □□□□ Windows 10 □□ □□ □□□ □□□ □□□□□.
Server1□ □□ □□ □□ □□(GPMC)□ □□□□□.
Server1□□ □□□□□ Windows □□□□ □□ □□ □□□ □□□□ □□□.
□□ □□: Windows 10 □□□□□ Server1□ □□ □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?

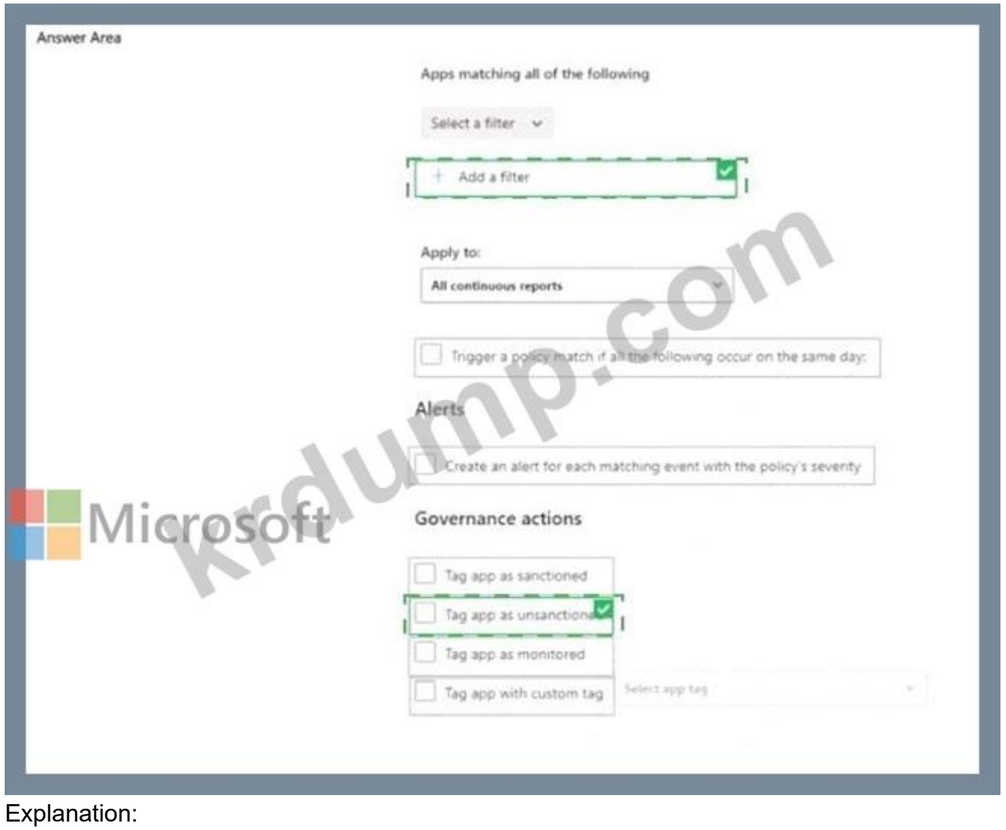
A. □□□
B. □
Answer: (SHOW ANSWER)

NEW QUESTION: 103
Microsoft 365 □□□ □□□□.
□□□□ □□ Microsoft Defender□ □□□□□□ Microsoft Defender□ □□□□□.
□□ □□□ 4□ □□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

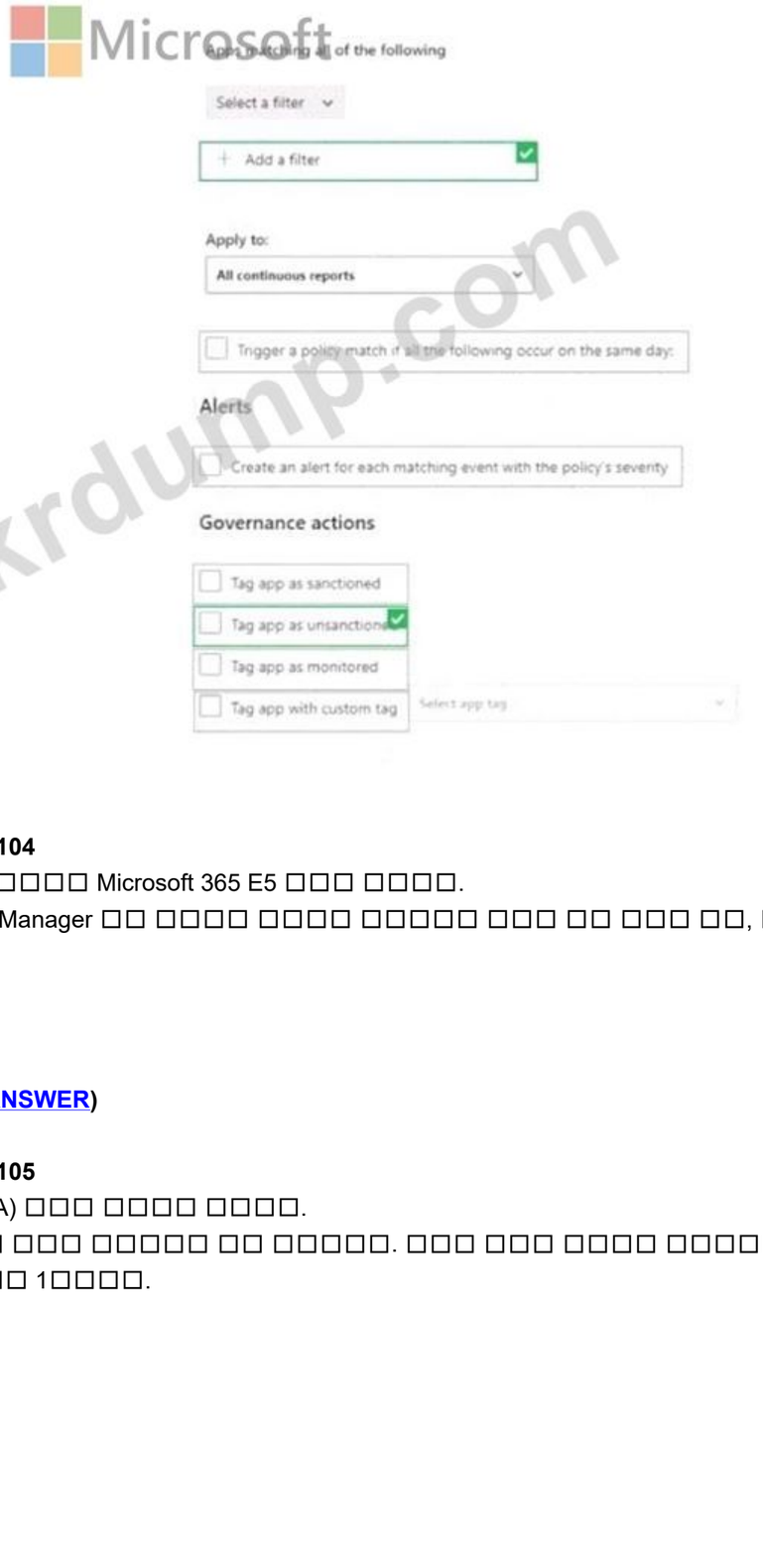


Answer:



Explanation:

Answer Area



NEW QUESTION: 104

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

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

A. 45

B. 90

C. 30

D. 10

Answer: (SHOW ANSWER)

NEW QUESTION: 105

□□ □□ □□(MFA) □□□ □□□□ □□□□.

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

□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 106

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

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

□□ □□□ □□□□ □□□.

* ZAP(□□□□ □□ □□)□ □□□ □□□ □□□ □

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

Answer:

Explanation:

NEW QUESTION: 107
□□□□ contoso.com□□□ Microsoft Entra □□□□ Microsoft 365 □□□ □□□□. □□ □□□□ Windows 10 □□□ □□□□ Microsoft 365 □□ □□□□□□. □□ □□□ □□ □□□ □□□□.
contoso.com□ □□□□ □□ □□□□□ □□□ □□□□□ □□□.
□□□ □□□ □□ □□□□ □□ □□ □□□ □□□□ □□□. □□ □□□□ □□□ □□□□ □□□?
A. □□ □□□ contoso.com□ □□□□□.
B. Microsoft Entra □□□□□□ □□□□ □□□□□.
C. Microsoft Authenticate □□ □□□□□.
D. Microsoft Entra Connect □□□□□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 108
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
SecAdmin1□□□ □□□□ □ □□ □□□ □□□ □□□□□.
SecAdmin1□ Microsoft Teams, SharePoint □ OneDrive□ □□ Microsoft Defender for Office 365 □□ □ □□□ □□□ □ □□□ □□ □□□.
□□ □□: Microsoft Entra ID □□ □□□□ SecAdmin1□□ Teams □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 109
□□ □□ □□□ □□ □□□ □□ □□□ □□□□ □□□. □□□ □□□□ □□□?
A. □□ □ □□ □□ □□ □□□ □□□ □□ □□(DLP) □□
B. □□ □ □□ □□ □□ □□□ □□ □□
C. Microsoft Cloud App Security□ □□ □□

D. Microsoft Cloud App Security☐ ☐☐ ☐☐

Answer: (SHOW ANSWER)

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

Topic 3, Litware Inc.Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overviews

Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.

Environment

Existing Environment

The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.

Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.

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

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

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

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.
The verified domain is linked to an Microsoft Entra ID (Microsoft Entra ID) tenant named litware.com. Audit log search is turned on for the litware.com tenant.
Problem Statements
Litware identifies the following issues:
Users open email attachments that contain malicious content.
Devices without an assigned compliance policy show a status of Compliant.
User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.
Requirements
Planned Changes
Litware plans to implement the following changes:
Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
Implement data loss prevention (DLP) policies to protect confidential information.
Grant User2 permissions to review the audit logs of he litware.com tenant.
Deploy new devices to the Seattle office as shown in the following table.

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

Implement a notification system for when DLP policies are triggered.
Configure a Safe Attachments policy for the litware.com tenant.
Technical Requirements
Litware identifies the following technical requirements:
Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Microsoft Entra ID.
Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
User2 must be granted the permissions to review audit logs for the following activities:
- Admin activities in Microsoft Exchange Online
- Admin activities in SharePoint Online

- Admin activities in Microsoft Entra ID
Users must be able to apply sensitivity labels to documents by using Office for the web.
Windows Autopilot must be used for device provisioning, whenever possible.
A DLP policy must be created to meet the following requirements:
- Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
- Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
The principle of least privilege must be used.

NEW QUESTION: 110
□□□ Microsoft Intune□ □□□ Windows □□ 500□□ □□□ Microsoft 365 □□□ □□□□ □□□□.
□□□ □□ □□□ □□ □□ □□□ □□□ □ □□□ □□ □□□. □□, □□□□ □□ □□□ □□□□□ □□□.
Microsoft Defender □□□□ □□ □□ □□□□ □□□□ □□□?
A. □□□□□ □□ □ □□
B. □□ □□
C. □□□□□□□ □□□ □□□□□□
D. Windows □□ □□
Answer: A (LEAVE A REPLY)
The correct policy template is Endpoint Detection and Response because vulnerability management recommendations require the devices to be onboarded to Microsoft Defender for Endpoint, where Defender Vulnerability Management can assess the endpoint inventory, detected weaknesses, exposure, and security recommendations. Microsoft states that after Intune is integrated with Defender for Endpoint, Defender Vulnerability Management identifies vulnerabilities on managed devices and allows security admins to review endpoint vulnerabilities and create remediation tasks.
For Intune-managed Windows devices, the lowest-administration deployment path is to use an endpoint security policy rather than manually deploying onboarding scripts or packages. Microsoft's Defender portal endpoint security policy documentation states that when Defender for Endpoint is integrated with Intune, administrators use endpoint detection and response endpoint security policies to manage EDR settings and onboard devices to Microsoft Defender for Endpoint. Microsoft's onboarding guidance also identifies deploying an endpoint detection and response policy with Intune as an onboarding deployment method.
Device Control manages removable/device access controls, Microsoft Defender Antivirus configures antivirus behavior, and Windows Security Experience controls end-user Windows Security app experience. None of those templates is the direct onboarding mechanism needed for Defender Vulnerability Management recommendations. References/topics: Microsoft Defender for Endpoint onboarding, Intune endpoint security policies, Endpoint Detection and Response policy, Defender Vulnerability Management recommendations.

NEW QUESTION: 111
Windows 10 □□□ □□ Intune □□ □□□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

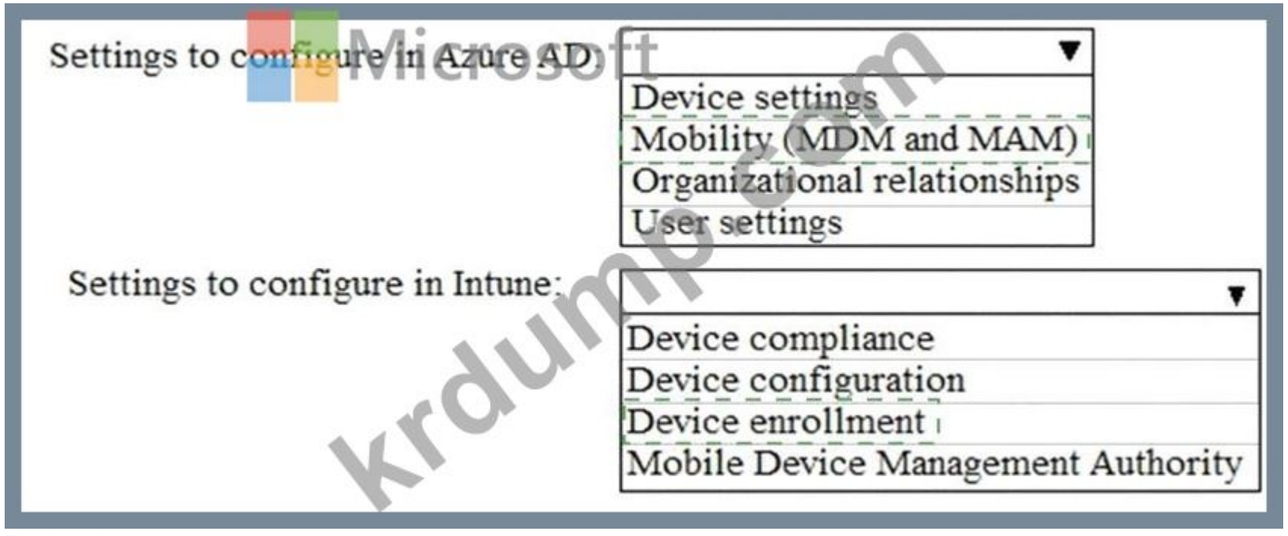
Settings to configure in Azure AD:

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

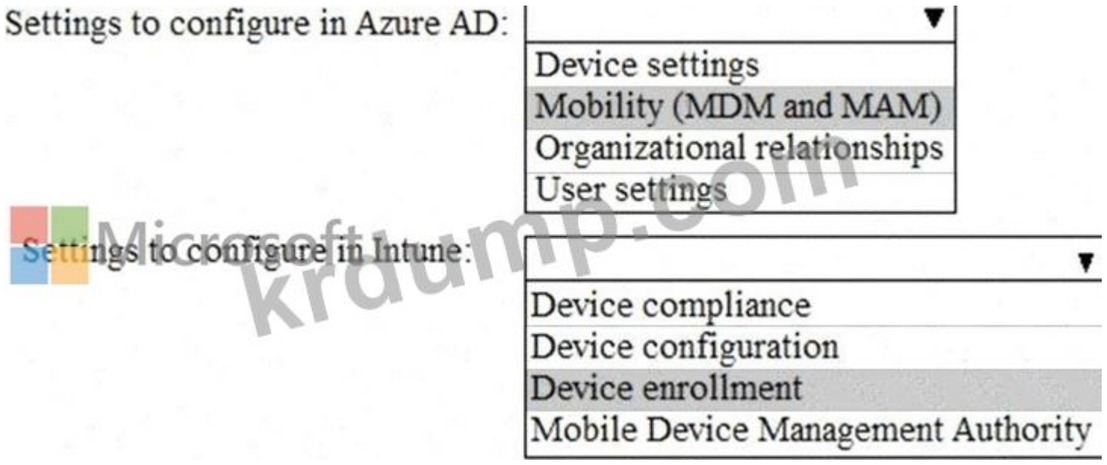
Settings to configure in Intune:

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

Answer:



Explanation:



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

NEW QUESTION: 112
□□□ □□□□ □□ □□ □□ □□ □□□□ □□□ Microsoft 365 □□□ □□□□.

Name	Role
User1	Global Administrator
User2	Security Administrator, Guest Inviter
User3	None
User4	Password Administrator

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

Answer:

Explanation:

NEW QUESTION: 113

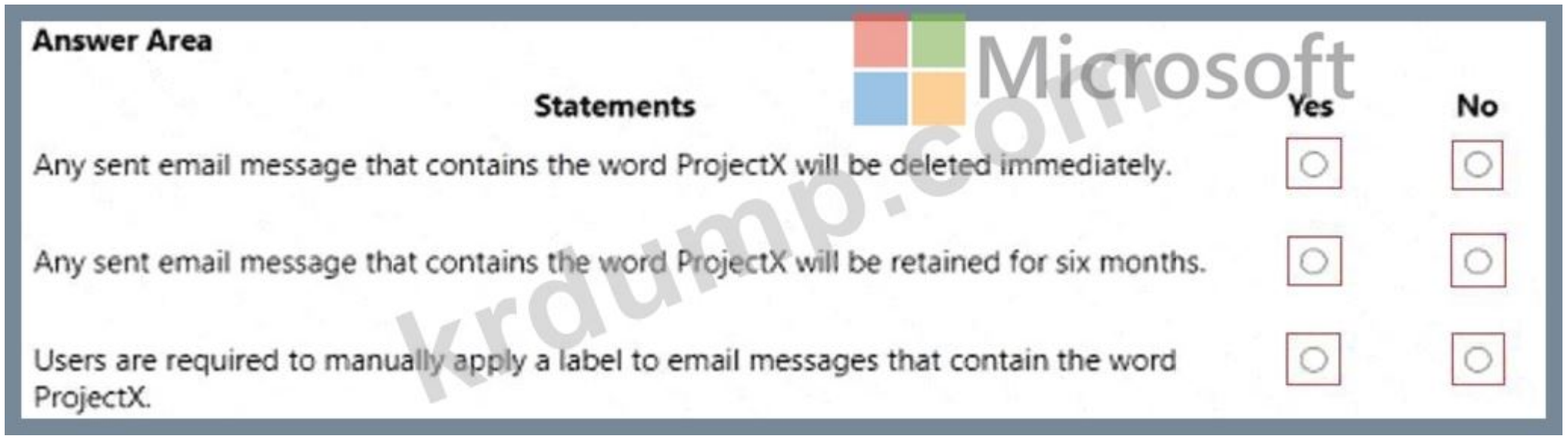
□□□
Microsoft 365 □□□□ □□□□.
□□ □□ □□□ □□□ □□ □□ □□□ □□□□. (□□ □□ □□ □□□□□.)

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

□□ □□□ □□ □□ □□ □□□□□.

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

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

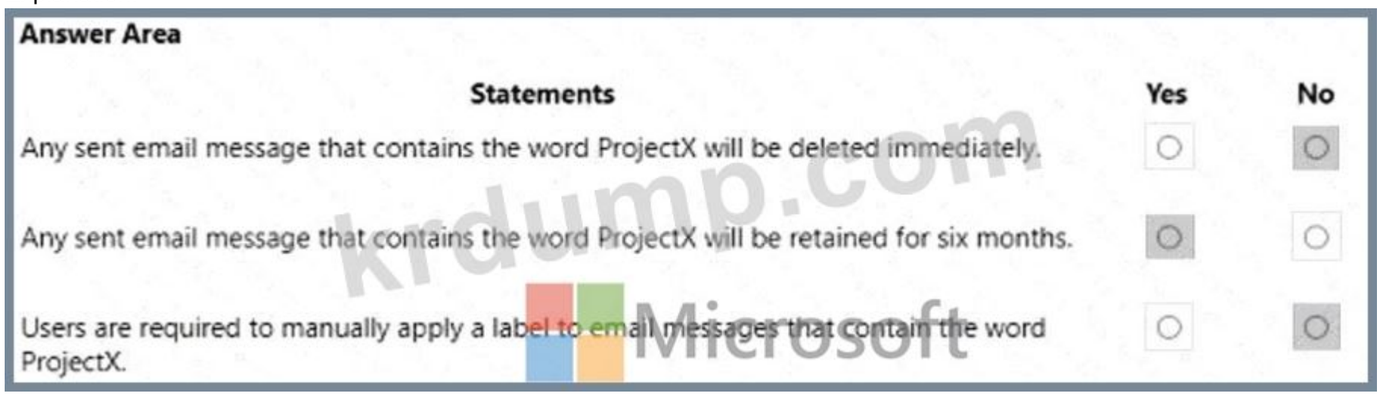


Answer:

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

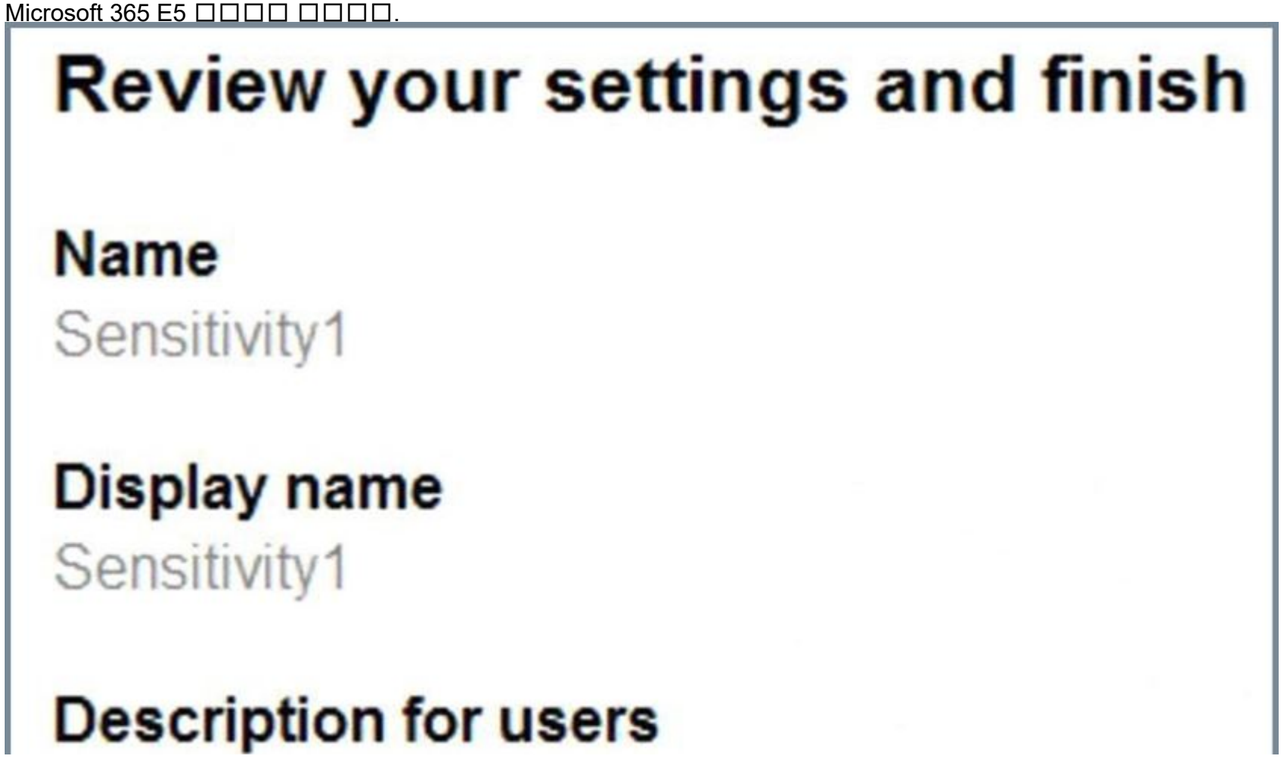
Box 3: No

Reference:

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

NEW QUESTION: 114
Microsoft 365 E5 □□□ □□□□ □□□ □□□□ □□ Microsoft Defender□ □□□□ □□□□.
□□ □□ □□□ □□□□ □□□□.
□□□□□ □□□□□□ □□□□ □□□□ □□□□ □□ □□□□ □□□□□ □□ □□□.
□□□ □□□□ □□□?
A. □□ □□ □□
B. IP □□ □□□
C. IP □□ □□
D. □□□ □□□ □□
Answer: C (LEAVE A REPLY)
The correct answer is C. an IP address range . In Microsoft Defender for Cloud Apps, IP address ranges are used to identify known network locations, such as physical offices, datacenters, VPN egress addresses, and administrative networks. Microsoft states that IP address ranges let you tag, categorize, and customize how logs and alerts are displayed and investigated. Each IP range can be assigned to a preset IP category, such as Administrative , Corporate , VPN , or other categories, so events from those IP addresses are categorized automatically in the Activity log.
This directly matches the requirement: events originating from the on-premises network must be categorized automatically as Administrative . To do that, you create an IP address range for the on-premises public IP addresses and assign the range the Administrative category. Defender for Cloud Apps then uses that categorization when displaying and filtering activity log events. Microsoft also confirms that IP address category can be manually overridden by using IP address ranges.
A named location is a Microsoft Entra Conditional Access construct, not the Defender for Cloud Apps activity-log categorization mechanism. An indicator for IP addresses is used for threat indicators in security tooling, not for activity-log categorization. A critical asset classification is unrelated to IP-based event categorization.

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



Sensitivity1

Scope

File.Email

Encryption

Content marking

Watermark: Watermark

Header: Header

Auto-labeling

Group settings

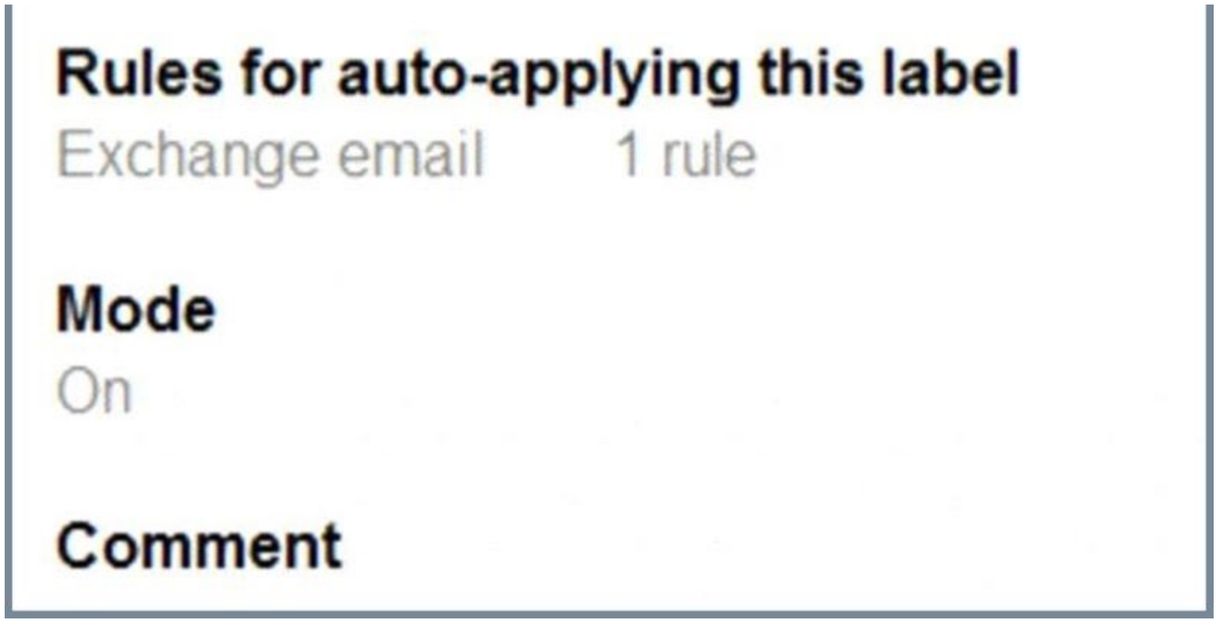
Site settings

Auto-labeling for database columns

None

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


Auto-labeling policy
Edit Policy
Delete Policy
Policy name
Auto-labeling policy
Description
Label in simulation
Sensitivity1
Info to label
IP Address
Apply to content in these locations
Exchange email All



□□□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□□.

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

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

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

Answer:

Explanation:

Reference:

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

NEW QUESTION: 116

□□□

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

□□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

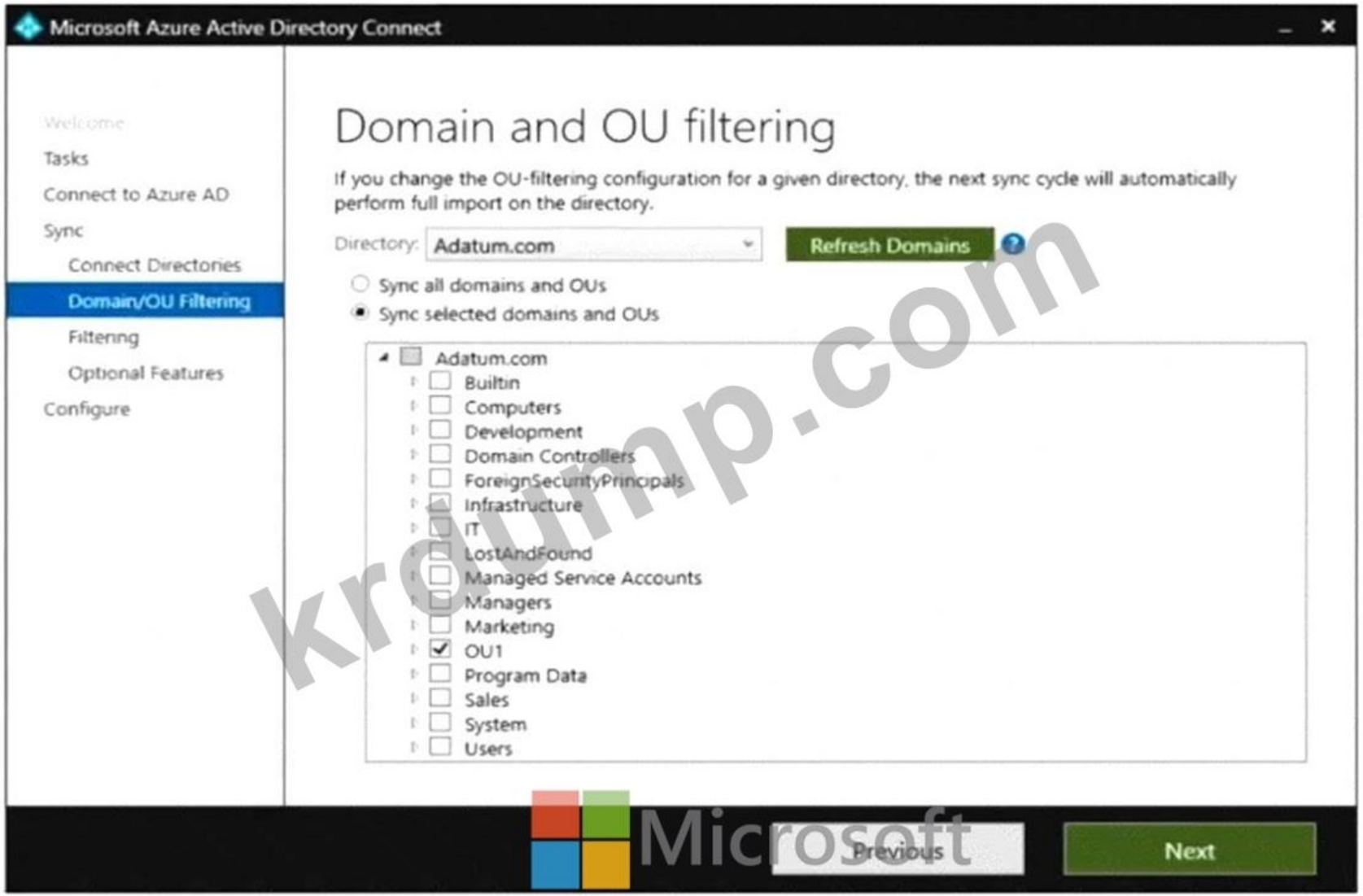
Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

□□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

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

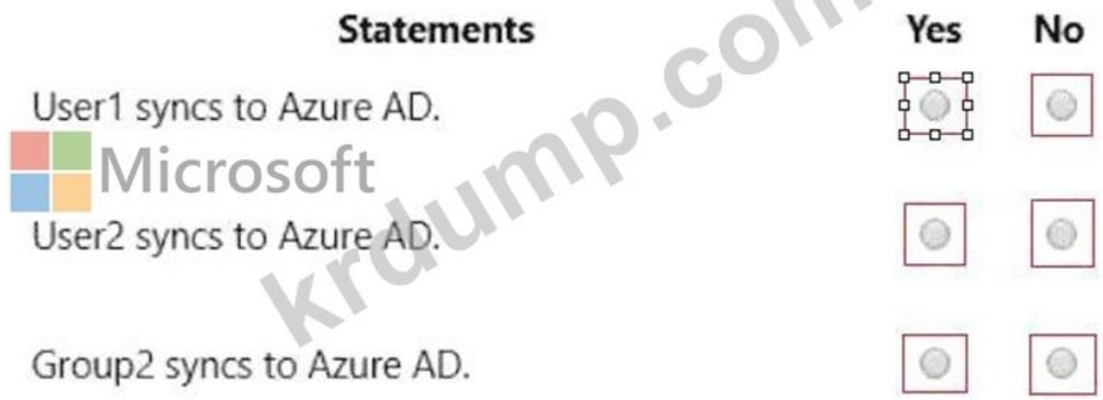
□□ □□□ □□ □□□ □ OU □□□□ □□□□□.


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

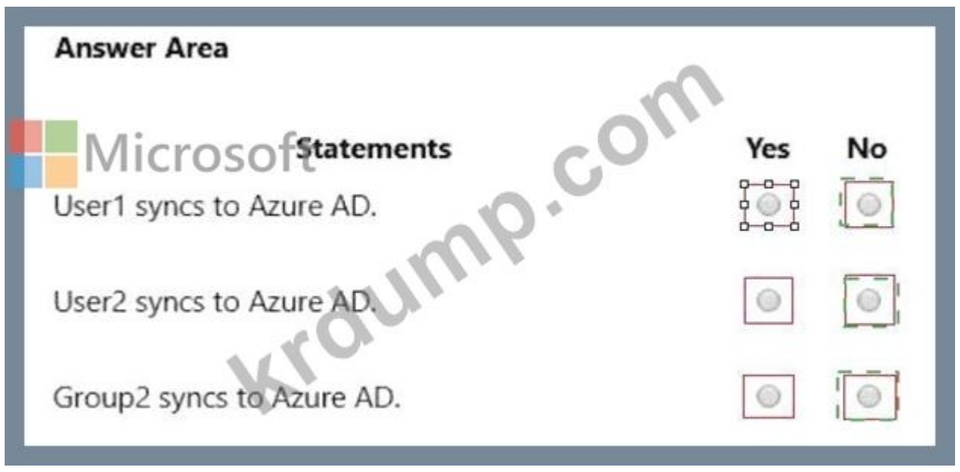
□□ □□□ □□ □□ □□□ □ □□□ □□□□□.

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

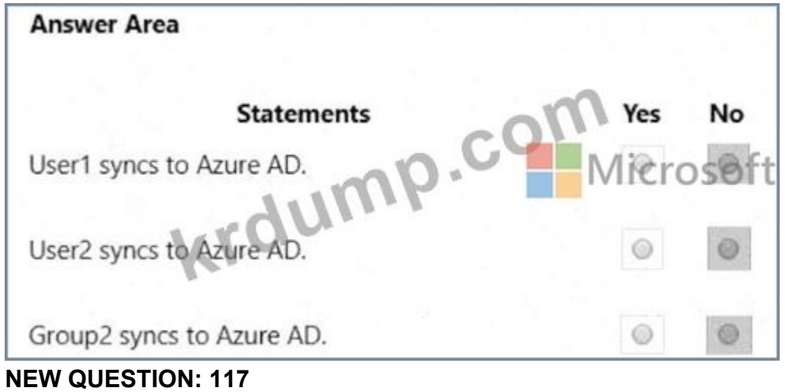
Answer Area



Answer:



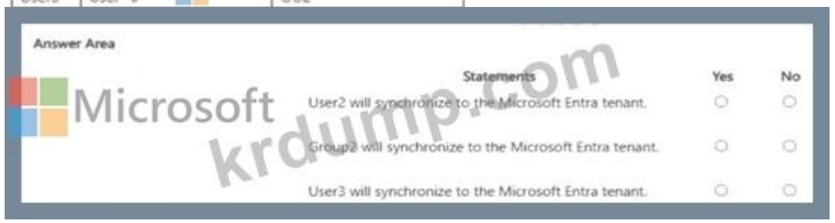
Explanation:



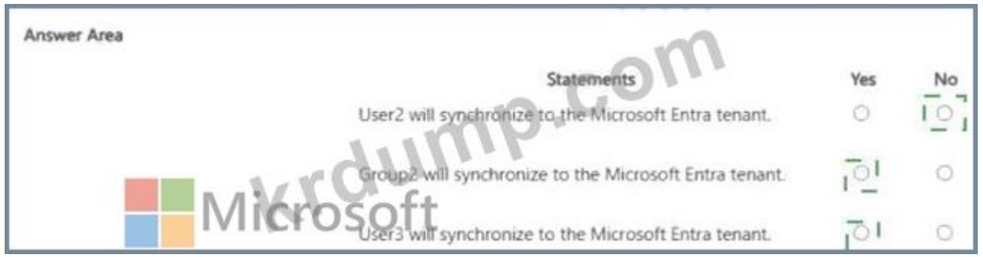
NEW QUESTION: 117

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

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



Answer:



Explanation:

NEW QUESTION: 118

Microsoft 365 E5 □□□□ □□□□.

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

Microsoft 365 □□ □□ □□□□ □□□ □□ □□□?

A. □□□ □□ □□(DSR) □□

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

C. EU GDPR □□ □□□□ □□□□ □□ □□

D. □□□ □□ □□ □□ □□□□ □□□□ □□ □□

Answer: C (LEAVE A REPLY)

Reference:

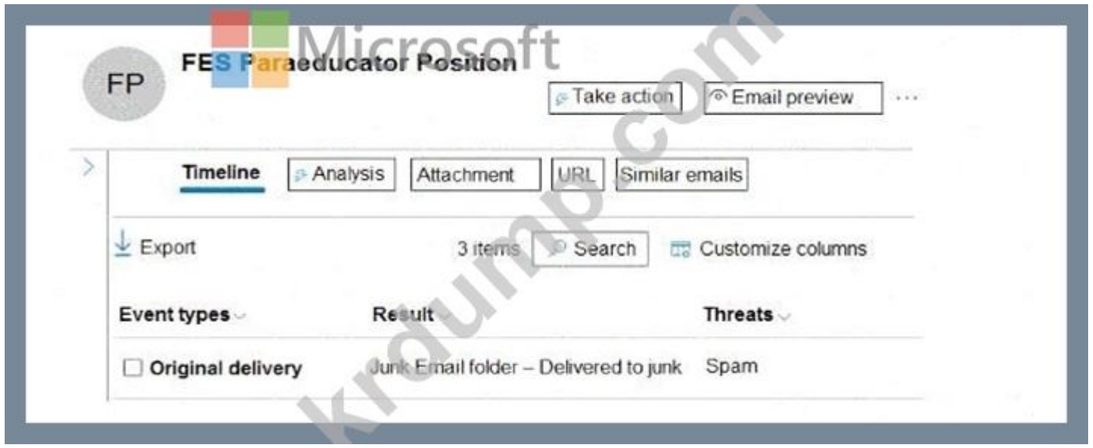
https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan

NEW QUESTION: 119

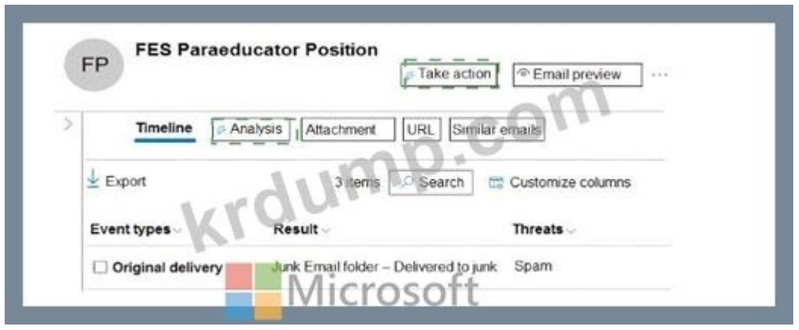
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

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

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



Answer:



Explanation:

1. Analysis 2. Take Action

NEW QUESTION: 120

Microsoft 365 □□□□ □□□□.

Endpoint Protection □□ □□ □□□□ □□□ □□□□□.

□□□□ □□□□ □□ □□□□ □□□ □ □□□?

A. □□□ □□□

B. □OS

C. iOS

D. □□□□□

Answer: B (LEAVE A REPLY)

Intune device configuration profiles can be applied to Windows 10 devices and macOS devices Note:

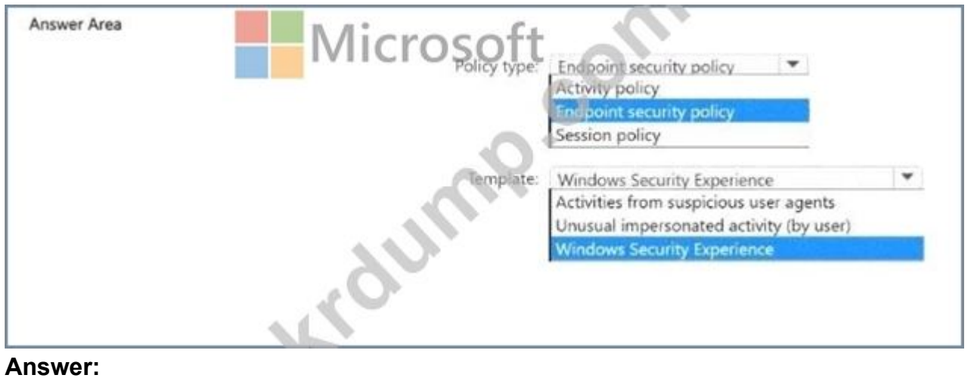
There are several versions of this question in the exam. The question has two possible correct answers:
Windows 10

macOS

Other incorrect answer options you may see on the exam include the following:
Android Enterprise
Windows 8.1
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

NEW QUESTION: 121
□□ □□ □□(MFA) □□□ □□□□ Microsoft 365 □□□ □□□□.
Microsoft Secure Score□ □□□□ □□ □□ □□□□ □□ □□ □□ □□□ □□□□□ □□□ □□ □□□ □□ □□□ □□□□ □□ □□□ □□ □□ □□□□□.
□□□ □□ □□ □□□□ □□□ □□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□□?
A. Microsoft Defender for Identity □□□ □□□□□.
B. □□ □□□ □□□□□.
C. □□□□□ □□□ □□□□□.
D. □□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 122
Microsoft 365 E5 □□□ □□ Microsoft Defender for Endpoint□ □□□□□. □□□□ Windows 11 □□□ □□□□ □□□□.
□□□ Windows Defender □□ □□□□ □□□□ □□ □□ □□□ □□ □□ □□□ □□□□□ □□ □□□□ □□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□, □□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:

Answer Area

Explanation:

Answer Area

NEW QUESTION: 123

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

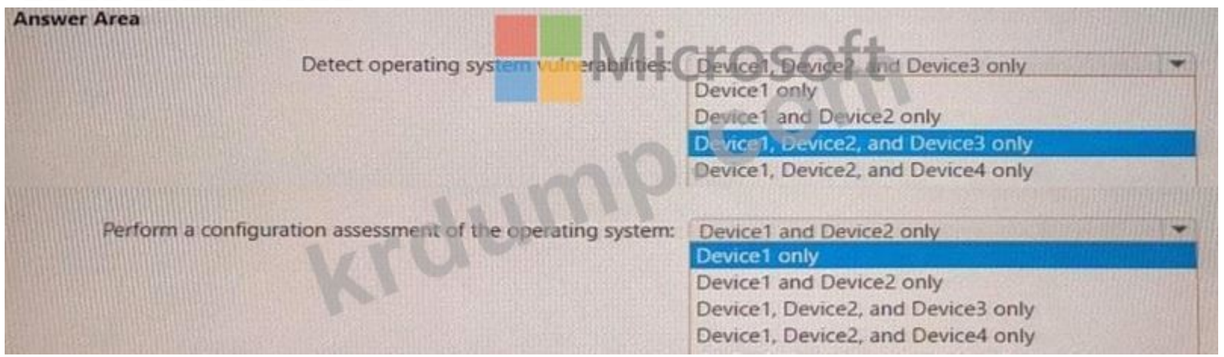
Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

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

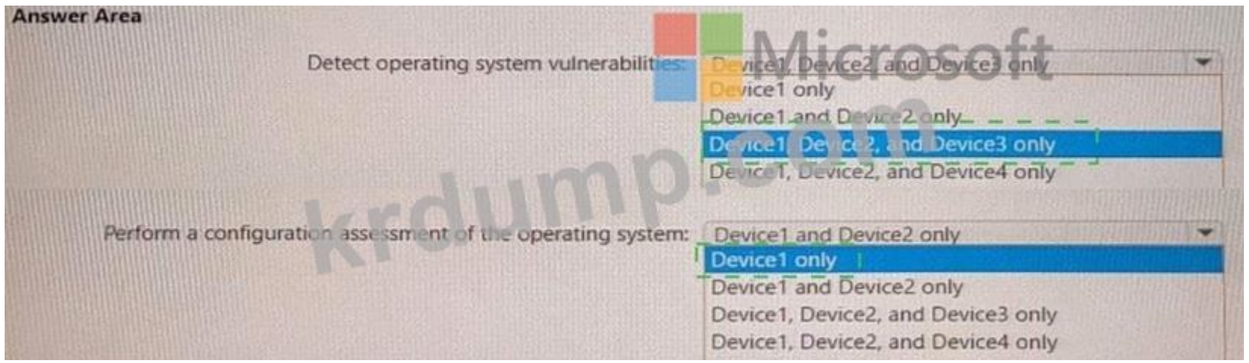
□□ □□ □□□ □□□□ □□ Microsoft Defender □□□ □□□ □□□ □□□□□.

* □□ □□ □□□□ □□□□□.

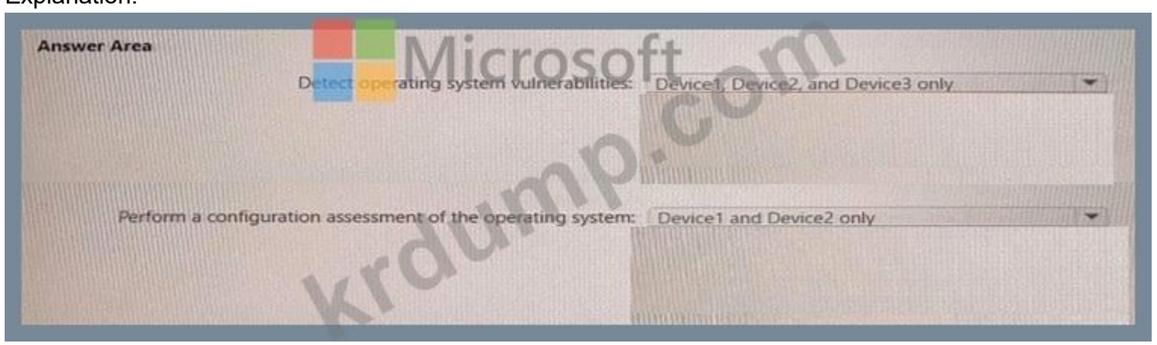
Answer Area



Answer:



Explanation:

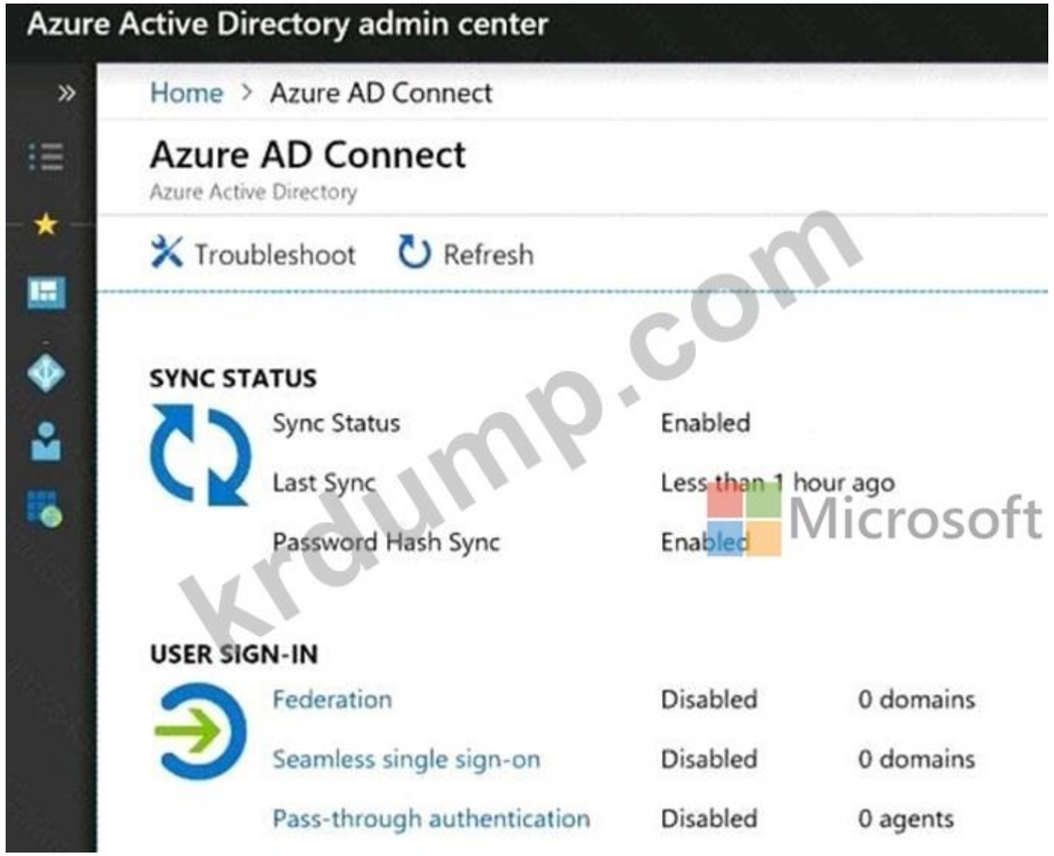


NEW QUESTION: 124

□□□

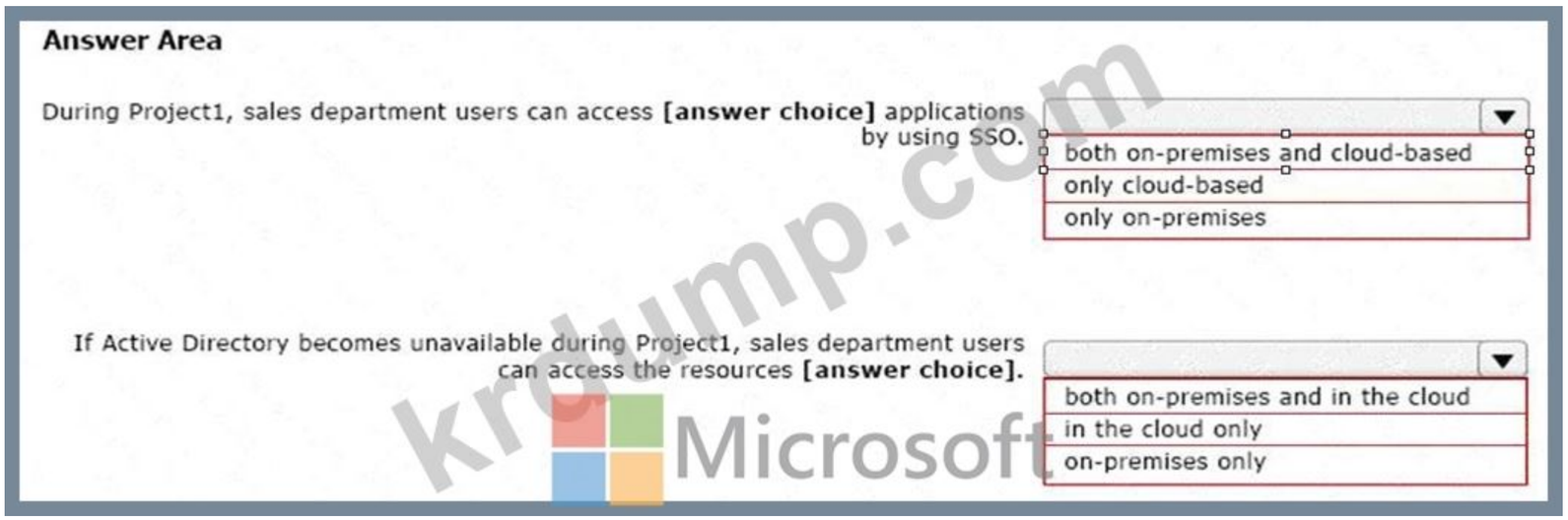
Microsoft 365 □□□□ □□□□□.

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

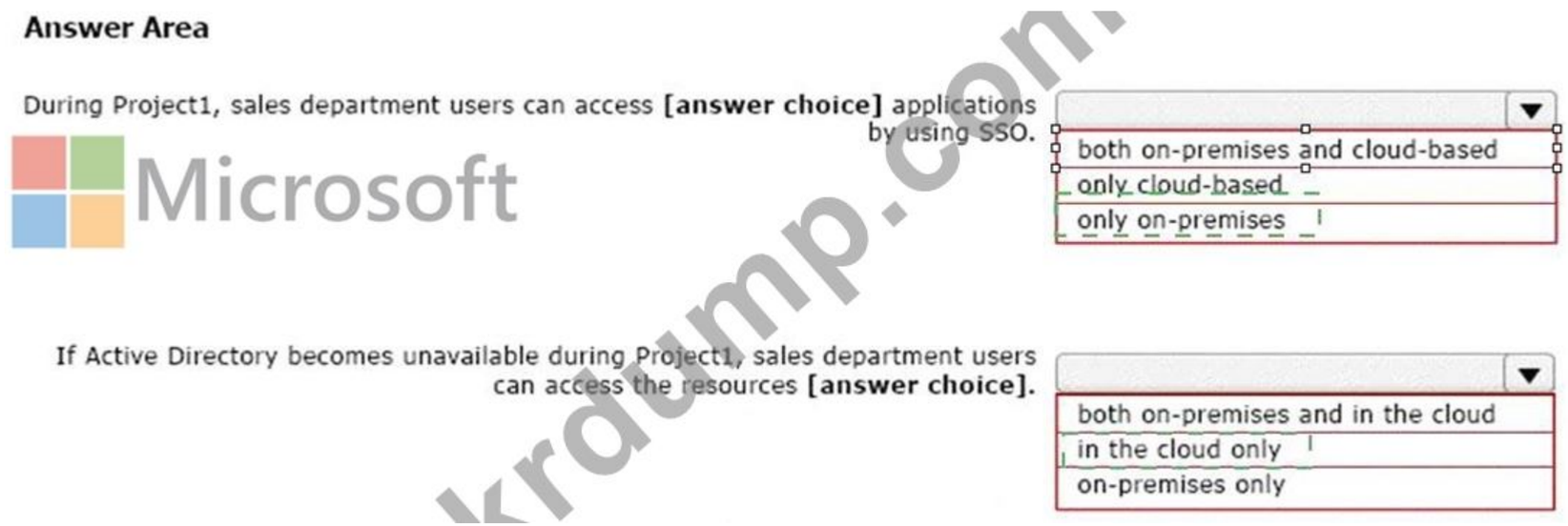

Azure Active Directory admin center
Home > Azure AD Connect
Azure AD Connect
Azure Active Directory
Troubleshoot
Refresh
SYNC STATUS
Sync Status
Enabled
Last Sync
Less than 1 hour ago
Password Hash Sync
Enabled
USER SIGN-IN
Federation
Disabled
0 domains
Seamless single sign-on
Disabled
0 domains
Pass-through authentication
Disabled
0 agents

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

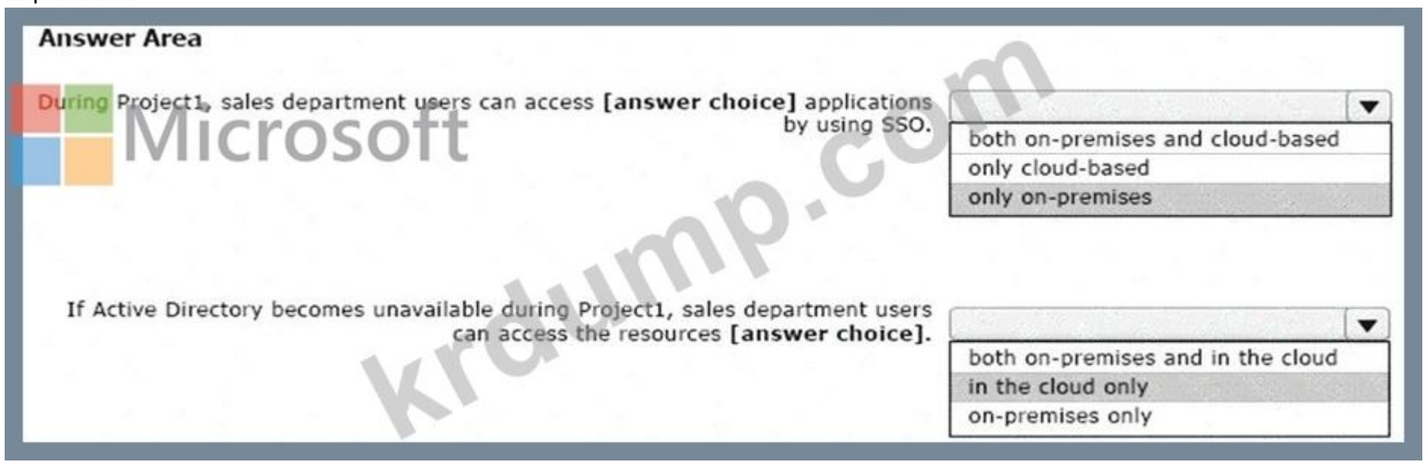
□□: □□ □□□ 1□□□□.


Answer Area
During Project1, sales department users can access [answer choice] applications by using SSO.
both on-premises and cloud-based
only cloud-based
only on-premises
If Active Directory becomes unavailable during Project1, sales department users can access the resources [answer choice].
both on-premises and in the cloud
in the cloud only
on-premises only

Answer:



Explanation:



Box 1: only on-premises

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

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

Box 2: in the cloud only

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 Microsoft Entra ID Premium P2 licenses.
The subscription contains a verified DNS domain named litware.com.
Microsoft Entra Connect Sync is installed and has the following configurations:
* Password hash synchronization is enabled.
* Synchronization is enabled for the UtwareAdmins OU only.
Users are assigned the roles shown in the following table.

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

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

* The principle of least privilege must be used.

NEW QUESTION: 125
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □ □ □□□ □□□□.
□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□, □□ □□□□ □□□□ □□□□.
□□□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft Entra □□□□ □□□□□.
□□ □□□□ □□□□ Microsoft Entra ID□ □□□□□□ □□□□□.
□□ □□(OU)□ □□ □□□ □□ 10□□ Microsoft Entra ID□ □□□□□ □□ □□ □□□□□□. □□□ □□□ □□□ □□ □□□□□ □□□□□□□□.
Microsoft Entra Connect □□□ □□□ □□ □□ □□□ □□ □□□□ □□□□□ □□□□□□ □□□□□□.
10□□ □□□ □□□ Microsoft Entra ID□ □□□□□□□ □□□□ □□□.
□□ □□: Microsoft Entra Connect Sync□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126
□□ □□ □□□ □□□ □□ □□ □□□ □□□□□.

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

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

Answer Area

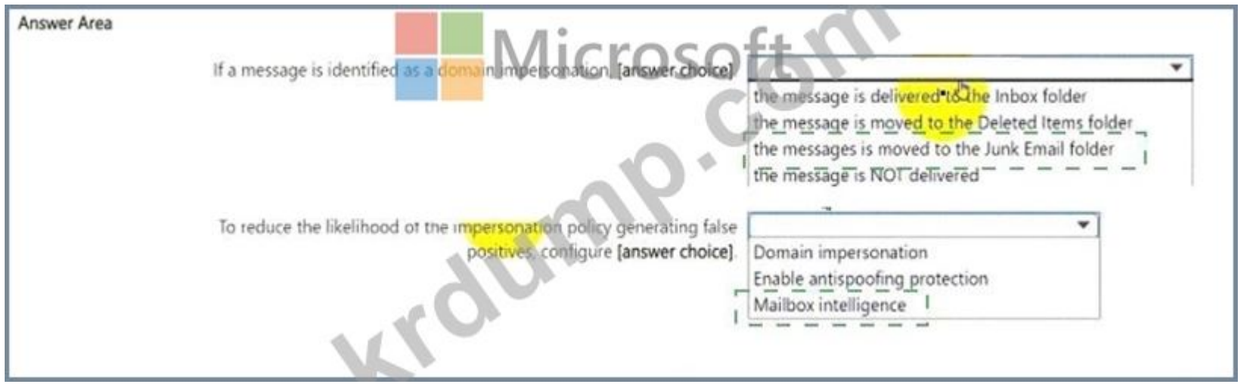
If a message is identified as a domain impersonation, **[answer choice]**.

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

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

- Domain impersonation
- Enable antispoofing protection
- Mailbox intelligence

Answer:



Explanation:

If a message is identified as a domain impersonation: the message is moved to the Junk Email 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: 127

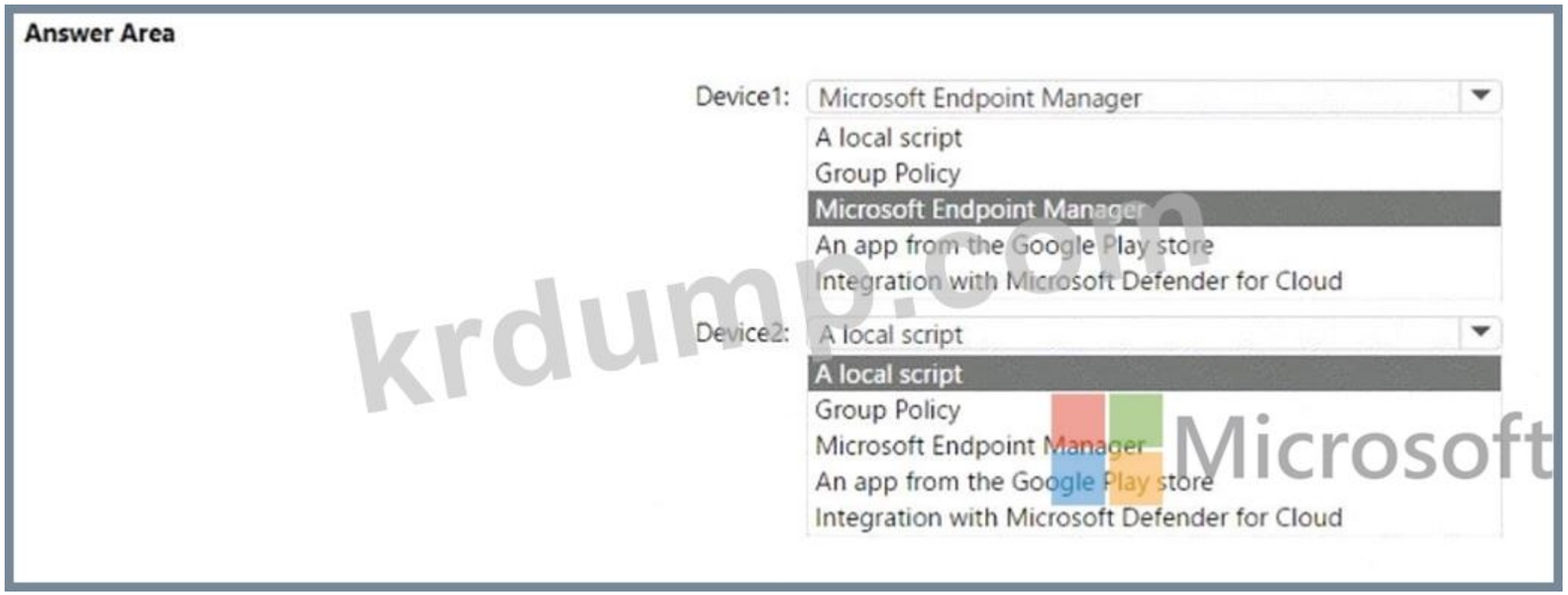
Microsoft Intune□ □□□□ □□ □□ □□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

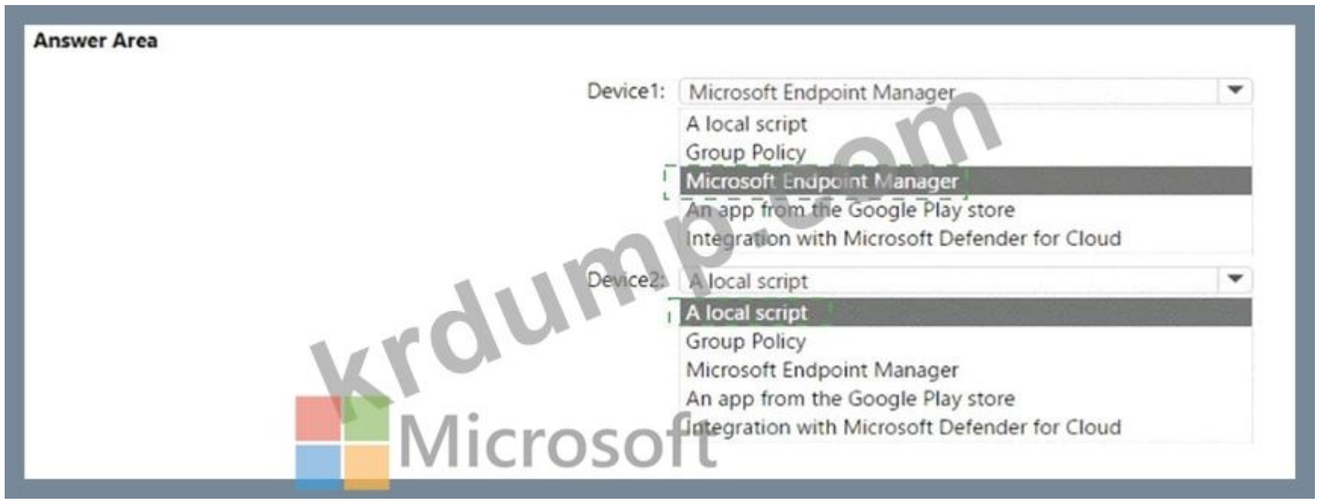
Device1□ Device2□ Microsoft Defender for Endpoint□ □□□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.



Answer:

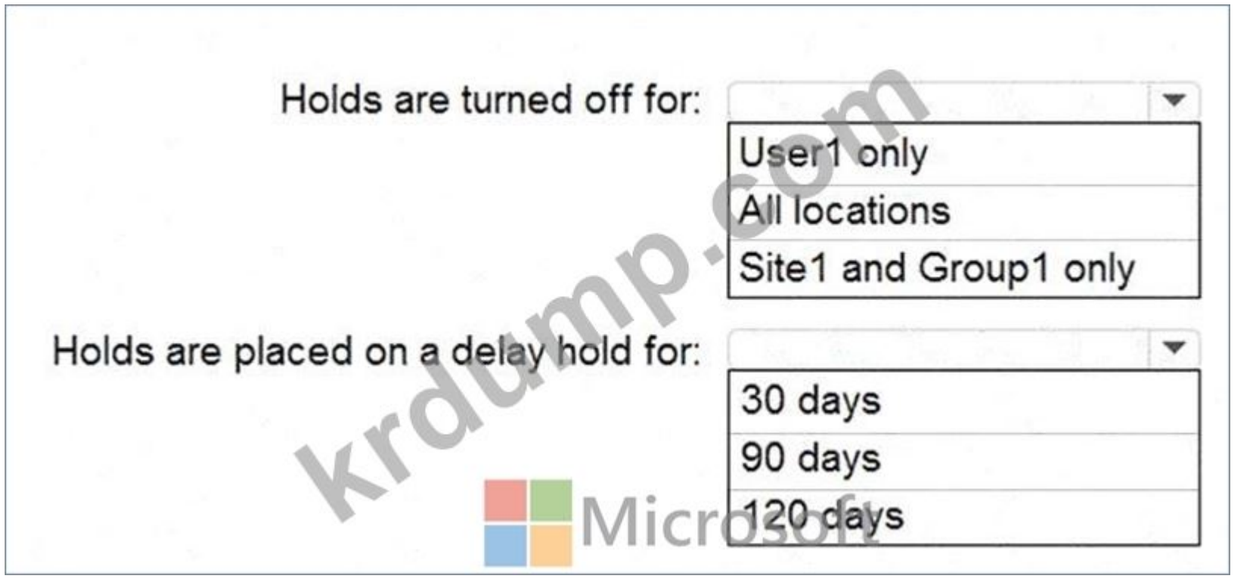


Explanation:

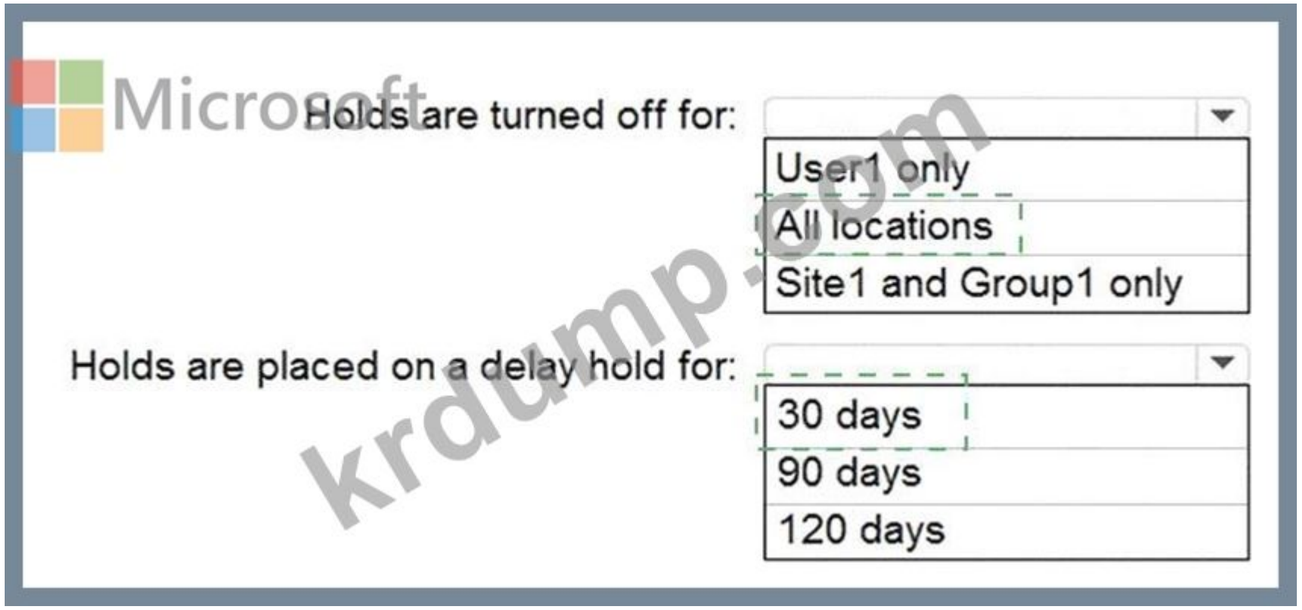
NEW QUESTION: 128

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

NEW QUESTION: 129
□□ □□ eDiscovery □□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□ : Case1
□□□ □□□: Group1, User1, Site1
□□ □□: Exchange □□□, SharePoint □□□, Exchange □□ □□ Case1□ □□ □□□ □□□□ □□□ □□□□.
Case1□ □□ □ □□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



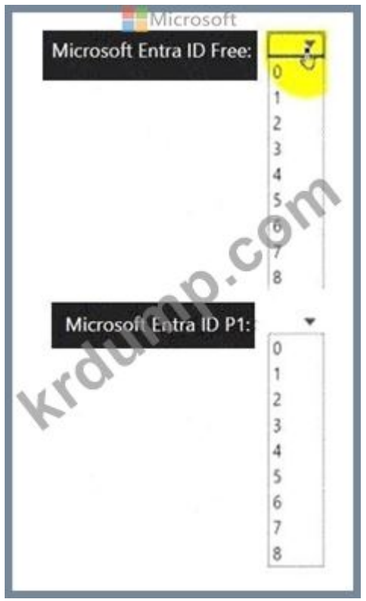
Explanation:

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

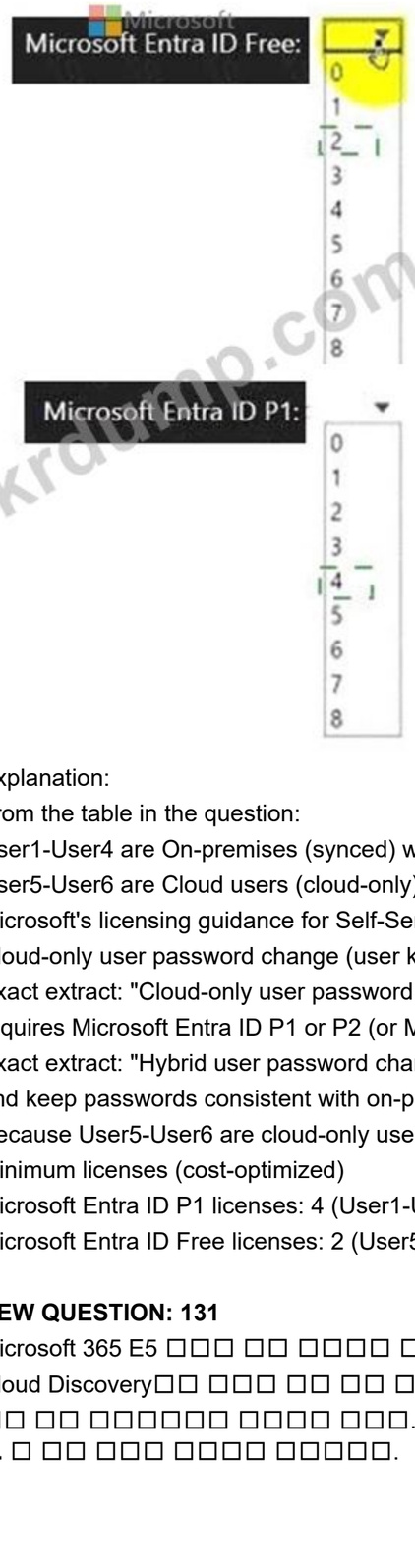
NEW QUESTION: 130
□□□□□□ □□□□□ Active Directory Domain Services(AD DS) □□□□ □□□□ □□□□.
□□□□ □□□□□ □□ □□ □□□□ □□□□ Microsoft Entra □□□□ □□□□. □□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

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



Answer:



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

NEW QUESTION: 131
Microsoft 365 E5 □□□ □□ □□□□ □□ Microsoft Defender□ □□□□ □□□□.
Cloud Discovery□□ □□□ □□ □□ □□ □□ □□□ □□□ □□□□□.
□□ □□ □□□□□□ □□□□ □□□. □□□□ □□□ □ □□□ □□□□ □ □□□□□ □□□ □ □□□ □□□.
A. □ □□ □□□ □□□□ □□□□□.

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

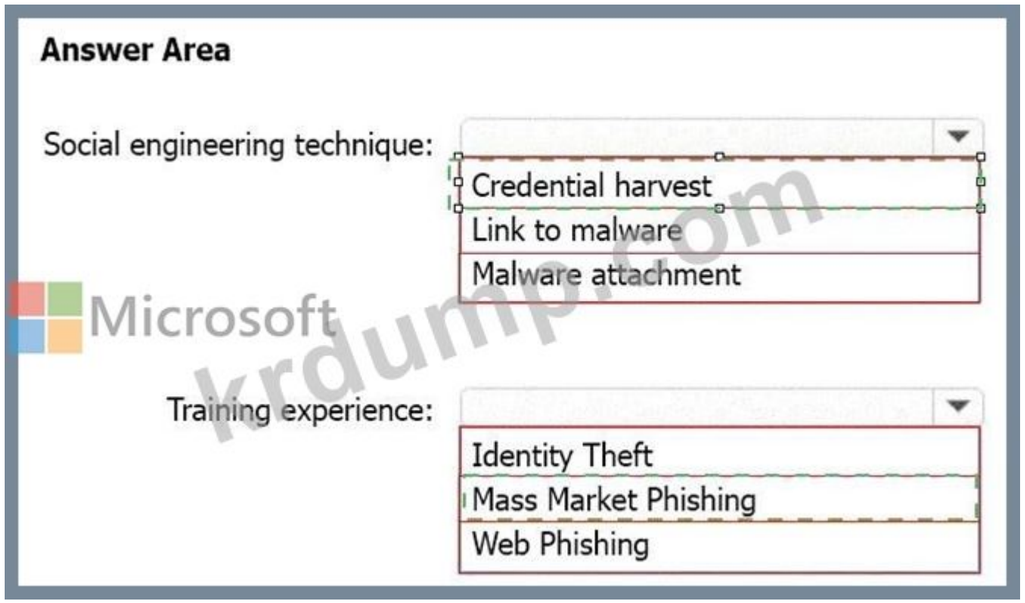
NEW QUESTION: 132
□□□
Microsoft 365 E3 □□□ □□□□.
□□ □□□□ □□□□ □□ □□□□□ □□□ □□□ □□□□□.
□□ □□ □□□□□ □□□ □□ □□□ □□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Social engineering technique:
- Credential harvest
- Link to malware
- Malware attachment

Training experience:
- Identity Theft
- Mass Market Phishing
- Web Phishing

Answer:



Explanation:

Box 1: Credential Harvest

Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select ' ISA Phishing ' or ' Mass Market Phishing ' training experiences. No other capabilities are part of the E3 trial offering.

Note: In Attack simulation training, multiple types of social engineering techniques are available:

Credential Harvest

Malware Attachment

Link to Malware

Etc.

Box 2: Mass Market Phishing

Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started

NEW QUESTION: 133
□□□ □□ □□ □□□ □□□□ □□□□ 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

Microsoft Entra Connect Sync□□ □□□ □□ □□□ □□□□.
□□□□ □□ □□□: □□□□
□□ □□: □□□□
□□□□□ Active Directory□ □□□ □□ □□□ □□□ □□ Microsoft Entra ID□ □□□□ □□□ □ □□ □□□□ □□□□ □□□.
□□ □□□□ □□□□ □□□?
A. □□
B. □□ □□ 1
C. User1□ User2□ □□
D. □□□1, □□□2, □□□3
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn¨

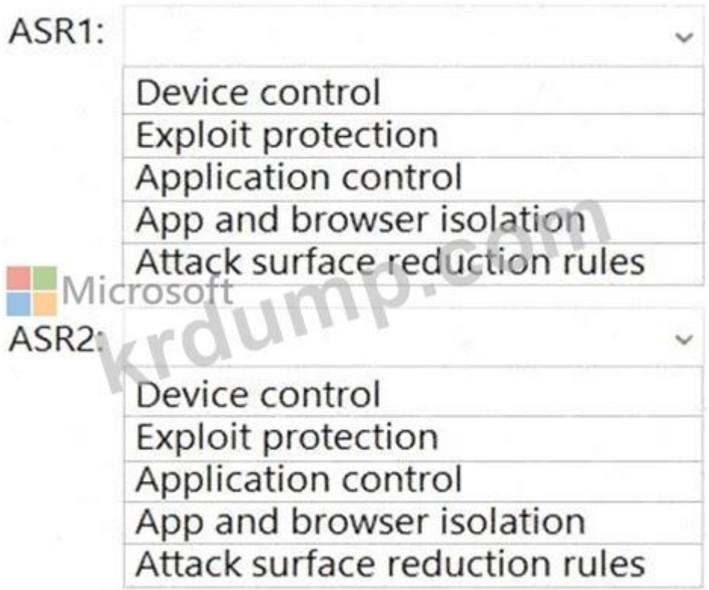
NEW QUESTION: 134
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □□ □□□ □□ Policy!□□ □□□□ □□□ □□□□.
* □□ □□□, □□ □ □□□□ □□□□□: User1
* □□ □□□ □□□: 3 - □ □□□
User1□ □□ □□ □□□ □□□ □□□□ □□□□.

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

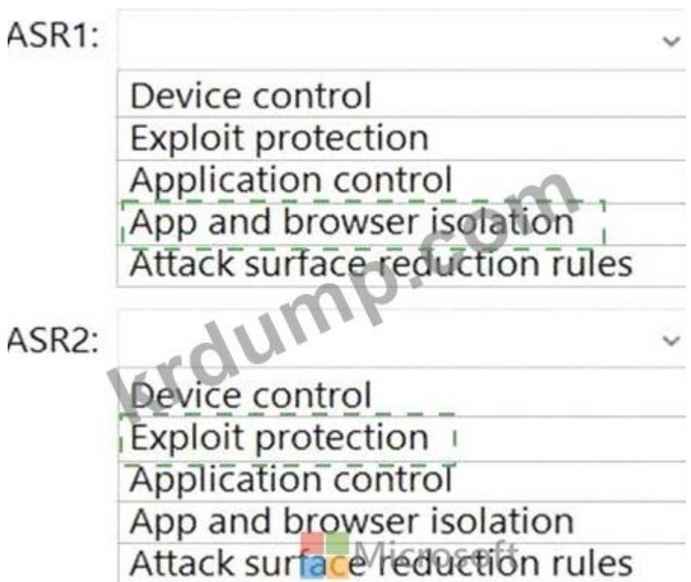
□□ □□□□ □□ □□□□□□?
A. Mail4□
B. Mail3 □ Mail4□ □□
C. Mail1, Mail2, Mail3, Mail4
D. Mail2, Mail3, Mail4□ □□

Answer: B (LEAVE A REPLY)

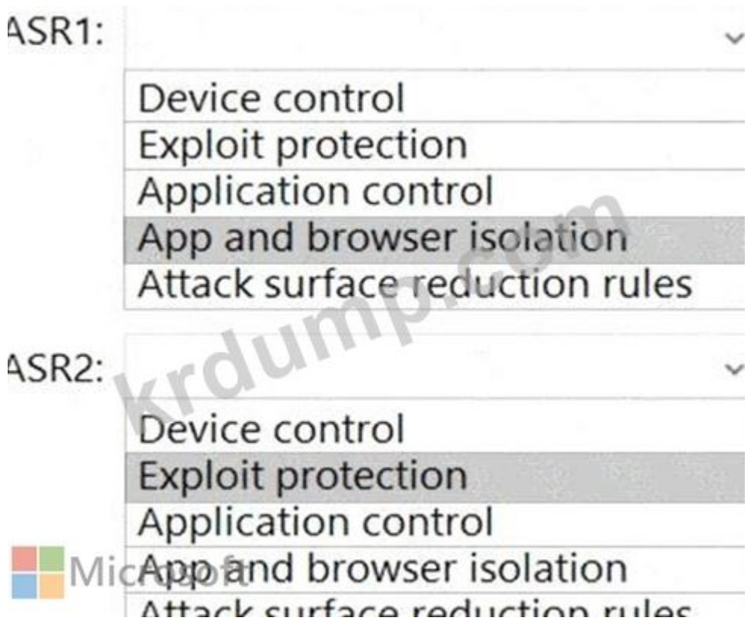
NEW QUESTION: 135
100□□ Windows 10 □□□□□ □□□□ Microsoft 365 □□□□ □□□□. □□□□□ Microsoft Endpoint Manager□ □□□□ □□□□□.
ASR1 □ ASR2□□ □ □□ □□ □□ □□(ASR) □□□ □□ □□□□□. ASR1□ Microsoft Defender Application Guard□ □□□□ □ □□□□□. ASR2□ Microsoft Defender SmartScreen□ □□□□ □ □□□□□.
□ □□□ □□ □□ ASR □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

NEW QUESTION: 136
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: 137
□□□ □□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ 1,000□□ Windows 10 □□□ □□□□.
10□□ □□□ □□□□□ □□ Microsoft Defender for Endpoint□ □□ □□(PoC) □□□ □□□□□. □□□ □□□□ □□ Microsoft Defender for Endpoint □□ □□□□ □□□ □□□□□ □□□□□.
□□ □□□ Microsoft Defender for Endpoint□ □□□□ □□□□□.
Microsoft Defender for Endpoint □□□□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. □□ □□□ □□□□□.
B. □□□□□ □□□□.
C. □□□ □□□ □□□□□.
D. □□□ □□□ □□□□ □□□□.
Answer: B (LEAVE A REPLY)
Storage locations
Understand where Defender for Cloud stores data and how you can work with your data:
* Machine information
- Stored in a Log Analytics workspace.
- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace

NEW QUESTION: 138
□□□□□□ □□□□□ Active Directory Domain Services(AD DS) □□□□ □□□□ □□□□.
□□□□ □□□□□ Microsoft 365 □□□ □□□□. □ □□□□ Microsoft Exchange Online□ □□□□ □□□□ □□ □□□ 500□□ □□□□ □□□□.
□□ □□ □□□ □□□□□ □□ □□□ □□ □□□(SSPR)□ □□□□ □□□.
* □□□□ □□ □□□□ SSPR□ □□□ □ □□□ □□□.
* □□□□□ □□□□ □□□□ □□□ □□□□ SSPR □□□ □□□ □ □□□ □□□.
□□ □□□□ □□□□ □□□ □□ □□□□□ □□□ □□□ □□□□□ □□□.
□ □□ □□□ □□ □□□□□ □□□□ □□□?

Answer:

Explanation:

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

Microsoft 365 Business Standard

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

Microsoft Entra ID P1

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

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

Therefore, Business Standard is enough for cloud-only users, while Entra ID P1 is the least-cost dedicated license for hybrid SSPR with writeback. Microsoft Entra ID P2 is unnecessary because risk-based identity protection features are not required.

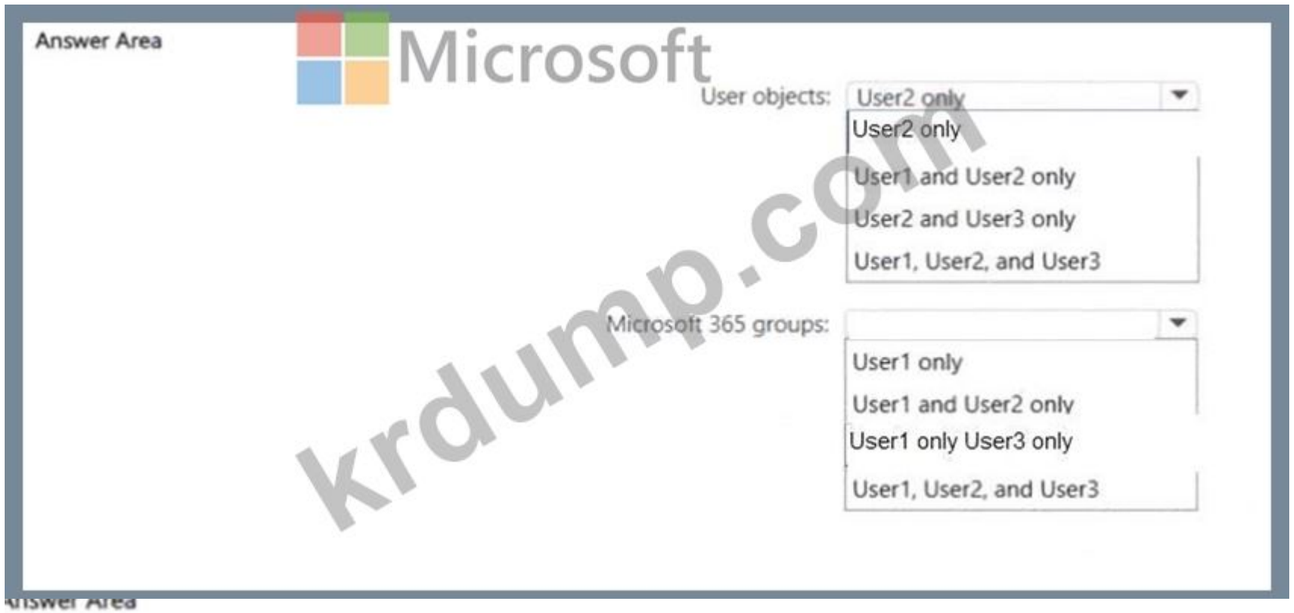
NEW QUESTION: 139

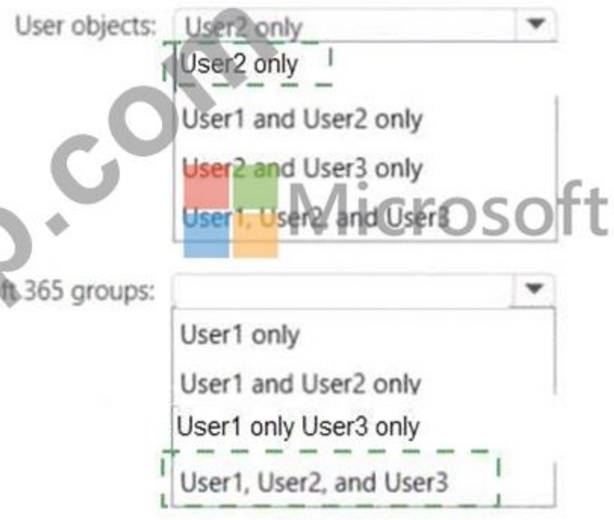
□□□ □□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

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

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

□□: □□ □□□ 1□□□□.





Explanation:

NEW QUESTION: 140

□□□

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.

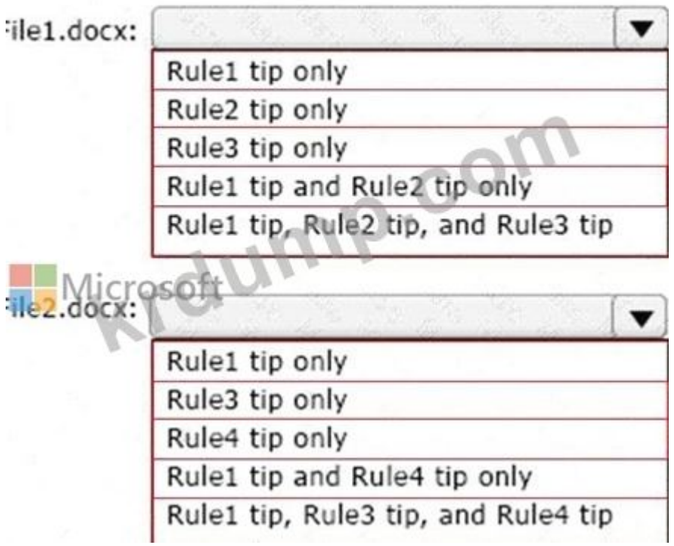
Site1□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

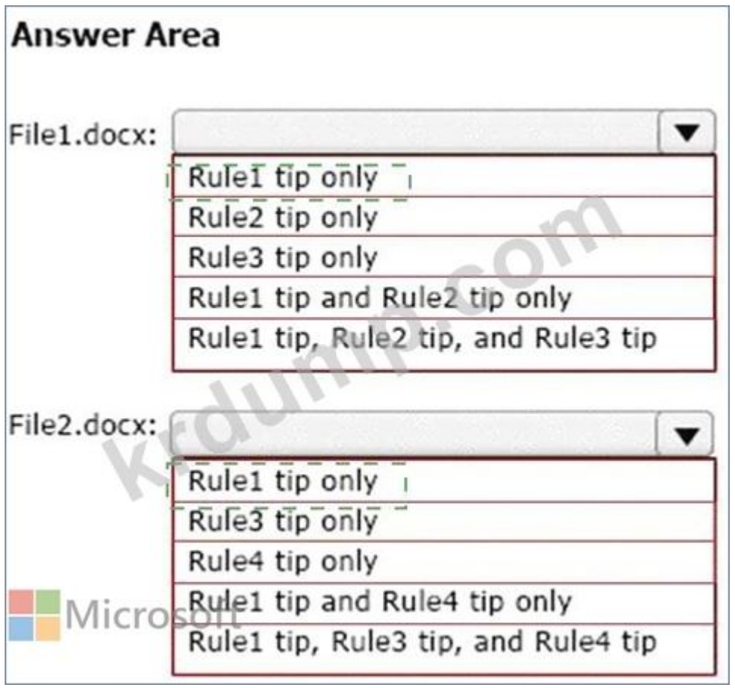
□ □□□ □□ □□ □□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

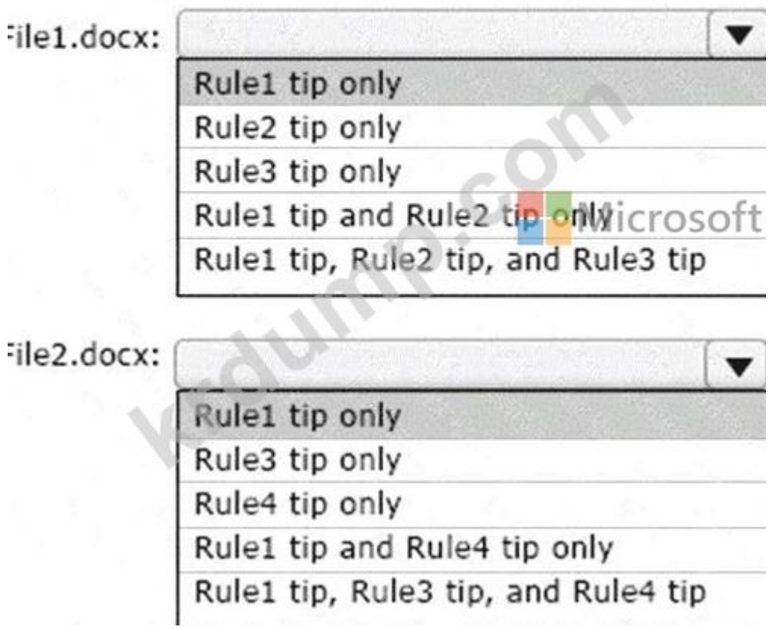


Answer:



Explanation:

Answer Area



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: 141

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

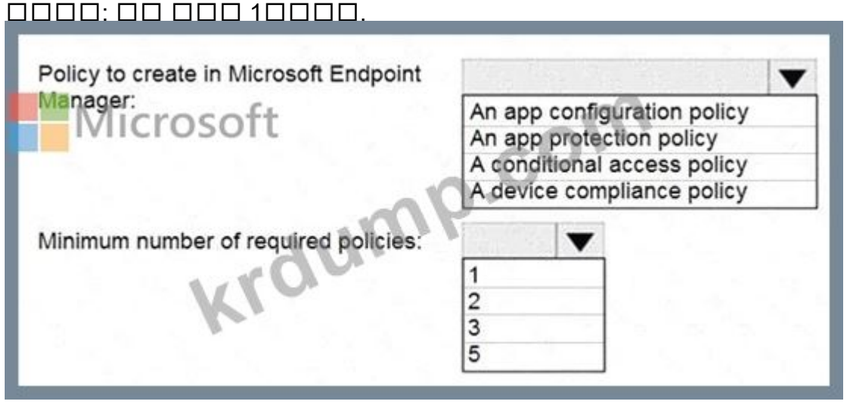
Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

□□ □□□□ App1□□□ □□ □□□□ □□□□.

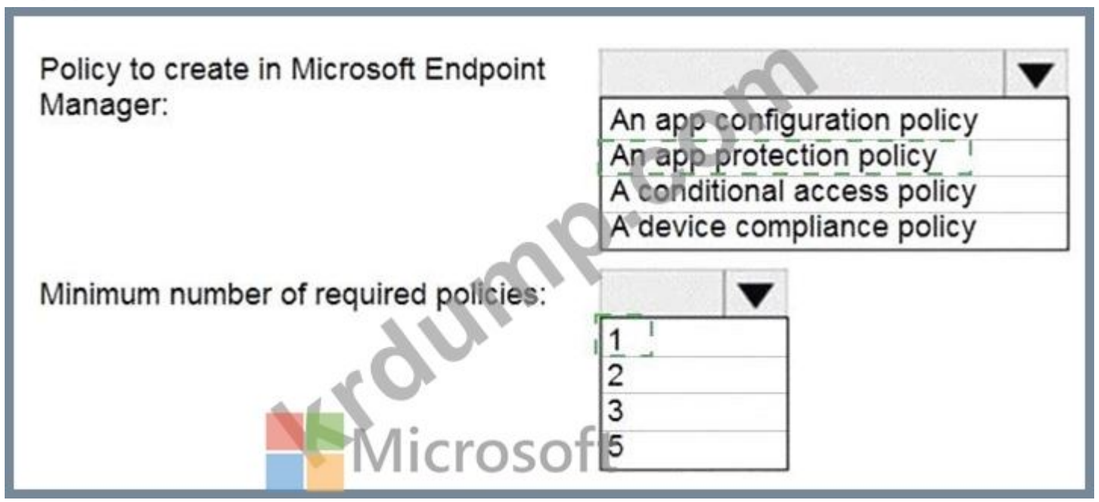
□□□□ App1□□ □□□□ □□□□ □□ □□ □□□□ □□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

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

NEW QUESTION: 142
Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□□□ □□□□ □□□ □□ □□□□ □□□ □ □□□ □ □□□□□.
□□ □□□ □□ □ □□□□ □□ □□□□ □□□□ □□□ □□□□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. □□□ □□ □□ □□□ □□□□□.
B. □□□ □□□ □□(EDM) □□□□ □□□□.
C. Sec-RegulacoryComplianceUI cmdlet□ □□□□□.
D. Sec-LabelPolicy cmdlet□ □□□□□.
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide

NEW QUESTION: 143
□□□□ □□□ □ □□□ □□□ OU□ □□ □□□ □□ □□□ □□□□□ Microsoft Entra Connect Sync□ □□□□ □□□.
□□□ □□ □□□?
A. PowerShell□□ start-ADSyncSyncCycle cmdlet□ □□□□□.
B. PowerShell□□ Add-ADSyncConnectorAttnbuteinclusion cmdlet□ □□□□□.
C. Microsoft Entra Connect □□□ □□□□□ □□□ □□ □□□ □□□ □□□□□.
D. Microsoft Entra Connect □□□ □□□□□ □□□□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 144
□□□ □□ □□□ □□□□□ □□ PII □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□□ □□□□ □□□ □□ □□(DLP) □□

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

NEW QUESTION: 145
AU1□ AU2□□ □ □□ □□ □□□ □□□ Microsoft 365 □□□ □□□□.
□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

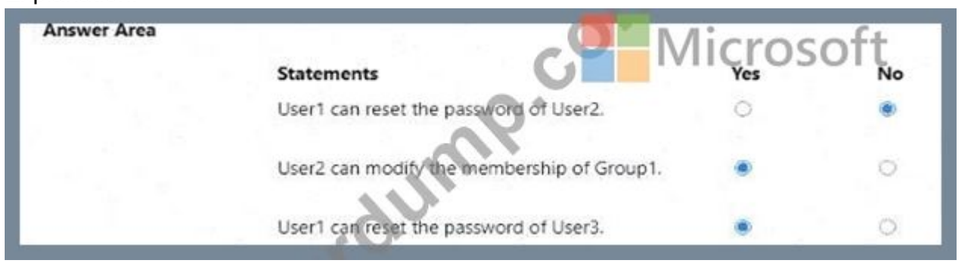
□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Members	Administrative unit
Group1	User3	AU2
Group2	User2 User3	AU1

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

Answer:

Explanation:



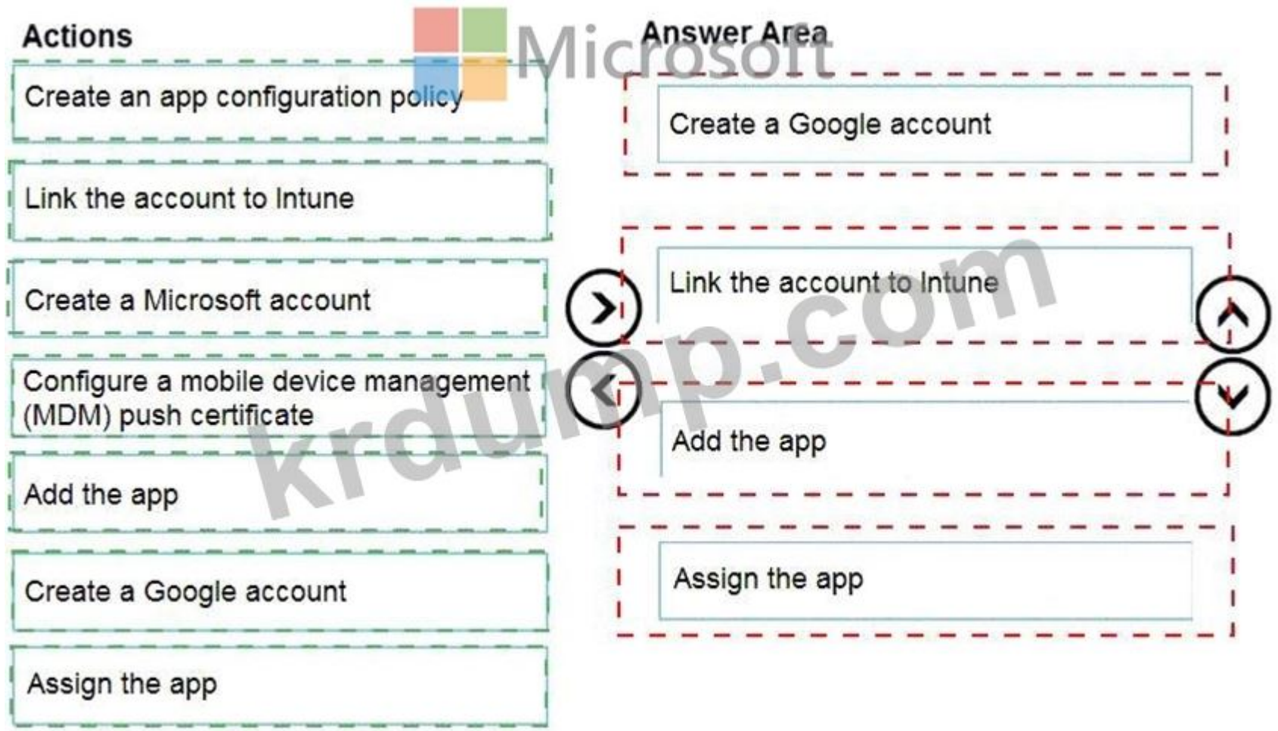
NEW QUESTION: 146

Microsoft Intune□ □□□ Android □□ 500□□ □□ Microsoft 365 E5 □□□□ □□□□.

□□□□ Google Play □□ □□□ □□□□□ Microsoft Endpoint Manager□ □□□□ □□□.

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

Answer:



Explanation:

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

NEW QUESTION: 147
□□ □□ □□□ □□□ □□□ 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: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/analytics/overview

NEW QUESTION: 148
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□□ □□□.
□□□□ □□□ □□□□ □□□□ □□□□□ □□□□ □□ □□□□ □□□□ □□□□ □ □□□ □□□.
□□□ □□□ □□ □□□□ □□□□ □□ □□□□ □□□□ □□□□□ □□□.
□□□□ □□ □□□ □□□□□ □ iOS □□□□ □□□□□ □□□□ □□□□ □□□.
□□ □□ □□□□ App1□□□ Microsoft Entra ID □□□□□□ □□□□□□□ □□□□ □ □□□ □□□. □□ □□ □□□□ App1□ □□□□ □ □□□ □□□□ □□□.
□□□ □□□ □□□ □□ □ □ □□ □□□□ □□□?
A. 3
B. 4
C. 5
D. 6
E. 7
F. 8
Answer: B (LEAVE A REPLY)
* Only users in the finance department must be able to sign in to an Microsoft Entra ID enterprise application named App1. All other users must be blocked from signing in to App1.
One Policy.
* Only users in the R & D department must be blocked from signing in from both Android and iOS devices.
One Policy.
* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.
All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.
One policy
* All users must be blocked from signing in from outside the United States and Canada.

Only users in the R & D department must be blocked from signing in from both Android One Policy Reference:
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

NEW QUESTION: 149
Endpoint Security□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□ □□□ □□ □□□ Endpoint Security Manager □□□ □□□□ □□□.
□□ □□□ □□□ □□□ □ □□□?
A. □□, □□ □□ □□, Microsoft 365 □ □□
B. Microsoft 365□ □□
C. □□ □□
D. □□ □□ □□ □ □□ □□
E. □□ □□ □□, Microsoft 365 □ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 150
User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
App1□□□ □□□□ □□ □□ □□□ □□□ □□□ □□□□ □□□□. App1□□ □□□ □□□ □ □□□ □□□□ □□□□.
User1□ App1□□ □□□□ □□ □□□□□ Microsoft Defender for Cloud Apps □□□ □□□□ □□□.
A. □□ □□
B. Cloud Discovery □□ □□ □□
C. □□ □□
D. OAuth □ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 151
□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.

Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	**None**	Purchaser	Group2
User3	**None**	Basic Purchaser	Group3

□□ □□□ □□□□□.
Microsoft Store for Business□□ □□ □□□□ □□□□□.
App1□□□ □□ □□ □□□□ □□□□□.
App1□ □□ □□□ □□□□ □□ □□□□ □□□ □□, Group3□ □□□□□.
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

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

NEW QUESTION: 152
Microsoft 365 E5 □□□ □□□□.
□□ □□□□ Mac □□□□ □□□ □□□□. □□ □□□□ Microsoft Endpoint Manager□ □□□□ □□□ Microsoft Defender Advanced Threat Protection(Microsoft Defender ATP)□ □□□□□ □□□□.
□□□□□ Microsoft Defender ATP□ □□□□ □□□.
Endpoint Management □□ □□□□ □□□ □□□□ □□□?
A. □□ □□ □□□

B. iOS □□□□ □□
C. Microsoft Defender ATP □□ □□□
D. □□□ □□ □□(MDM) □□ □□ □□□
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

NEW QUESTION: 153
□□ □□ □□ □□ □□□□ □□□ 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: 154
□□□ Microsoft 365 E5 □□□ □□□□ □□□ Office 365□ Microsoft Defender□ □□□□ □□□□.
□□ □□ □□□ □□□□ □□ □□□□□ □□ □□ □□□□ □□□□ □□□.
* □□□□ □□□□□ □□□□□ □□□ □□□ □□□ □□□ □□□□ □□□□□□□□.
* □□□ □□□ □□□ □□□ □□□□ □□□□□.
* □□□□ □□□ □□ □□ □□□ □□□□□.
Microsoft Defender □□□□ □□□ □□□□ □□□?
A. □□ □□□
B. □□ □□
C. □□ □□□□□ □□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 155
contoso.com□□□ □□□□ □□□ Microsoft 365 ES □□□ □□ □□, user1@contoso.com□□□ □□□□ □□ □□□ □□ □□□ □□□□ Policy1□□□ □ Microsoft Defender(□□ Office 365 □□ □□ □□)□ □□□□□.
Policy1□ usei1@fabunkam.com□□□ □□ □□□□□ □□ □□□ □□□□ □□□□□ □□ □□ □□□□□.
□□□□ □□□□□ □□□□□□ □□□□ □□□.
Policy1□ □□ □□□ □□ □□□?
A. □□□ □□□□□ □□□□ □□□□□
B. □□□ □□□ □□□□□□ □□□□□.
C. □□□ □□□□ □□□□□.
D. □□ □□□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 156
□□□ Contoso.com□□□ □□□ Microsoft Entra ID(Microsoft Entra ID) □□□□ □□□□ □□□□.
Contoso□□ ID □□□□□ □□ Microsoft Defender□ □□□□□.
□□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□ □□□ □□ □□□□ □□□ □□□□ □□□.
□□ □□: User3□□ ID □□ □□□ □□ Defender□ □□□□□ □□□□□.
□□□ □□□ □□□□□?
A. □

B. □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 157
3□□□ □ □□□□ □□□□ □□ □□ Microsoft□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

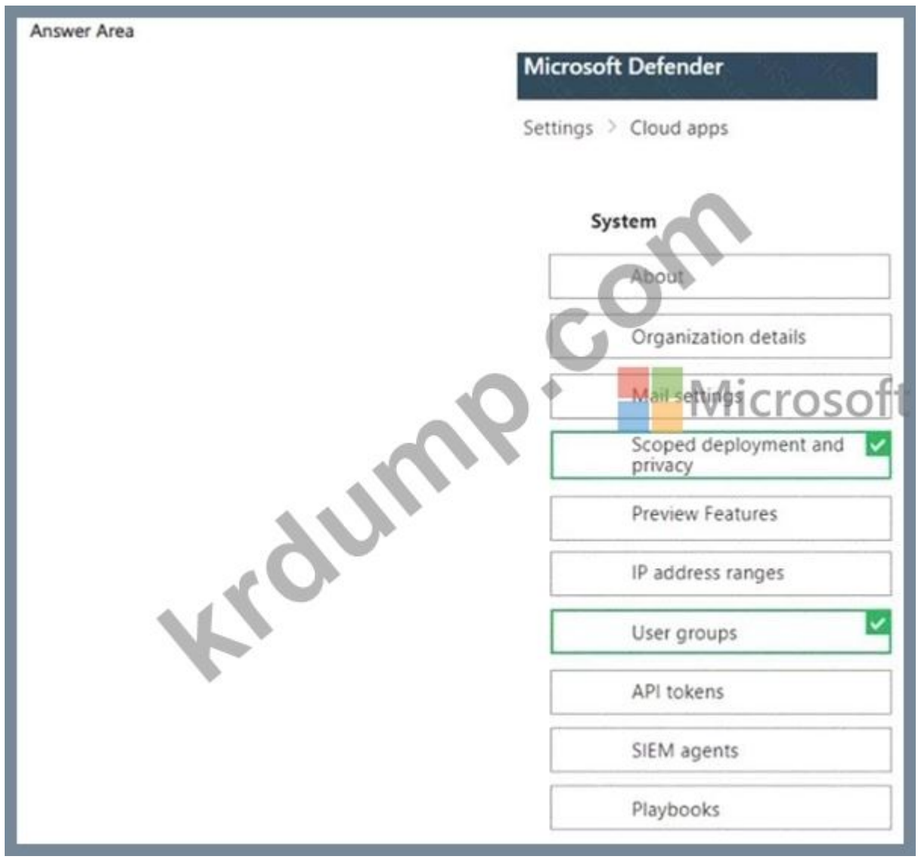
Explanation:

https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet March Feature Updates:
Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date References:
https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

NEW QUESTION: 158
□□□ User1□□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□ □□□□.
□□□ □□□ □□ □□ □□□ □□□□□.
User1□□ □□ □□ □□□ □□□□ □□□. '□□ □□□ □□ □□□ □□□'.
□□□ □□ □□ □□□?
A. □□ □□ □□□□□ □□ □□□□ □□□.
B. Microsoft Entra ID □□ □□□□ □□ □□□ □□ □□□(SSPR)□ □□□□□□.
C. Microsoft 365 □□ □□□□ □□ □□□ □□ □□□(SSPR) □□□ □□□□□.
D. Microsoft Entra ID □□ □□□□ 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

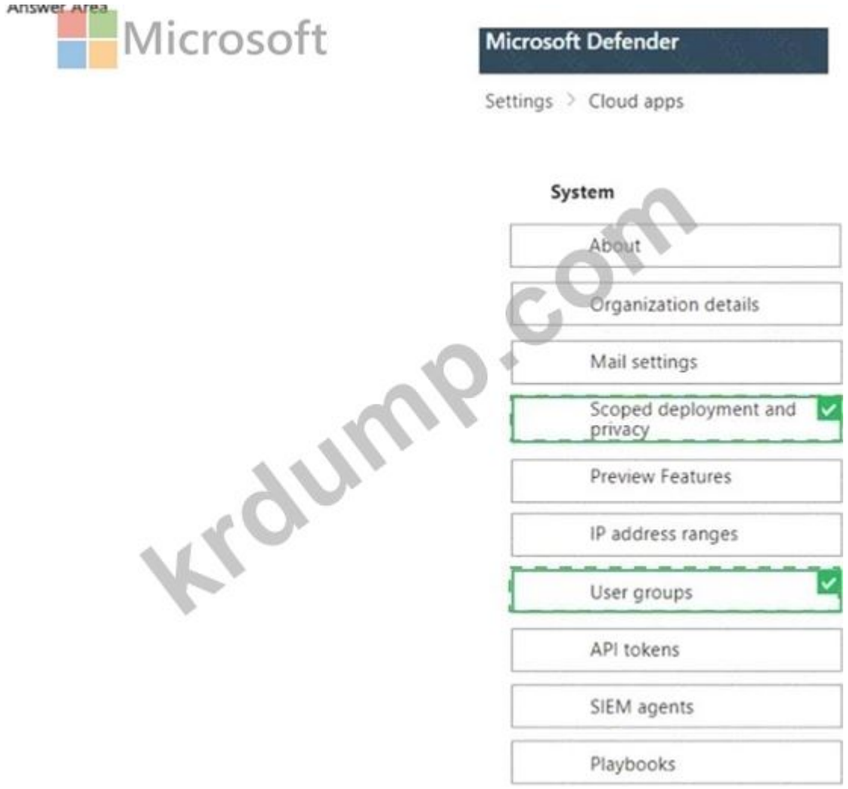
NEW QUESTION: 159
□□ □□ □□□ □□□□ User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
User1□ □□□ 1,000□□ □□□ □□□□ □□ □, □□□□ □□ □□□□ □□□ □□ □□□□□□ □□□□□. □□□ □□□□ □□□.
* User1□ □□□ □□□ □ □□ □□□□ □□□□□?
* User1□ □□□□ □□ □□□ □□ 2,000□□ □□□□ □□ □ □□□ □□□□ □□ □ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area



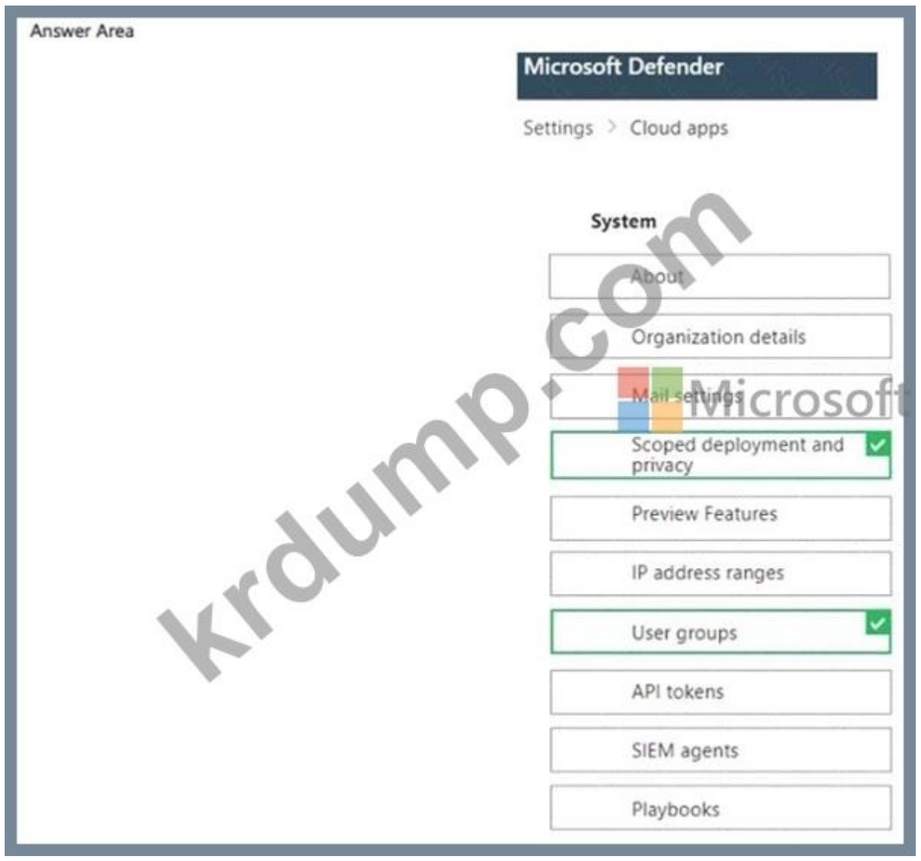
Answer:

Answer Area



Explanation:

Answer Area



NEW QUESTION: 160
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: 161
□□ □□ □□□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Home > sensitivity

Labels | Label policies | Auto-labeling (preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

+ Create a label | Publish labels | Refresh

Name ↑	Order	Created by	Last modified
Label1	0 - highest	Prvi	04/24/2020
Label2	1	Prvi	04/24/2020
Label3	0 - highest	Prvi	04/24/2020
Label4	0 - highest	Prvi	04/24/2020
Label5	5	Prvi	04/24/2020
Label6	0 - highest	Prvi	04/24/2020

□□□□ □□□□ □□ □□□ □□□ □ □□□?

A. Label1, Label2, Label5□

B. Label3, Label4, Label6□

C. Label1, Label3, Labe2, Label6□

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 162

□□□ □□□ □□□□ □□ □□□□.

□□□ Microsoft 365 □□□ □□□□ □□□□.

□□ □□ □□□ □□□□ Policy1□□□ □□□ □□□ □□□ □□□□ □□□.

* □□□□ FIDO2 □□ □, Windows Hello for Business □ □□□□ □□□□□ □□□.

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

Policy1□ □□□ □□□□ □□□?

Answer:

Explanation:

Setting

Correct selection

Authentication strength

Phishing-resistant MFA

Named location

IP ranges

The correct authentication strength is Phishing-resistant MFA . Microsoft Entra authentication strengths let administrators control which authentication methods satisfy a Conditional Access policy. The built-in phishing-resistant MFA strength is designed for methods such as FIDO2/passkeys , Windows Hello for Business , and certificate-based authentication , which matches the requirement exactly. Regular "Multifactor authentication" would allow broader MFA methods such as push notification, SMS, voice, or OTP, so it is too permissive. "Passwordless MFA" is also not exact because passwordless methods can include methods that are not necessarily the same phishing-resistant set required here.

The correct named location type is IP ranges . To mark a physical office such as London as trusted, you define the office's public egress IP addresses as a Conditional Access named location and mark that IP range as trusted. Microsoft's Conditional Access location guidance states that named locations can be created as countries/regions or IP ranges , and that when you select IP ranges, you can optionally Mark as trusted location .

Therefore, configure Policy1 with Phishing-resistant MFA and exclude a trusted named location created from the London office IP ranges .

NEW QUESTION: 163

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

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

Microsoft Entra Connect Sync□ □□□□ □□□ □□ □ □□ □□□ Azure □□□□(Microsoft Entra ID)□ □□□□□□. □□ □□ □□□□ □□□□□□ □□□□.

□□□ □□ □□□ □□□ □□□□□.

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

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

□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 164

Microsoft 365 □□□ □□□□.

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

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

D18912E1457D5D1DDCBD40AB3BF70D5D

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

A. □□□ □□ □□

B. □□□ □□□

C. □□ □□

D. □□ □□

Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 165

Microsoft 365 □□□ □□□□.

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

□□□ □□□□□ □□□□□□□□ □□□□ □□□□ □□□.
□□□ □□□ □ □□ □ □□ □□□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. Microsoft 365 □□ □□□□ □□□ □□ □□□□□ □□□□□.
B. Microsoft 365 □□ □□□□ □□□ □□ □□□□□ □□□□□.
C. Microsoft 365 □□ □□□□ □□ □□□□□ □□□□□.
D. Microsoft 365 □□□ □□□ agg□□ □□□□ □□□□□.
Answer: B,D (LEAVE A REPLY)
The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where Microsoft posts official messages with information including new and changed features, planned maintenance, or other important announcements.
The messages displayed in the Message center can also be viewed by using the Office 365 Admin mobile app.
Reference:
https://docs.microsoft.com/en-us/office365/admin/manage/message-center
https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app

NEW QUESTION: 166
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: 167
□□□
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

□□□ □□□ □□□ □□ □□ □□□ □□□□□.
* □□ □□: □□□□
* □□□□ : Group1

* □□ □□ : □□
* □□ □□□: 2023□ 3□ 15□
* □□ □□□: 2023□ 8□ 15□

Exchange □□□ □□□ □□ □□ □□□ □□□□□.

* □□ □□: □□□□
* □□□ □□ : Group2
* □□ □□ : □□
* □□ □□□: 2023□ 6□ 15□
* □□ □□□: 2023□ 10□ 15□

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

□□□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

Box 1: Yes
Admin1 is member of Group1.
The User Administrator role assignment has Group1 as a member.
The assignment type: Active
July 15, 2023 is with the assignment period.
A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.
Box 2: No
Admin2 is member of Group2.
The Exchange Administrator role assignment has Group2 as a member.
The assignment type: Eligible
June 20, 2023 is with the assignment period.
The assignment must be approved.
Note: Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.
Box 3: Yes
Admin3 is member of Gropu1 and Group2.
The User Administrator role assignment has Group1 as a member.
The assignment type: Active
May 1, 2023 is with the assignment period.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-assign-member-owner

NEW QUESTION: 168
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 Area

Statements	Yes	No
Defender for Endpoint blocks access to IP address 20.30.40.50 from Device1.	○	○
Defender for Endpoint blocks access to IP address 2.23.10.15 from Computer2.	○	○
Defender for Endpoint blocks access to IP address 131.107.10.50 from Device3.	○	○

Answer:

Answer Area

Statements	Yes	No
Defender for Endpoint blocks access to IP address 20.30.40.50 from Device1.	○	○
Defender for Endpoint blocks access to IP address 2.23.10.15 from Computer2.	○	○
Defender for Endpoint blocks access to IP address 131.107.10.50 from Device3.	○	○

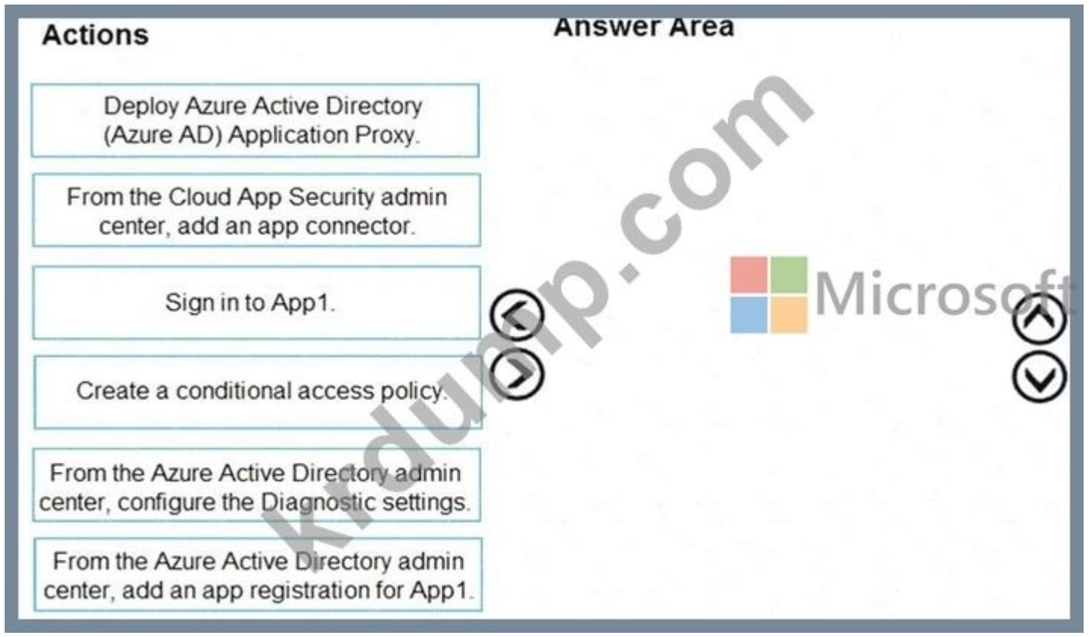
Explanation:

Answer Area

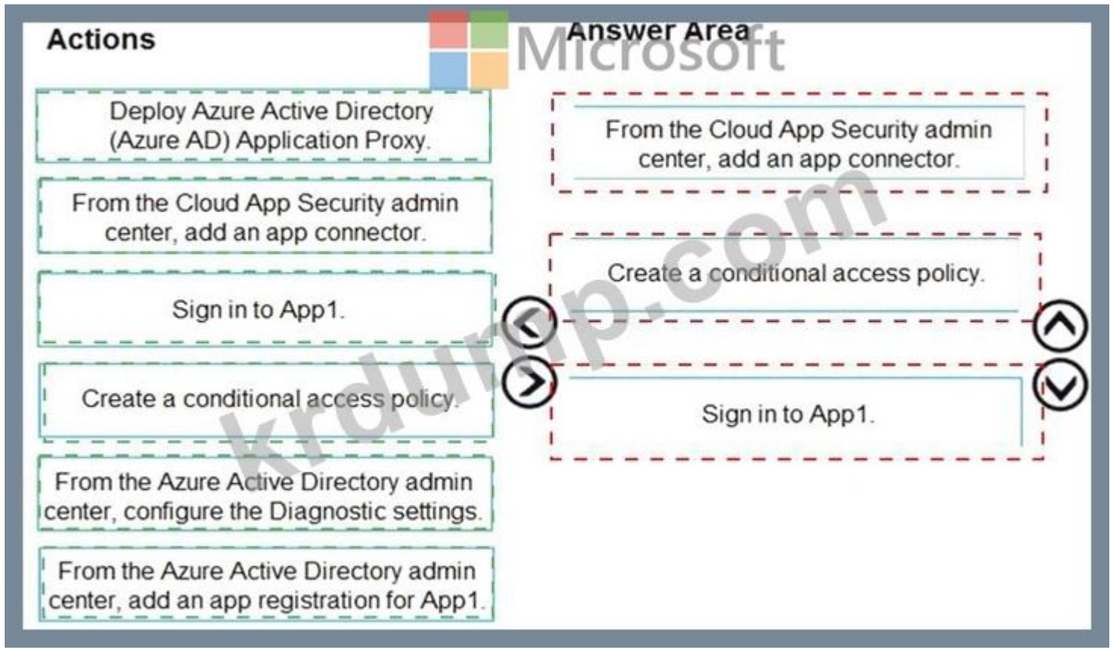
Statements	Yes	No
Defender for Endpoint blocks access to IP address 20.30.40.50 from Device1.	●	○
Defender for Endpoint blocks access to IP address 2.23.10.15 from Computer2.	○	●
Defender for Endpoint blocks access to IP address 131.107.10.50 from Device3.	○	●

NEW QUESTION: 169

□□□ App1□□□ □□□□ □□ □□□□□□.
App1□□ □□□□□ □□□□ □□ Microsoft Cloud App Security□ □□□ □ □□□ □□□□ □□□. App1□ □□ □□□ □□□□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□□.



Answer:



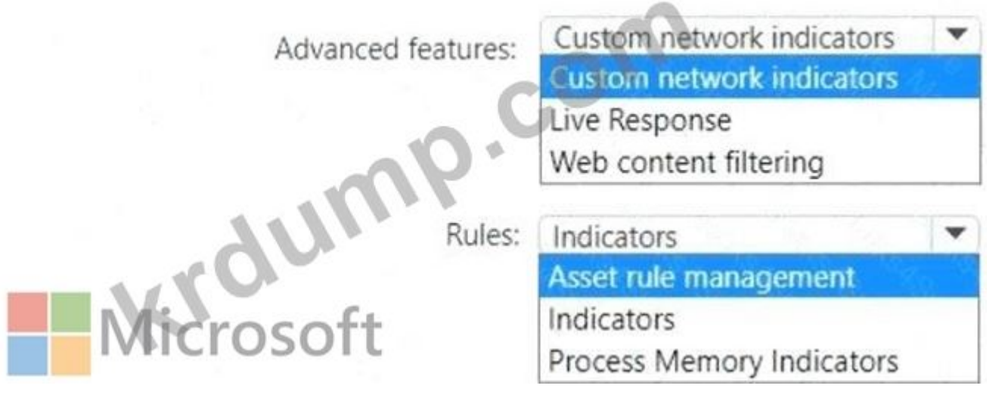
Explanation:

Reference:
https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security

NEW QUESTION: 170
□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□. □ □□□□□ Windows 10□ □□□□ □□□ 2,000□□ □□□□ □□□□.
Microsoft 365 □□□ □□□□□.
□□ □□ □□□ □ Microsoft Entra ID Seamless Single Sign-On(Seamless SSO)□ □□□□□.
Windows 10 □□□□□ □□□□ Seamless SSO□ □□□ □ □□□ □□ □□□.
□□□ □□ □□□?
A. □□ □□□ □□□□ □□□□ □□ □□□ □□□□□.
B. Microsoft Entra ID□□ □□□ □□□ □□□ □□□□□.
C. Microsoft Entra Connect Sync □□□□ □□□ □□□□□.
D. □□□□ Microsoft Entra ID□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 171
Device1□□□ Windows 11 □□□ □□□ Microsoft 365 E5 □□□ □□□□.
Device1□ Microsoft Defender for Endpoint□ □□□□□□□.
Device1□ IP □□ 131.107.10.15□ □□□□ □□ □□□□ □□□.
Microsoft Defender □□□□□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Explanation:

NEW QUESTION: 172

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

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

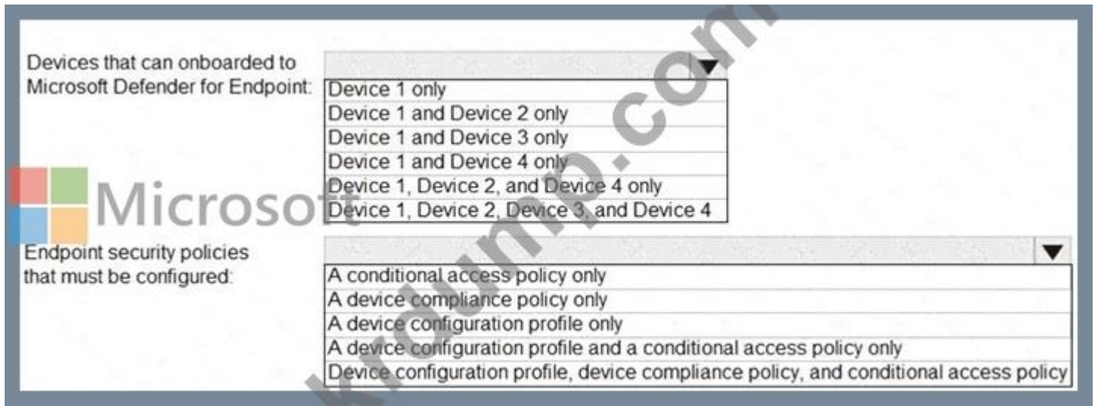
Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

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

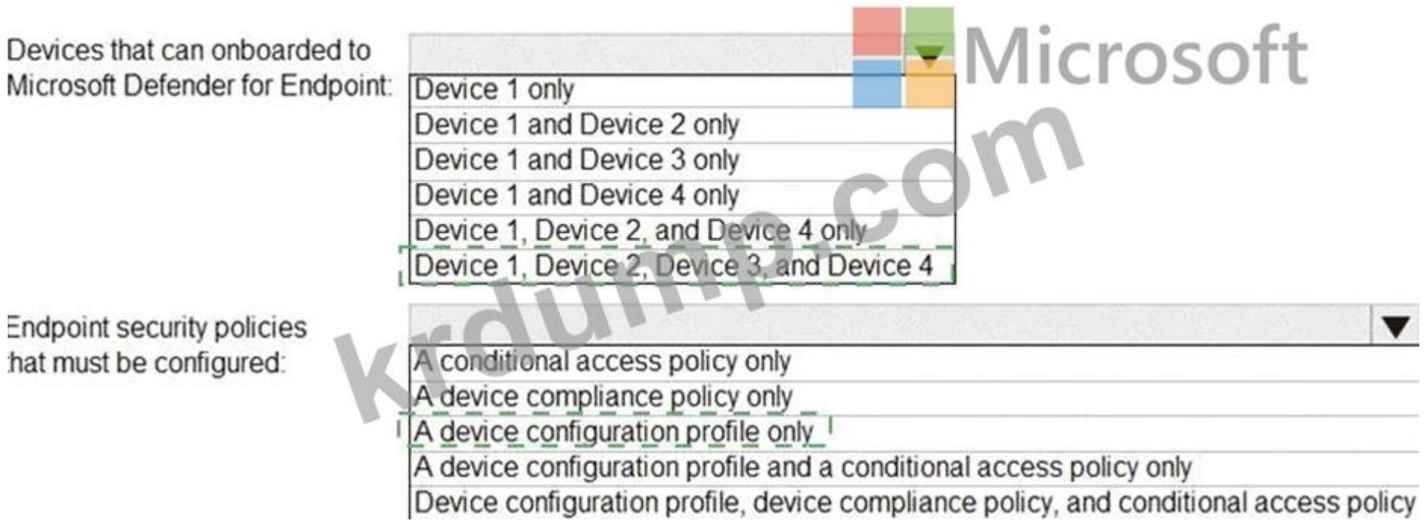
□□ □□□ Microsoft Defender for Endpoint□ □□□□ □ □□□, □□□ □□ Endpoint □□ □□□ □□□□ □□□ □□□□ □□□.

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

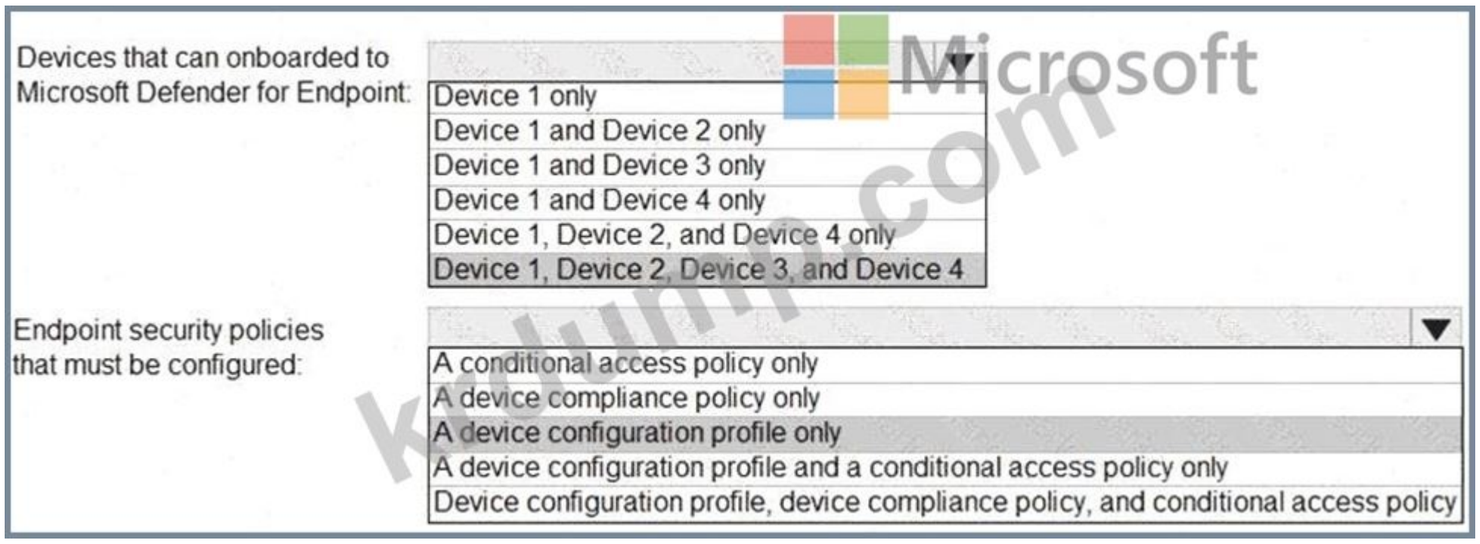
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

NEW QUESTION: 173
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□□□ User1□□□ □□□ □ □□□□ □□□□□.
□□□□ User1□ □□□□ □□□□□ □□□ □□ □□□ □□□□□.
* □□ IP □□□□ Microsoft Exchange Online□ □□□□□□.
* □□□□ □□ □□□□ Microsoft SharePoint Online□ □□□□□□.
* □□□□ □□□ □□ □□□□ □□ □□□□ □□□ □□□ □□, □□ □□ □□□□ □□□ □□ SharePoint Online□ □□□□□□. Microsoft Entra ID Protection□ User1□ □□ □□ □□□ □□□ □□□ □□□ □□?
A. □□ IP □□, □□□□□ □□ □□ □ □□□□ □□ □□□ □□
B. □□ IP □□ □ □□□ □□
C. □□□□ □□ □□□ □□ □ □□□ □□□ □□
D. □□ IP □□ □ □□□□ □□ □□□ □□□ □□
E. □□ IP □□□ □□
Answer: E (LEAVE A REPLY)

NEW QUESTION: 174
□□□ contoso.com□□□ Microsoft Entra □□□□ □□□□ Microsoft 365 □□□ □□□□ □□□□. □□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

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

Answer:

Explanation:

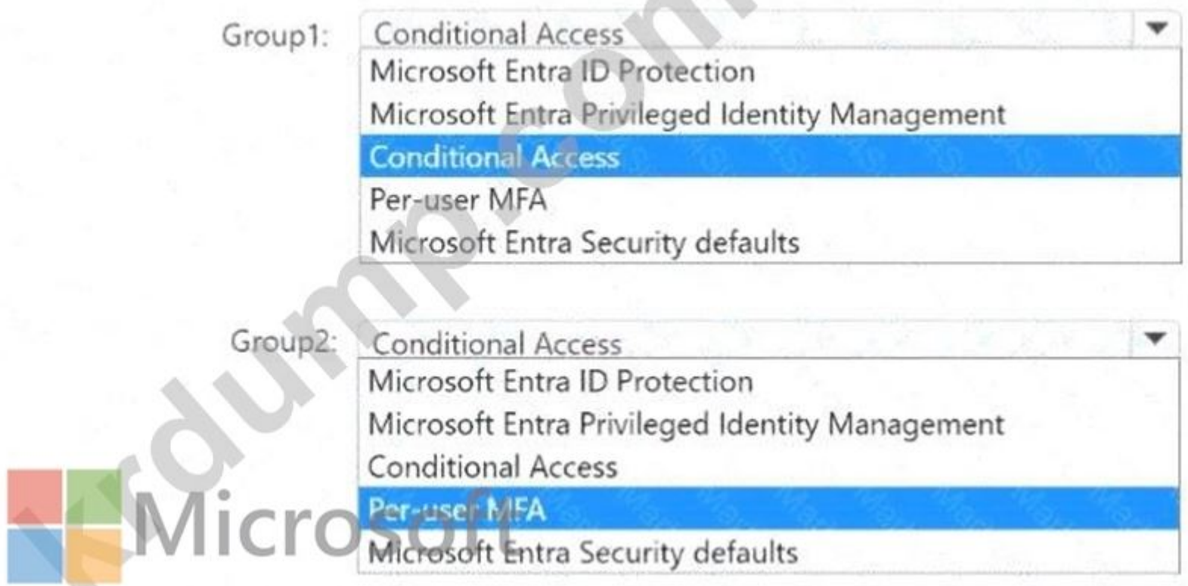
NEW QUESTION: 175
Microsoft Defender for Endpoint□ □□□□ Microsoft 365 E5 □□□ □□□□.
Endpoint□ Microsoft Defender□□ □□ □□ □□ □□ □□ □□□ □□□.
□□□□ File1.exe□□ □□□ □□□□□□ □□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□
B. □□ □□ □□□
C. □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 176
□□□□□□ □□□□□ Active Directory Domain Services(AD DS) □□□□ □□□□. □ □□□□□ 2,000□□ □□□ □□□ □□□□.
□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□□□ Microsoft Entra □□□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□□ □□□□□□.
□□ □□ □□□ □□□□□□□.
□□□ □□□ □□□□□□.
□□□ □□□□ □□□?
A. □□□ □□□□ □□□□□ □□□(AD FS)
B. Microsoft Entra □□□□ □□□
C. Microsoft Entra Connect □□□
D. □□ □□
Answer: B (LEAVE A REPLY)
Microsoft Entra Cloud Sync is the correct choice because the requirement is directory synchronization with the least infrastructure, least administrative overhead, and reduced single points of failure. Microsoft describes Entra Cloud Sync as a cloud-managed hybrid identity synchronization service for synchronizing users, groups, and contacts between Active Directory and Microsoft Entra ID, using a lightweight agent-based model. Microsoft also positions Cloud Sync as its strategic direction for hybrid identity synchronization.
For resilience, Cloud Sync supports multiple active provisioning agents. Microsoft states that high availability is achieved by having multiple active agents installed and running, so synchronization can continue if one agent fails, and Microsoft recommends three active agents for high availability. This directly satisfies
"minimize single points of failure."
Microsoft Entra Connect Sync can synchronize AD DS to Entra ID, but it requires a more substantial dedicated synchronization server design and more operational management. Microsoft's migration guidance notes that

Cloud Sync's lightweight provisioning agent model requires minimal server resources compared with Connect Sync's fuller installation. AD FS and pass-through authentication are authentication/sign-in solutions, not the best answer for directory synchronization. References/topics: Microsoft Entra Cloud Sync, hybrid identity synchronization, provisioning agents, high availability, Microsoft Entra Connect comparison.

NEW QUESTION: 177
□□: □ □□□□ □□□ □□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□ □□□□ □□□.
□□□ □□ □ □ □□□ □□□□ □□□ □□□ □ □□□□. □□□ □□ □□□ □ □□ □□ □□□ □□□□ □□ □□ □□□□.
□ □□□ □□□ □□ □□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Microsoft 365 E5 □□□ □□ Office 365□ Microsoft Defender□ □□□□ □□□□.
□□, □□, □□□□□□ □□□□ □□ □□ □□ □□ □□ □□□□ □□□□ □□ □□□ □□□□ □□□.
□□□: □□ □□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 178
Group1□ Group2□□ □ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.
Group1 □ Group2□ □□□ □□ □□ □□ □□(MFA)□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Group1 □□□ Android □□□□ Microsoft Entra ID□ □□□ □□ MFA□ □□□□□ □□□□ □□□ □□□.
* □□ 2 □□□□ □□ □□□□ □□□□ Microsoft Exchange Online□ □□□□ □□ MFA□ □□□□ □□□.
* □□□ □□□ □□□□□ □□□.
□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
Answer Area



Answer:

Answer Area

Explanation:

NEW QUESTION: 179
site1□□□ Microsoft SharePoint □□□□ □□□ Microsoft 365 E5 □□□ □□□□. site1□ □□ □□ □□□ □□□□□ □□□□ □□□.
* □□ □□□□ 10□□ □□□□□.
* □□ □□□□ □□□ □□□ □□□□□.
site1□ □□ □ □□□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□. □□: □ □□□ 1□□□□.
A. □□ □□ □□
B. □□ □□
C. □□□ □□ □□
D. □□□ □□□
E. □□□ □□ □□(DLP) □□
F. □□ □□
Answer: E,F (LEAVE A REPLY)

NEW QUESTION: 180
□□□ Microsoft 365 □□□ □□□□ □□□□.
□□□ □□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□ □□□□.

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

□□ □□□ □□ □□□ □□□ □□□□□.

□□□□□ □□□ □□ □□□ □□□ □□ Microsoft□ □□ □□□□□ □□□ □□□□?

A. □□□ □□

B. User2 □□

C. User3 □□

D. □□□ □ User2 □□

E. User2 □ User3□ □□

Answer: B (LEAVE A REPLY)

Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer ' s tenant administrator will be notified.

Reference:

https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365

NEW QUESTION: 181

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

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

□□□ □□ □□□ □□□ □ □□□?

A. □□□

B. □□ □ □□□

C. □□ □ □□□□

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

NEW QUESTION: 182
□□ □□ □□ □□ □□□□ □□□ 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. User1, User2, User3, User4
B. User1□ User3□
C. Userl1□
D. User2□ User4□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 183
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

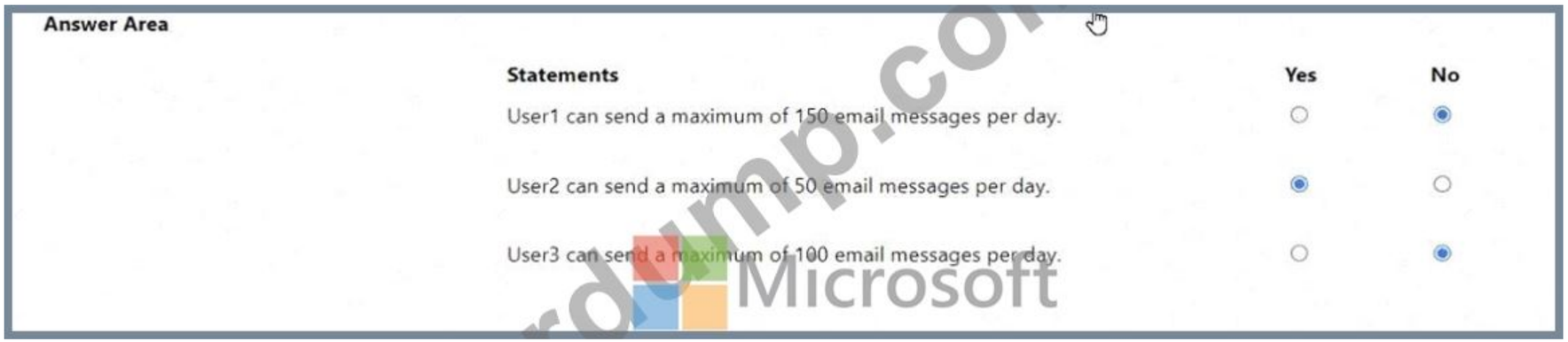
□□ □□□□ □□□ □ □□ □□ □□ □□□ □□□□□.
* □□ : AntiSpam1
* □□□□ : 0
* □□□ □□□, □□ □ □□□□ □□□□□.
o □□□: User3
o □□ : Group1
* □□ □□□, □□ □ □□□ □□

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

Answer:

Answer Area

Explanation:



NEW QUESTION: 184
□□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□. □ □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

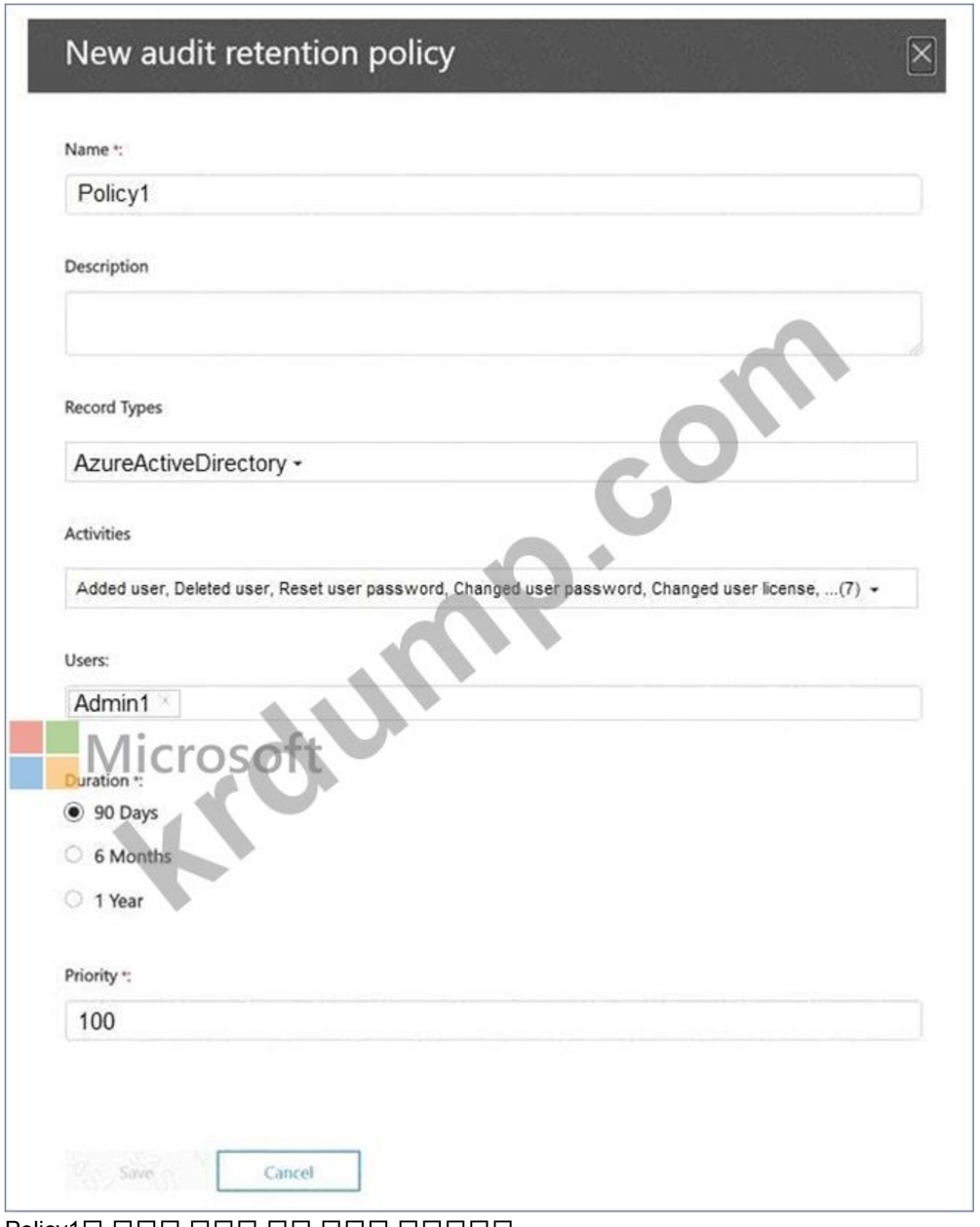
contoso.com□ Microsoft Entra ID□ □□□□□□ Microsoft Entra Connect Sync□ □□□□□.
□□ □□□ Microsoft Entra ID□ □□□□□□?
A. □□1□ □□
B. User1□ User2□ □□
C. □□1 □ □□□1□ □□
D. □□1, □□□1, □□□2
Answer: D (LEAVE A REPLY)
Disabled accounts
Disabled accounts are synchronized as well to Microsoft Entra ID. Disabled accounts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

NEW QUESTION: 185
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
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: 186
□□□ □□ 3□□ □□ 1□□ □□□□ □□□□. □□□ □□ □□□□ □□□□□.
□□ □□□ □□□□□□□ 365 □□□□ □□□□ □□□ □□□ □□□ □□□□□.
□□ □□□□□ □□□ □□□ □□□□□ Microsoft 365 □□□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□□?
A. Microsoft Entra □□□ □□□
B. Microsoft Intune □□ □□ □□ □□
C. Microsoft Entra ID □□ □□
D. Microsoft Intune □□ □□ □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 187
Admin1□ Admin2□□ □ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□□□ Microsoft 365 Enterprise E5 □□□□□ □□□□ □□ □□□ □□ □□□□.
□□□ □□□ □□ □□ □□□ □□□□. (□□ □□ □□□□□.)



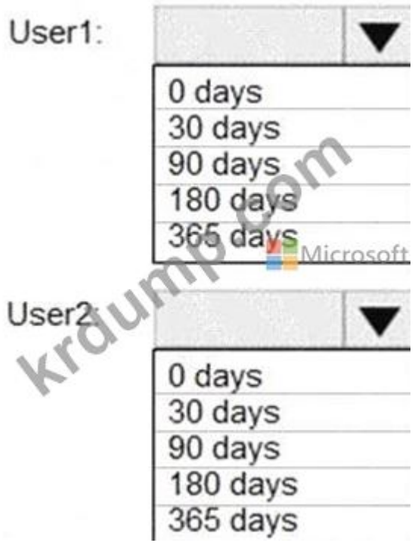
Policy1□ □□□ □□□ □□ □□□ □□□□□.

* Admin1□ User1□□□ □□□□ □□□□□.

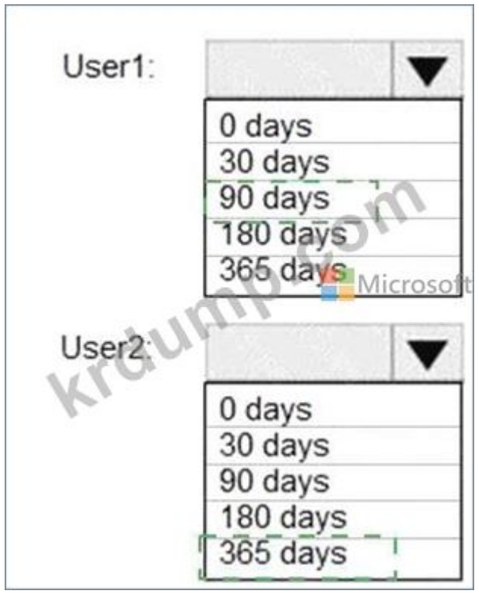
* Admin2□ User2□□ □□□□ □□□□□.

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

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

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

NEW QUESTION: 188
□□□ □□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

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

Microsoft 365 □□ □□□□ □□ □□□ □□□ □ □□ □□□□ □□□□□?
A. □□□1, □□□2 □ □□□3
B. User1□ User3□ □□
C. User2only
D. User1□ User2□ □□
E. □□□1 □□
Answer: (SHOW ANSWER)

NEW QUESTION: 189
□□ □□ □□□ □□□ User1, User2□□ □ □□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.

Name	Members
Group1	User1
Group2	User2, Group1

□□ □□□ □□□ Microsoft Intune □□ □□□ □□□□.
* MDM □□□ □□ : □□

* □□ : □□1
* MAM □□□ □□ : □□
* □□ : □□2
□□ □□ □□□ □□□ □□□□□.

Name	Platform
Device1	Windows 10
Device2	Android

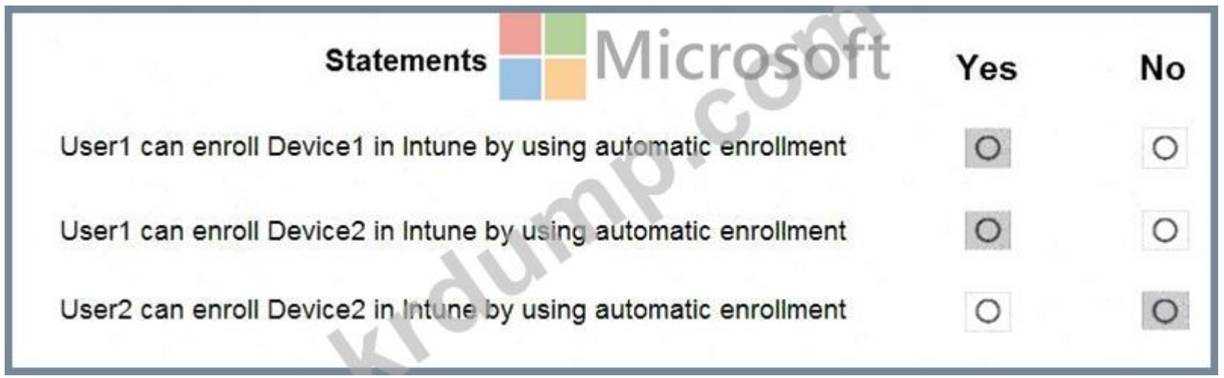
□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

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

Answer:

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

Explanation:



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

NEW QUESTION: 190
Microsoft Endpoint Manager□ □□ □□□ □□□□ □□□□.
□□□ □□ □□ □□□ □□□□ □□□ Microsoft Entra ID(Microsoft Entra ID) □□□□ □□□□ □□□□.

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:

Answer Area

NEW QUESTION: 191

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

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

USER SIGN-IN

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

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

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

□□ □□: □□□□□ Active Directory □□□□□ User2□□ □□ □□□ □□ □□□ □□□□□. □□ □□ User2□□ user2@fabrikam.com□□ □□□□□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

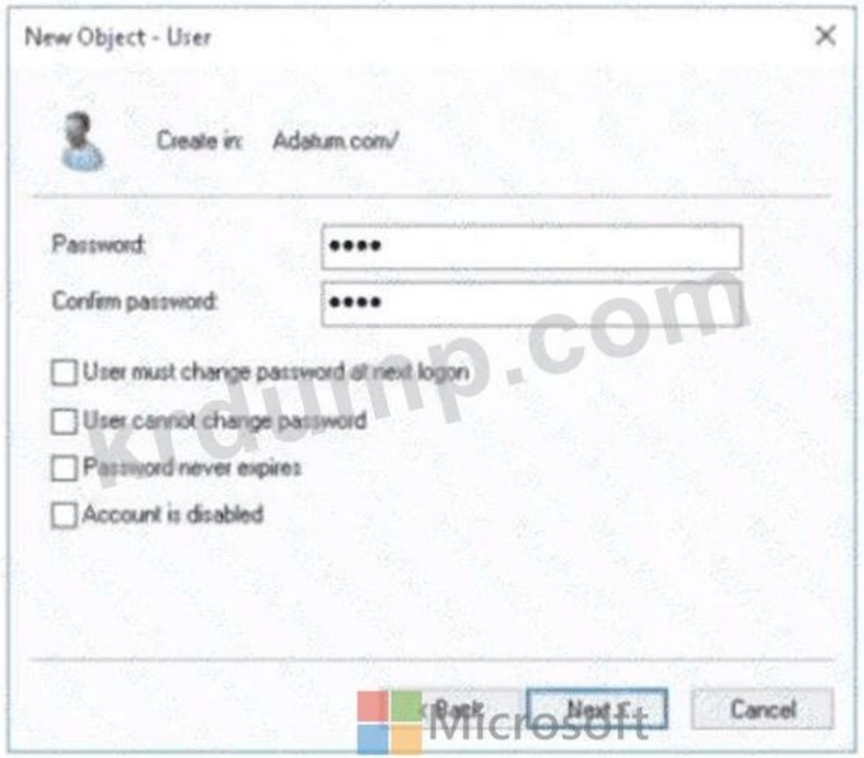
This is not a permissions issue.

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

NEW QUESTION: 192

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

User1□□□ □□□ □□□□ □□□□ □□ □□□ □□ □□ □□□ Pass□ □□□□□.



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

□□□□ □□

□□ □ □□ □□□□ □□ □□ □□□ □□□□□.

□□□□ □□ 90□ □

□□□□ 14□ □□ □□□ □□□□.

□□

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

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

□□: □□ □□□ 1□□□□.

Answer 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: 193

□□□ Microsoft E5 □□□ □□□□ □□□□.

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

□□□ □□□□ □□□?

A. Microsoft Entra □□ □□ ID □□(PIM)

B. □□□ □□ □□

C. □□ □□ □□ □□)

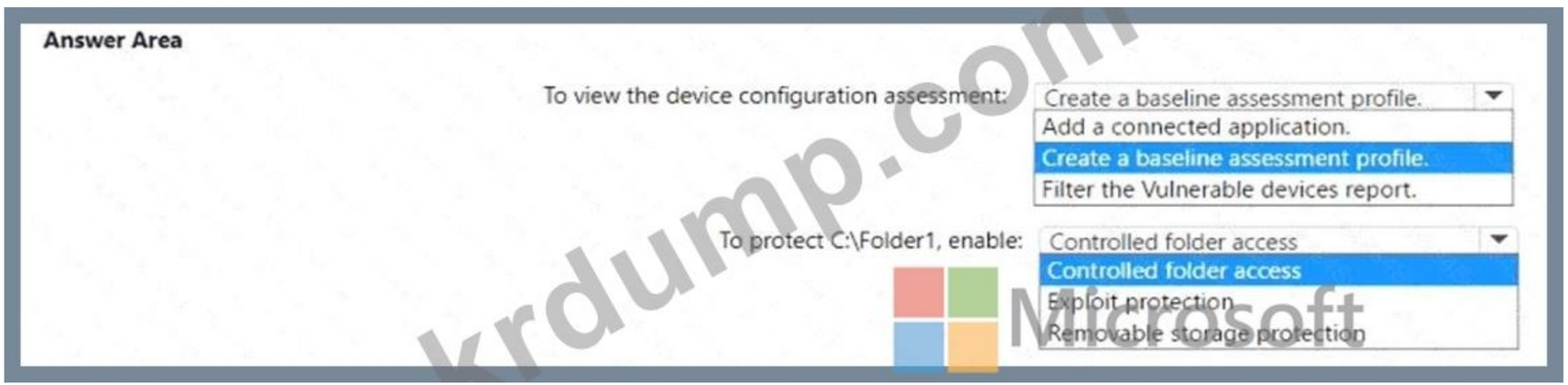
D. Microsoft Entra ID □□

E. □□ □□□□ □□ □□

Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

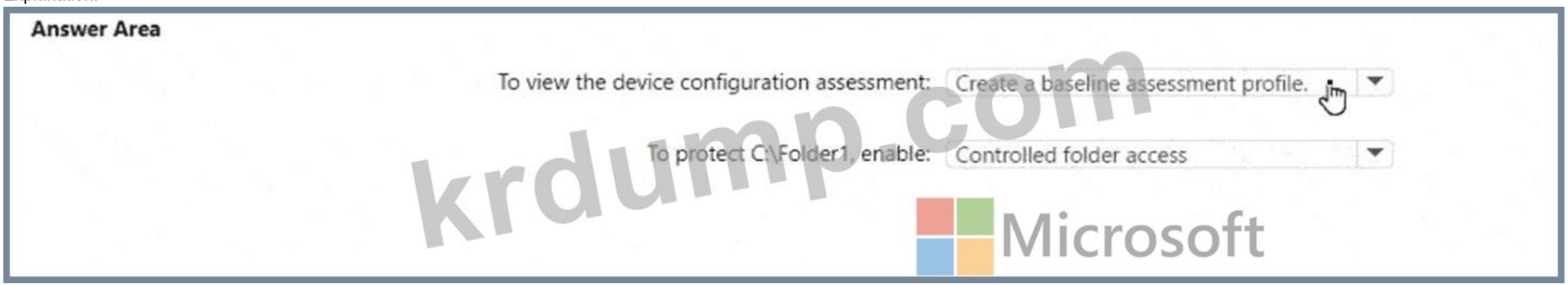
NEW QUESTION: 194
Microsoft Store for Business□ □□□□ □□ User1□□□ □□□□ □□□□ Microsoft 365 □□□□ □□□□. User1□ Microsoft Store for Business□□ □□ □□□ □□□ □ □□□ □□□□ □□□.
* □□□□□ □□□□□ □□□□□.
* Microsoft Store□□ □□ □□□□□.
* □□ □□□ □□ □□ □□□ □□□ □□□□□.
□□□□ □□ □□□ □□□ □□□□ □□□.
User1□□ □□ Microsoft Store for Business □□□ □□□□ □□□?
A. □□□□□
B. Device Guard □□□
C. □□□
D. □□□
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

NEW QUESTION: 195
Microsoft 365 E5 □□□ □□□□.
□□ □□□ Windows 11 □□□ Microsoft Intune□ □□□□ □□□□ Microsoft Defender for Endpoint□ □□□□□.
□□ □□ □□□ □□□□ □□□.
* Center for Internet Security(CIS) vl.0.0 □□□□□ □□ □□ □□ □□□ □□□□□.
* □□□□ □□□ □ □□ □□□□□□□ C:\Folder1□□□ □□□ □□□□ □□ □□□□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.



Answer:

Explanation:



NEW QUESTION: 196

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

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

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

* □□ □□□, □□ □ □□□□ □□□□□

o □□□: User3 o □□: Group1

* □□ □□□, □□ □ □□□□ □□□□□.

o □□□: User1

Policy1□□ □□□ □□ □□ □□□ □□□ □ □□ □□ □□□ □□□□.

* □□□□ □□□□

o □ □□□: □□ o HTML□ □□ □□: □□ o □□□ □□: □□ o □□□: □□ Policy1□□ □□□ □□ □□ □□□ □□□□.

* □□□ □□

□□: □□ □□□□ □□ □□ □□□ □□

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

Answer:

Explanation:

NEW QUESTION: 197

□□□

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

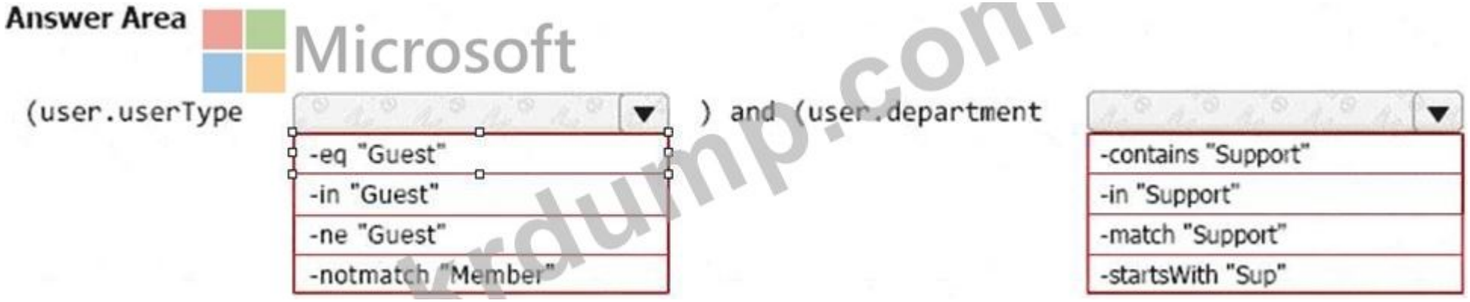
Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

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

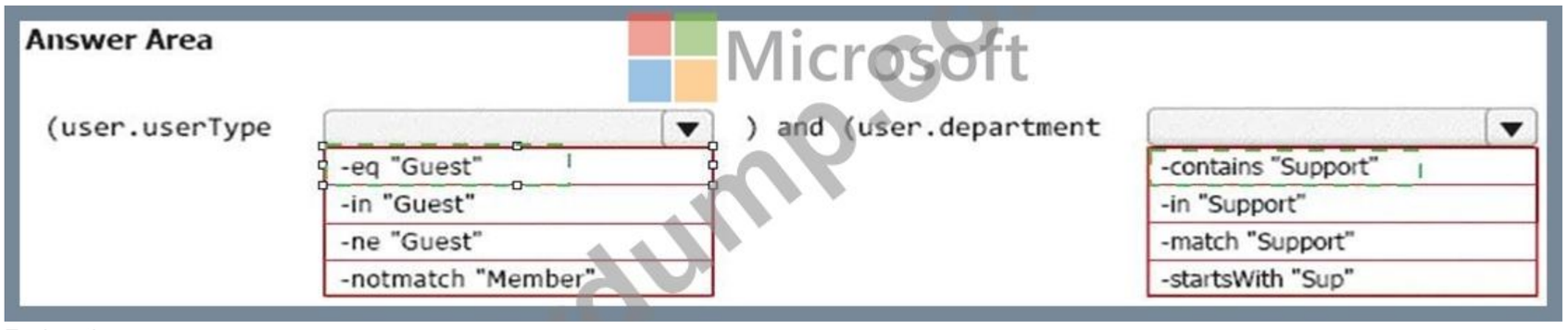
□□□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

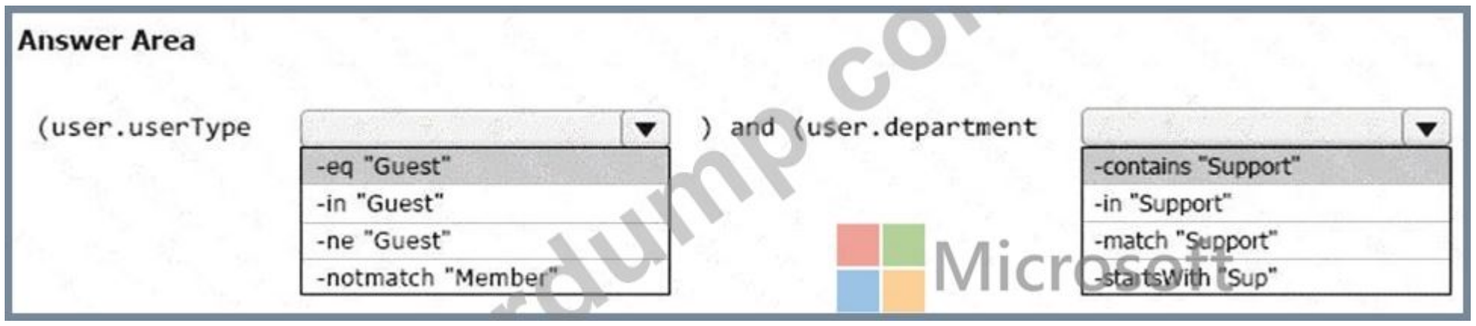
Answer Area



Answer:



Explanation:



Box 1: -eq " Guest "

Dynamic membership rules for groups in Microsoft Entra ID

Supported expression operators

The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.

* Equals

-eq

* Contains

-contains

* Etc.

Box 2: -contains " Support "

Incorrect:

* -in

If you want to compare the value of a user attribute against multiple values, you can use the -in or -notIn operators.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

NEW QUESTION: 198

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

Name	Type
Label1	Sensitivity
Label2	Retention

□□ □□ □□ □□ □□□ □□□□.

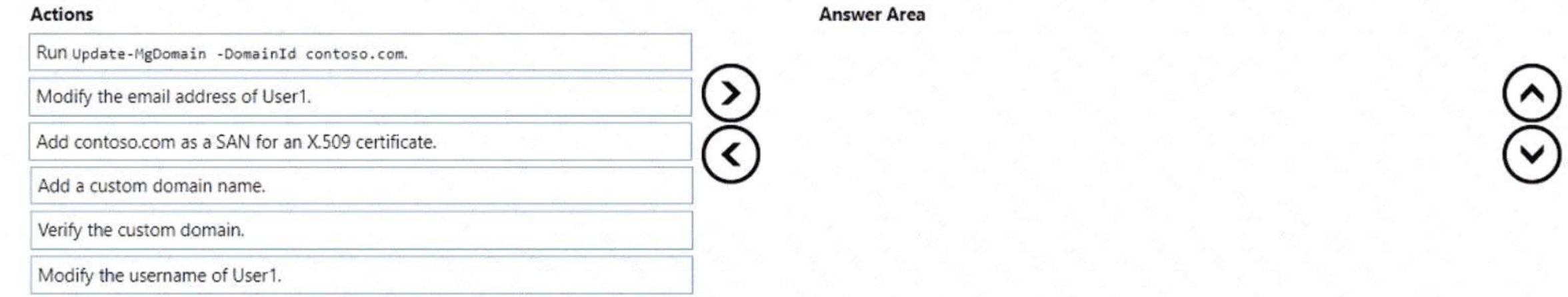
Name	Stored in	Description
File1	Microsoft SharePoint	File document that has Label1 applied
File2	Microsoft Teams channel	File document that has Label2 applied
Mail1	Microsoft Exchange Online	Email message that has Label1 applied
Mail2	Microsoft Exchange Online	Email message that has Label2 applied

□□□ □□□□□ □□ □□□ □ □ □□□?
A. File1, File2, Mail1, Mail2
B. File2□ Mail2□
C. File1□
D. File1□ File2□
E. File1□ Mail!□
Answer: (SHOW ANSWER)

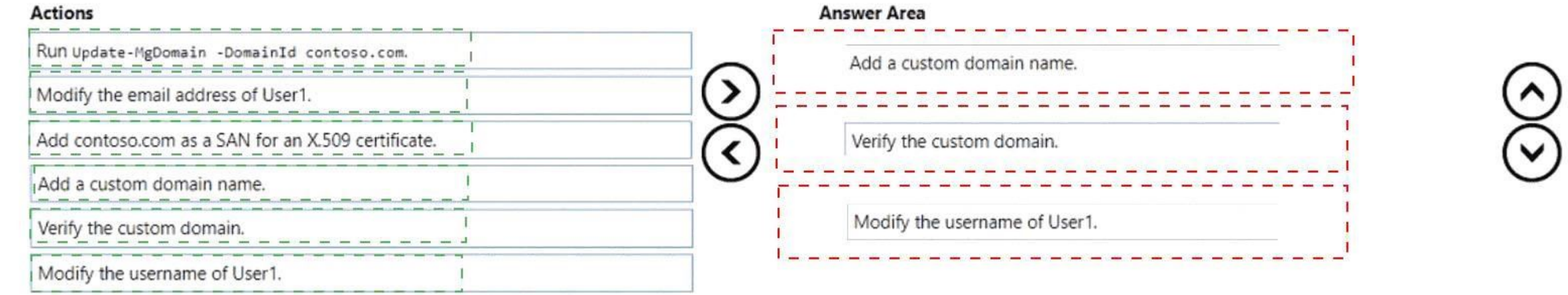
NEW QUESTION: 199
Microsoft 365 □□□ □□□□.
□□□ □□□□□ □□□ □□□□ □□□□ □□ □□□□ □□□ □□ □□(DLP) □□□ □□□□.
□□□ □□□□ □□□ □□□ □□□□ □□ □ □□ □□□□□ □□ □□□ □□, □□ □□□□ □□ □□□□□□ □□□□ □□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. DLP □□ □□
B. □□ □□ □□
C. □□ □□ □□
D. □□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 200
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Microsoft Defender XDR□□ □□□□ □□ □□ □□□ □□□ □ □□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□□ □□ □□ □□
C. □□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)

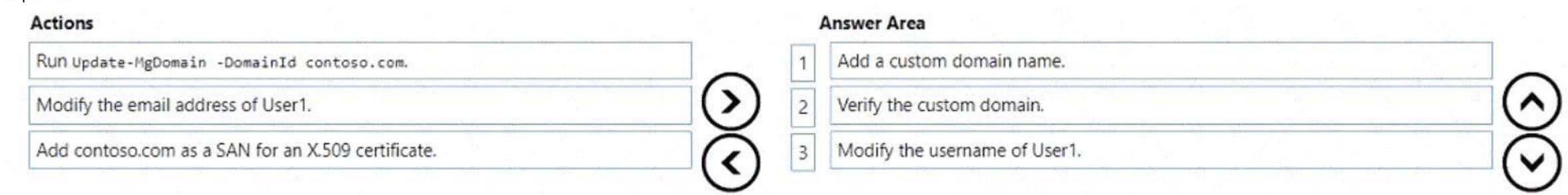
NEW QUESTION: 201
□□□ contoso.onmicrosoft.com□□□ □□□ Microsoft Entra □□□□ □□□□ □□□□.
□□□ □□□□□□ contoso.com□□□ □□□□ □□□□ □□□ □□ DNS □□□□ □□□□□.
User1□□□ □□□ □□□ □□□□□. User1□ userl@contoso.onmicrosoft.com□□ □□□□□□ □□□□□.
User1□ user1@contoso.com□□ □□□□□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:



NEW QUESTION: 202

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

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

Microsoft Defender for Endpoint□ □□□ □□□□□.
Microsoft Defender for Endpoint□□ □□ □□ □□□ □□(RBAC)□ □□ □□□ □□□□□.
Microsoft Defender XDR □□□□ □□ □□□ □ □ □□ □□□□ □□□□ □□□.
□□ □□□□ □□□□ □□□?
A. □□□4
B. □□□3
C. □□□2
D. □□□1
Answer: D (LEAVE A REPLY)

NEW QUESTION: 203
□□□□□ □□□□□□ Contoso.com□□□ Active Directory □□□□ macOS, Windows 8.1, Windows 10 □□ Windows 11□ □□□□ 500□□ □□□ □□□□. □□ □□□ Microsoft Endpoint Configuration Manager□ □□□□ □□□□□. □□□□ Microsoft Entra ID□ □□□□□□.
Microsoft 365 E5 □□□ □□□□ □□ □□□ □□□□ □□□□□. □□ □ □□ □□□ □□ □□□ □ □□□□?
A. Windows 11 □□
B. Windows 11, Windows 10-Windows 8.1 □ macOS
C. Windows 11 □ macOS□□□ □□ □□
D. Windows 11 □ Windows 10□□□ □□ □□
E. Windows 11, Windows 10 □ Windows 8.1□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 204
□□□
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□ □□□.
Microsoft OneDrive □ SharePoint□ □□□ □□□ □□□□ □□□□□□.
□□□ □□□□ □□□□ □□□□ Microsoft Office □□□ □□ □□□ □□□□□□.
Microsoft Purview □□ □□ □□□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area

Explanation:

Answer Area

Box 1: Information protection

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files without the need to

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

NEW QUESTION: 205
Microsoft Defender XDR□ □□□ Microsoft 365 □□□ □□□□.
Microsoft Defender □□□□ □□ □□ □□□ Microsoft Secure Score □□ □□□ □□□□□.

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

□□ □□ □□□ □□ □□ □□□ □□□ □□□□□ □□□□□.

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

□□□□ □ □□ □□□ □□□ □□□□□?

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

Answer: (SHOW ANSWER)

NEW QUESTION: 206
Windows 10 □□□ □□ □□ □□ □□ □□□ □□□□ □□□.
Intune □□ □□□□ □□□ □□□□ □□□?
A. □□ □□□□ □□
B. □□ □□ □□□
C. □ □□ □□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 207
□□ □□□ □□ □□ □□ □□□ □□ □□□□.

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

□□ □□□□ □ □□□ □□ □□ □□ □□□ □□□□□.

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

□□□□: □□ □□□ 1□□□□.
Answer Area

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

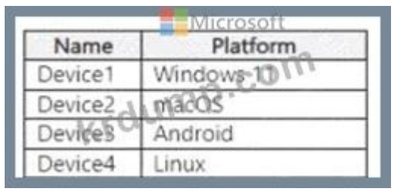
Answer:
Answer Area

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

Explanation:

NEW QUESTION: 208

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



Name	Platform
Device1	Windows 10
Device2	macOS
Device3	Android
Device4	Linux

□□ □□□ Microsoft Defender for Endpoint□ □□□□□□. Endpoint □□□ □□ □□(Endpoint DLP) □□□ □□□ □□□□□. DLP □□□ □□□□ □□□ □ □□ □□□ □□□□□?

A. Device1□ Device2□

B. Device1, Device3, Device4□

C. Device1, Device2, Device3□

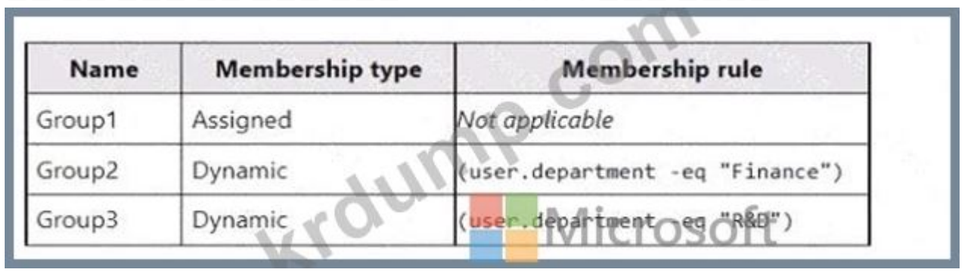
D. Device1, Device2, Device3, Device4

E. Device1□

Answer: (SHOW ANSWER)

NEW QUESTION: 209

□□ □□ □□□ □□ □□□ □□□ 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

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

Explanation:

Answer Area

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

NEW QUESTION: 210
Admin1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□□ Branch□□ □□□ □□□ □□□ □□□□□□!
Admin1□□ Branch1 □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Admin1□ □□□ □□□ Branch1□ □□□ □□□□ □□□ □ □□□ □□□.
* Admin1□ Branch1□ □□□□ □□□□ □□□□ □□□, □□□ □□□□ □□, □□□ □□ □□□ □□□□ □□□.
Branch1 □□□□ □□□ □□□□ □□, Admin1□□□ □□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.
Answer Area

Answer:
Answer Area

Explanation:

NEW QUESTION: 211
Microsoft Store for Business□ □□□□ □□□. □□ □□□□ □□□□ □□ □ □□□?

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

NEW QUESTION: 212
□□ □□ □□□ Microsoft Endpoint Manager □□□ Device1□□□ Windows 10 □□□ □□□ Microsoft 365 □□□□ □□□□.

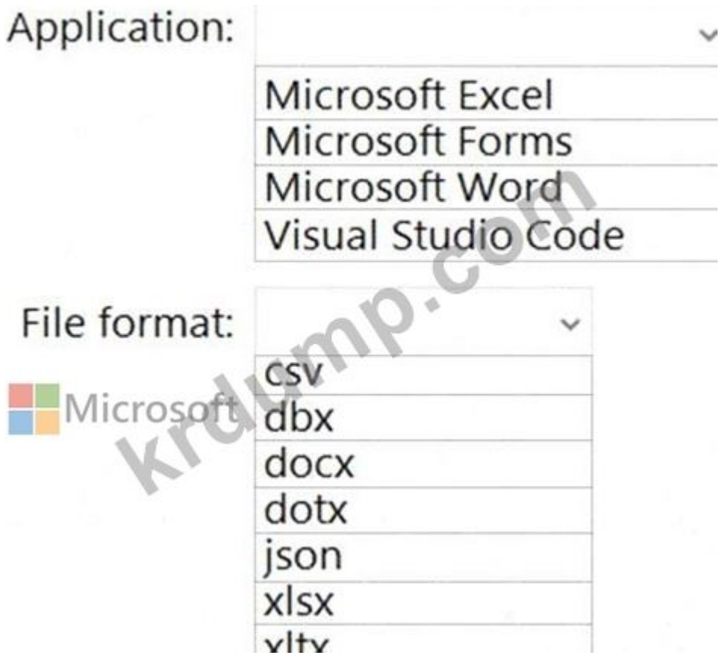
Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

A. □□ □□
B. □□□ □□□!
C. Policy2□ □□□
D. Policy3□ □□□
Answer: (**SHOW ANSWER**)

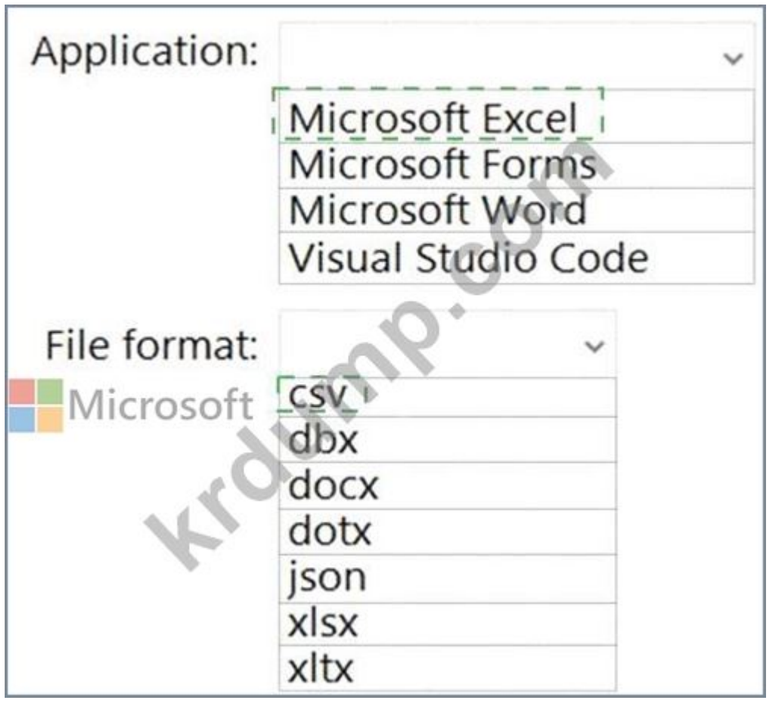
NEW QUESTION: 213
□□□□□ Active Directory □□□□□ □□□□ □□□□.
Microsoft 365□ □□□□□.
□□□□ □□□□ □□□ □□□□□.
□□□□ ID□ □□ □□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Active Directory□ □□□ □ □□ □□ □□□□ Microsoft 365 □□□□ □□□□□ □□□ □ □□□ □□□.
* □□□ □□□□□ 10□ □□□□□ □□□.
□□□: □□□□ □□□ □□□□ Microsoft Entra Password □□□ □□□□□. □□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 214

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



Answer:



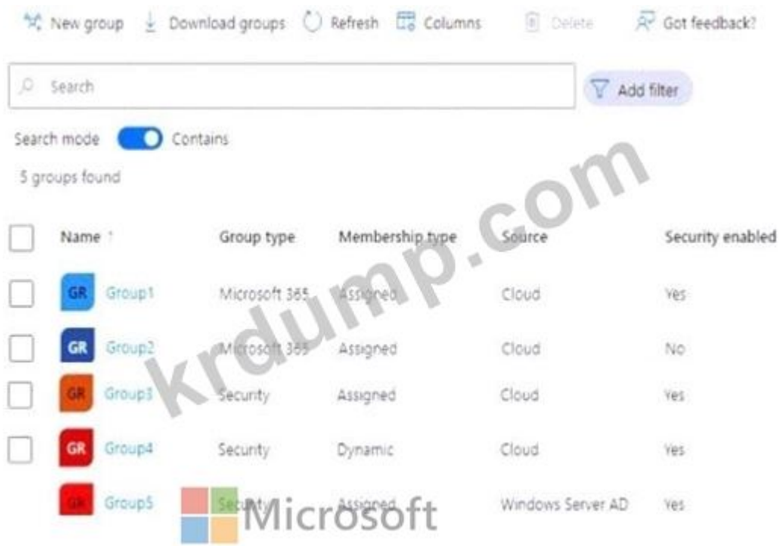
Explanation:

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

NEW QUESTION: 215
Youi □□□□□□ Active Directory □□□□ □□□□ □□□□.
□□ □□□□ □□□□□ Microsoft Entra □□□□ □□□□.
Microsoft Entra Connect Sync□ □□□□ □□□□ □□ □□□□□□□. □□ □□ □□□ □ □□□□ □□□ □□□□□□□□□.
□□□ □□ □□□ □□□□□ Microsoft Entra ID Protection□ □□□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Microsoft Entra Connect□□ □□□□ □□□ □□□□□□.
B. Microsoft Entra □□ □□□□ □□ □□□ □□ □□□ □□□□□.
C. Microsoft Entra □□ □□□□ □□ □□□□ □□□□□□.
D. Microsoft Entra Connect□□ □□□□ □□ □□□□ □□□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 216
Microsoft 365 E5 □□□ □□, □□□□ □□ Microsoft Defender□ □□□□ □□□□. OAuth □ □□□ □□ □ □□□ □□□□ □□□.
□□ □□: Defender for Cloud Apps□ API □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: A (LEAVE A REPLY)

NEW QUESTION: 217
□□ □□□ □□□ □□□ □□□ Microsoft Entra □□□□ □□□□.

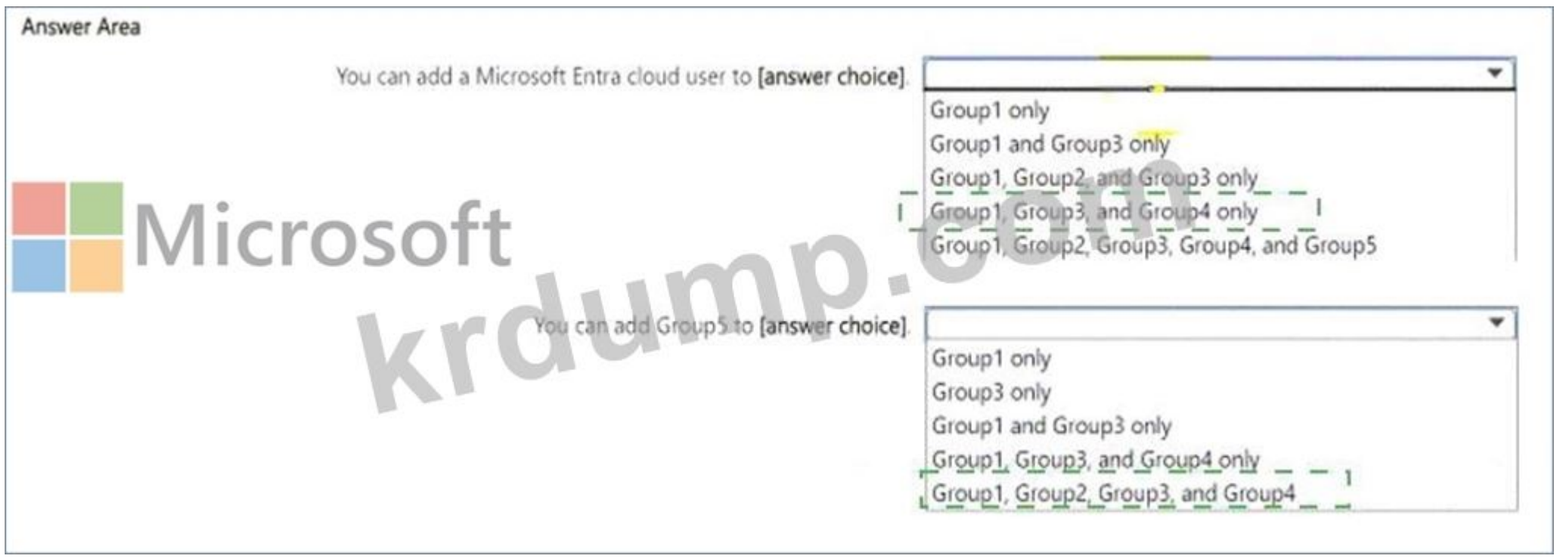


□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□□ □□□□□.
Answer Area

You can add a Microsoft Entra cloud user to [answer choice].
- Group1 only
- Group1 and Group3 only
- Group1, Group2, and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, Group4, and Group5

You can add Group5 to [answer choice].
- Group1 only
- Group3 only
- Group1 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Answer:



Explanation:

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

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

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

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

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

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

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

NEW QUESTION: 218

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

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

Microsoft 365 E5 □□□ □□□□.

SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.

SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Office 365 Advanced Threat Protection(ATP) □□ □ □□□ □□□ □ □□□ □□□□ □□□.

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

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

You need to assign the Security Administrator role.

Reference:

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

NEW QUESTION: 219

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

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

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

□□□ □□ □□□?

A. □□ □□□□ □□□ □□ □□□ □□□□.

B. □□ □□□□□ □□ □□□ □□□ □□□ □□□□□.

C. Microsoft Purview □□ □□ □□□□ DLP(□□□ □□ □□) □□□ □□□□.

D. Microsoft Purview □□ □□ □□□□ □□ □□ □□□ □□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 220

□□ □□ □□ □□ □□□□ □□□□ □□□ Microsoft Store for Business□ □□□ Microsoft 365 □□□□ □□□□.

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

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

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

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

□□□□: □□ □□□ 1□□□□.

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

Answer:

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

Explanation:

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

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

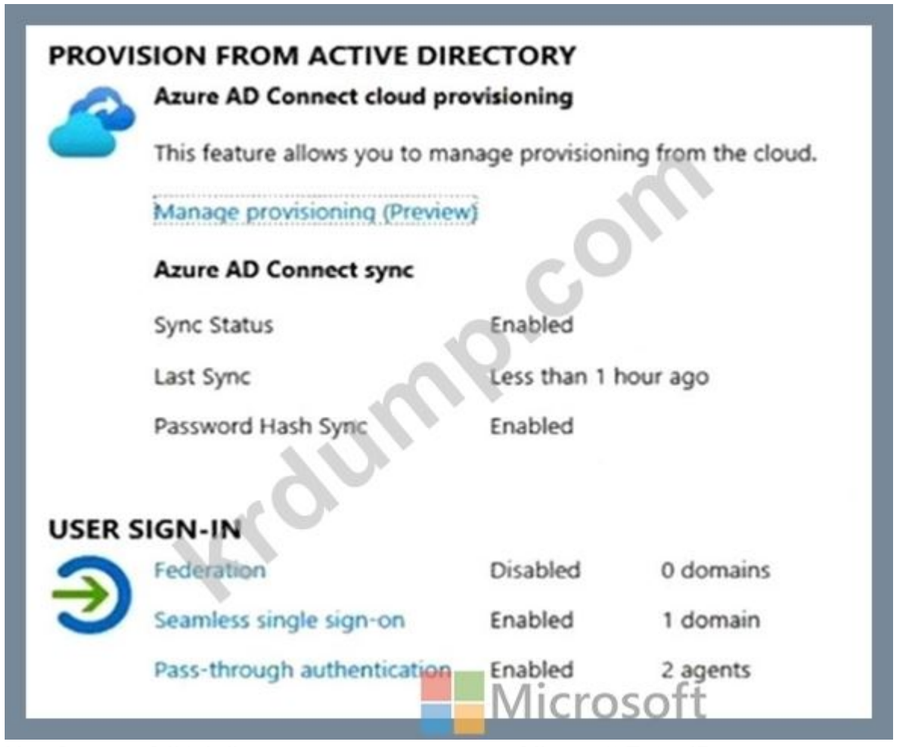
NEW QUESTION: 221
□□□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□□□ □□□ □□□□ □□□□□.
□□ □□ □□□□ □□□ □□□□ □□□ □□□ □□□□□□ □□□□ □□□□□ □□□□ □□ □□□□□ □□□□□ □□ □□□□ □□□. □□ □□□ □□□□ □□□□□□ □ □□□.
□□□ □□ □□□?
A. □□□□ □□□ □□□ □□ □□□ □□ □□(DLP) □□□ □□□□.
B. □□□ □□ □□ □□□ □□□ □□□□□.
C. □□□□ □□□□ □□ □□□ □□ □□□ □□ □□(DLP) □□□ □□□□.
D. □□□ □□□ □□ □□□ □□□□.
Answer: D (LEAVE A REPLY)
Use the Microsoft Defender XDR portal to create Safe Links policies
In the Microsoft Defender XDR portal at https://security.microsoft.com, go to Email & Collaboration > Policies & Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use https://security.microsoft.com/safelinksv2.
1. On the Safe Links page, select Create to start the new Safe Links policy wizard.
2. On the Name your policy page, configure the following settings:
Name: Enter a unique, descriptive name for the policy.
Description: Enter an optional description for the policy.
3. When you ' re finished on the Name your policy page, select Next.
4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions):
Users: The specified mailboxes, mail users, or mail contacts.
*- > Groups:
Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren ' t supported).

The specified Microsoft 365 Groups.
Domains: All recipients in the specified accepted domains in your organization.
Etc.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure

NEW QUESTION: 222
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □ □ □□□ □□□□.
□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □ □□□□ □□ □□□ □□□□ □□□□.
□□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□. □ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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



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

B. □□□

Answer: (SHOW ANSWER)

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

NEW QUESTION: 223

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

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

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

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

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

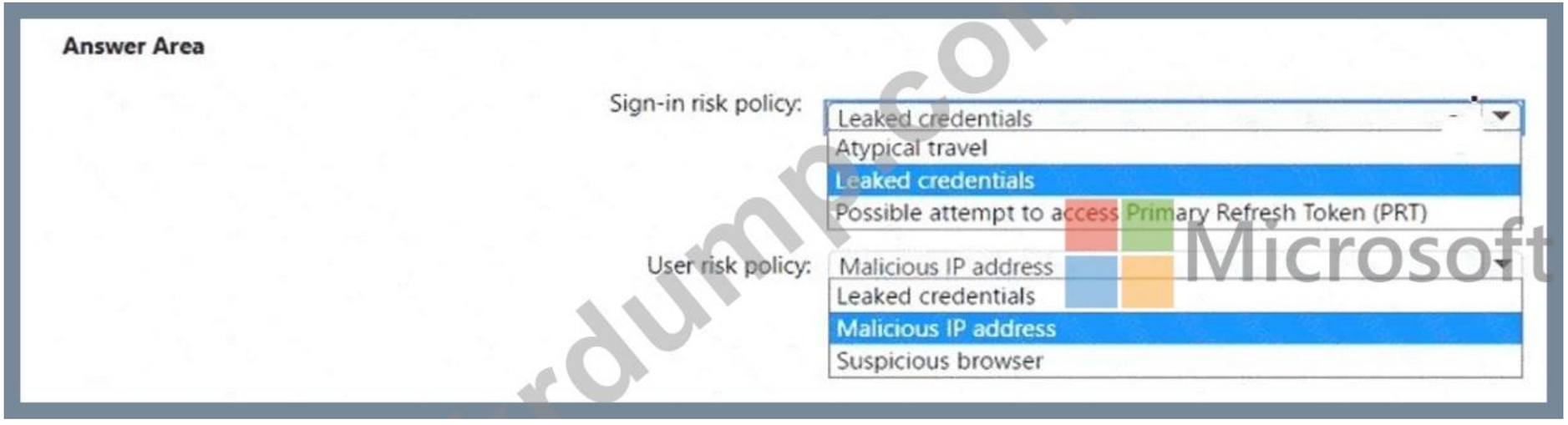
Answer: B (LEAVE A REPLY)

References:

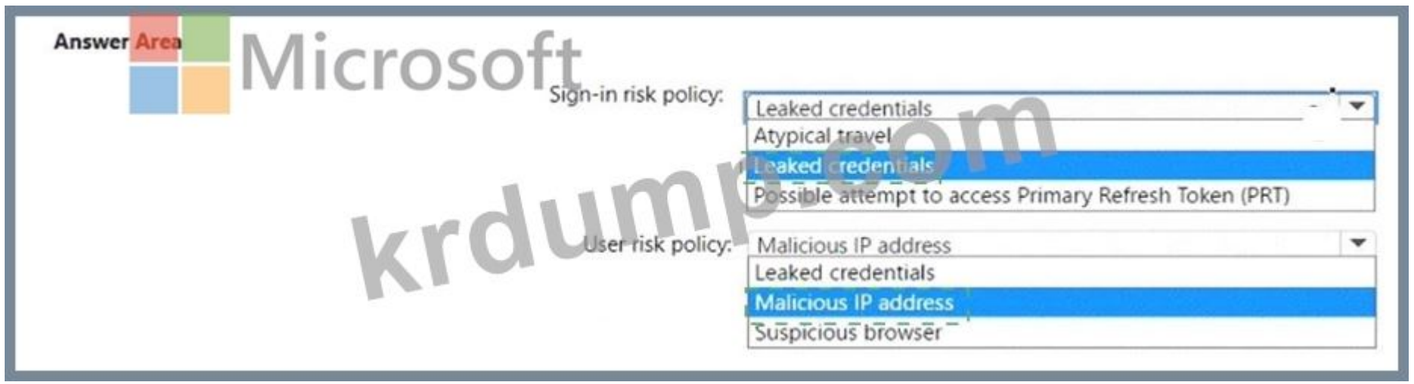
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access- conditions#sign-in-risk states clearly that Sign-in risk

NEW QUESTION: 224

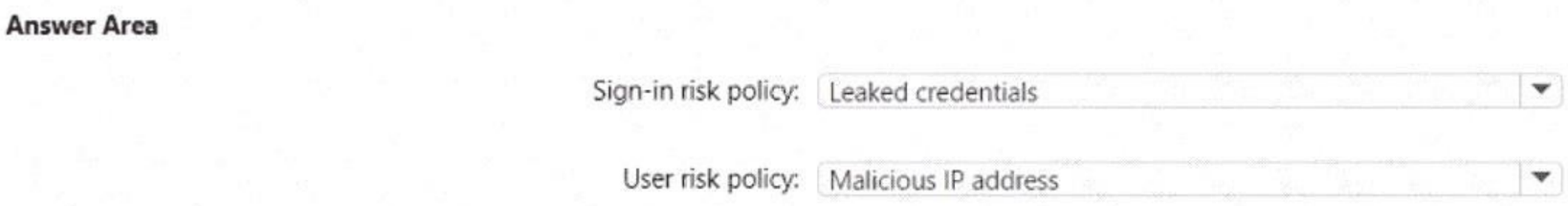
Microsoft 365 E5 □□□ □□□□.
□□□ □□ □□□ □□□ □□ □□□ □□□□ ID □□□ □□□ □□□□□. □ □□□□ □□□□ □□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

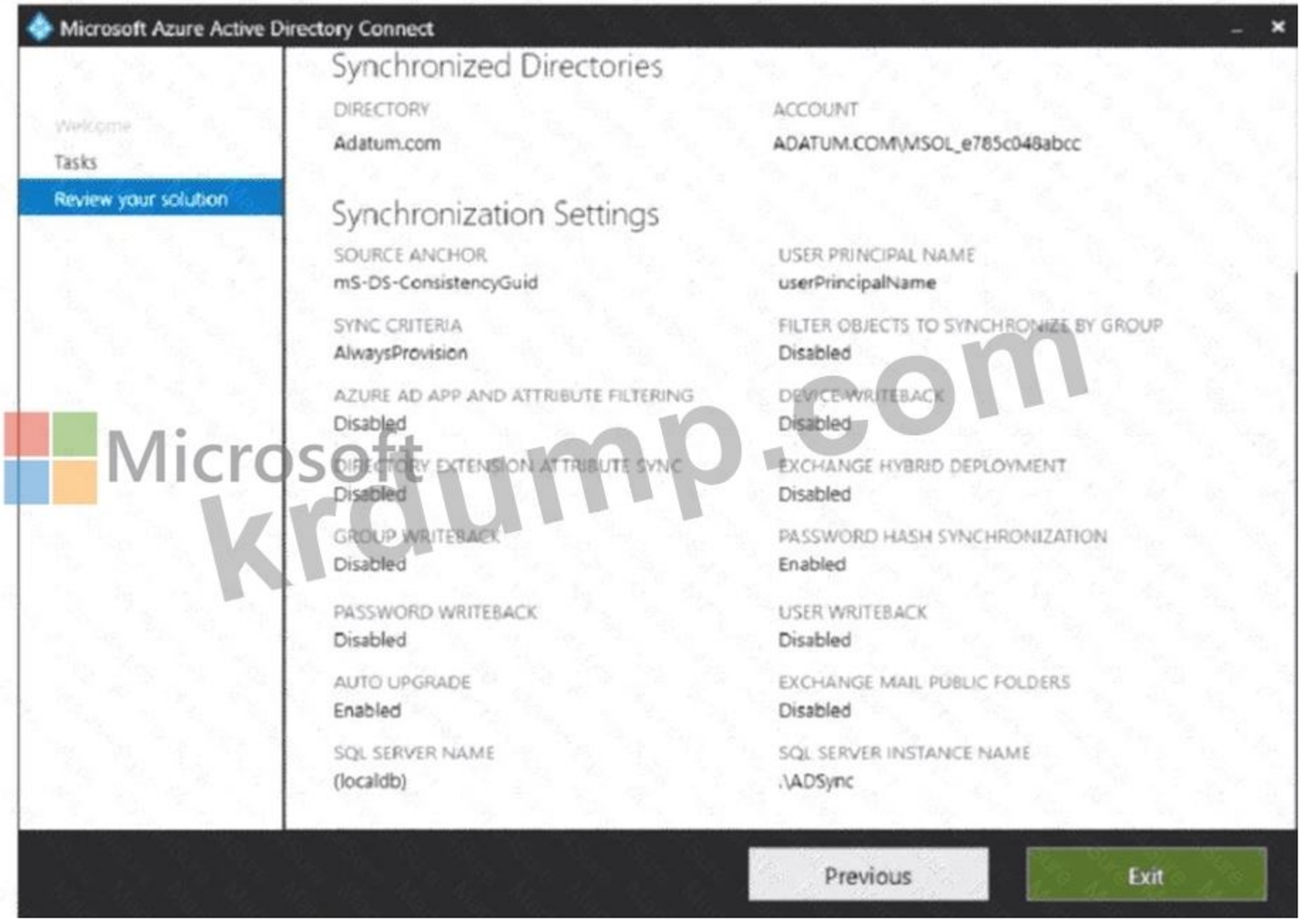


NEW QUESTION: 225
Microsoft 365 □□□□ □□□□.
Microsoft Intune□ □□□□ □□ Windows 10 □□□□□ □□ BitLocker □□□ □□□(BitLocker)□ □□□□ □□□□ □□□□□.
□□□ □□□□ □□□?
A. □□ □□ □□(ASR) □□
B. □ □□ □□
C. □□ □□ □□
D. □□ □□ □□□
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

NEW QUESTION: 226
(□□□ Microsoft 365 E5 □□□ □□□□ □□□□.)
Microsoft Defender for Cloud Apps□ □□□□ □□□□.
OAuth □ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□: □□□ □□□ □ □□□□ □□□□□.
□□□ □□□ □□□□□?)
A. □
B. □□□

Answer: B (LEAVE A REPLY)
OAuth app policies are a feature of Microsoft Defender for Cloud Apps (MDCA) that allow you to:
Monitor OAuth-connected apps
Control app permissions
Detect risky or overprivileged OAuth applications
Microsoft documentation clearly states that OAuth app policies are created and managed directly within Microsoft Defender for Cloud Apps, under Control # Policies # OAuth app policies.
Why Conditional Access app control does NOT meet the goal
Conditional Access app control is a different capability that:
Integrates Microsoft Defender for Cloud Apps with Microsoft Entra Conditional Access Provides real-time session control for cloud apps Is used to control user actions (download, upload, copy, etc.) during app sessions
Microsoft documentation explicitly distinguishes these features:
Conditional Access app control is for session-based access control
OAuth app policies are for app governance and permission monitoring
Configuring Conditional Access app control does not enable or affect the ability to create OAuth app policies.

NEW QUESTION: 227
□□□□□□ □□ □□□ □□ Microsoft Entra ID□ □□□□ □□□□□ Active Directory □□□□ □□□□ □□□□.



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

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

□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

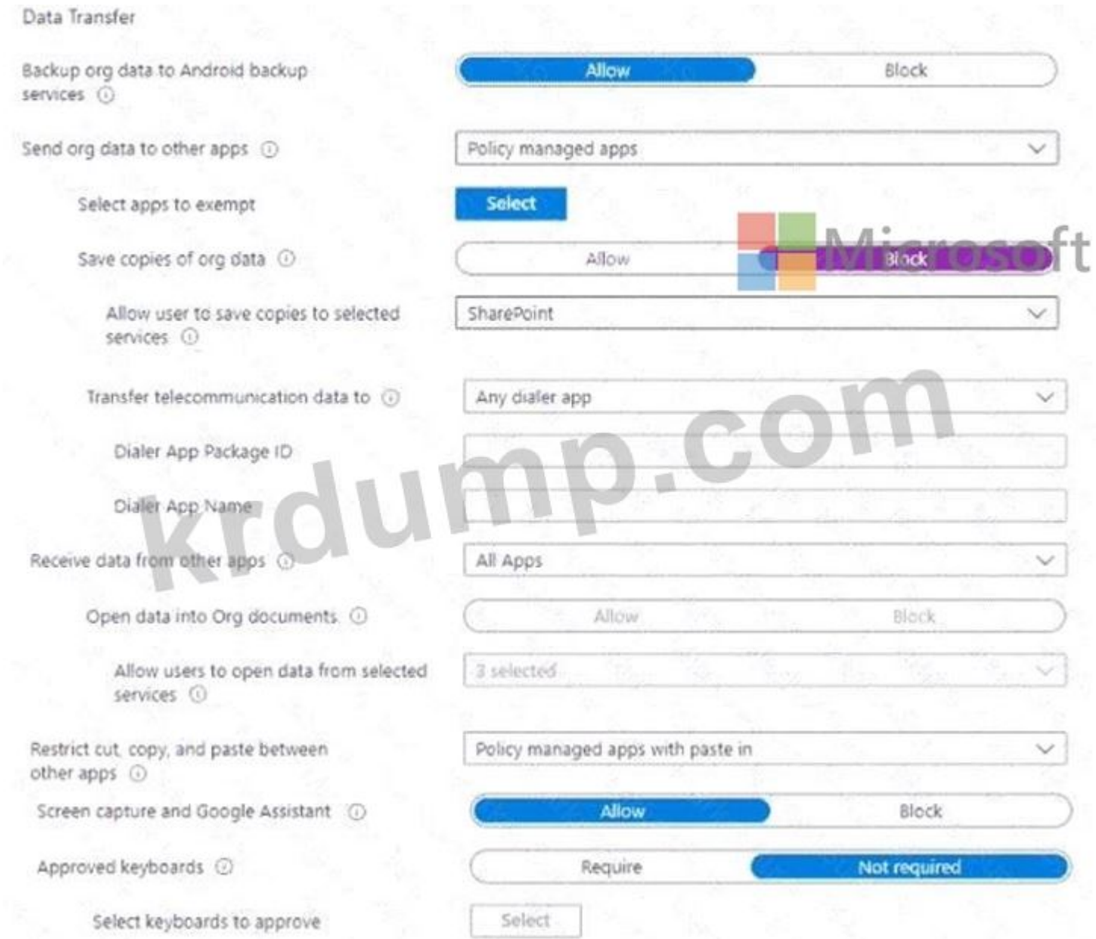
Explanation:

NEW QUESTION: 228

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

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

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

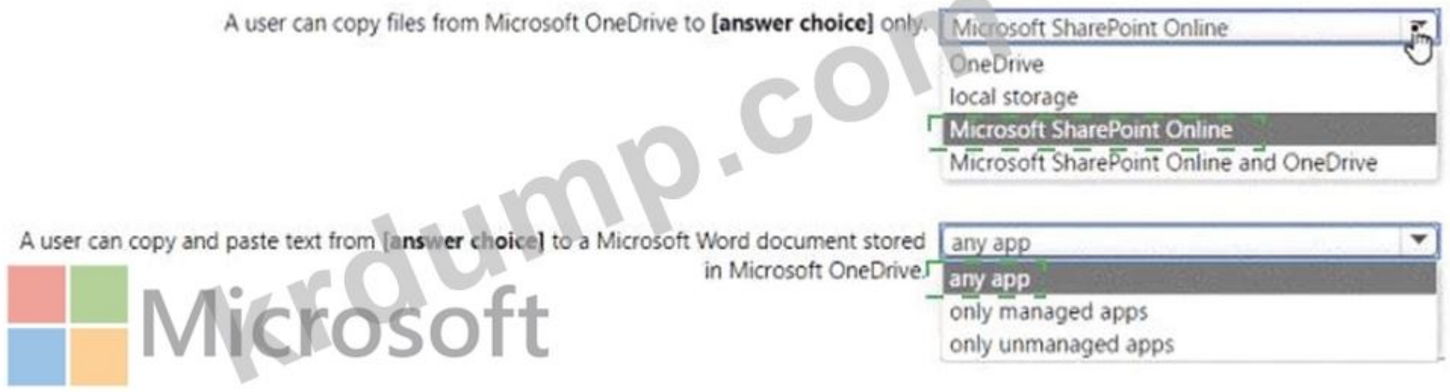

Data Transfer
Backup org data to Android backup services
Allow
Block
Send org data to other apps
Policy managed apps
Select apps to exempt
Select
Save copies of org data
Allow
Block
Allow user to save copies to selected services
SharePoint
Transfer telecommunication data to
Any dialer app
Dialer App 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
3 selected
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

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


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

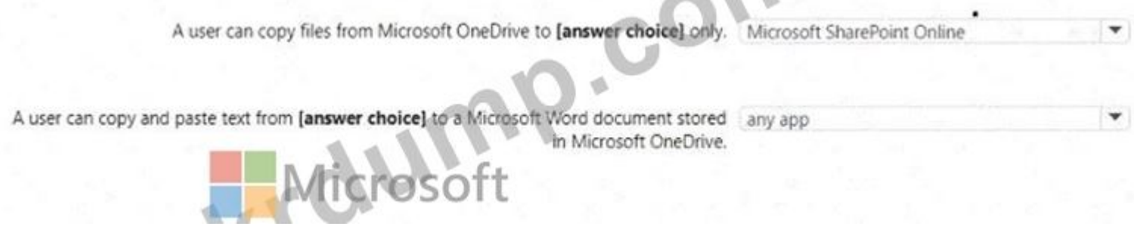
Answer:

Answer Area



Explanation:

Answer Area



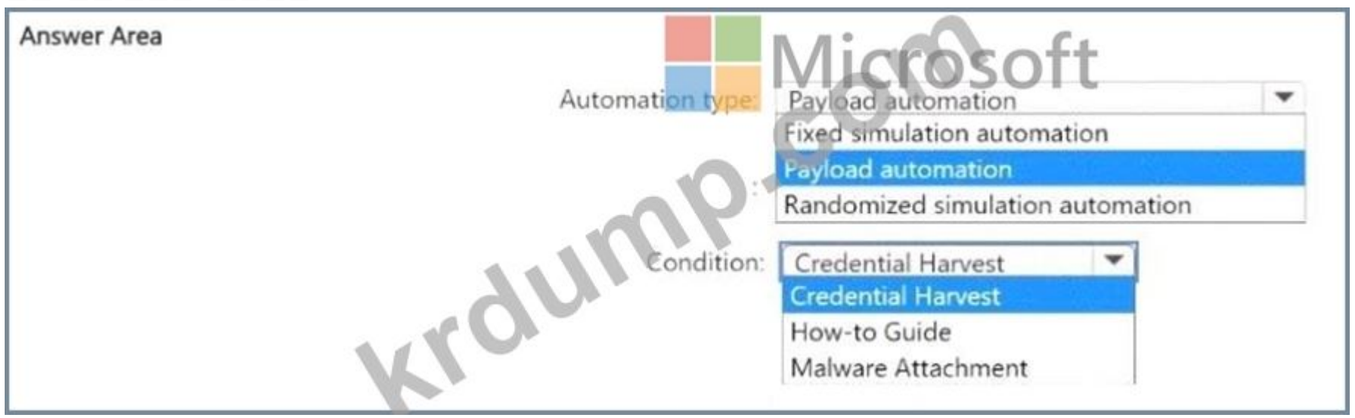
NEW QUESTION: 229

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

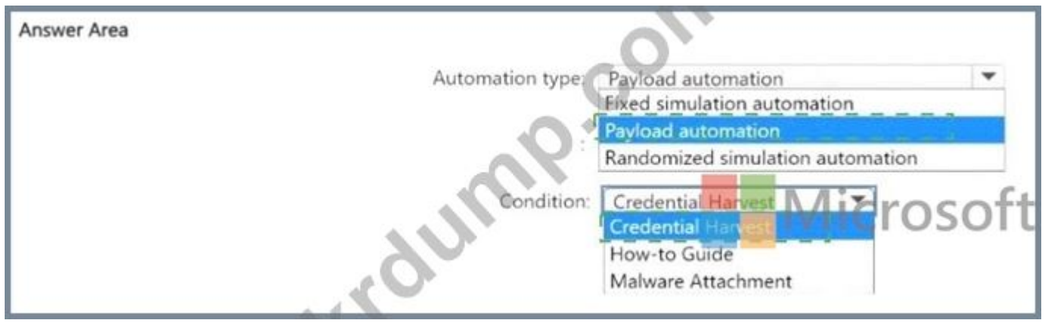
□□ □□□□ □□□□□ □□□□ □□□□ □□ □□ □□□□□ □□□ □□□□□ □□□.

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

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 230

□□□□□□ □ □□ Active Directory □□□□□ □□□□. □□□□ □□□ □□□□ □□□□ □□□ □□□□ □□□□.
Microsoft Entra □□□□ □□□□□.
□□□□□ Active Directory□ Microsoft Entra ID□ □□□□ □□□□□.
□□□ □□□□ □□□ □□□ □□□. □□ □□□□ □□ □□□ □□□ □□□□□□ □□□□ □□□□□, □□□ □□□ □□□□ □□□ □ □□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□□?

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

Answer: (SHOW ANSWER)

Microsoft Entra Connect Sync can be active on only one server. You can install Microsoft Entra Connect Sync on another server for redundancy but the additional installation would need to be in Staging mode. An Microsoft Entra Connect Sync installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

NEW QUESTION: 231

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

* □□□ 10
* □□□□□
* □□□ OS

□□ □□□□ Endpoint DLP □□□ □□□ □ □□□?

A. Windows 10□ □□

B. Windows 10 □ Android□ □□
C. Windows 10 □ macOS □□
D. Windows 10, Android □ iOS
Answer: A (LEAVE A REPLY)
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: 232
□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□□ Windows 10 Pro□ □□□□ Microsoft Entra ID□ □□□ □□□ 1,000□□ □□□□ □□□□.
Microsoft 365 E3 □□□ □□□□□□□.
□□□□ Windows 10 Enterprise□ □□□□ □□□. □□□□ □□ □□□□ □□□□□ □□□.
□□□ □□ □□□?
A. Windows □□ □□□□□□ EditionUpgrade □□□ □□□ □□□□□ □□□□ □□□ □□ □□□□ Microsoft SharePoint Online □□□□ □□□□□□. □□□□□ SharePoint Online□□ □□□□□ □□□□ □ □□□□ □□□□□.
B. Microsoft Endpoint Manager □□ □□□□ Windows Autopilot □□ □□□□ □□□□.
□□ □□□□ □□□□ □□□□□. □□□□□ □□□□ □□□□□ □□□□□ □□□□□□ □□□□□.
C. □□□□ Microsoft Intune□ □□□□□. □□□ □□□□□ □ □□ □□ □□□□ □□□□ □□ □□□□ □□□□. Microsoft Endpoint Manager □□ □□□□ □□ □□□□ □□□□ □□□□ □□□□□ □□□ □ □□ □□□□□ □□□□□.
D. Microsoft Entra ID □□ □□□□ □□ □□ □□□□ □□□□ □□ □□□ □□□□. □□□ □□□□□ □□□□ □□□□ □□□□ □□□□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 233
□□□□□□ Microsoft Entra ID□ □□□□ adatum.com□□□ Active Directory □□□□ □□□□.
□□ □□□□□ 100□□ □□□ □□□ □□□□.
□□ □□□□ □□ □□□ □□□□ □□□□ □□□ □□□□□.
□□ □□ □□ □ □□□ □ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□□?
A. □□□ □□□□□ Windows PowerShell□□ Gec-ADUser □ Sec-ADUser cmdlet□ □□□□□.
B. Azure Cloud Shell□□ Gec-ADUser □ Sec-ADUser cmdlet□ □□□□□.
C. □□□ □□□□□ Windows PowerShell□□ Gec-MgUser □ Updace-MgUser cmdlet□ □□□□□.
D. Azure Cloud Shell□□ Gec-MgUser □ Update-MgUser cmdlet□ □□□□□.
Answer: A (LEAVE A REPLY)
The user accounts are synced from the on-premise Active Directory to the Microsoft Microsoft Entra ID (Microsoft Entra ID). Therefore, the city attribute must be changed in the on-premise Active Directory.
You can use Windows PowerShell on a domain controller and run the Get-ADUser cmdlet to get the required users and pipe the results into Set-ADUser cmdlet to modify the city attribute.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.

Other incorrect answer options you may see on the exam include the following:
1. From the Azure portal, select all the Microsoft Entra ID users, and then use the User settings blade.
2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set-AzureADUser cmdlets.
3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
4. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.
Reference:
https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser

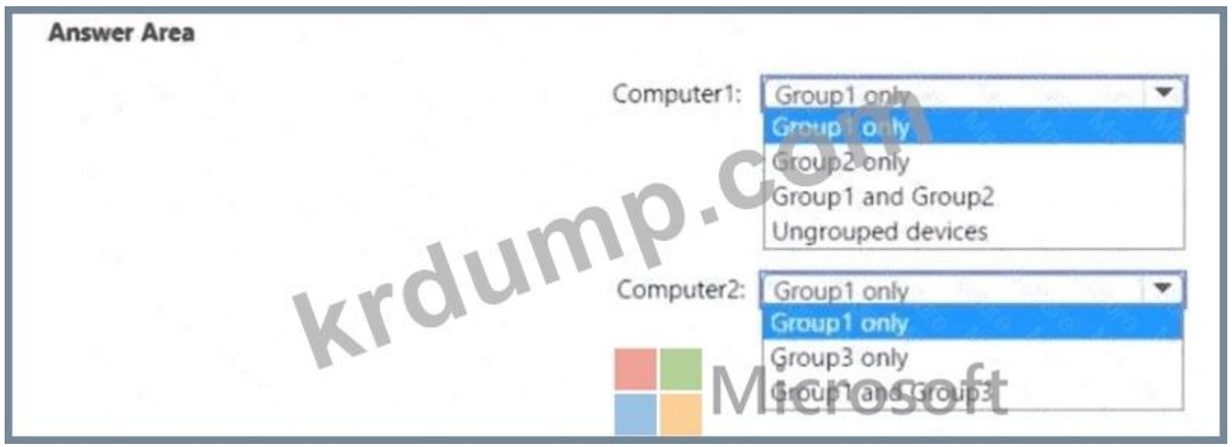
NEW QUESTION: 234
□□□ Microsoft Defender for Endpoint□ □□□□□. Microsoft Defender for Endpoint□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

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

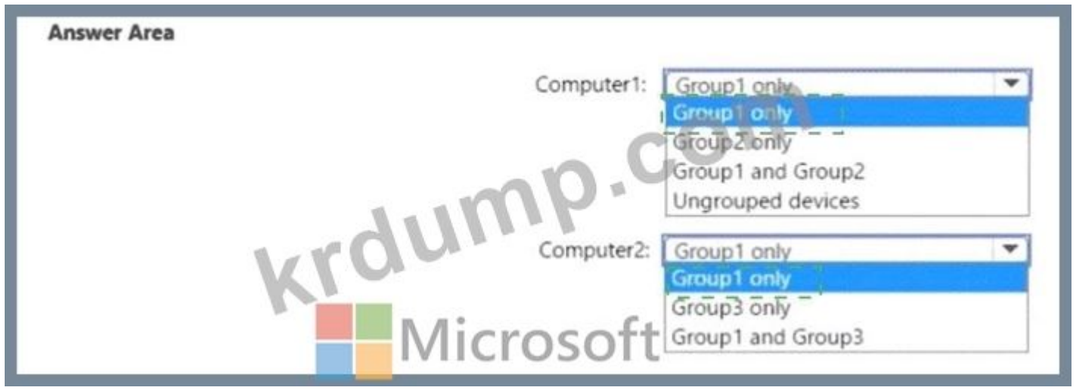
□□ □□ □□□ □□ Microsoft Defender for Endpoint□ □□□□ □□□□□□.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

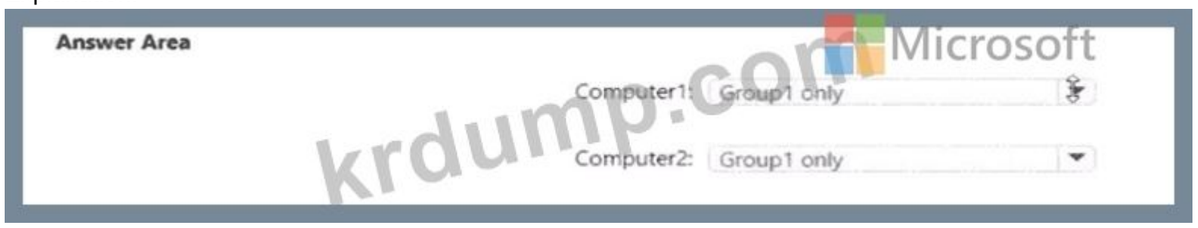
□□ □□□ Computer!□ Computed □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 235

□□□ □□□□ Microsoft 365 □□□□ □□□□.

Engineering□□□ □□□ □□□□ □□□□ □□□ □□ □□(MDM)□ □□□ □□□ □□□□□ □□□□□ □□□. □□ □□ □□□ □□ □□ □□ □□□□□.

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

□□ □□ □□□ □□ □□ □□ □□□□□.

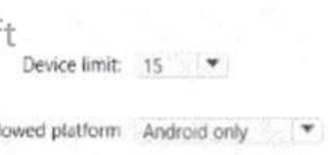
Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

Answer:

Answer Area

Explanation:

Answer Area



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

NEW QUESTION: 236

□□□

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

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

User4□□ Microsoft 365 □□ □ □□□ □□□□□ □□ □□ □□□ □□□ □□□ □□□□□.

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

□□□□ □□ □□□ □□□ □□□□ □□□.

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

□□□□: □□ □□□ 1□□□□.

Answer Area

Microsoft 365 setting:

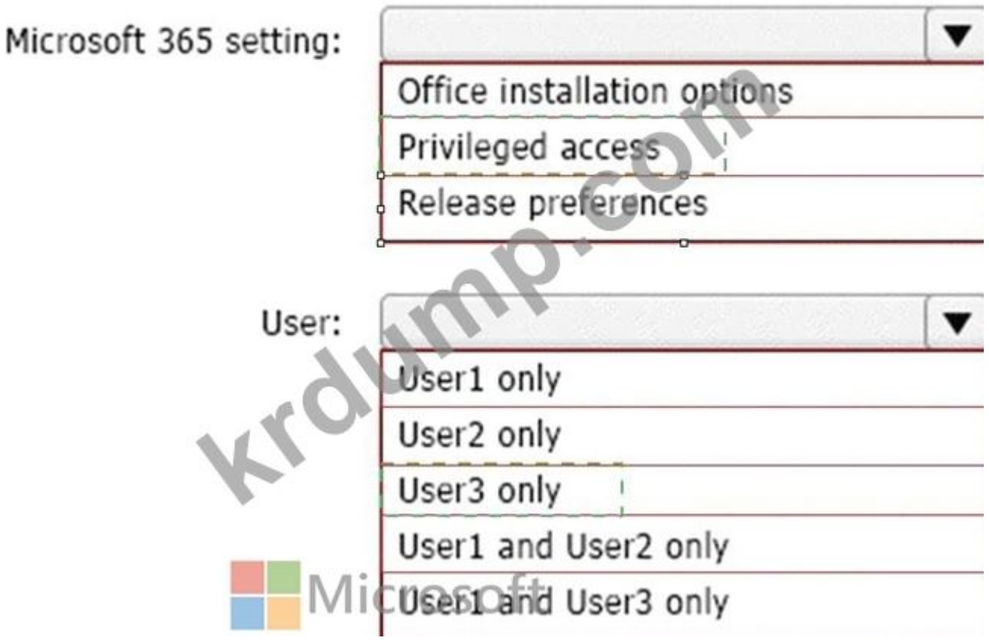
- Office installation options
- Privileged access
- Release preferences

User:

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

Answer:

Answer Area



Explanation:

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: 237
Microsoft Endpoint Manager□ □□□□ □□□□ Windows 10 □□□ □□□□.
Microsoft Edge□□ □□ □□□ □□□□ □□□.
Microsoft Endpoint Manager□□ □□□ □□□□ □□□?
A. □ □□ □□
B. □
C. □□ □□ □□□
D. □□ □□ □□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

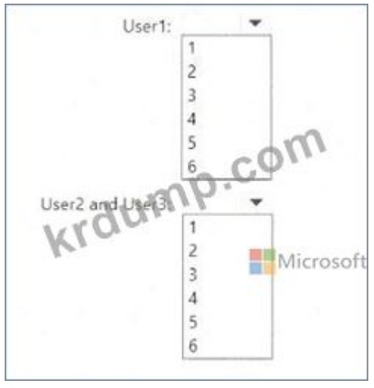
NEW QUESTION: 238
User1□□□ □□□□ □□□ Microsoft 365 □□□ □□□□.
User1□ □□ □ □□ □□ □□ □□□□ Microsoft 365 □□ □□□ □□□ □ □□□ □□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□ □ □□ □□ □□ □□□ □□ □□ □□ □□

B. Exchange □□ □□□ □□ □□ □□ □□
C. Microsoft Entra ID □□ □□□ □□ □□□
D. □□ □ □□ □□ □□ □□□ □□ □□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

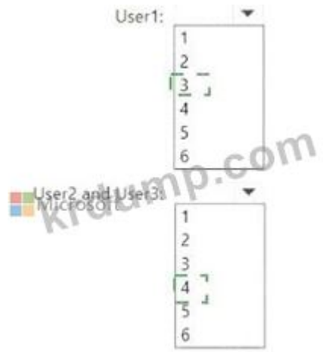
NEW QUESTION: 239
□□□ User1, User2, User3□□□ □□□ □□□ 3□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Microsoft Entra ID Protection□ □□□□ □□□□.
'□□ □□□ □□ □□' □□□ □□□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□ □□□□□.
□□□□□□ □□ □□ □□□ □□ □□□ □□□□□.

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

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



Answer:



Explanation:
User1: 3
User2 and User3: 4
Microsoft Entra ID Protection generates a Users at risk detected email when a user's calculated risk level reaches the configured threshold. In this case, the threshold is Low or above, so Low, Medium, and High risk events all qualify. Microsoft states that the email is generated when the user's risk level reaches the configured risk level, and additional emails can be generated when later detections recalculate the user risk level at the configured level or higher. Microsoft also states that only one email is sent within a five-second period, and if multiple users move to the configured risk level during that same five-second period, the data is aggregated into one email.
For User1, alerts occur at 8:00:10, 8:02:00, and 8:05:00. The 8:02:04 High event is within five seconds of the
8:02:00 Medium event, so it does not create a separate alert. Therefore, User1 receives 3 alerts.
For User2 and User3, the 8:00:00 events are aggregated into one alert, the 8:03:01 events are aggregated into one alert, then User3 at 8:10:00 generates another, and User2 at 9:00:00 generates another. Total: 4 alerts.
References/topics: Microsoft Entra ID Protection, Users at risk detected alerts, user risk threshold, alert aggregation window.

NEW QUESTION: 240
Microsoft 365 E5 □□□ □□ □□□□ □□ Microsoft Defender□ □□□□ □□□□. □ □□□□ Windows 11 □□□ □□□□ □□□□ □□□□ □□□□.
□□□ □□□□ □ □□□□ □□□□□ Cloud Discovery □□□ □□□□ □□□□ □□□. □□□□ □□□□ □□ □□□ □□ □□□?
A. □□□ Azure Monitor Agent□ □□□□□.
B. □□ □□□ □□□□.
C. □□□□ □□□□□ □□□ □□□ □□□□□.
D. □ □□ □□□ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 241
□□ □□ □□□ □□□ □□□ Microsoft 365 ES □□□ □□□□.

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

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

Answer:

Explanation:

NEW QUESTION: 242

Microsoft 365 E5 □□□□ □□□□.

□□ □□ □□□ □□□ □□ □□ □□□ □□□□□.

Compliance settings Edit

Microsoft Defender ATP

Require the device to be at or under the machine risk score:	Low

Device Health

Rooted devices	Block
Require the device to be at or under the Device Threat Level	

System Security

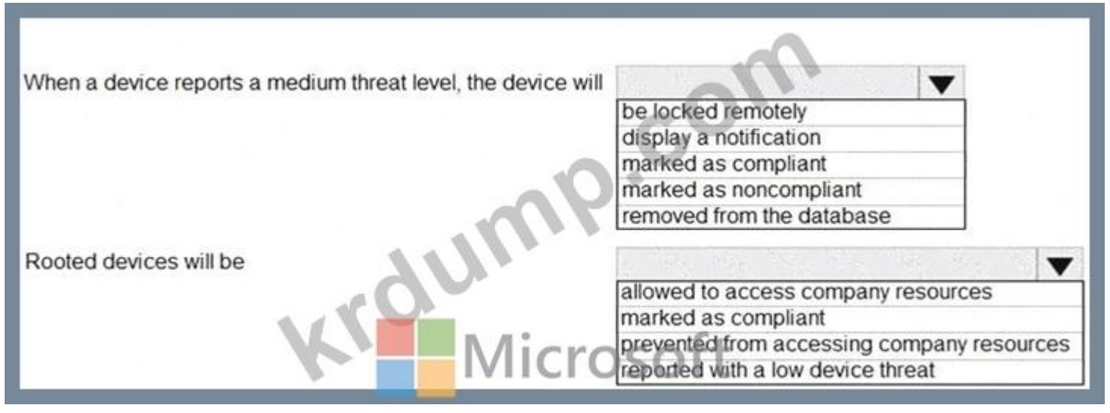
Require a password to unlock mobile devices	Require
Required password type	Device default
Encryption of data storage on device.	Require
Block apps from unknown sources	Block

Actions for noncompliance Edit

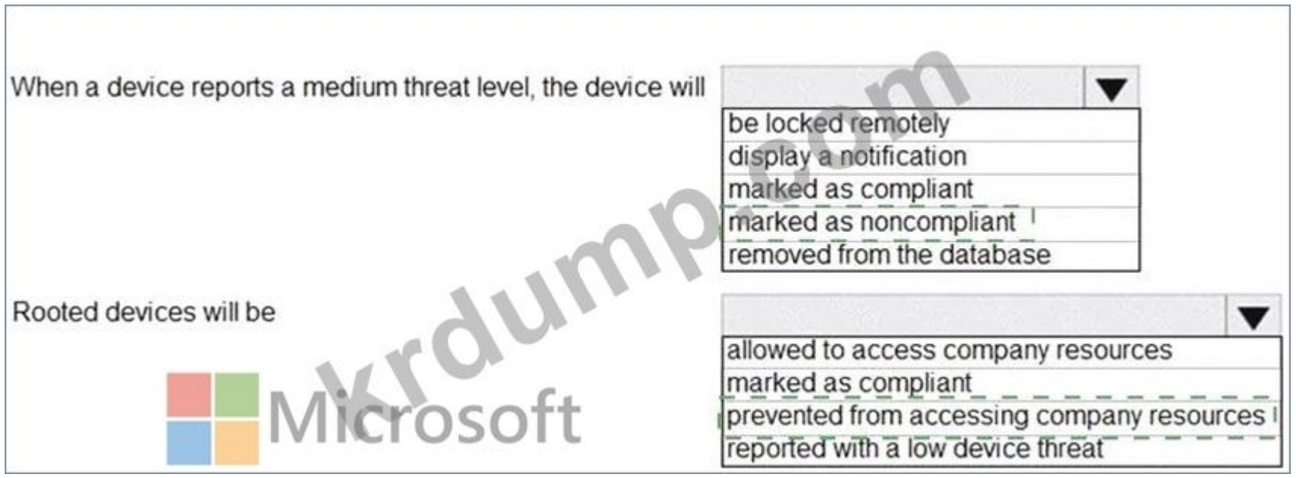
Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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

□□□□: □□ □□□ 1□□□□.



Answer:



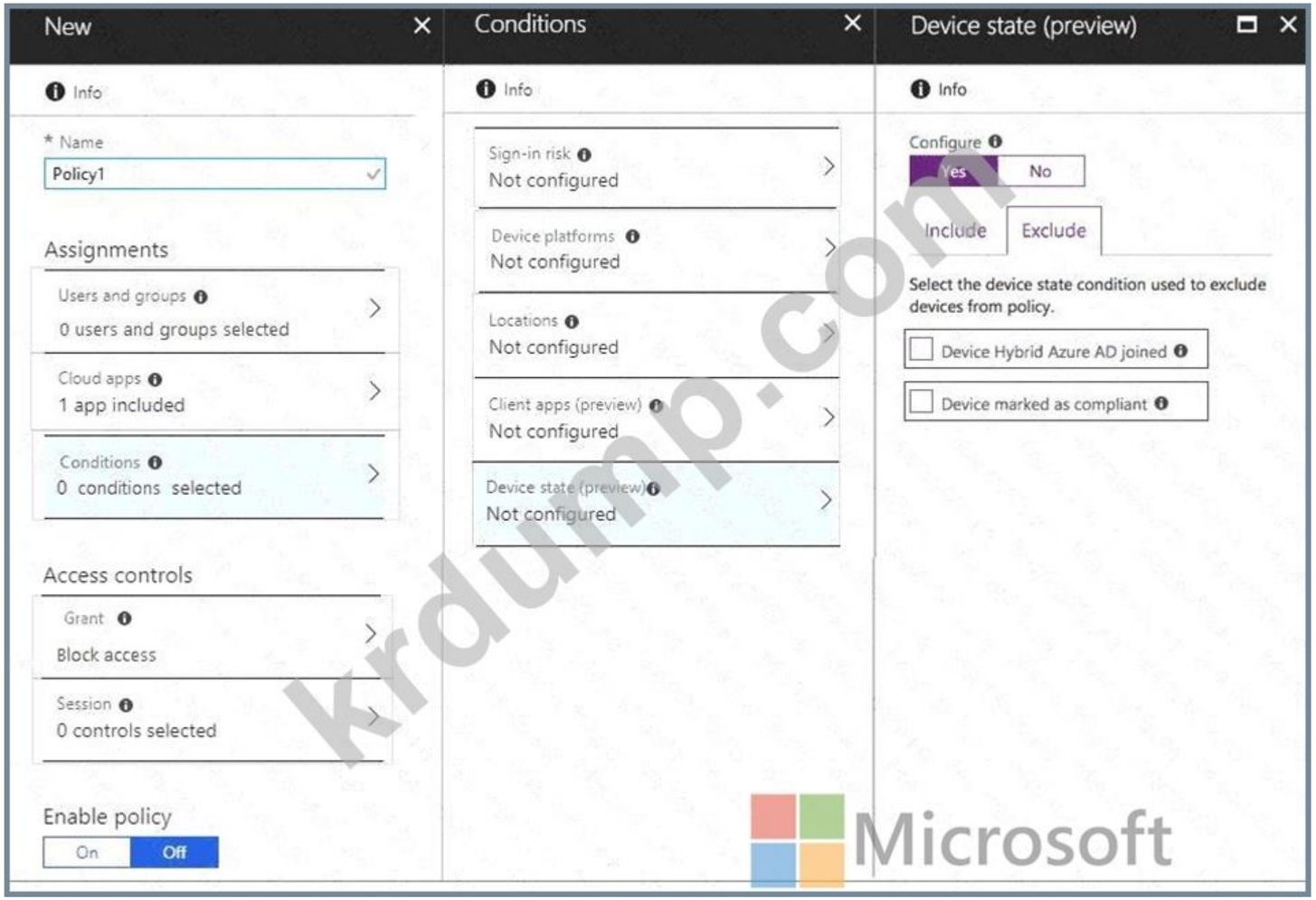
Explanation:

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

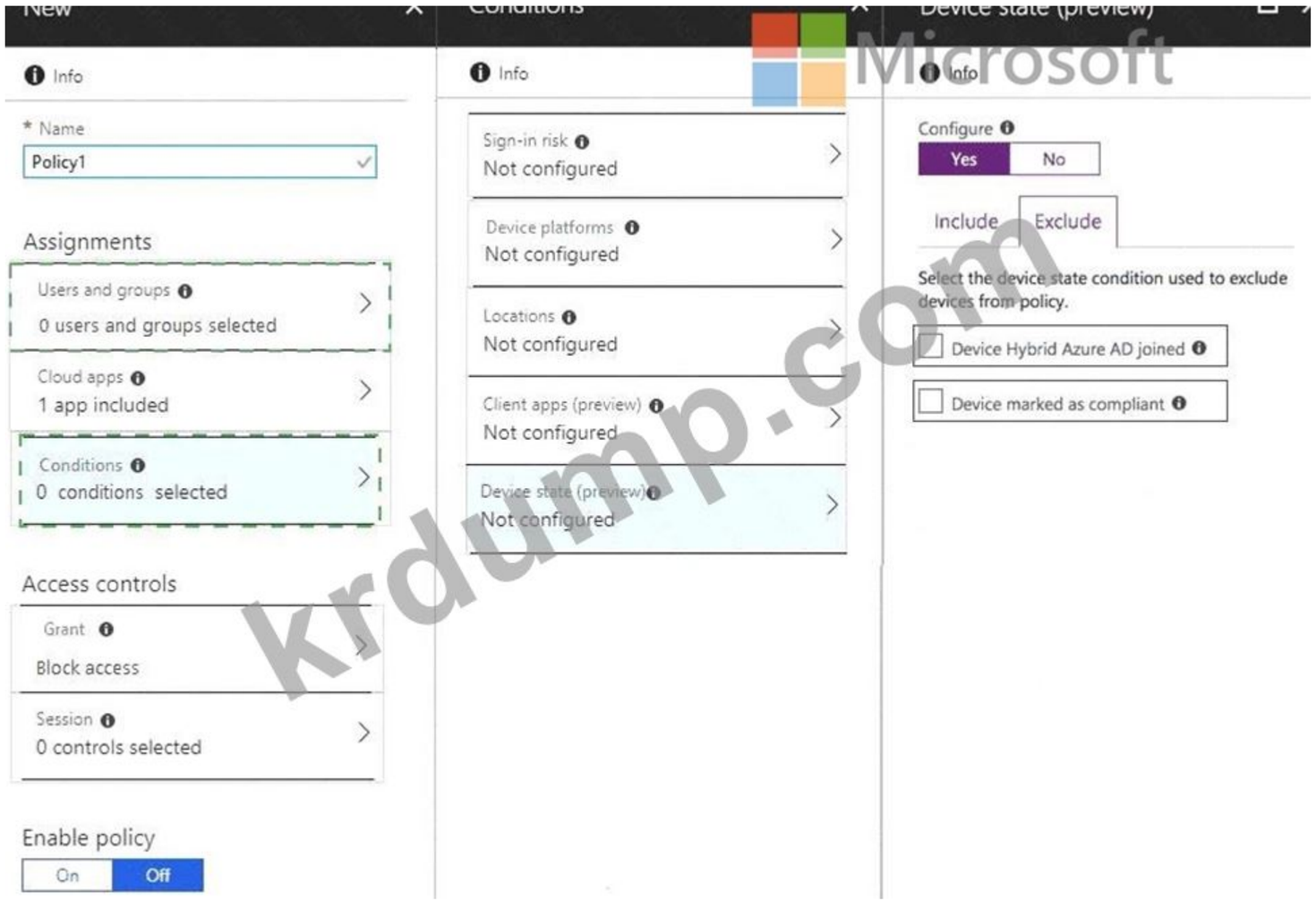
NEW QUESTION: 243
□□□ □□□□□ □□□ Microsoft Entra □□□□ □□□□ □□□□.
□ □ □, □□ □□□ Microsoft Entra Connect Health □□□□□ □□□□□□□.
□□ □□□ □□□ □□□□□ □□□□□.
□□□ Server1□□□ □□□ □□□ □□□□□ □□□□□, □□ □□□ Microsoft Entra Connect □□□ □□ □□□ □□□□ □□ □□ □□□□□□.
□□ □□□□ Server1□ □□□□ □□□□ □□□□ □□□ □□□□□□□.
Server1□ □□□ □□□ □ □□□ □□□□ □□□.
□□□ □□□ □ □□ □ □□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. Azure □□□□ □□□ Connect-Microsoft Entra ID cmdlet□ □□□□□.
B. Server1□□ Microsoft Entra Connect Health □□□□□ □□ □□□□□□.
C. Server1□□ Microsoft Entra Connect Health Services □□ □□□ □□(□□ □□)□□ □□□□□.
D. Windows PowerShell□□ Rejister-ArureADConnectHealthsyncAgent cmdlet□ □□□□□.
E. Server1□□ Microsoft Entra Connect Health Services □□ □□□ □□□□ □□□□□.

Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 244
□□ □□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□□ □□□.
Exchange Online□ □□□□ □□□ □□□□□.
Policy1□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

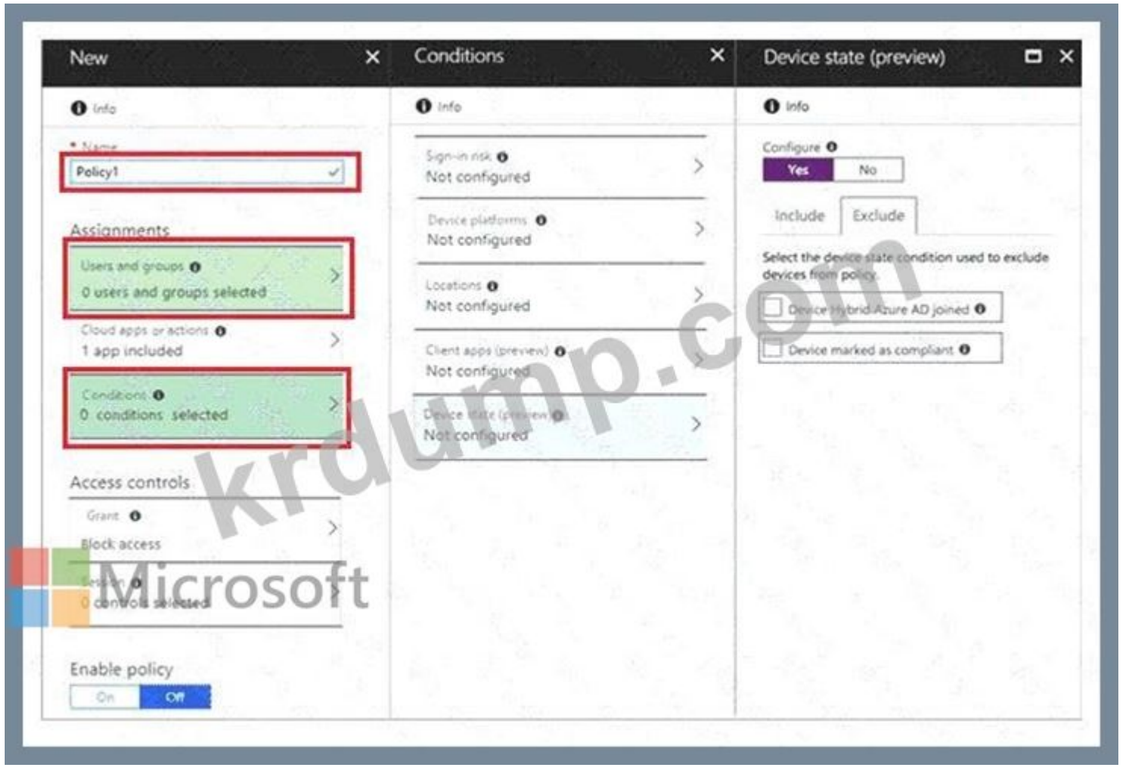


Answer:



Explanation:

Suggested answer:



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

Topic 1, Contoso, LtdOverview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 ES subscription.

Existing Environment

Requirement

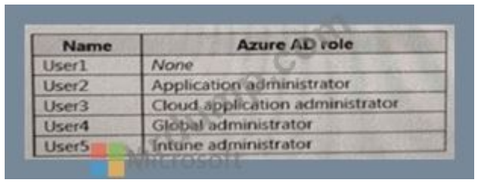
The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops are Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Microsoft Entra ID (Microsoft Entra ID) and includes the users shown in the following table.



Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.
Planned Changes
Contoso plans to implement the following changes:
*Implement Microsoft 365.
*Manage devices by using Microsoft Intune.
*Implement Microsoft Entra IDvanced Threat Protection (ATP).
*Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.
Technical Requirements
Contoso identifies the following technical requirements:
*When a Windows 10 device is joined to Microsoft Entra ID, the device must enroll in Intune automaticity.
*Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
*User1 must be able to enroll all the New York office mobile devices in Intune.
*Azure ATP sensors must be installed and must NOT use port mirroring.
*Whenever possible, the principle of least privilege must be used.
*A Microsoft Store for Business must be created.
Compliance Requirements
Contoso identifies the following compliance requirements:
*Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
*Configure Windows Information Protection (W1P) for the Windows 10 devices.

NEW QUESTION: 245
Microsoft 365 E5 □□□ □□□□.
Mailbox1□□□ □□□□ □□□□ □□ □□□ □□□□ □□□ □□□□□.
□□ □□ □□□ □□□□□ Office 365□ Microsoft Defender□ □□□□ □□□.
* Mailbox1□□ □□ □□□□ □□□□□ □□□□ □□□□□.
* □□□ □□ □□ □□ □□□□ □□ □□ □ □□□ □□□ □□□□□.
□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

Answer Area

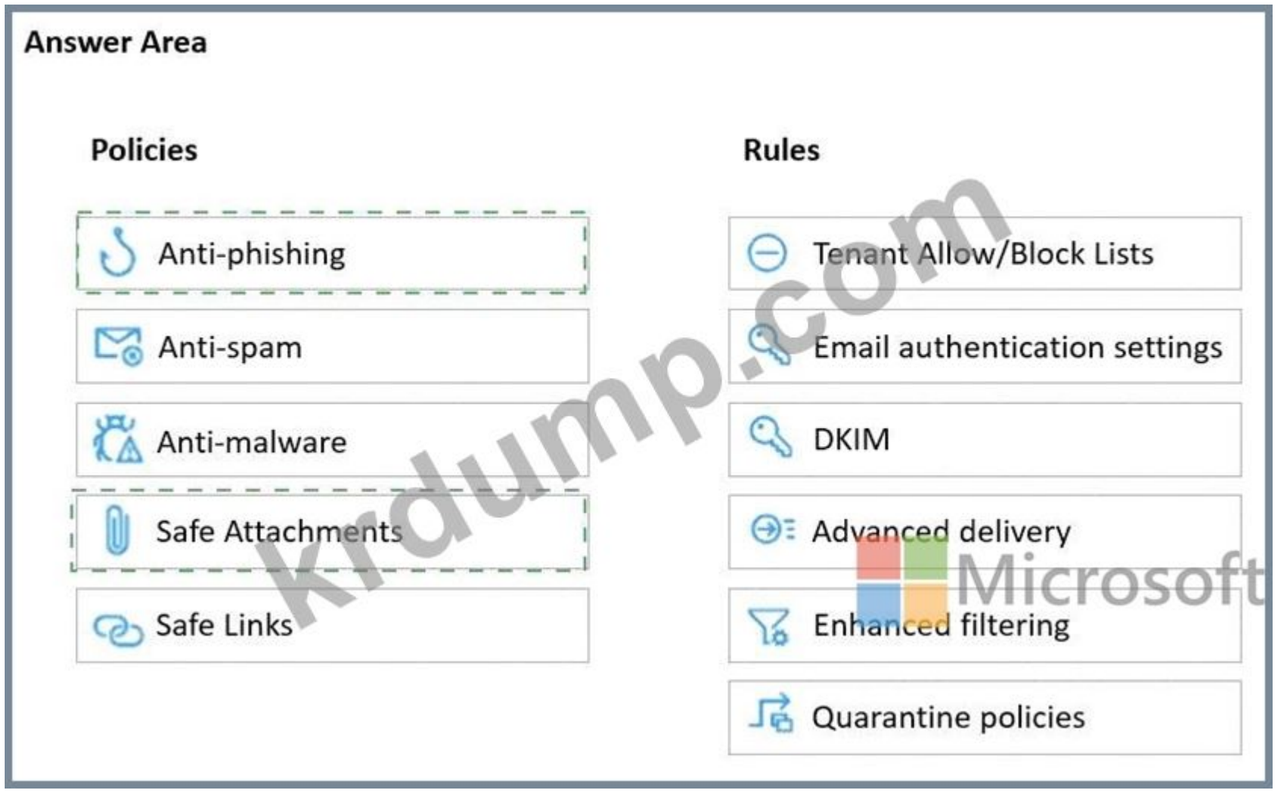
Policies

- 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: 246
Microsoft 365 E5 □□□ □□□□.
Policy1□□□ □□□ □□□ □□ □□□ □□ □□□□□.
Policy1□ □□□□ □□□□ □□ □□□ □□ □□□ □□□□ □□□ □ □□□ □□ □□□.
Microsoft Defender □□□□ □□□ □□ □□□?
A. □□□ □□□□ □□□□□□.
B. □□ □□□ □□□□□.
C. 0□□ □□ □□(ZAP)□ □□□□□□.
D. □□□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 247
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 □□□ □□□□.

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

□□ □□□ □□ □□ □□ □□□ □□□□ □□□□□.

Settings

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

Show app and profile installation progress.	Yes / No
Show time limit error when installation takes longer than specified number of minutes.	60
Show custom message when time limit error occurs.	Yes / No
Allow users to collect logs about instalattion errors.	Yes / No
Only show page to devices provisioned by out-of-box experience (OOBE)	Yes / No
Block device use until all apps and profiles are installed	Yes / No

□□ □□□ Group1□ □□□□□.

□□ □□ □□□ □□□ □□□□□.

Name	Platform
Device1	Windows 10
Device2	Android

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

□□□□: □□ □□□ 1□□□□.

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

Answer:

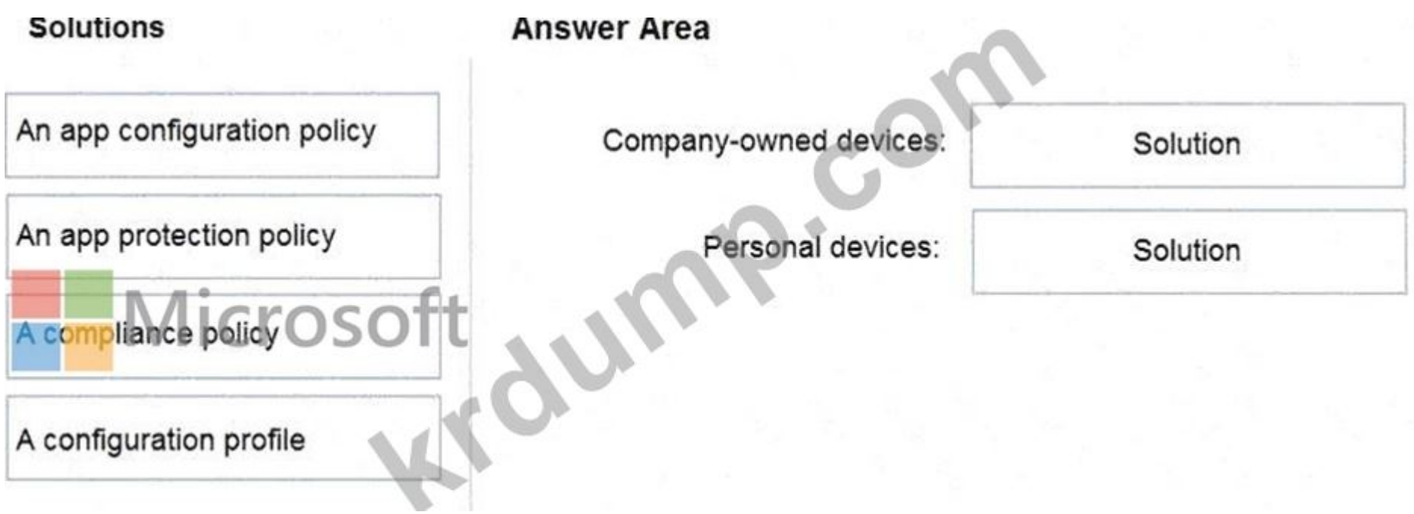
Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	○	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○
If User2 performs the initial device enrollment for Device2, the Enrollment Status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

Explanation:

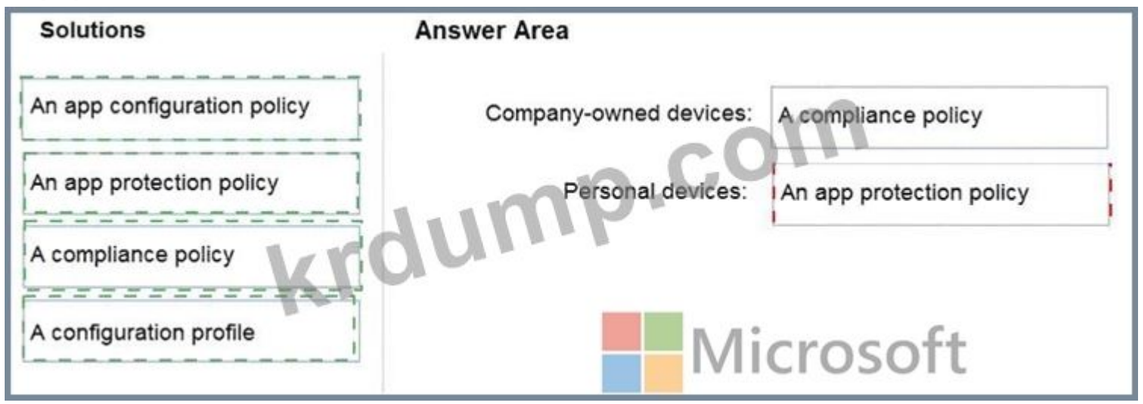
Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	○	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○
If User2 performs the initial device enrollment for Device2, the Enrollment Status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

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

NEW QUESTION: 248
□□□ □□□□ Microsoft 365 E5 □□□□ □□□□.
□□□□ □□ □ □□ □□□ Android □□□ □□ □□□□ □□□□ □□□□ □□□□□□. □□ □□□ □□ □□□ □□ □□□ □□ □□□□ Microsoft Exchange Online □□□□ □□□□ □ □□□□.
□□□ □□ □□□ □□□□ □□□ □□□□ □□ □□□□ □□□ □ □□ □□□□ □□□□ □□□.
□ □□ □□□ □□ □□□□ □□□ □□□□ □□□? □□□□ □□□ □□ □□□ □□□ □□□ □□□□□□. □ □□ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□ □ □□ □□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 249

□□□ Microsoft 365 □□□ □□□□ □□□□.

□□ □□□ □□□□ □□□.

* Microsoft 365 □□□ □□□ □□□□□.

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

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

□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 250

□□ □□□ Azure ATP □□□ □□□□ □□□?

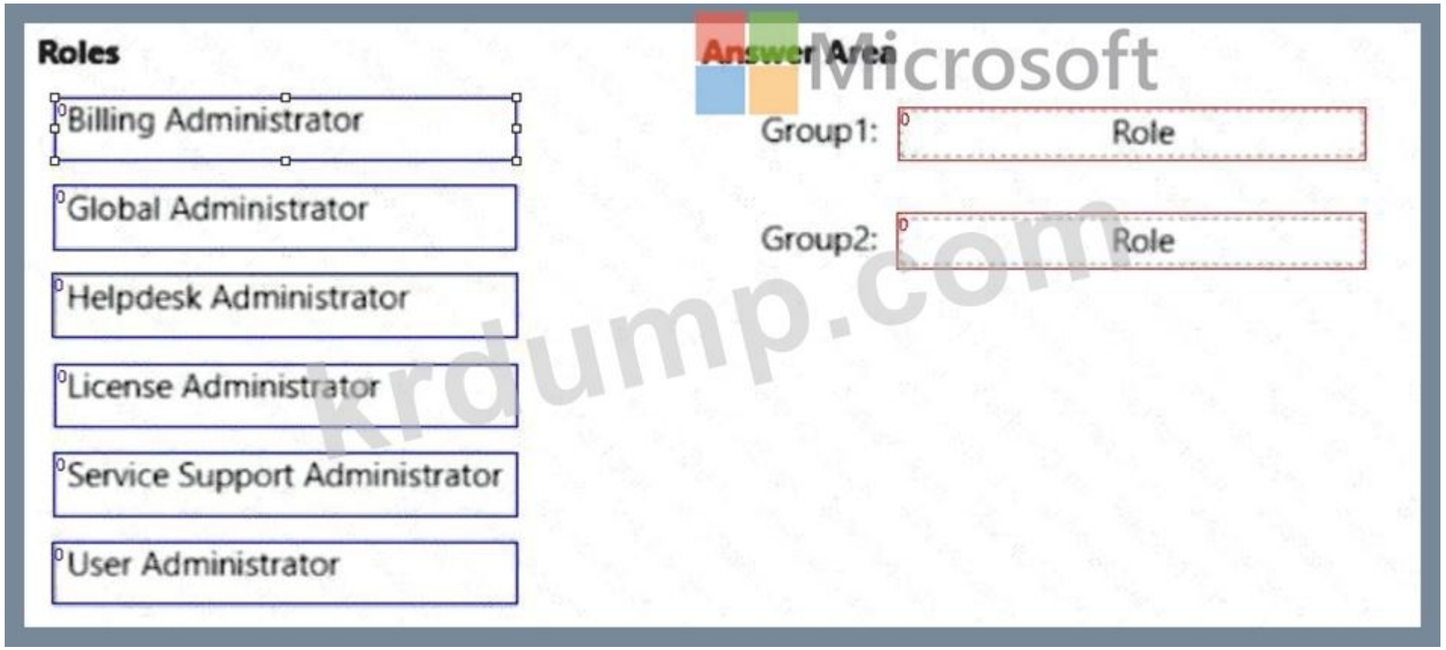
A. □□ 1

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

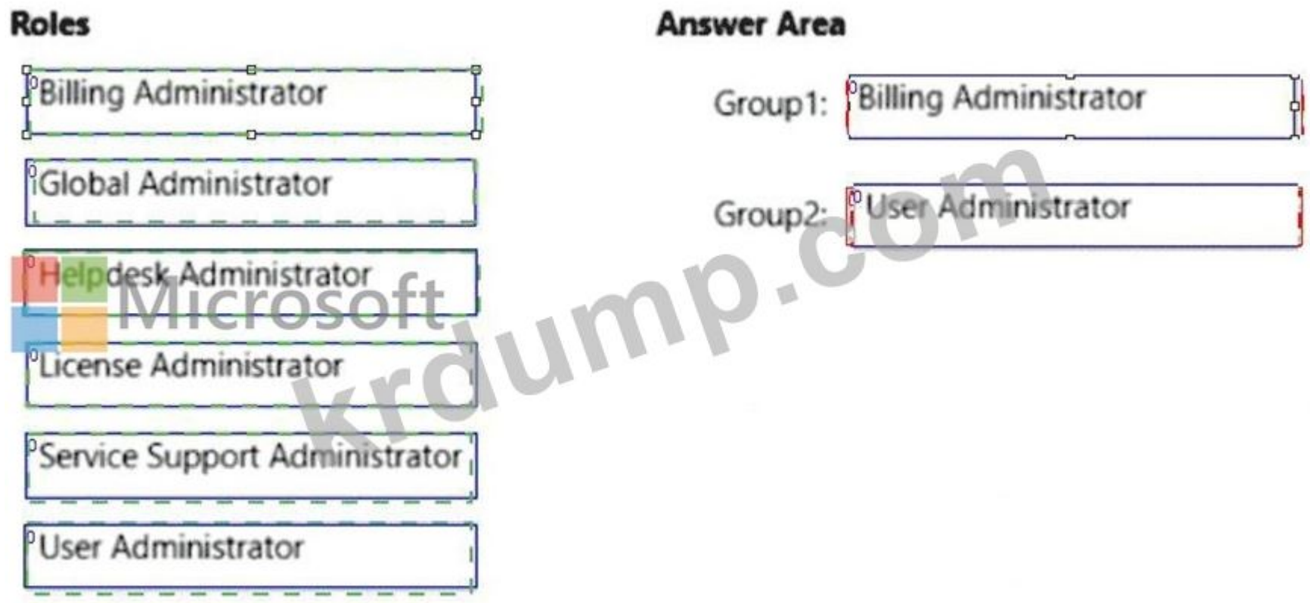
NEW QUESTION: 251
□□□ □ □□
Group1□ Group2□□ □ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.
□ □□□ □□ □□ □□□ □□□ □□□ □ □□□ □□□□ □□□.

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

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



Answer:



Explanation:

Box 1: Billing admin

manage service request

Purchase new services

Etc.

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

Box 2: User admin

User admin

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

- Add users and groups
- Assign licenses
- Manage most users properties
- Create and manage user views
- Update password expiration policies
- Manage service requests
- Monitor service health

Reference:

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

NEW QUESTION: 252

□□□

□□□□□□ □□□□□ 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 □□□ □□□□□□□.

Microsoft Entra □□□□ □□□□ □□□□ □□□.

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

□□: □□ □□□ 1□□□□.

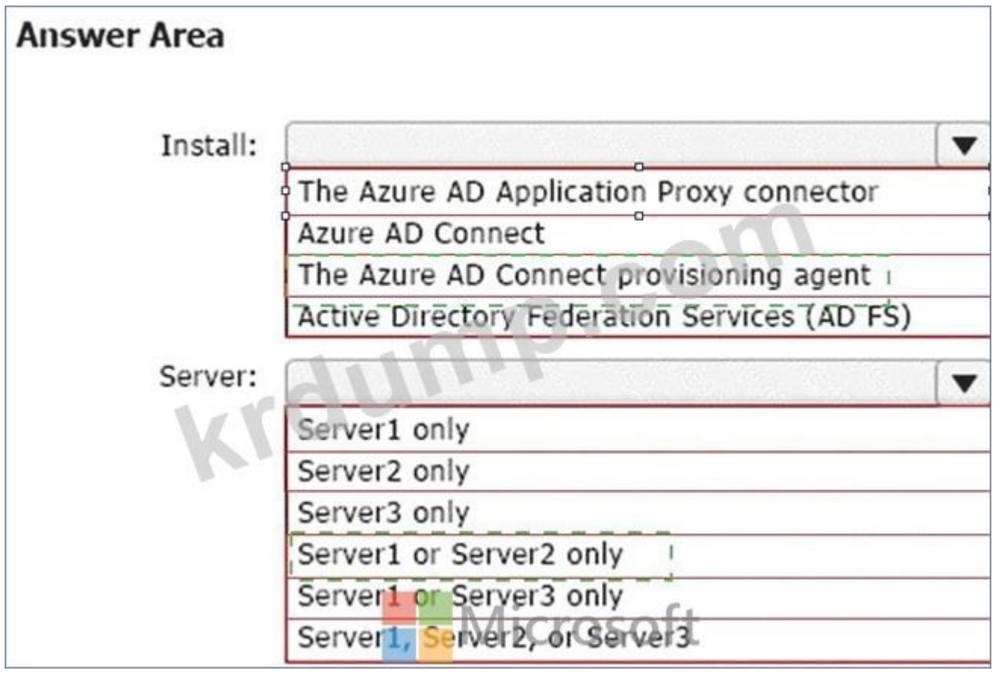
Answer Area

Install:
- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:
- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

Answer:

Answer Area



Explanation:

Answer Area

Microsoft

Install:

- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:

- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

Box 1: The Microsoft Entra Connect Sync provisioning agent

Install the Microsoft Entra Connect Sync provisioning agent

How is Microsoft Entra Cloud Sync different from Microsoft Entra Connect Sync sync?

With Microsoft Entra Cloud Sync, provisioning from AD to Microsoft Entra ID 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 Microsoft Entra ID and AD. The provisioning configuration is stored in Microsoft Entra ID 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: 253

□□□□□ contoso.local□□□ Active Directory □□□□□ □□□□.

Microsoft 365 □□□ □□□□□.

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

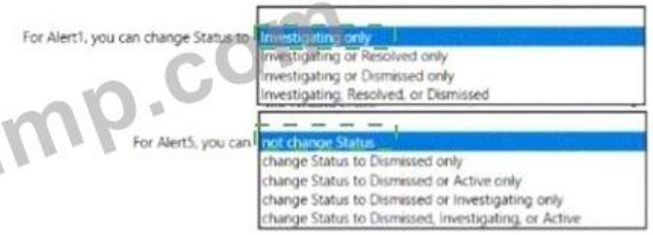
Microsoft 365□□ □□□ □□□ □□□□ □□□.
□□□□ □□□□ □□□□ □□ □□□ □□ □□ □□□ □□□□□? □ □ □□□ □□ □□□□ □□□ □□□ □ □□□□. □□ □□ □□□ □□□□□.
A. □□ X.509 □□□□ □□□□□.
B. □□ □□□□ □□□□□ □□□□.
C. Active Directory □□□□□ □□□ □□□□.
D. □□□ □□ □□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on-premise Active Directory if it's a routable domain name, for example, contoso.com.
If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active Directory.
Incorrect:
Not C: No need to rename the Active Directory forest. As we use a non-routable domain name contoso.local, we just need to add the routable domain name as a UPN suffix in Active Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization

NEW QUESTION: 254
Microsoft 365 ES □□□□ □□□□.
□□ □□□□□ □□□ □□□ □ □□□□.

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

Answer:

Answer Area



Explanation:

Answer Area

NEW QUESTION: 255

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

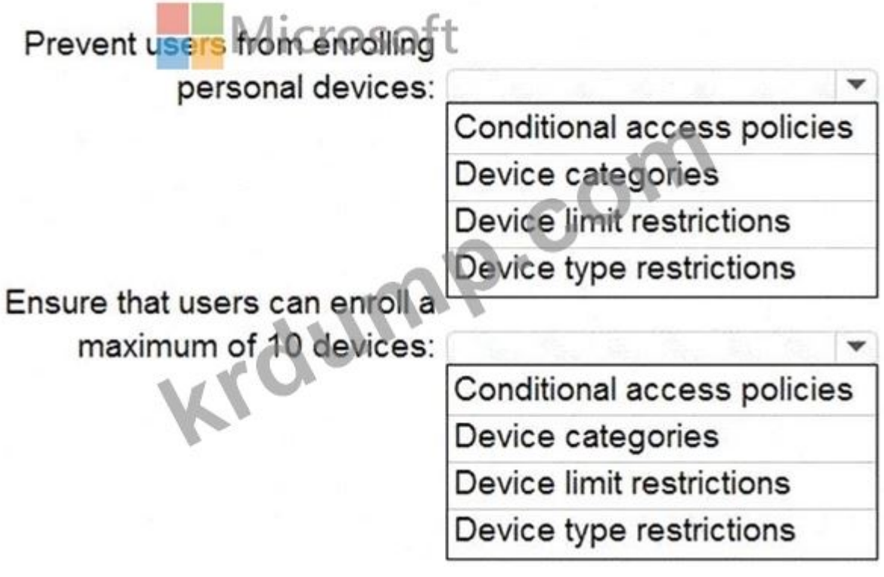
□□ □□ □□□ □□□□□ Intune□ □□□□ □□□.

□□□□ □□ □□□ □□□□ □□□□ □□□.

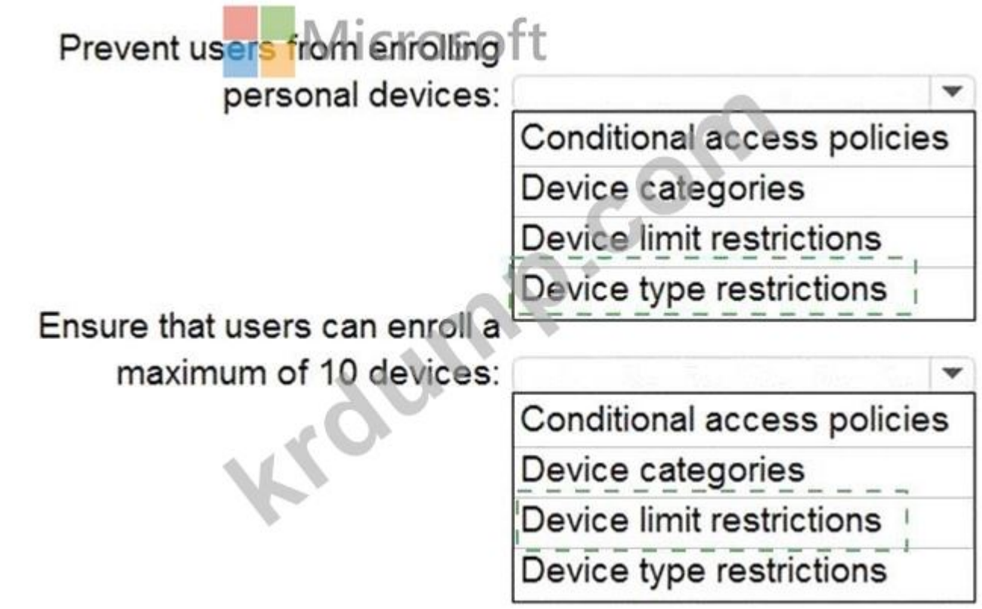
□□□□ □□ 10□□ □□□ □□□ □ □□□ □□□□□.

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

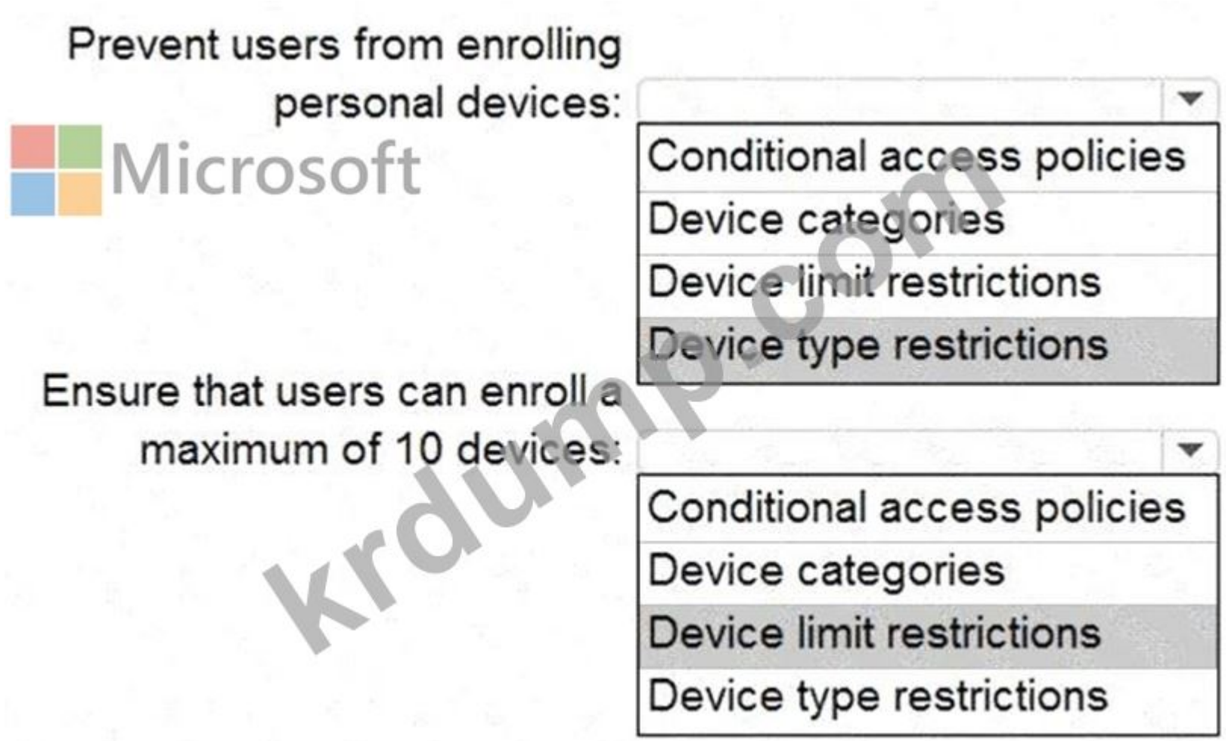
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#blocking-personal-windows-devices

NEW QUESTION: 256
Microsoft 365 E5 □□□ □□□□.
□□ □□□ □□ □□□ □□□ □□□ □□ □□(DLP) □□□ □□ □□□□□.
□□□ DLP □□□□ □□ □□□ □□□ □ □□□?
A. □□□ □□ □□
B. □□□ □□ □□
C. □□□
D. □□□ □□□
Answer: (SHOW ANSWER)
Apply retention labels to content automatically if it matches specific conditions, that includes cloud attachments that are shared in email or Teams, or when the content contains:
Specific types of sensitive information.
Specific keywords that match a query you create.
Pattern matches for a trainable classifier.
Note: Retention policies can be applied to the following locations:
Exchange mailboxes
SharePoint classic and communication sites
OneDrive accounts
Microsoft 365 Group mailboxes & sites
Skype for Business
Exchange public folders
Teams channel messages (standard channels and shared channels)
Teams chats
Teams private channel messages
Yammer community messages
Yammer user messages
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-exchange-conditions-and-actions

NEW QUESTION: 257
□□□ Contoso, Ltd.□□ □□□□ □□□□.
Contoso□ □□ □□ □□□ DNS □□□□ □□□□□ □□□ Microsoft 365 □□□ □□□□ □□□□.
Contoso□ Fabrikam, Inc.□□ □□□ □□□□□.
Contoso□ □□ □□□□ Microsoft 365 □□□ □□□ □□□□□.
* □□□□□□

* □□□.□□□□□□
* □□□.□□□.com
□□ □□□ □□□□ □ □□□□ □□□ □□□ □ □□□ □□□□ □□□.
□ □□ □□□□ □□□□ □□, □□□□ □□ □□ □□□□□□ □□ DNS □□□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 258

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

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

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

NEW QUESTION: 259

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

A. □

B. □□□

NEW QUESTION: 260

Answer: A (LEAVE A REPLY)

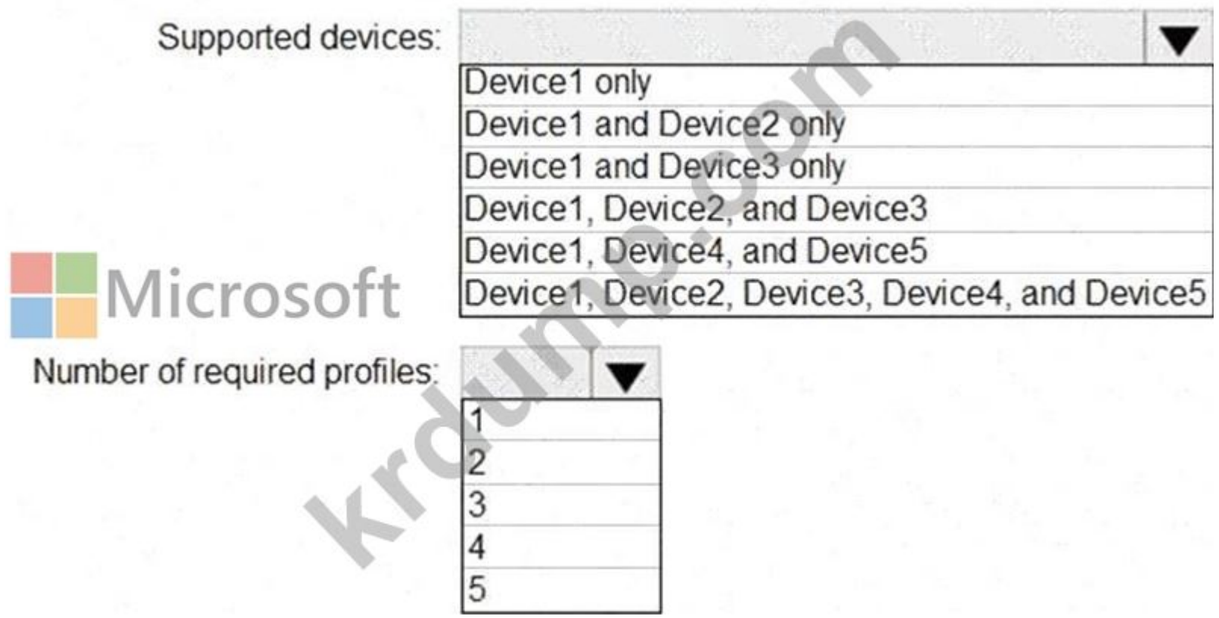
Microsoft 365 □□□ □□□□.

□□□□ eDiscovery □□□ □□□ □□□□ □□□□ □□□.

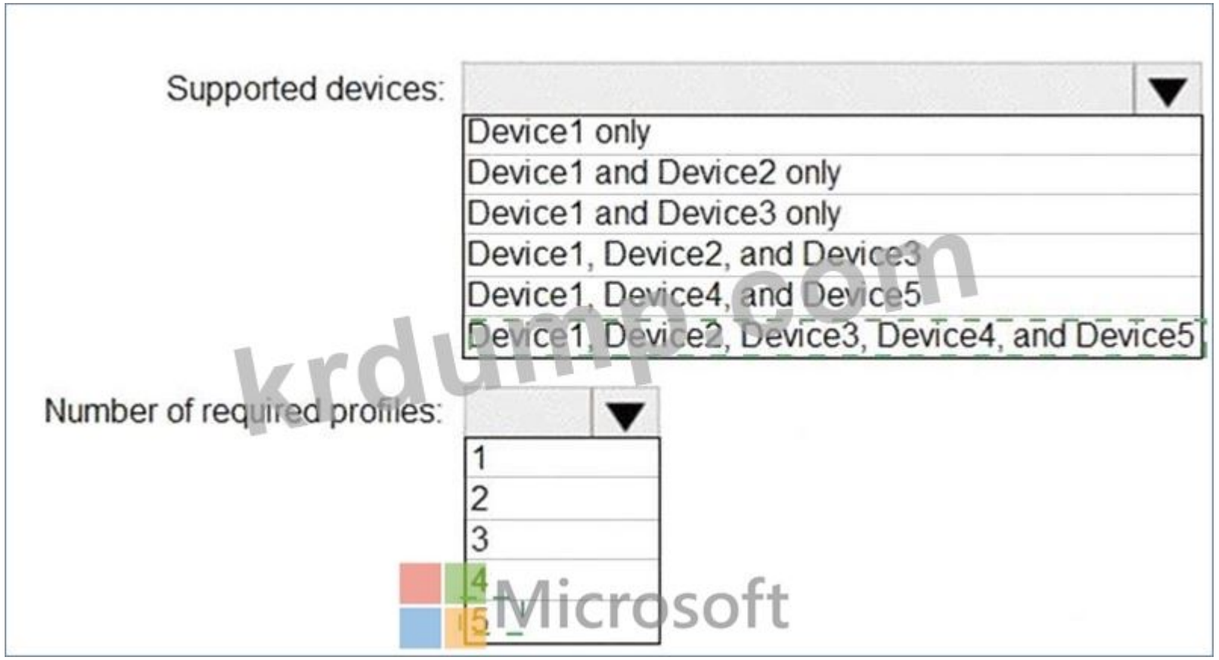
□□ □ □□ □□ □□ □□□□ □□□ □□ □□□?
A. □□ □□ □□ □□
B. □□ □□ □□
C. □□□ □□□ □□□□□.
D. eDiscovery □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 261
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□□ □□ □□□□ □□□(FIDO2)□ □□□□ □□ □□□ □□□ □□□□□.
□□ □□□□ □ □□□(FIDO2)□ FIDO □□□□□ □□□□□ □□□□ □□□□ □□□□□□ □□□□ □□□.
□□ □□□ □□□□□ □□□?
A. □ □□ □□
B. □□ □□ □□
C. □□ □□□ □□ □□
D. □□ □ □□
Answer: B (LEAVE A REPLY)
The correct setting is Enforce attestation. In Microsoft Entra ID authentication methods policy, passkeys /FIDO2 can be configured so that attestation is required during registration. Microsoft states that when Enforce attestation is set to Yes, attestation is required at registration time, and Microsoft Entra ID can verify the authenticator's make and model against trusted metadata. This is exactly what the question asks for: validating the passkey during enrollment by using trusted metadata from the FIDO ecosystem.
Microsoft also explains that Microsoft relies on the FIDO Alliance Metadata Service (MDS) to determine passkey/FIDO2 authenticator compatibility, and that vendors publish authenticator metadata to the FIDO MDS. When attestation is enforced, Microsoft requires extra metadata from passkeys registered with the tenant, allowing Microsoft Entra ID to validate whether the authenticator meets attestation requirements.
Enforce key restrictions is different: it allows or blocks specific passkey models or providers by AAGUID.
Allow self-service setup only permits users to register passkeys themselves. Restrict specific keys is not the setting that performs FIDO MDS verification during enrollment. References/topics: Microsoft Entra authentication methods policy, Passkey/FIDO2 configuration, FIDO2 attestation, FIDO Alliance Metadata Service.

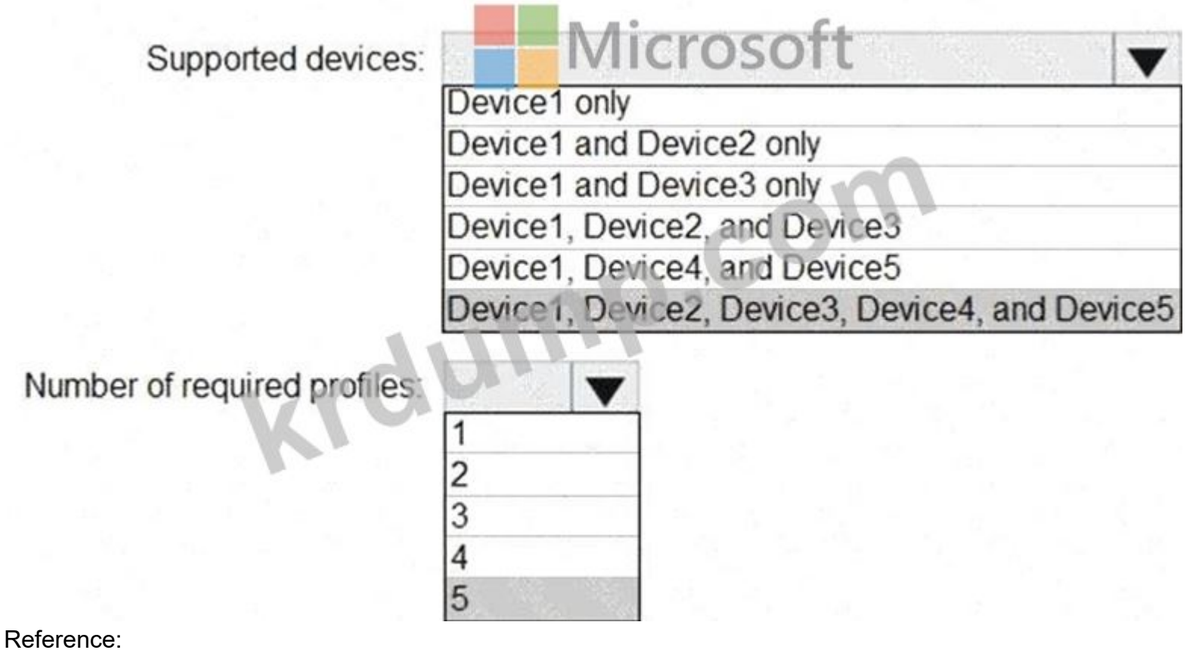
NEW QUESTION: 262
□□□ □□ □□□ □□□□ □□ □□□□□ □□ □□ □□ □□□□ □□□ □□□□□.
□□ □□□ □□□□, □□□ □□□ □□ □□□□ □□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



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

NEW QUESTION: 263
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

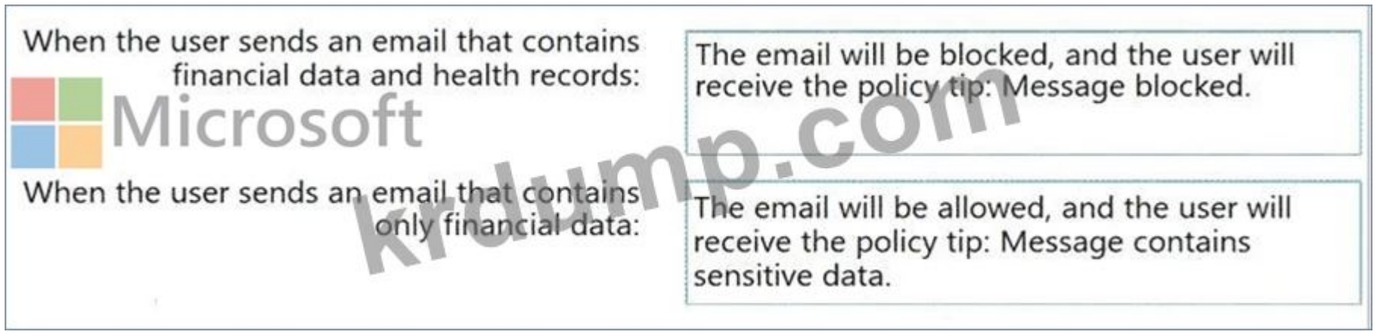
- The email will be blocked, and the user will receive the policy tip: Message blocked.
- The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.
- The email will be allowed, and the user will receive the policy tip: Message blocked.
- The email will be allowed, 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: 264

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

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

□□ □ □□ □□□ □□□□ □□□ □□□□ □ □□□?

□□□ □□□ □□□ □□□□ □□□□□.

A. □□□□ □□ □□

B. Microsoft Power Automate □□□□

C. □□□ □□ □□ □□

D. □□ □□□□

E. □□□ □□

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 265

□□□□□□ contoso.local□□□ □□□ □□□□□ Active Directory □□□□ □□□□. □ □□□□□ 5□□ □□□ □□□□□ □□□□.

□□□ Microsoft 365□ □□□□ contoso.onmicrosoft□□ □□□ Microsoft Entra □□□□ □□□□□.

□ □□.

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

□□□ □□ □□ □□□ □□ □□□ □□□□ □□□.

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

□□: □□ □□□ 1□□□□.

A. □□□ □□□□□□ □□ □□□□□ □□□□□.

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

C. Active Director□ '□□□ □ □□□□□ UPN □□□ □□'□□

D. □ □□□ □□□ □□□ □□ □□□ □□□□□.

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

F. □ □□□ □□□ □□□ □□□ □□□ □□□□□.
Answer: A,B,E (LEAVE A REPLY)
Deploy Microsoft Entra ID Pass-through Authentication
Step 1: Check the prerequisites
Ensure that the following prerequisites are in place.
In the Entra admin center
1. Create a cloud-only Hybrid Identity Administrator account or a Hybrid Identity administrator account on your Microsoft Entra tenant. This way, you can manage the configuration of your tenant should your on- premises services fail or become unavailable.
(E) 2. Add one or more custom domain names to your Microsoft Entra tenant. Your users can sign in with one of these domain names.
(A) In your on-premises environment
1. Identify a server running Windows Server 2016 or later to run Microsoft Entra Connect Sync. If not enabled already, enable TLS 1.2 on the server. Add the server to the same Active Directory forest as the users whose passwords you need to validate. It should be noted that installation of Pass-Through Authentication agent on Windows Server Core versions is not supported.
2. Install the latest version of Microsoft Entra Connect Sync on the server identified in the preceding step. If you already have Microsoft Entra Connect Sync running, ensure that the version is supported.
3. Identify one or more additional servers (running Windows Server 2016 or later, with TLS 1.2 enabled) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.
4. Etc.
(B) Step 2: Enable the feature
Enable Pass-through Authentication through Microsoft Entra Connect Sync.
If you ' re installing Microsoft Entra Connect Sync for the first time, choose the custom installation path. At the User sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Microsoft Entra Connect Sync. In addition, the Pass-through Authentication feature is enabled on your tenant.
Incorrect:
Not C: From Active Directory Domains and Trusts, add a UPN suffix
Not D. Modify the email address attribute for each user account.
Not F. Modify the User logon name for each user account.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start

NEW QUESTION: 266
□□□ Microsoft 365 □□□ □□□□ □□□□.
Microsoft Defender XDR□□ eDiscovery Manager □□ □□□ □□□□ US eDiscovery Managers□□ □□ □□□ □□□□.
□ □□ □□□ □□ □□□□ □□□ □□ □□□□ □□□ □□□□ □□□□ □□□ □□□ □□□ □ □□□ □□ □□□.
□□ □□: Windows PowerShell□□ □□□ □□□□□ □□□□ New-complianceSecurityFilter cmdlet□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 267
Microsoft 365 □□□ □□□□.
□□ □□□ □□ □□□ □□ □□□□.

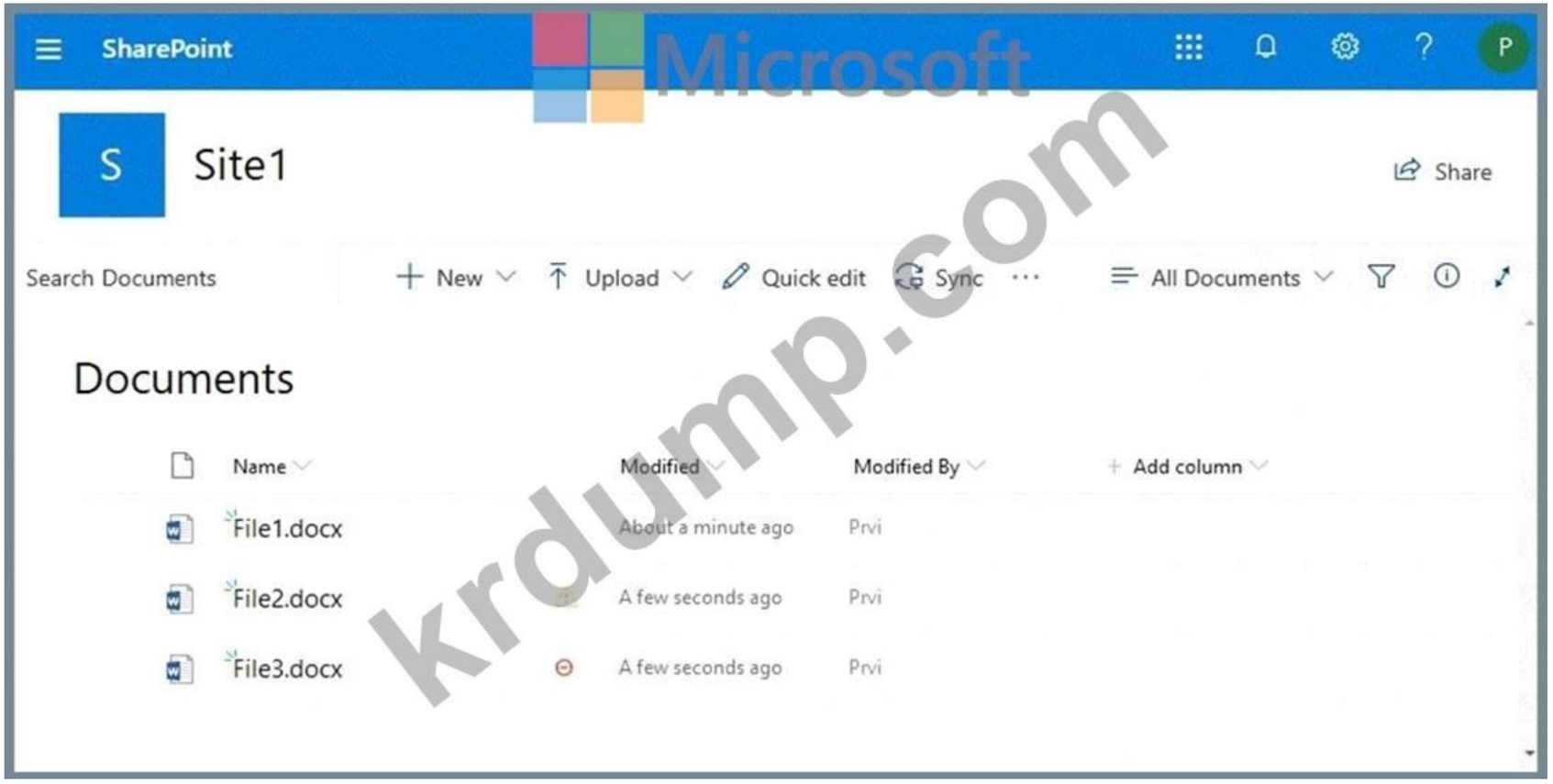
Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

□ □□ □□ File1.docx□□ □□□ □□□ Site1□□□ Microsoft SharePoint □□□□ □□□□□.
File1.docx□ 2022□ 1□ 1□□ □□□□□ □□□□□ 2022□ 1□ 31□□ □□□□□□□. □ □□□ □□ □□□□ □□□□□.
File1.docx□ □□ □□□□ □□□□□?
A. 2023□ 1□ 1□
B. 2024□ 1□ 1□
C. 2023□ 1□ 31□
D. 2024□ 1□ 31□
E. □□ □□
Answer: D (LEAVE A REPLY)
Retention wins over deletion.
Note:
Explanation for the four different principles:
1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system-initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.
2. Etc.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

NEW QUESTION: 268
Microsoft 365 □□ □□ □□□□ Site1□□□ Microsoft SharePoint Online □□□□ □□ □□□ □□ □□(DLP) □□□ □□□□□. Site1□□ □□ □□ □□□ □□□ □□□□ □□□□.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

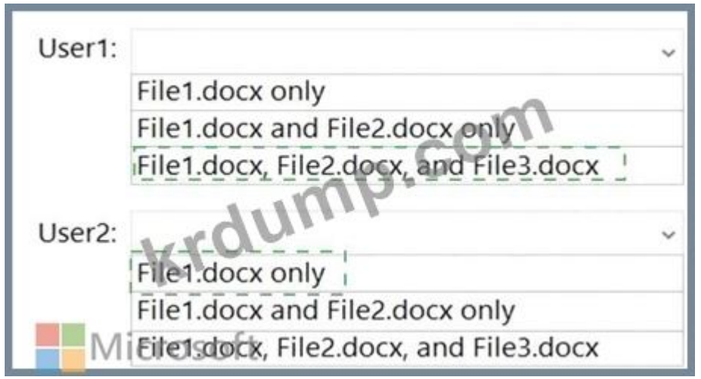
Prvi□ □□□ □□□ □□□ □□□□. (□□ □□ □□□□□.)



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: 269

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

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

□□ 8□□ □□□ □□ □□□□ □□ □□ □□□ □□□□□.

* □□: □□!
* □□ □□
o □□ 70□ □□: □□
o □□ □□ □□: □□(3)

o □□ □□: □□□ □□ □□
* □□□: Userl@contoso.com, User2@contoso.com
□□ 8□ 2□□ □□□ □□ □□□□ □□□□ □□ □□□ □□□□□.
* □□: □□
* □□ □□
o □□ □□□: □□, □□□ □□ □□ □□
o □□ □□ □□: DeviceGroup1, DeviceGroup2
* □□□: Userl@contoso.com
Microsoft Defender XDR□□□ □□ □□ □□ □□□ □□□□□.

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

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

Answer 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:

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.	○	●

NEW QUESTION: 270

□□□ Microsoft 365 □□□ □□□□ □□□□.

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

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

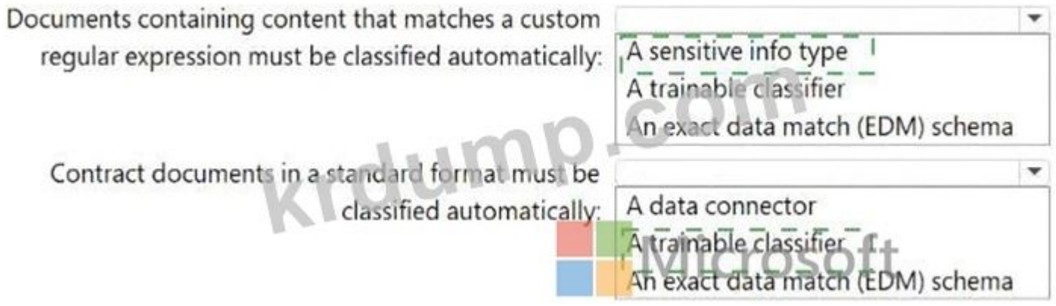
□ □□ □□□ □□ □□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Documents containing content that matches a custom regular expression must be classified automatically:
- A sensitive info type
- A trainable classifier
- An exact data match (EDM) schema

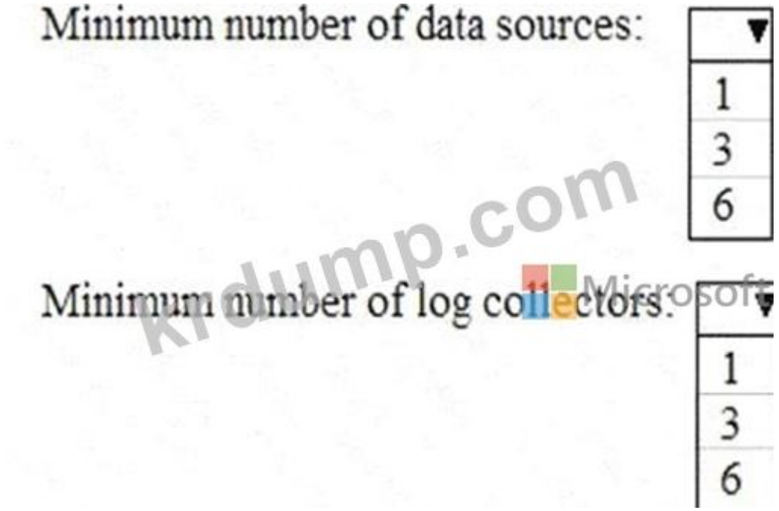
Contract documents in a standard format must be classified automatically:
- A data connector
- A trainable classifier
- An exact data match (EDM) schema

Answer:

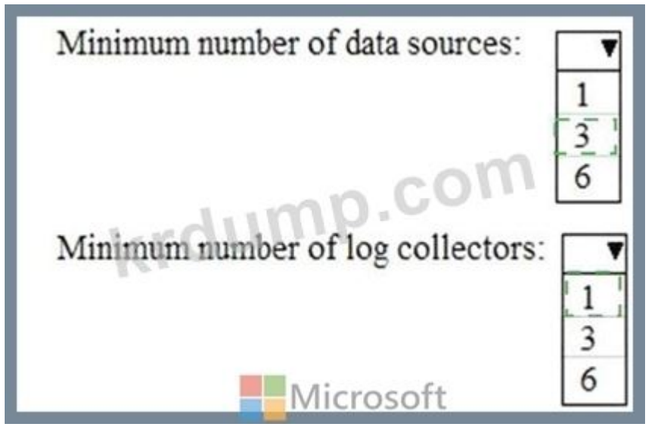


Explanation:
Requirement
Correct selection
Documents containing content that matches a custom regular expression must be classified automatically.
A sensitive info type
Contract documents in a standard format must be classified automatically.
A trainable classifier
The first requirement must use a sensitive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

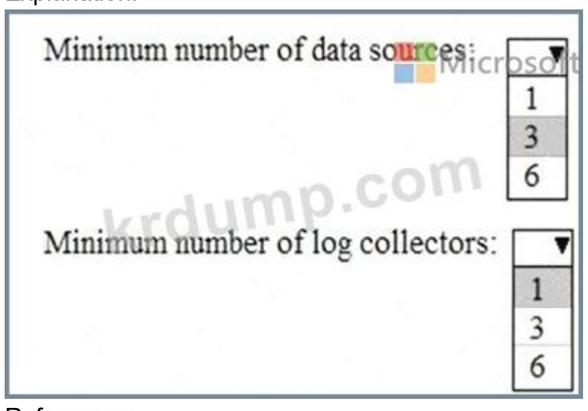
NEW QUESTION: 271
□□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□.
Microsoft Cloud App Security□□ □□□□ □□ □□ □□□ □□ □ □□ □□□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



References:

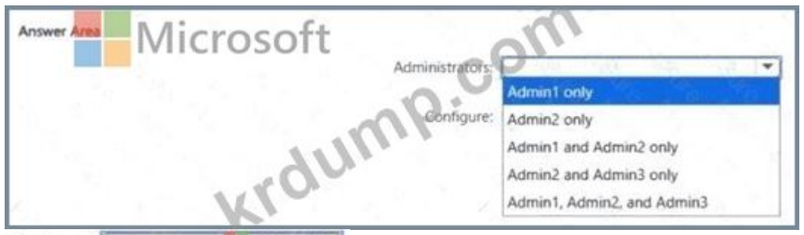
https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

NEW QUESTION: 272

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

Name	Role
Admin1	Exchange Administrator
Admin2	Security Administrator
Admin3	User Administrator

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



Answer:

Explanation:

Answer Area

Administrators: Admin2 only

Configure: Anti-spam

NEW QUESTION: 273

□□□

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

Microsoft 365 E5 □□□ □□□□.

□□ □□□ □□□□□.

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

Groups that can be restored:

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

Retention period:

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

Answer:

Groups that can be restored:

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

Retention period:

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

Explanation:

Answer Area

Groups that can be restored:

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

Retention period:

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

Box 1: Group3 only

Box 2: 30 days

If you ' ve deleted a group, it will be retained for 30 days by default. This 30-day period is considered a " soft- delete " because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

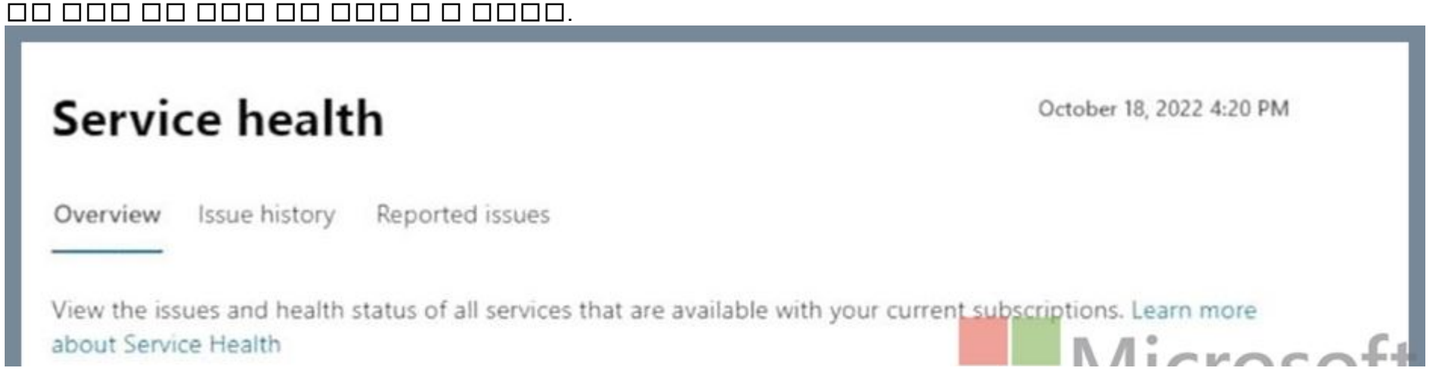
Reference:

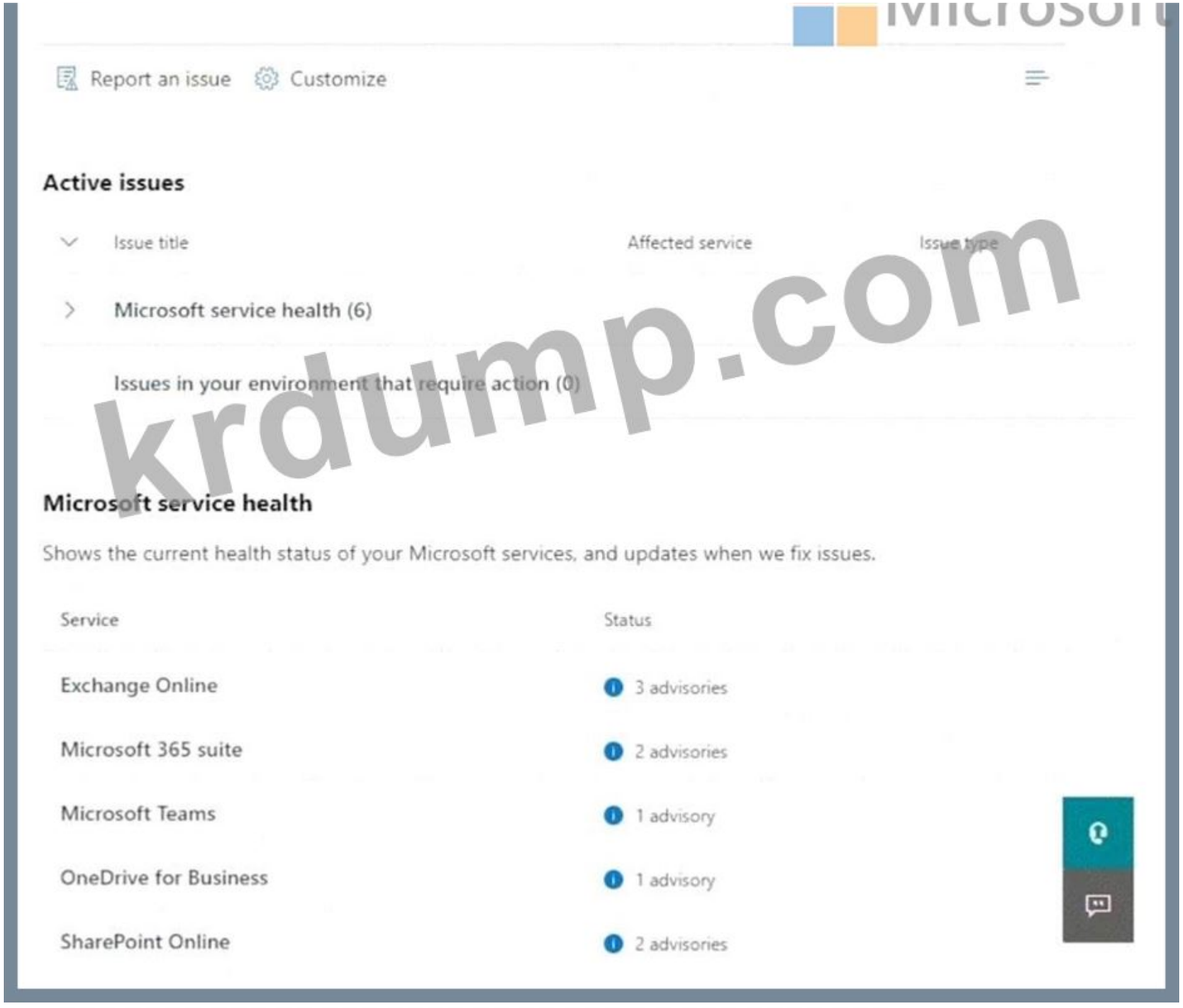
https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/restore-deleted-group

NEW QUESTION: 274

Microsoft 365 □□□ □□□□.

□□ □□□ □□ □□□ □□ □□□ □ □ □□□□.





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

User1□□ □□ □□□ □□□□ □□□?

A. □□□ □□ □□

B. □□ □□□

C. □□□ □□ □□□

D. □□ □□ □□□

Answer: (**SHOW ANSWER**)

Service Support admin

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

NEW QUESTION: 275
□□□ Microsoft 365 E5 □□□ contoso.com□□□ □□□ Microsoft Entra □□□□ □□□□ □□□□.
□□ □□□□ Windows 11□ □□□ □□□□ □□□□ □□□, contoso.com□ □□□□ □□, BitLocker □□□□ □□□(BitLocker)□ □□□□ □□□□ □□□□.
□□□ □□□ □□ □□□ □□□ Admin1□□□ □□□ □□□□ □□□ □□□□□.
* BitLocker □□ □□ □□□□□.
* contoso.com□□ □□□□ □□ □□□ □□□□□□.
□□ □□□ □□□□□ Admin1□ □□□ □□□□ □□□. □ □□□□ □□ □□ □□□ □□□ □□□. □□ □ □□ □□□ □□□□ □□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Devices

- ☐ Cloud Device Administrator ⓘ
- ☐ Desktop Analytics Administrator ⓘ
- ☐ Intune Administrator ⓘ
- ☐ Printer Administrator ⓘ
- ☐ Printer Technician ⓘ
- ☐ Windows 365 Administrator ⓘ

Global

- ☐ Global Administrator ⓘ

Identity

- ☐ Application Administrator ⓘ
- ☐ Application Developer ⓘ
- ☐ Authentication Administrator ⓘ
- ☐ Cloud Application Administrator ⓘ
- ☐ Conditional Access Administrator ⓘ
- ☐ Domain Name Administrator ⓘ
- ☐ External Identity Provider Administrator ⓘ
- ☐ Guest Inviter ⓘ
- ☐ Helpdesk Administrator ⓘ
- ☐ Hybrid Identity Administrator ⓘ
- ☐ License Administrator ⓘ
- ☐ Password Administrator ⓘ

Answer:

Answer Area

Devices

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

Global

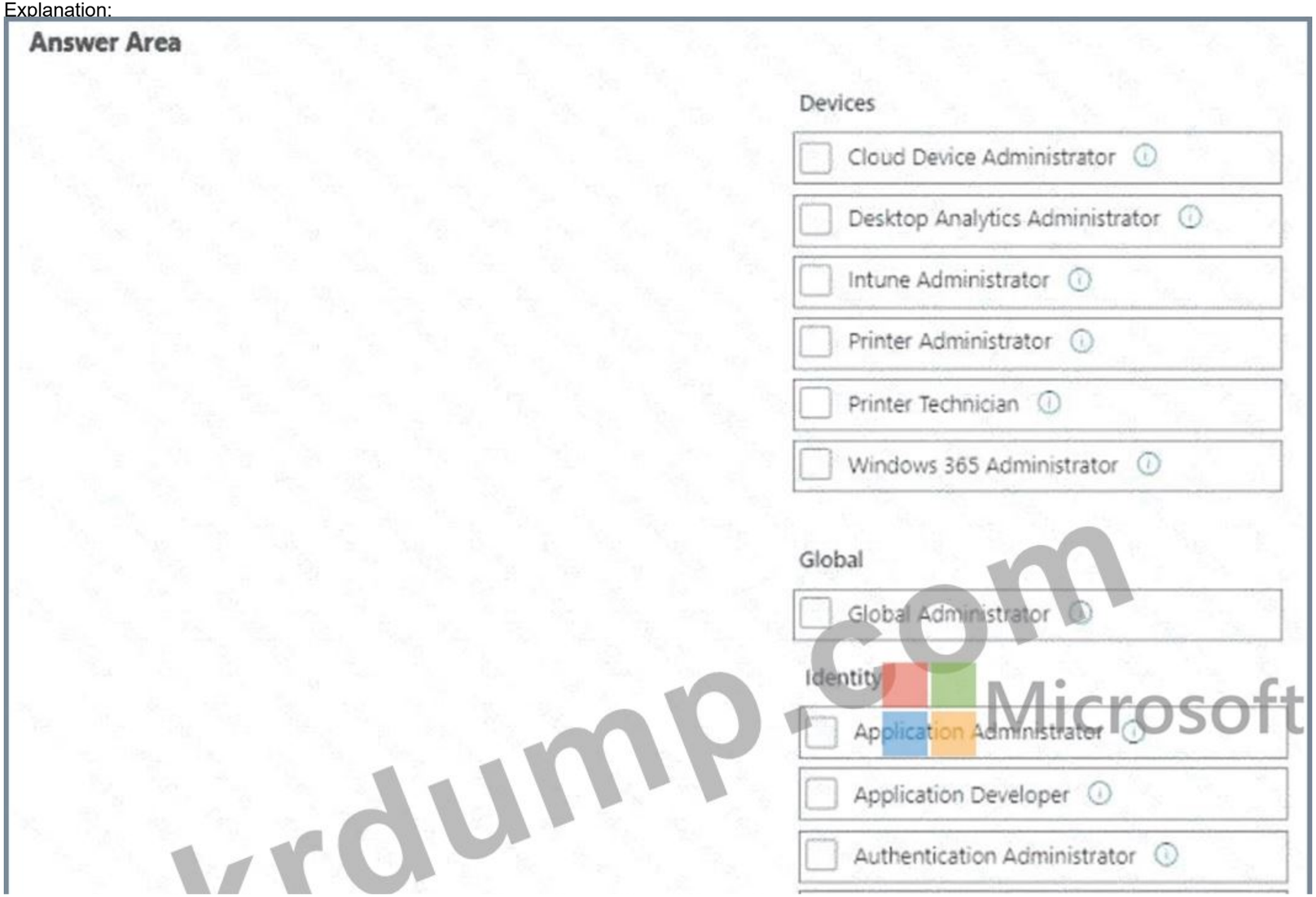
- [ ] Global Administrator

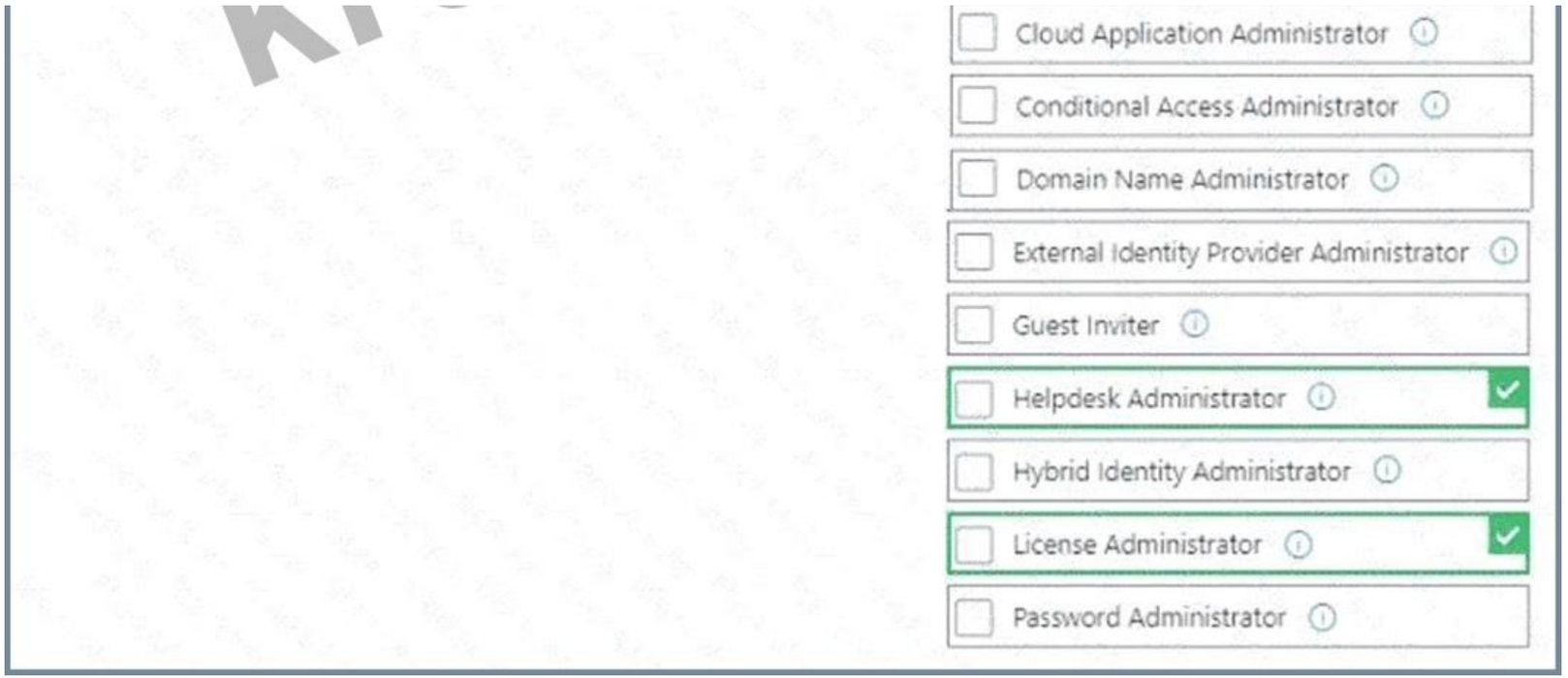
Identity

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

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

Explanation:



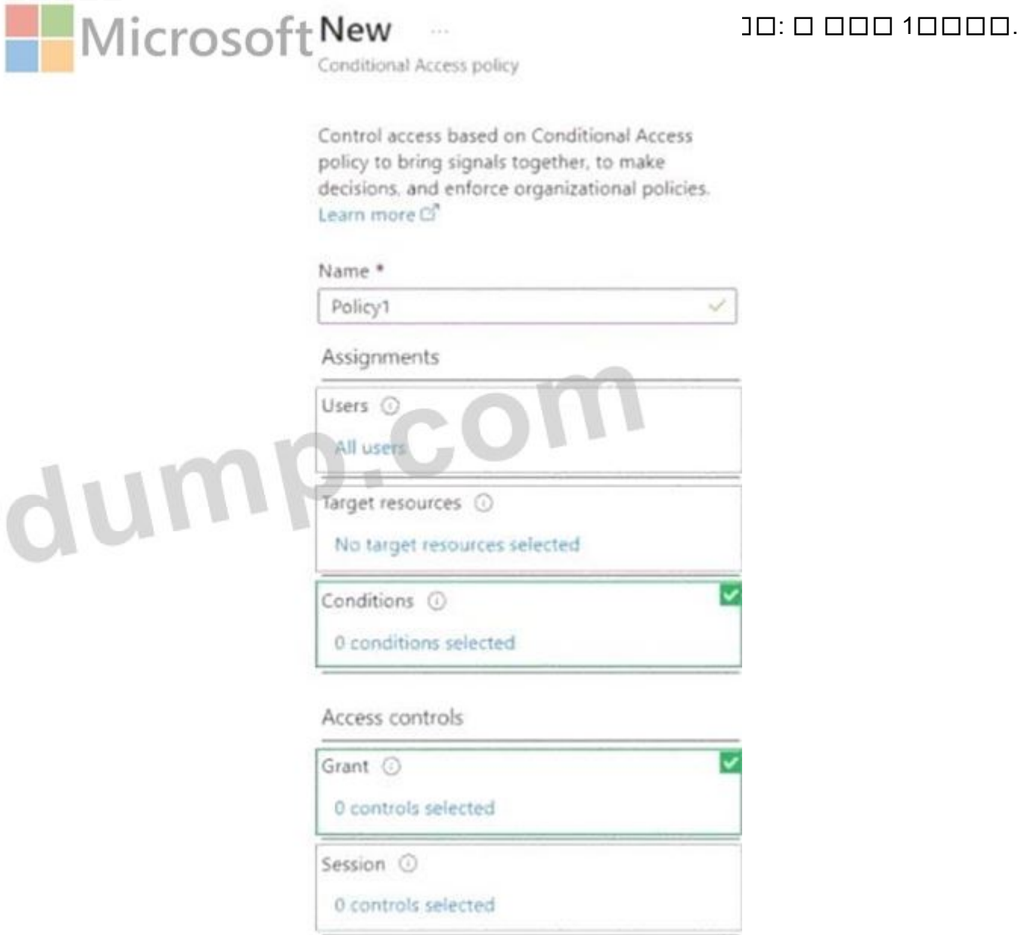


NEW QUESTION: 276
User1□□□ □□□□ □□□ Microsoft 365 □□□ □□□□.
User1□ □□ □□□ □□□□ □□ □□□ □□□ □□□□□.
Microsoft Exchange Online □□□ □□□□□.
Microsoft 365 □□□ □□□□.
User1□ □□□ □□□ 8□□ □□□ □□□ □□, □□ □□□ □□□□□ □□ □□□ □□□ □□ □□□.
□□□ □□□□ □□□?
A. Zure AD ID □□
B. Microsoft Entra □□ ID
C. □□□ □□
D. Microsoft Entra ID □□ □□ 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 Microsoft Entra ID 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: 277

Microsoft 365 E5 □□□ □□□□. Microsoft Entra ID Protection□ □□□ □□□□□.
□□ □□ □□□ □□ □□ □□ □□□□□ □□□ □□□□ □□□. □□□ □□□□ □□□?
A. □□ □□□ □□□□ □□□(SSPR)
B. □□□ □□ □□
C. □□ □□
D. □□□ □□ □□
Answer: (SHOW ANSWER)

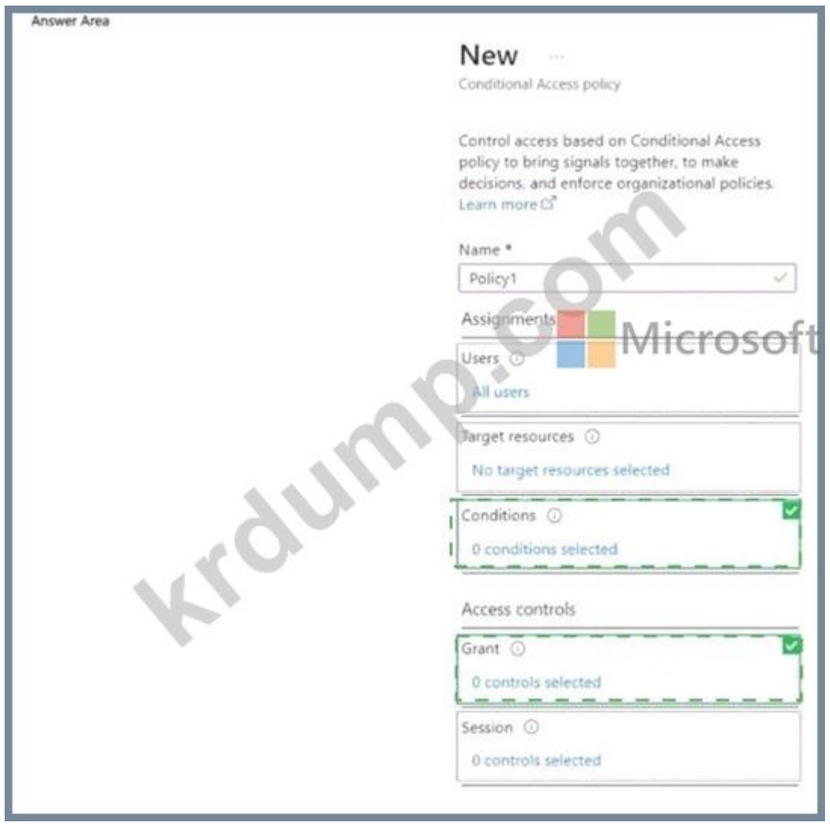
NEW QUESTION: 278
Microsoft 365 E5 □□□ □□□□.
□□ □□ □□□ □□□□ Policy□□ □□□ □□□ □□□ □□□□ □□□.
* □□□ □□□□□ □□□□□.
* □□ □□(MFA)□ □□□□□.



]□: □ □□□ 1□□□□.

Answer:

Answer Area



Explanation:

NEW QUESTION: 279

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

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

□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

SecAdmin1□□□ □□□□ □ □□ □□□ □□□ □□□□□.

SecAdmin1□ Microsoft Teams, SharePoint □ OneDrive□ □□ Office 365 □□ □□ □□(ATP) □□ □ □□□ □□□ □ □□□ □□ □□□.

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

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 280

□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

□□ Safe Links □□□ Microsoft□□ □□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□□□□□ □□ □□
B. Microsoft Entra ID □□
C. □□ □□□
D. □□□□□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 281
□□ □□ □□ □□ □□□□ □□□ Microsoft 365 □□□ □□□□.

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

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

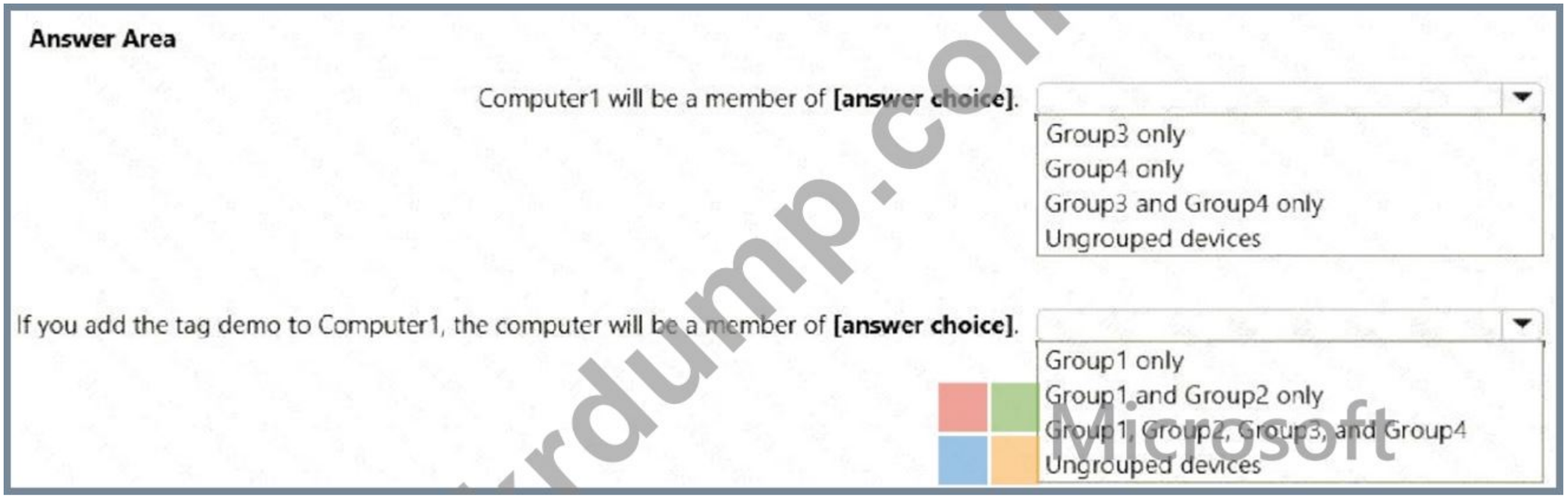
NEW QUESTION: 282
□□□
□□□ Microsoft Defender for Endpoint□ □□□□□. Microsoft Defender for Endpoint□□ □□ □□ □□□ □□ □□□ □□□□□.

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*

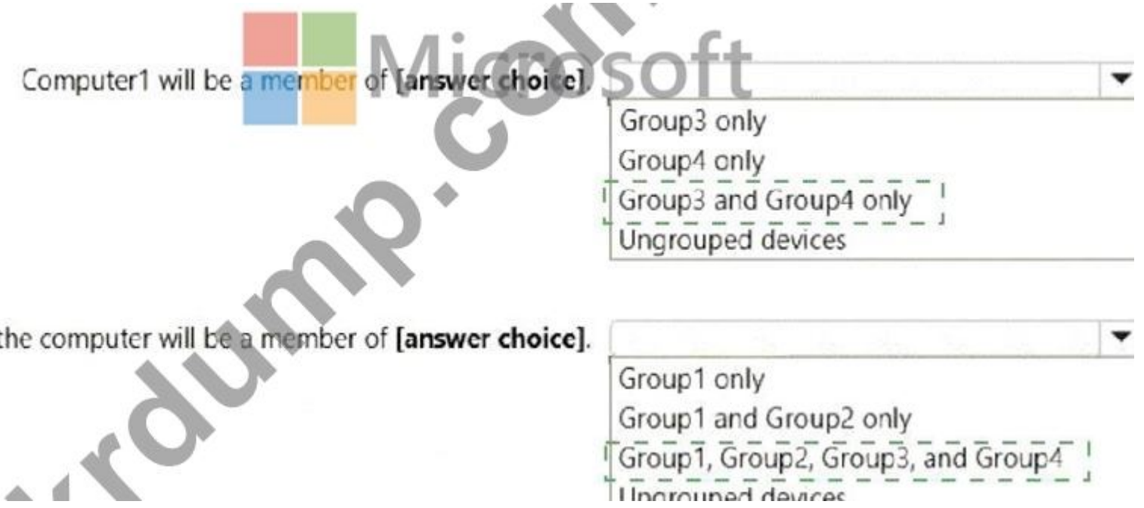
□□ □□□ □□ Microsoft Defender for Endpoint□ computer1□□□ □□□□ □□□□□□.


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

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



Answer:
Answer Area



Explanation:

Answer Area

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

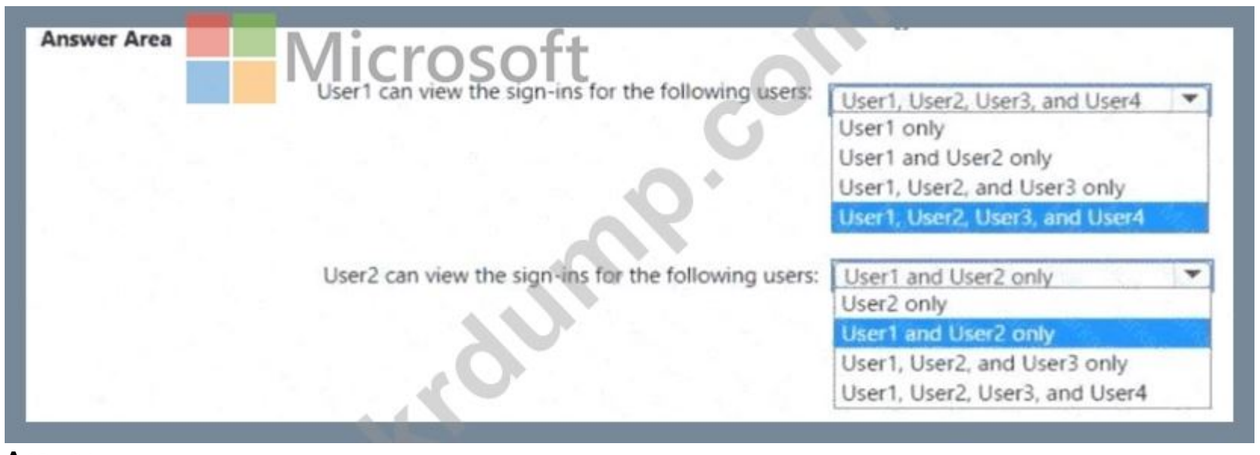
- Group3 only
- Group4 only
- **Group3 and Group4 only**
- Ungrouped devices

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

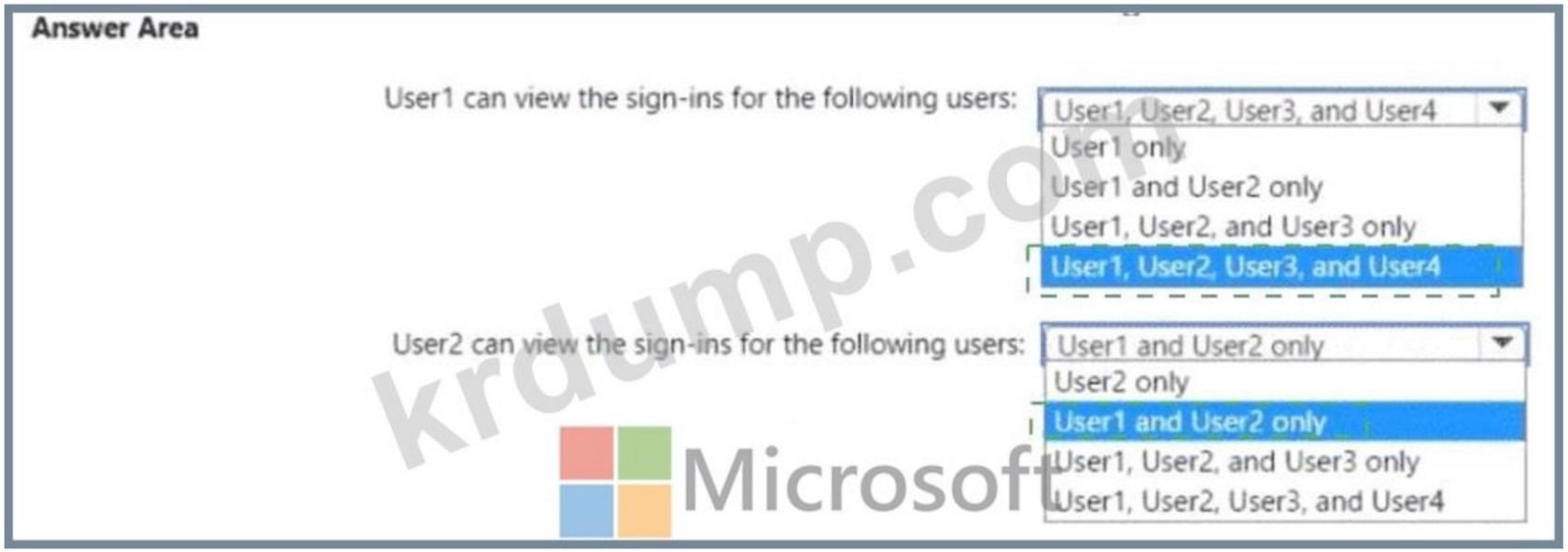
- Group1 only
- Group1 and Group2 only
- **Group1, Group2, Group3, and Group4**
- Ungrouped devices

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: 283
contoso.com□□□ Microsoft Entra □□□□ □□□□ Microsoft 365 □□□ □□□□. □□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.
Microsoft Entra □□ □□□ □□□ □□□□□□ User1□ User2□ □□ □□□□ □□□ □□□ □ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

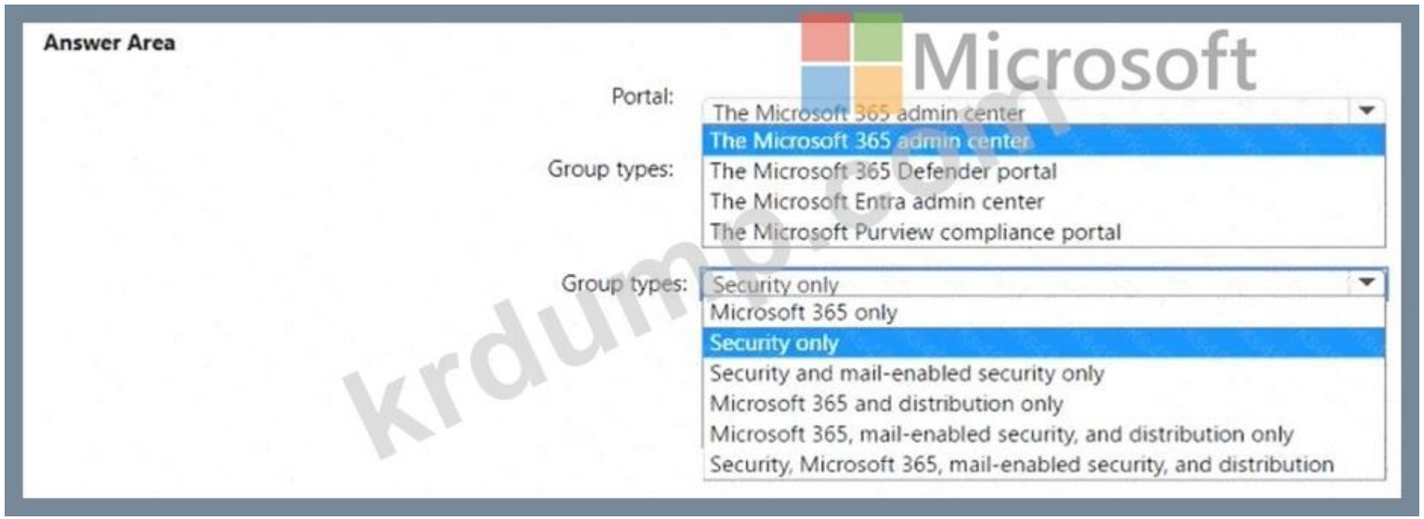
NEW QUESTION: 284

Microsoft 365 E5 □□□ □□□□.

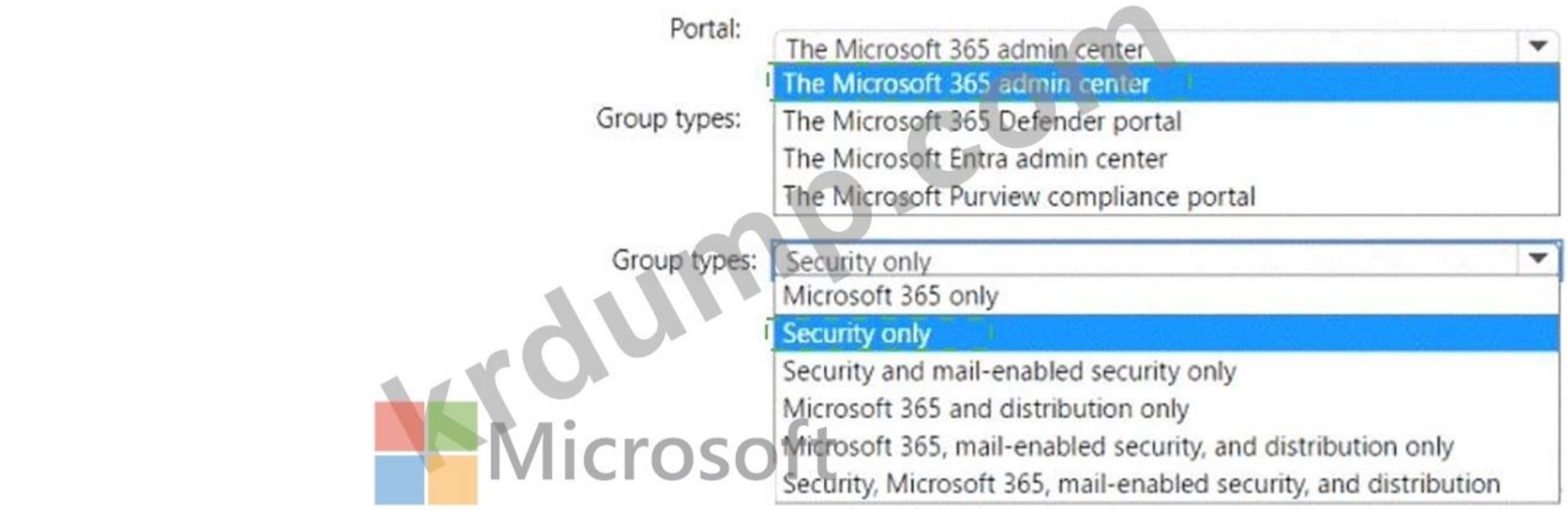
□□ □□ □□□ □□□□ □□□.

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

□□□□: □□ □□□ 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 (**598** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)