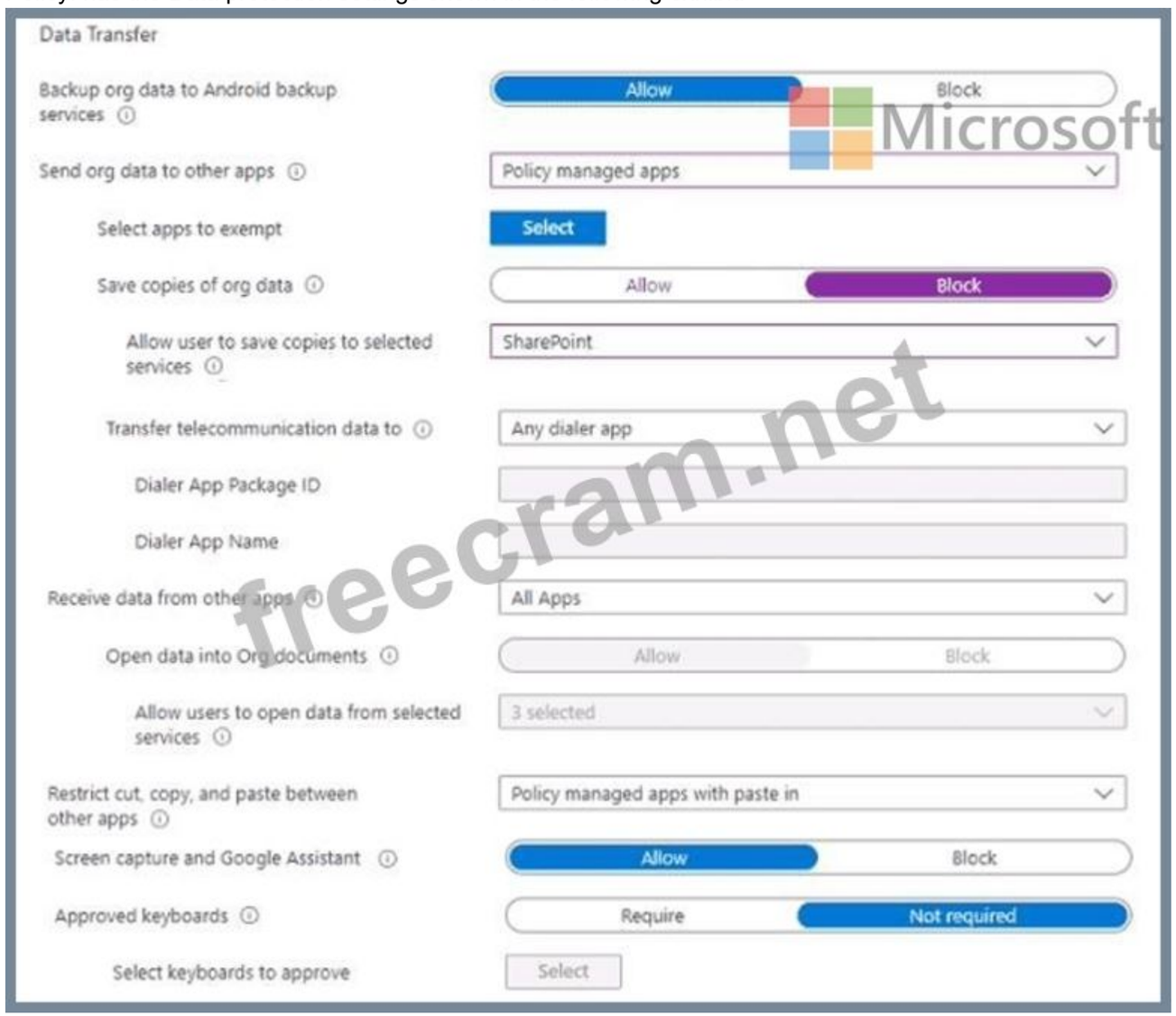
Microsoft.MS-102.v2026-06-01.q246

Exam Code:	MS-102
Exam Name:	Microsoft 365 Administrator
Certification Provider:	Microsoft
Free Question Number:	246
Version:	v2026-06-01
# of views:	106
# of Questions views:	2708
https://www.freecram.net/torrent/Microsoft.MS-102.v2026-06-01.q246.html	

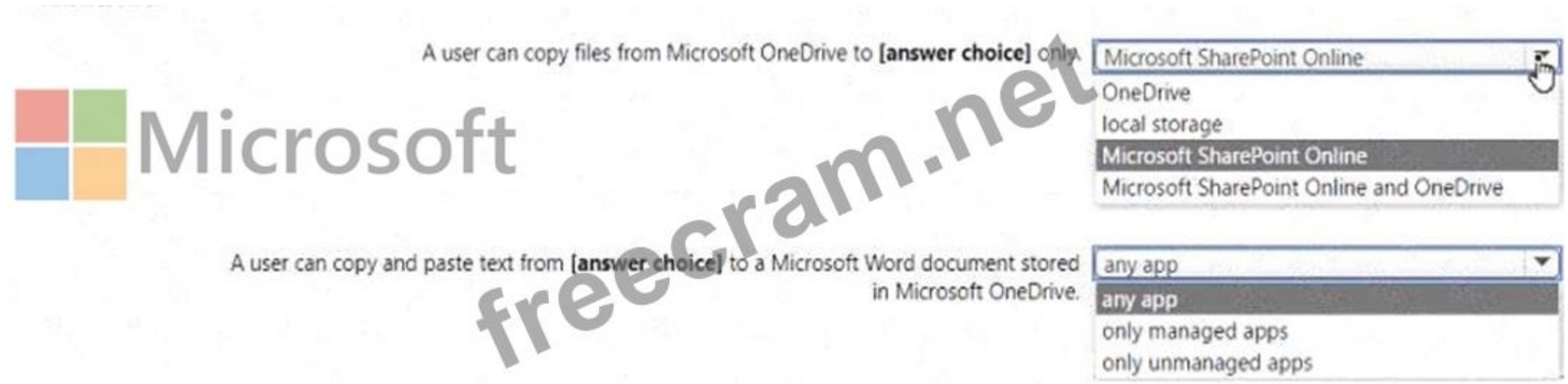
NEW QUESTION: 1
(You have a Microsoft 365 E5 subscription.
You are implementing Microsoft Defender for Cloud Apps.
You need to ensure that you can create OAuth app policies.
Solution: You configure Conditional Access app control.
Does this meet the goal?)
A. Yes
B. No
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract of Microsoft 365 Admin documents guides:
Explanation:
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: 2
You have a Microsoft 365 E5 subscription that contains 200 Android devices enrolled in Microsoft Intune.

You create an Android app protection policy named Policy! that is targeted to all Microsoft apps and assigned to all users.
Policy! has the Data protection settings shown in the following exhibit.



Use the drop-down menus to select 'he answer choice that completes each statement based on the information presented in the graphic.



Answer:

Explanation:

NEW QUESTION: 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

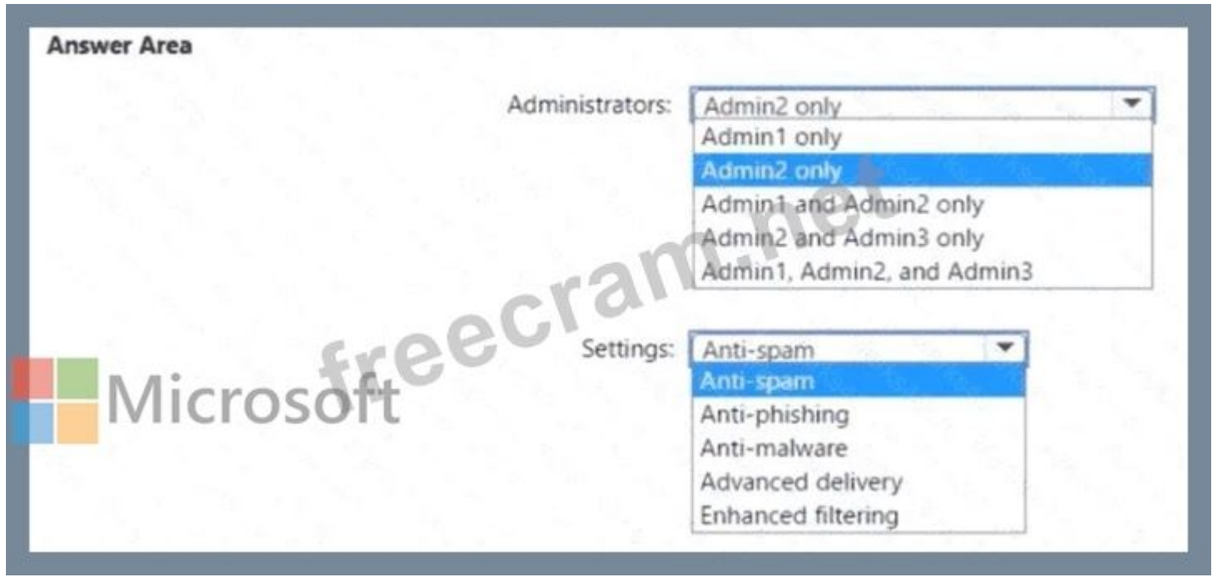
You have a Microsoft 365 subscription.

From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

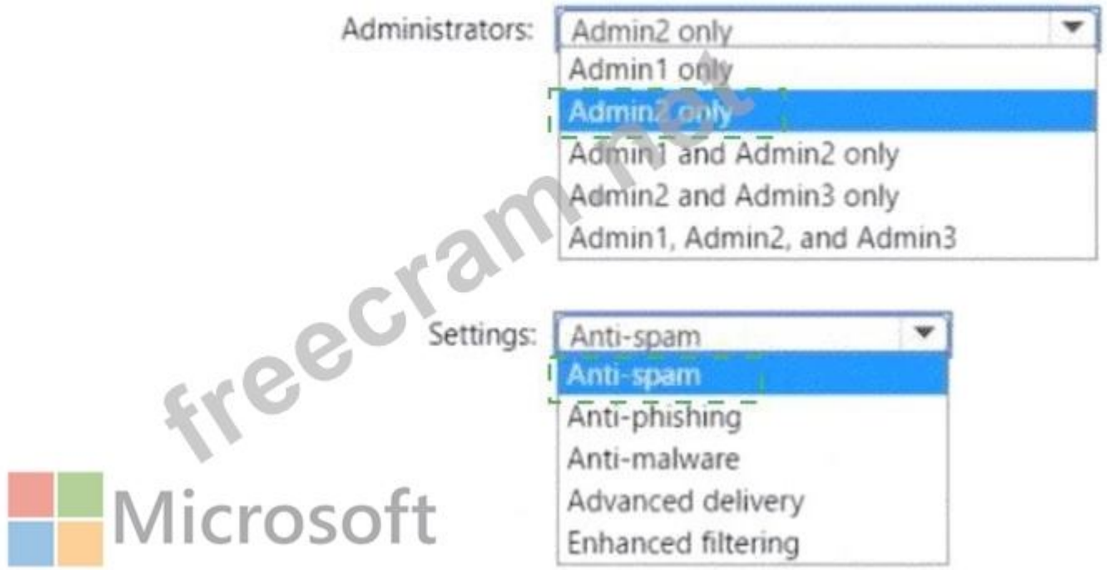
Solution: From the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group.
Does this meet the goal?
A. No
B. Yes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table.
User1 reports that after sending 1,000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:
* Which administrators can unblock User1
* What to configure to allow User1 to send at least 2,000 emails per day without being blocked What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Answer Area



Explanation:

NEW QUESTION: 5

You purchase a new computer that has Windows 10, version 2004 preinstalled.

You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.

What should you do on the computer?

A. install the latest feature update and all the quality updates released since version 2004.

B. install the West feature update and the latest quality update only.

C. Install all the feature updates released since version 2004 and all the quality updates released since version 2004 only.

D. install all the feature updates released since version 2004 and the latest quality update only.

Answer: (SHOW ANSWER)

NEW QUESTION: 6

You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.

Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. advanced hunting

B. security reports
C. digital certificate assessment
D. device discovery
E. attack surface reduction (ASR)
Answer: (SHOW ANSWER)
B: Overview of Microsoft Defender for Endpoint Plan 1, Reporting
The Microsoft 365 Defender portal (https://security.microsoft.com) provides easy access to information about detected threats and actions to address those threats.
The Home page includes cards to show at a glance which users or devices are at risk, how many threats were detected, and what alerts/incidents were created.
The Incidents & alerts section lists any incidents that were created as a result of triggered alerts. Alerts and incidents are generated as threats are detected across devices.
The Action center lists remediation actions that were taken. For example, if a file is sent to quarantine, or a URL is blocked, each action is listed in the Action center on the History tab.
The Reports section includes reports that show threats detected and their status.
E: What can you expect from Microsoft Defender for Endpoint P1?
Microsoft Defender for Endpoint P1 is focused on prevention/EPP including:
Next-generation antimalware that is cloud-based with built-in AI that helps to stop ransomware, known and unknown malware, and other threats in their tracks.
(E) Attack surface reduction capabilities that harden the device, prevent zero days, and offer granular control over access and behaviors on the endpoint.
Device based conditional access that offers an additional layer of data protection and breach prevention and enables a Zero Trust approach.
The below table offers a comparison of capabilities are offered in Plan 1 versus Plan 2.

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL backing	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
APIs, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts**		✓

*Includes Targeted Attack Notifications (TAN) and Experts On Demand (EOD).
Customers must apply for TAN. EOD is available for purchase as an add-on.

Incorrect:

Not A: P2 is by far the best fit for enterprises that need an EDR solution including automated investigation and remediation tools, advanced threat prevention and threat and vulnerability management (TVM), and hunting capabilities.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft-defender-for-endpoint-plan-1-now-included-in-m365-e3/ba-p/3060639

NEW QUESTION: 7

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1. You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:

* Assign licenses to users.
* Procure apps from Microsoft Store.
* Manage private store availability for all items.

The solution must use the principle of least privilege.

Which Microsoft Store for Business role should you assign to User1?

A. Basic Purchaser

B. Device Guard signer

C. Admin

D. Purchaser

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

NEW QUESTION: 8

You have a Microsoft 365 E5 subscription that contains two security groups named Group1 and Group2.

You need to enable multi-factor authentication (MFA) for the members of Group1 and Group2. The solution must meet the following requirements:

* The Group1 members must be prompted for MFA only when authenticating to Microsoft Entra ID from Android devices.

* The Group2 members must be prompted for MFA only when accessing Microsoft Exchange Online from outside the corporate network.

* Administrative effort must be minimized.

What should you configure for each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

NEW QUESTION: 9

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has he files in the following table.

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

The Site1 users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Visitor

You create a data less prevention (DLP) policy names Policy1 as shown in the following exhibit.

How many files will be visible to user1 and User2 after Policy' is applied to answer, selected select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 10

Your company has a Microsoft 365 tenant

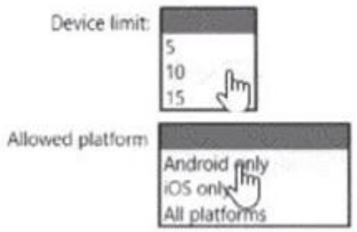
You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM) The device type restriction are configured as shown in the following table.

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

The device limit restriction are configured as shown in the following table.

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

Answer Area



Answer:

Explanation:

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

NEW QUESTION: 11

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.

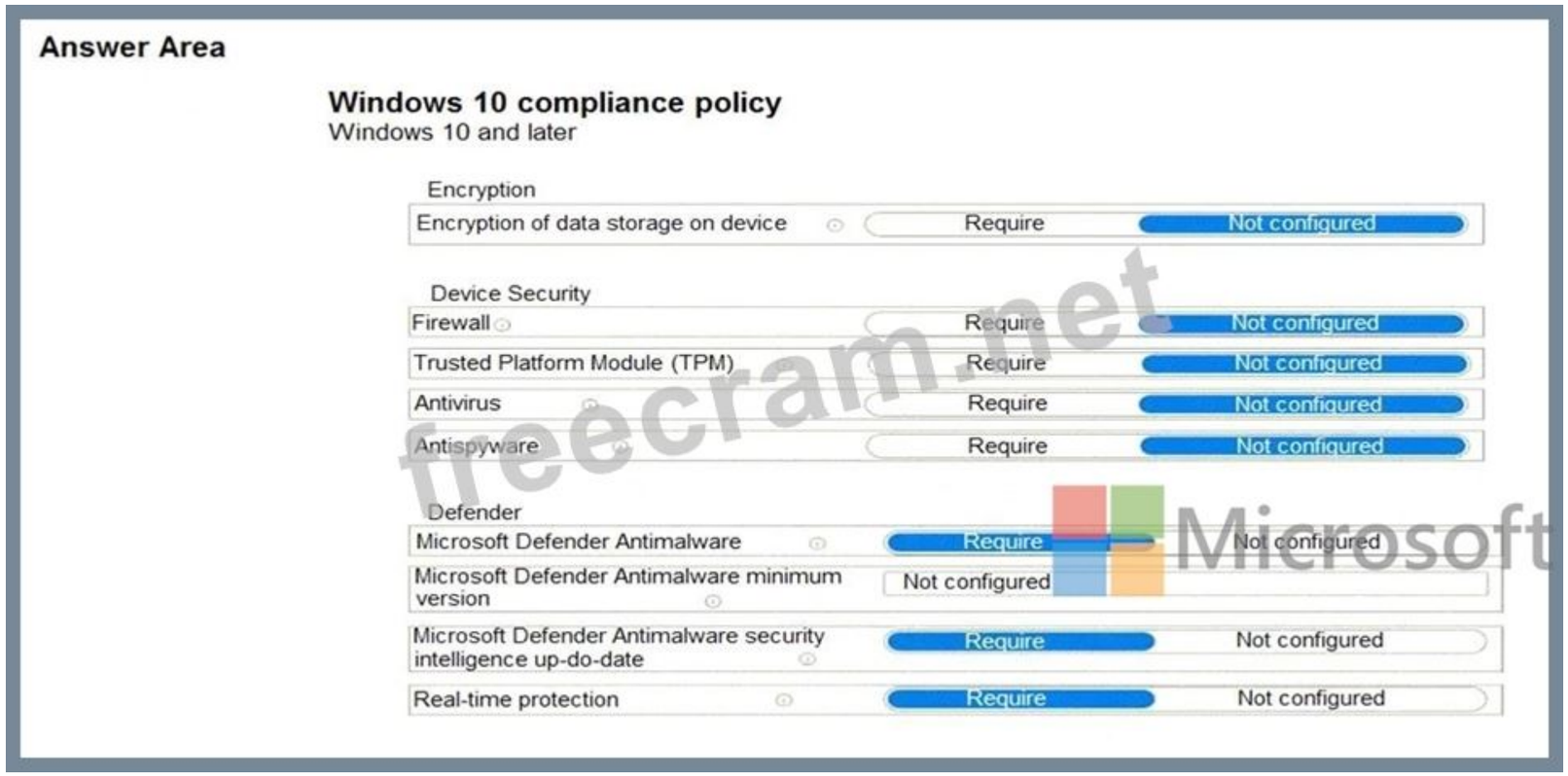
You deploy a third-party antivirus solution to the devices.

You need to ensure that the devices are marked as compliant.

Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.

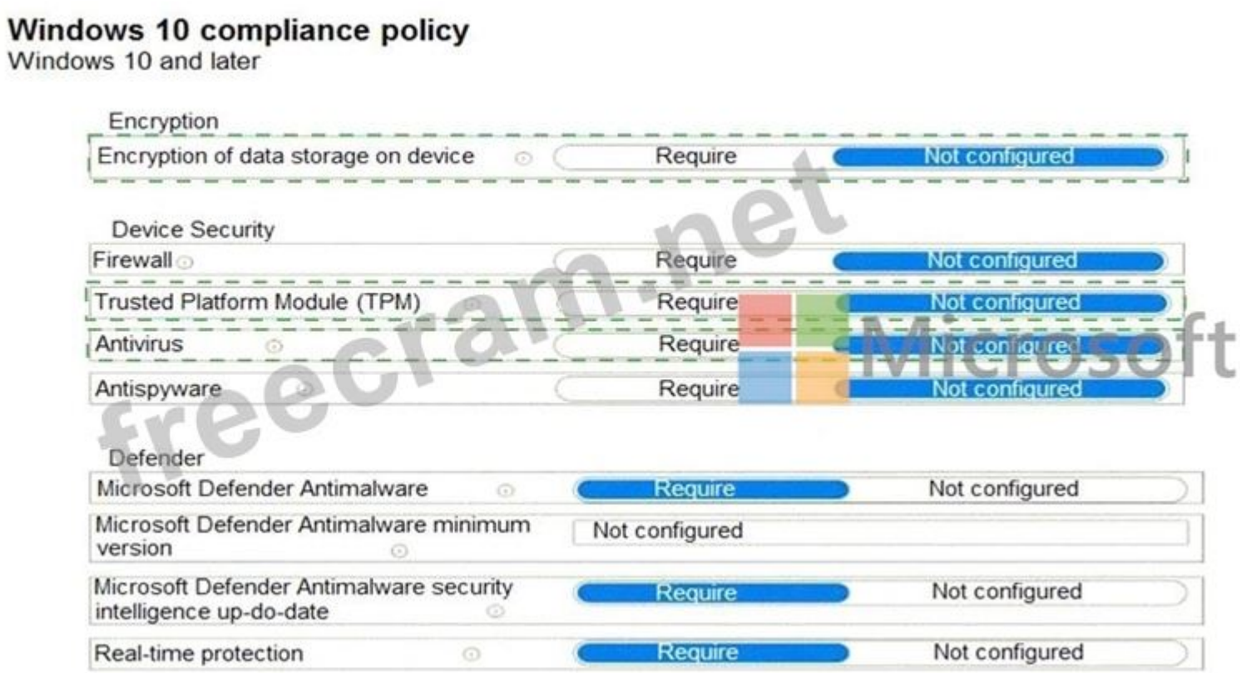
NOTE: Each correct selection is worth one point.

Answer Area

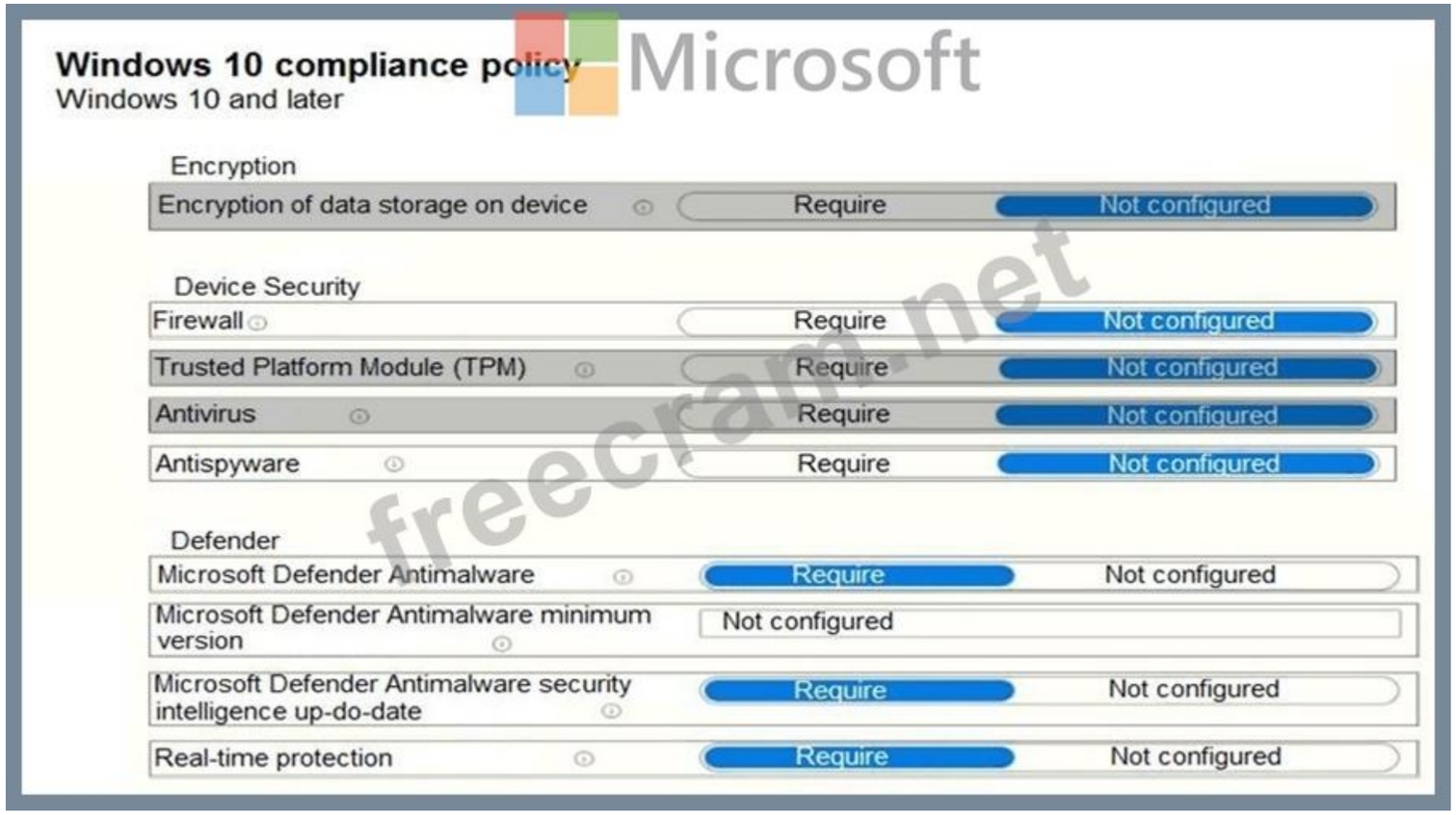


Answer:

Answer Area



Explanation:



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

NEW QUESTION: 12

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

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

You add another user named User5 to the User Administrator role.

You need to identify which two management tasks User5 can perform.

Which two tasks should you identify? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Delete User2 and User4 only.

B. Reset the password of User4 only

C. Reset the password of any user in Azure AD.

D. Delete User1, User2, and User4 only.

E. Reset the password of User2 and User4 only.

F. Delete any user in Azure AD.

Answer: A,E (LEAVE A REPLY)

Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).

Only on users who are non-admins or in any of the following limited admin roles:

* Directory Readers
* Guest Inviter
* Helpdesk Administrator
* Message Center Reader
* Reports Reader
* User Administrator

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin- roles#available-roles

NEW QUESTION: 13

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

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

You add custom apps to the private store in Microsoft Store Business.

You plan to create a policy to show only the private store in Microsoft Store for Business.

To which devices can the policy be applied?

A. Device2, Device3, and Device5 only

B. Device2 and Device4 only

C. Device1, Device2, Device3, Device4, and Device5

D. Device1 and Device3 only

E. Device2 only

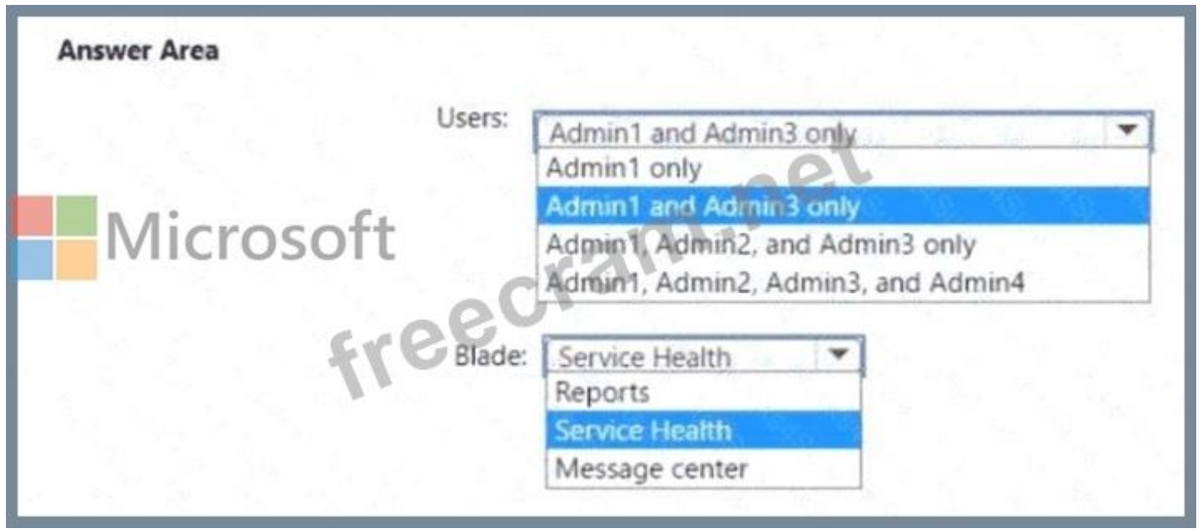
Answer: (SHOW ANSWER)

NEW QUESTION: 14

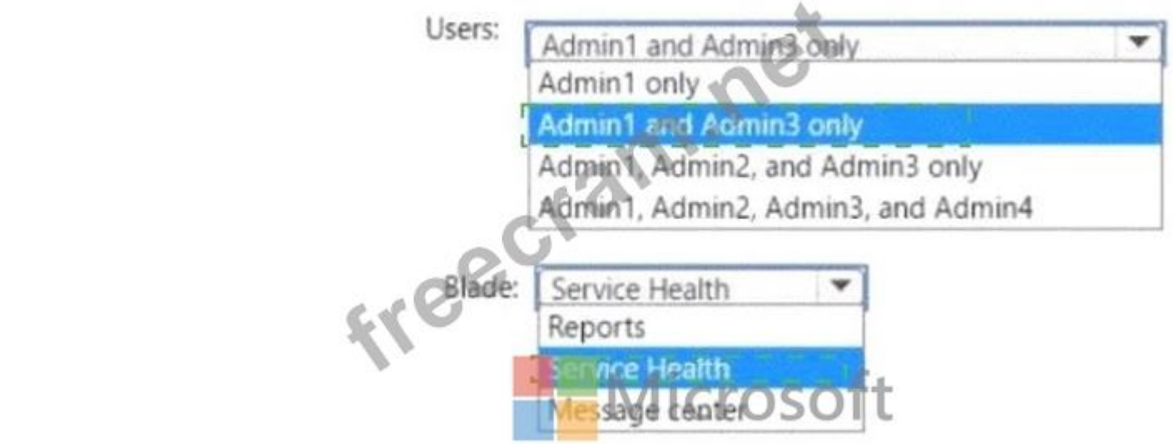
You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.

Which users can review the incidents and advisories, and which blade should the users use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

NEW QUESTION: 15

You have a Microsoft 365 E5 tenant.

You create a retention label named Retention1 as shown in the following exhibit.

When users attempt to apply Retention1, the label is unavailable.

You need to ensure that Retention1 is available to all the users.

What should you do?

A. Create a new label policy

B. Modify the Authority type setting for Retention!

C. Modify the Business function/department setting for Retention 1.

D. Use a file plan CSV template to import Retention1.

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 16

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goats. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint. and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint Administrator role.

Does this meet the goal?

A. No

B. Yes

Answer: (SHOW ANSWER)

NEW QUESTION: 17

You have a Microsoft 365 tenant that contains the groups shown in the following table.

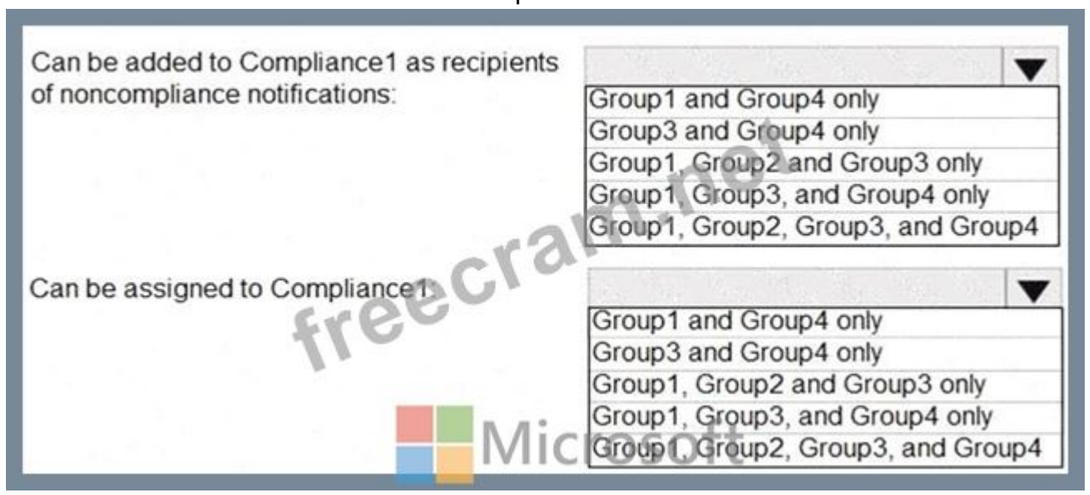
Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to create a compliance policy named Compliance1.

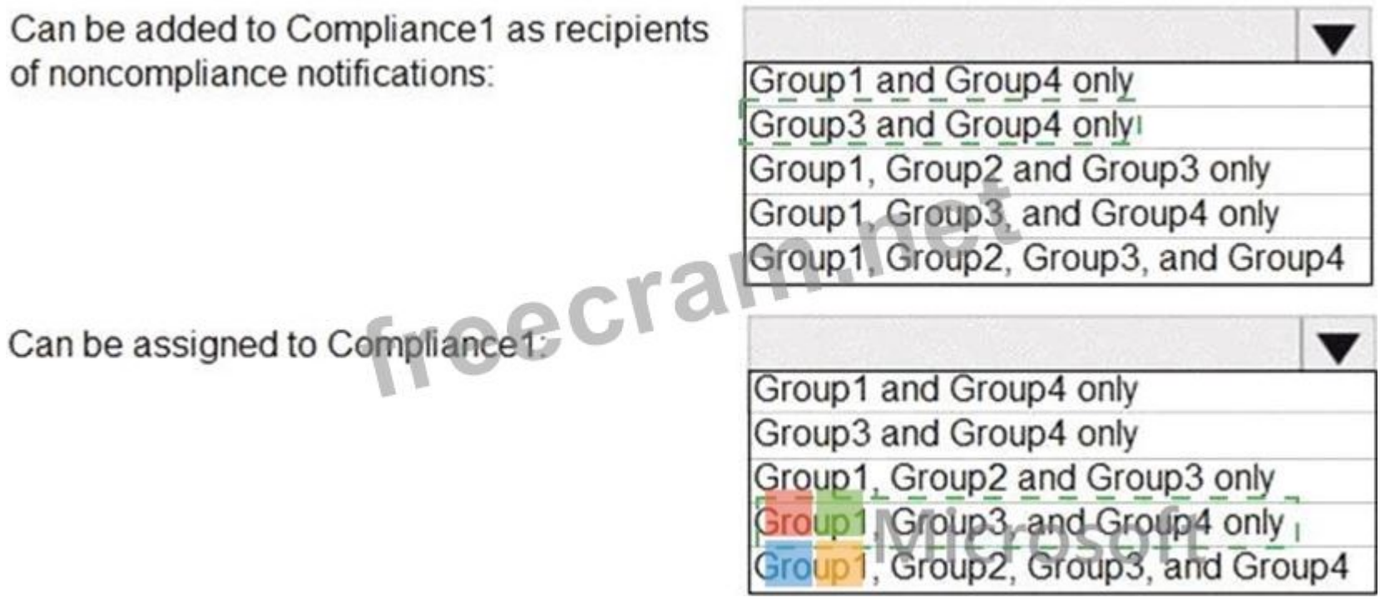
You need to identify the groups that meet the following requirements:

Can be added to Compliance1 as recipients of noncompliance notifications Can be assigned to Compliance1 To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

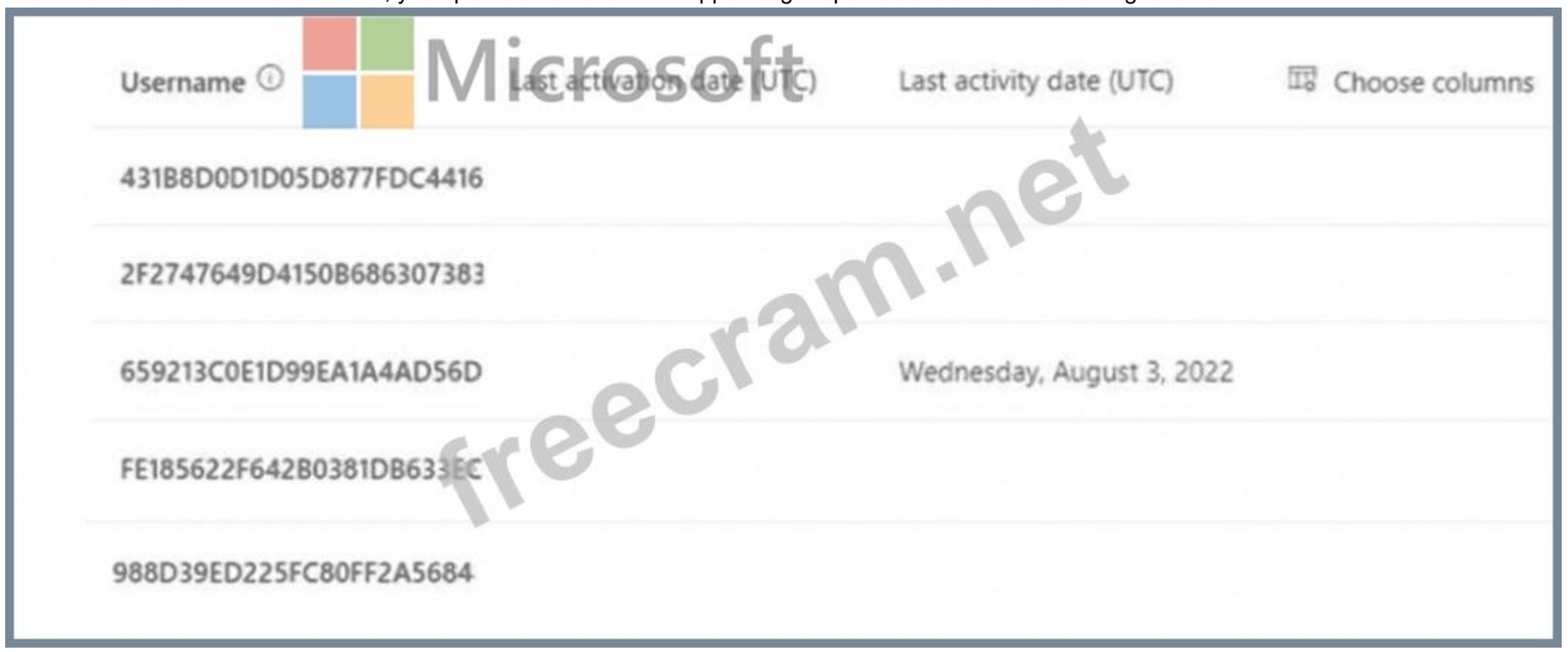
Reference:
https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint- manager-intune/

NEW QUESTION: 18
You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?
A. From the Microsoft 365 security center, view the Threat tracker.
B. From the Microsoft 365 admin center, view the Security & compliance report.
C. From the Azure Active Directory admin center, view the Risky sign-ins report.
D. From the Cloud App Security admin center, select Users and accounts.
Answer: (SHOW ANSWER)

NEW QUESTION: 19

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you open the Microsoft 365 Apps usage report as shown in the following exhibit.

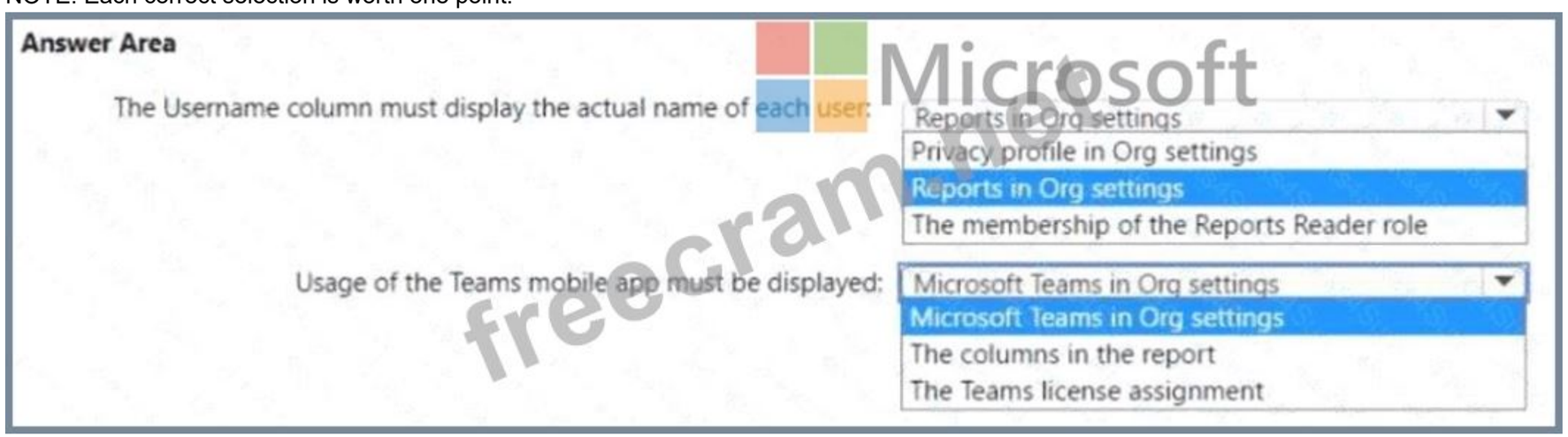


You need ensure that the report meets the following requirements:

* The Username column must display the actual name of each user.
* Usage of the Microsoft Teams mobile app must be displayed.

What should you modify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Answer Area

Explanation:

Answer Area

NEW QUESTION: 20

You have a Microsoft 365 subscription.
From Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.
You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.
Solution: From Windows PowerShell, you run the New-complianceSecurityFilter cmdlet with the appropriate parameters.
Does this meet the goal?

A. No

B. Yes

Answer: (SHOW ANSWER)

NEW QUESTION: 21

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

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

You perform the following actions:
Provision the private store in Microsoft Store for Business.
Add an app named App1 to the private store.
Set Private store availability for App1 to Specific groups, and then select Group3.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

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

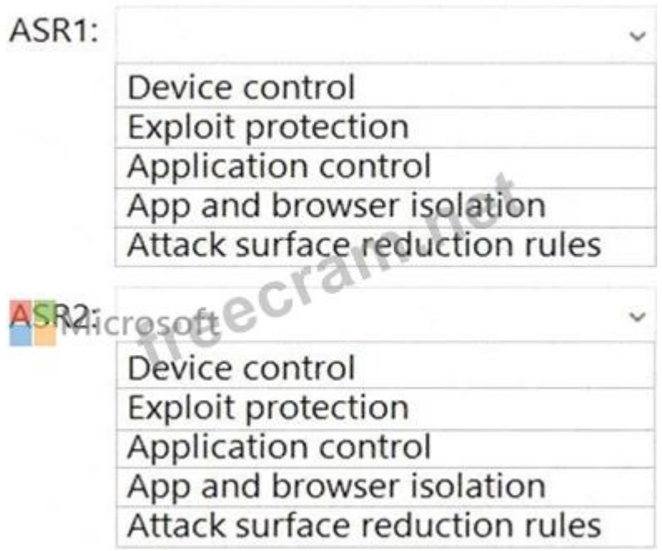
NEW QUESTION: 22
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to be notified when a single user downloads more than 50 files during any 60-second period.
What should you configure?
A. a session policy
B. a file policy
C. an activity policy

D. an anomaly detection policy
Answer: (SHOW ANSWER)

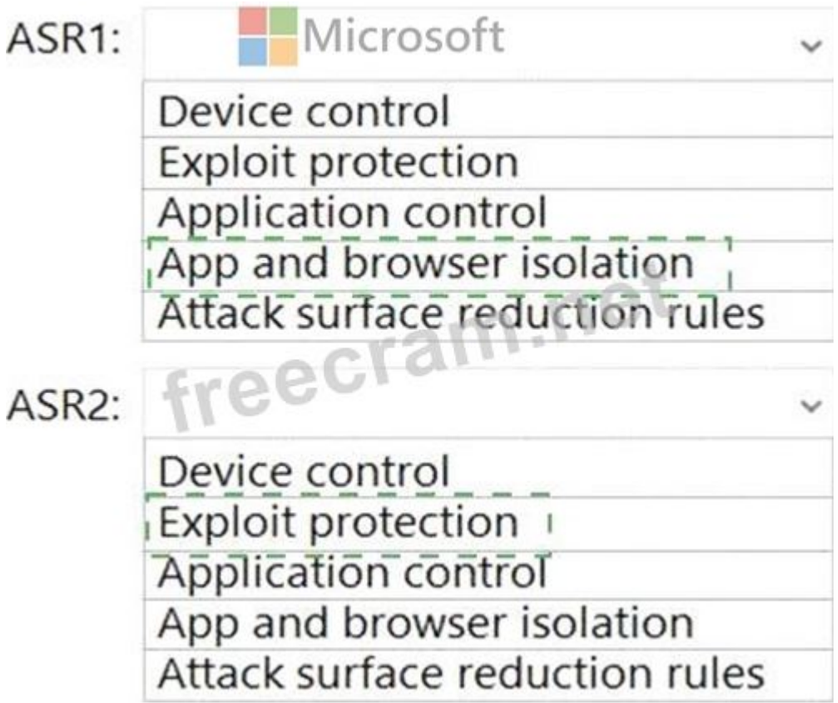
NEW QUESTION: 23
Your network contains an on-premises Active Directory domain. You have a Microsoft 365 subscription.
You implement a directory synchronization solution that uses pass-through authentication.
You configure Microsoft Entra Password protection as shown in the following exhibit.

You discover that Active Directory users can use the passwords in the custom banned passwords list.
You need to ensure that banned passwords are banned for all users.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. From a domain controller, install the Microsoft Entra Password Protection Proxy.
B. From Custom banned passwords, modify the Enforce custom list setting.
C. From Password protection for Windows Server Active Directory, modify the Mode setting.
D. From a domain controller, install the Microsoft Entra Application Proxy connector.
E. From all the domain controllers, install the Microsoft Entra Password Protection DC Agent.
F. From Active Directory, modify the Default Domain Policy.
Answer: (SHOW ANSWER)

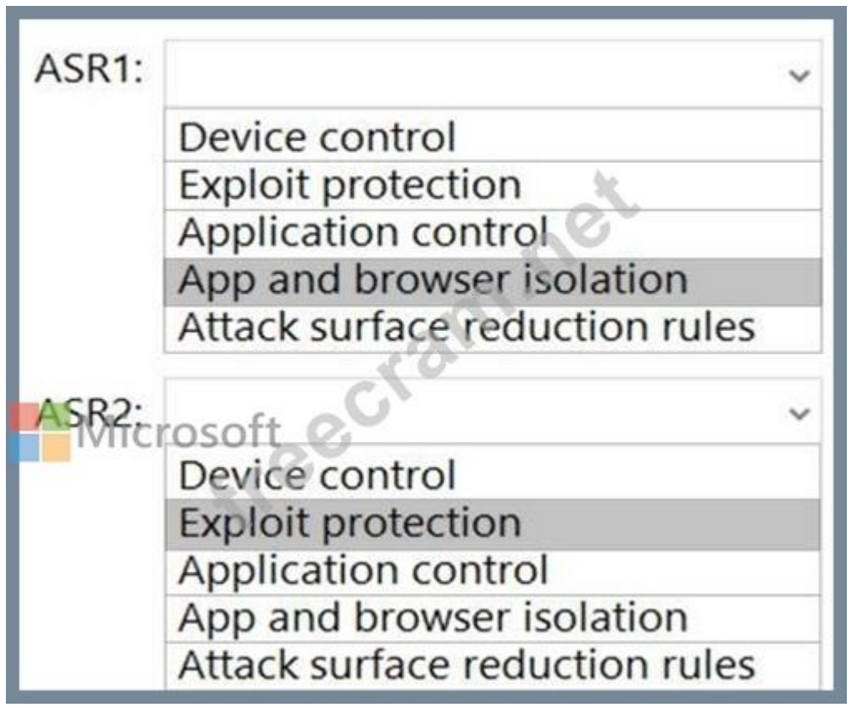
NEW QUESTION: 24
You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.
You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard. ASR2 will be used to configure Microsoft Defender SmartScreen.
Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

NEW QUESTION: 25
Your company has a Microsoft 365 E5 tenant that contains a user named User1.
You review the company's compliance score.
You need to assign the following improvement action to User1:Enable self-service password reset.
What should you do first?
A. From Compliance Manager, turn off automated testing.
B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.
Answer: (SHOW ANSWER)
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: 26
You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.

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

You plan to enable VPN access for the devices.

What is the minimum number of configuration policies required?

A. 4

B. 3

C. 1

D. 5

Answer: (SHOW ANSWER)

NEW QUESTION: 27

Your network contains an on-premises Active Directory Domain Services (AD DS) domain.

You have a Microsoft Entra tenant that syncs with the domain and has password hash synchronization enabled. The tenant contains the users shown in the following table.

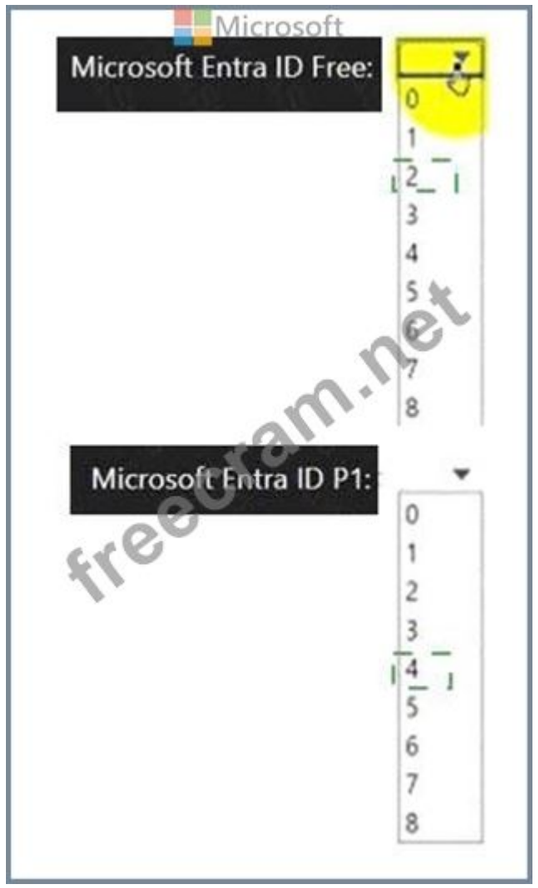
Name	Source location	Authentication method
User1	On-premises	Password hash
User2	On-premises	Password hash
User3	On-premises	Password hash
User4	On-premises	Password hash
User5	Cloud	Cloud-only
User6	Cloud	Cloud-only

You need to ensure that all the users can change their password by using a Microsoft 365 portal. The solution must minimize costs.

What is the minimum number of Microsoft Entra ID Free and Microsoft Entra ID P1 licenses required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:

From the table in the question:

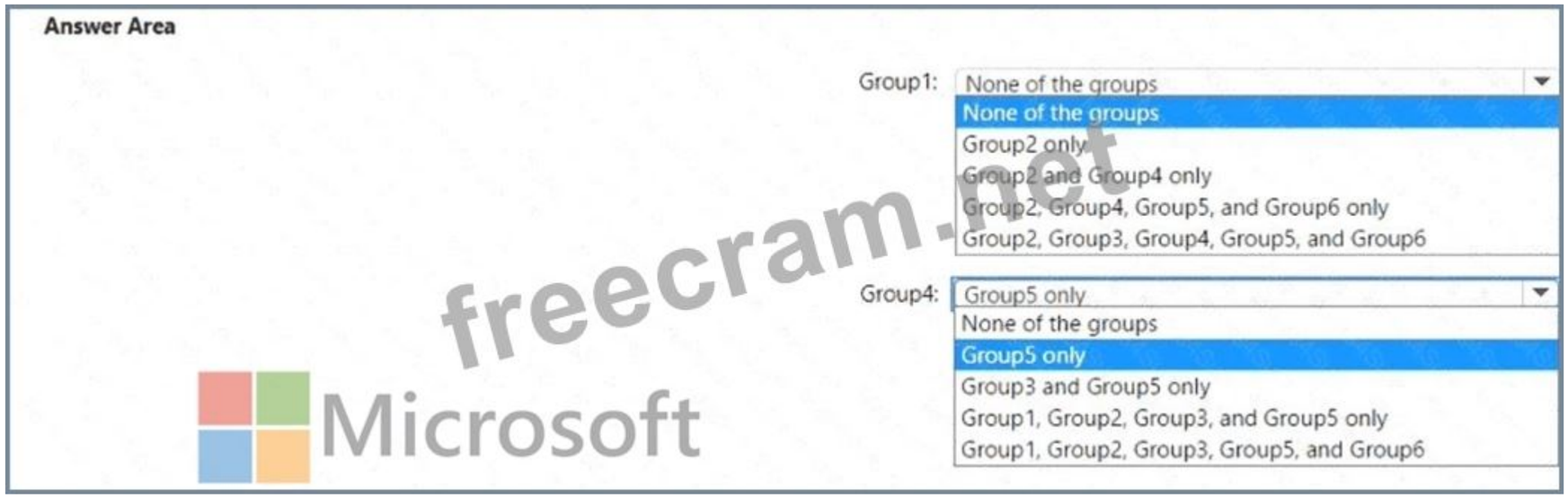
* User1-User4 are On-premises (synced) with Password hash authentication.
* User5-User6 are Cloud users (cloud-only).
Microsoft's licensing guidance for Self-Service Password Reset (SSPR) scenarios (which includes password change) states:
* Cloud-only user password change (user knows their password and 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: 28
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365 and contains a user named User1.
User1 emails a product catalog in the PDF format to 300 vendors. Only 200 vendors receive the email message, and User1 is blocked from sending email until the next day.
You need to prevent this issue from reoccurring.
What should you configure?
A. anti-spam policies
B. anti-malware policies
C. Safe Attachments policies
D. anti-phishing policies
Answer: (SHOW ANSWER)

NEW QUESTION: 29
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

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

Which groups can be members of Group1 and Group4? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

NEW QUESTION: 30

You implement Microsoft Azure Advanced Threat Protection (Azure ATP).

You have an Azure ATP sensor configured as shown in the following exhibit.

How long after the Azure ATP cloud service is updated will the sensor update?

A. 48 hours

B. 20 hours

C. 7 hours

D. 12 hours

Answer: (SHOW ANSWER)

NEW QUESTION: 31

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.

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

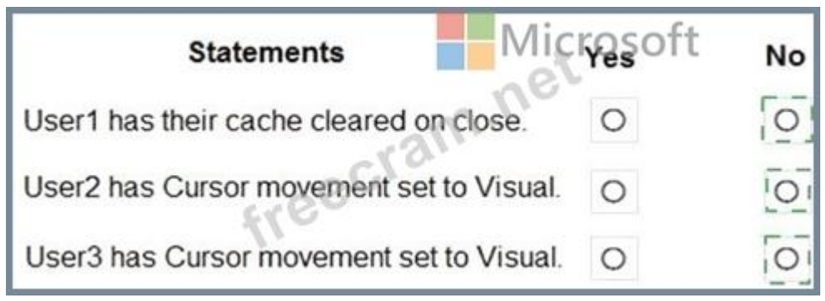
The policies use the settings shown in the following table.

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

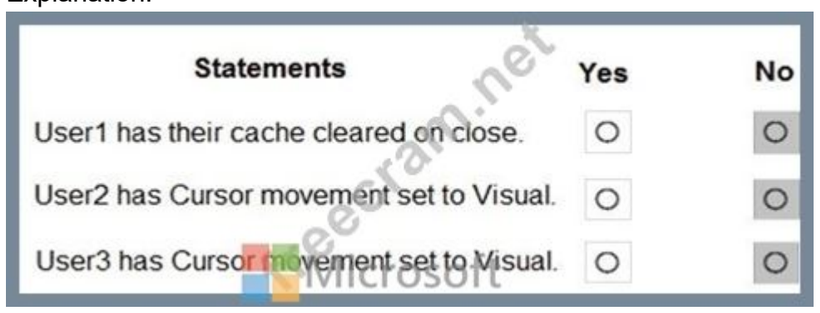
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:



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

NEW QUESTION: 32
Your company has offices in five cities.
The company has a Microsoft 365 tenant.
Each office is managed by a local administrator.
You plan to deploy Microsoft Intune.
You need to recommend a solution to manage resources in intune that meets the following requirements:
Local administrators must be able to manage only the resources in their respective office.

Local administrators must be prevented from managing resources in other offices.
Administrative effort must be minimized.
What should you include in the recommendation?
A. device categories
B. scope tags
C. configuration profiles
D. conditional access policies
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

NEW QUESTION: 33
You have a Microsoft 365 subscription.
You have an Azure AD tenant that contains the users shown in the following table.

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

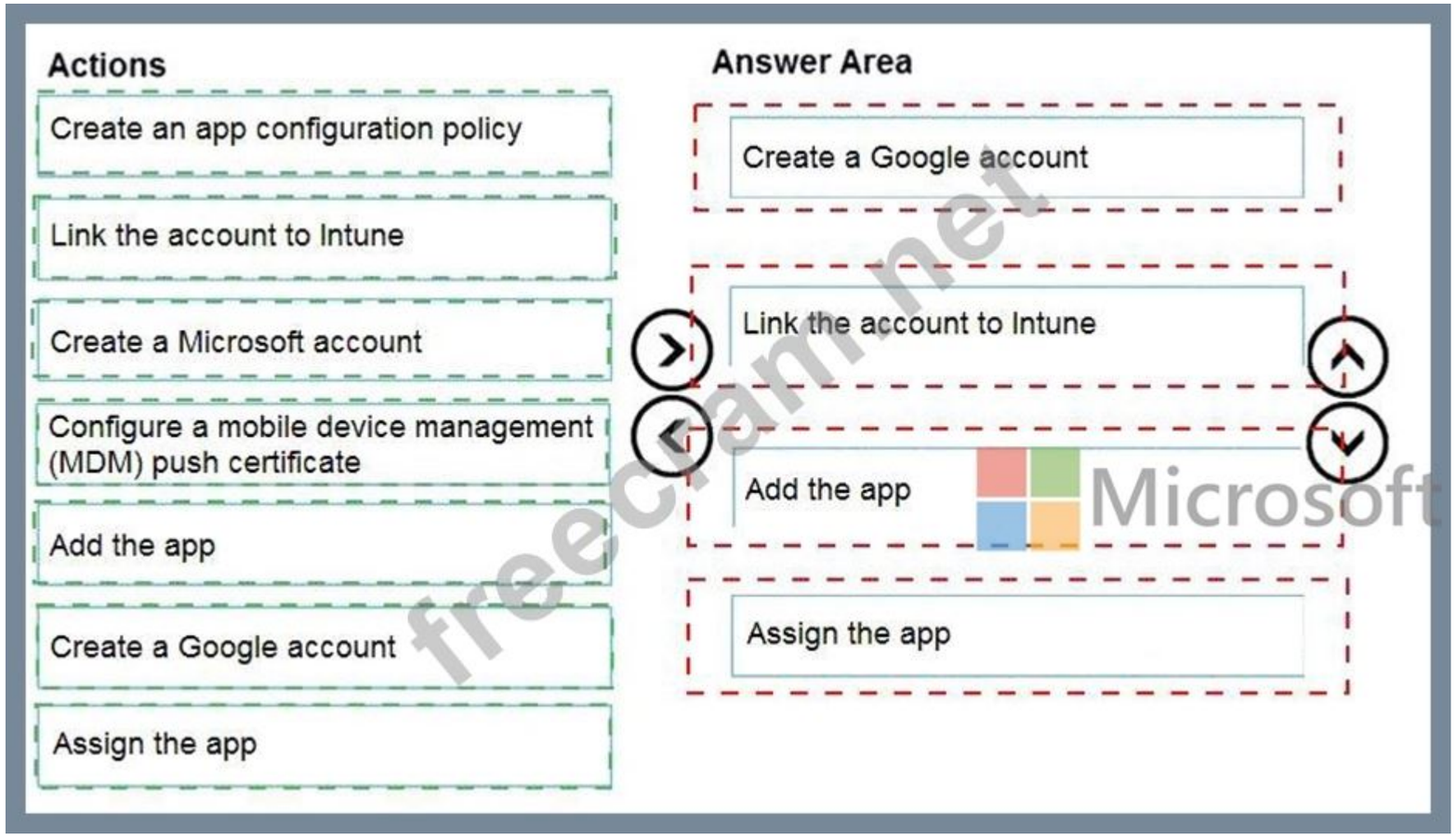
You configure Tenant properties as shown in the following exhibit.

Which users will be contacted by Microsoft if the tenant experiences a data breach?
A. Used only
B. User2 only
C. User3 only
D. Used and User2 only
E. User2 and User3 only
Answer: (SHOW ANSWER)
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

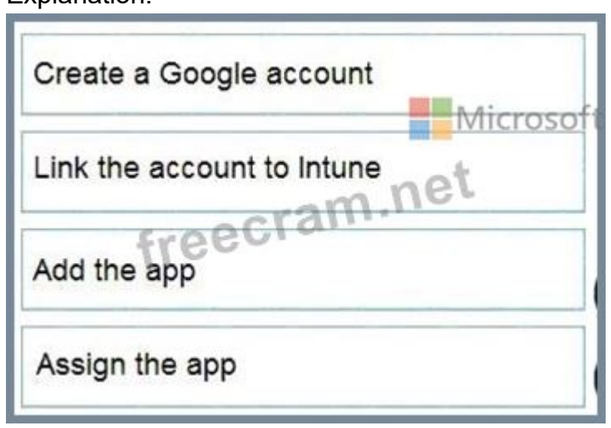
NEW QUESTION: 34
You have a Microsoft 365 E5 subscription that contains users in the United States, Europe, and Asia.
You use Microsoft Entra ID Protection.
You have a virtual desktop infrastructure (VDI). All VDI servers are located in the United States.
Users connect to Microsoft 365 from laptops and the VDI.
Some VDI users report that they are blocked from signing in to Microsoft 365 due to a high sign-in risk.
You need to reduce the likelihood that the VDI users will be erroneously blocked from signing in to Microsoft 365. The solution must ensure that sign-ins from the VDI environment are protected by using ID Protection.
A. ExpressRoute for Microsoft 365
B. A Satellite Geography location
C. A Conditional Access policy
D. A trusted location
Answer: (SHOW ANSWER)

NEW QUESTION: 35
You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune.
You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

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: 36
You have a Microsoft 365 subscription that contains the users shown in the following table.

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

You plan to use Exchange Online to manage email for a DNS domain.
An administrator adds the DNS domain to the subscription.
The DNS domain has a status of Incomplete setup.
You need to identify which user can complete the setup of the DNS domain. The solution must use the principle of least privilege.
Which user should you identify?

A. User2
B. User1
C. User3
D. User4

Answer: (SHOW ANSWER)

NEW QUESTION: 37

Your on-premises network contains an Active Directory domain named Contoso.com and 500 devices that run either macOS, Windows 8.1. Windows 10, or Windows 11. All the devices are managed by using Microsoft Endpoint Configuration Manager. The domain syncs with Azure Active Directory (Azure AD).
You plan to implement a Microsoft 365 E5 subscription and enable co-management. Which devices can be co-managed after the implementation?

A. Windows 11 and macOS only
B. Windows 11 and Windows 10 only
C. Windows 11 only
D. Windows 11. Windows 10, and Windows8.1 only
E. Windows 11, Windows 10-Windows8.1.andmacOS

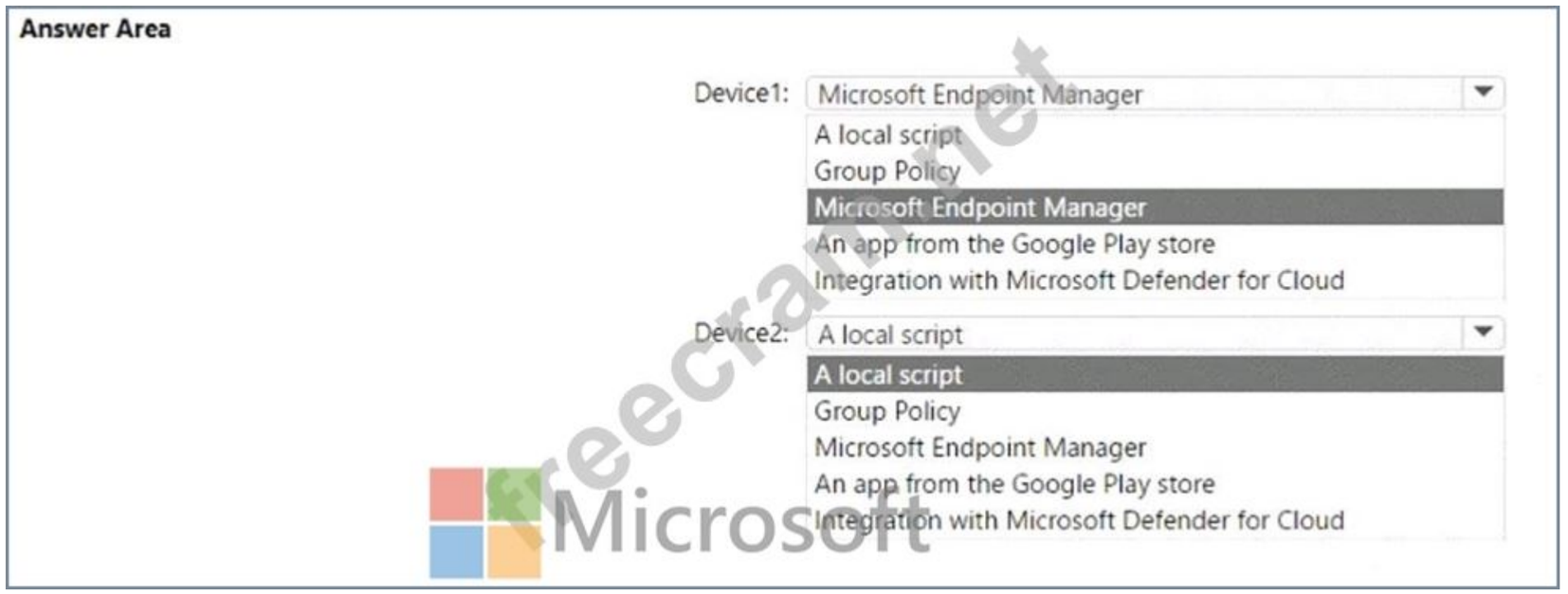
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38

You have a Microsoft 365 E5 subscription that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.
What should you use to onboard each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area

Device1: Microsoft Endpoint Manager

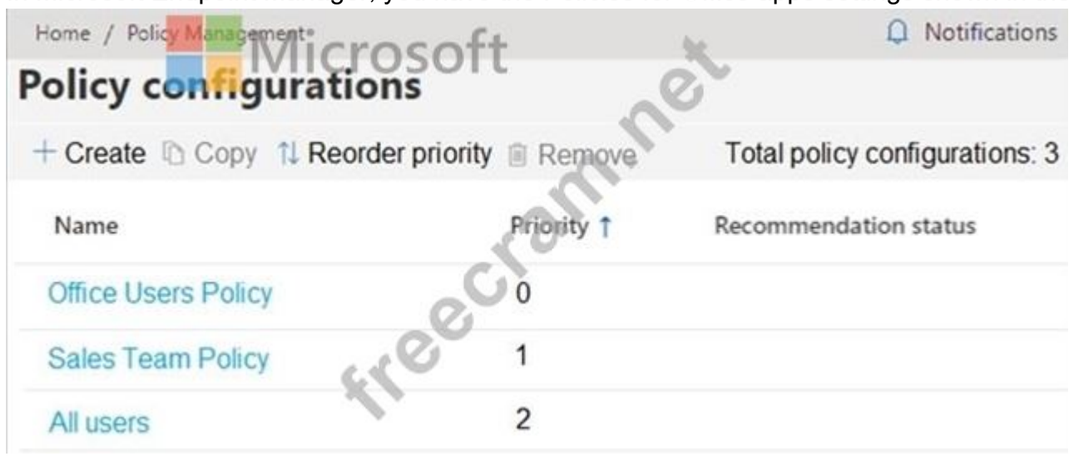
Device2: A local script

NEW QUESTION: 39

You have a Microsoft 365 subscription that contains three groups named All users, Sales team, and Office users, and two users shown in the following table.

Name	Member of
User1	All users, Sales team
User2	All users, Office users

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following exhibit.

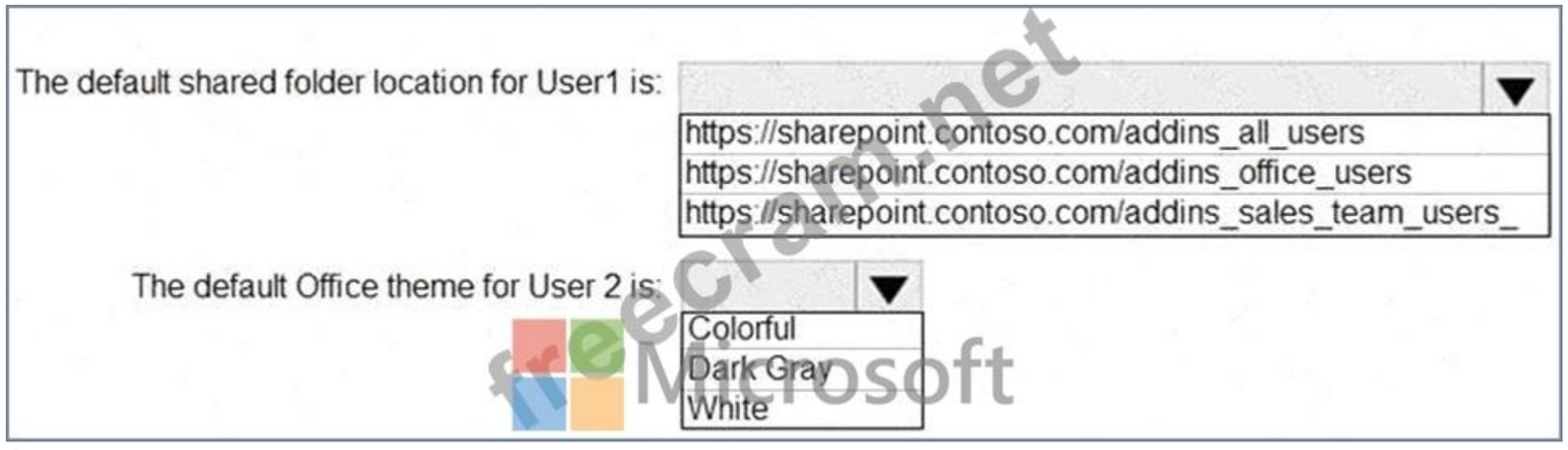


The policies use the settings shown in the following table.

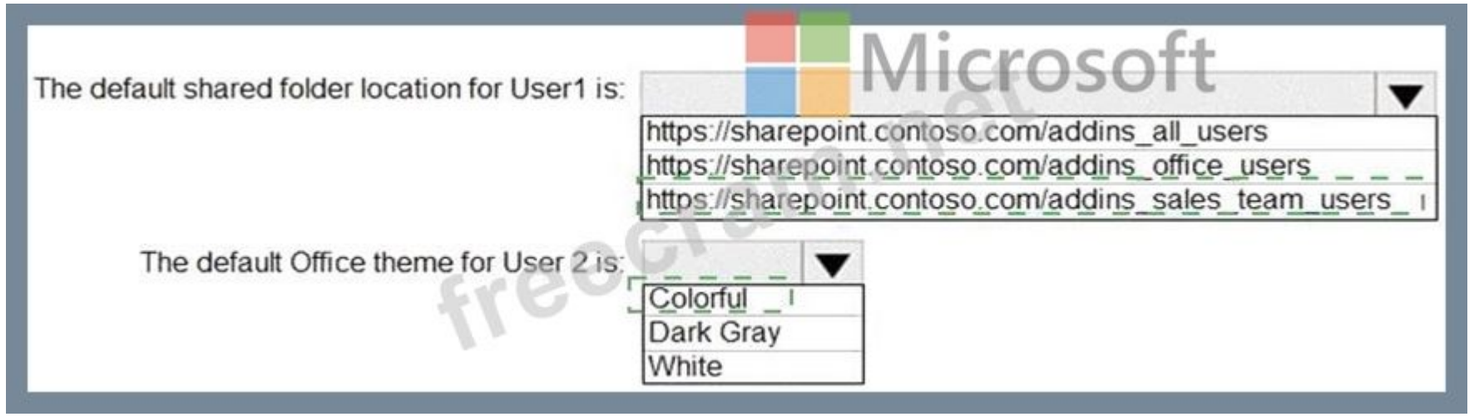
Policy	Default Shared Folder Location	Default Office Theme
All users	https://sharepoint.contoso.com/addins_all_users	Colorful
Office Users Policy	https://sharepoint.contoso.com/addins_office_users	White
Sales Team Policy	https://sharepoint.contoso.com/addins_sales_team_users_	Dark Gray

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.

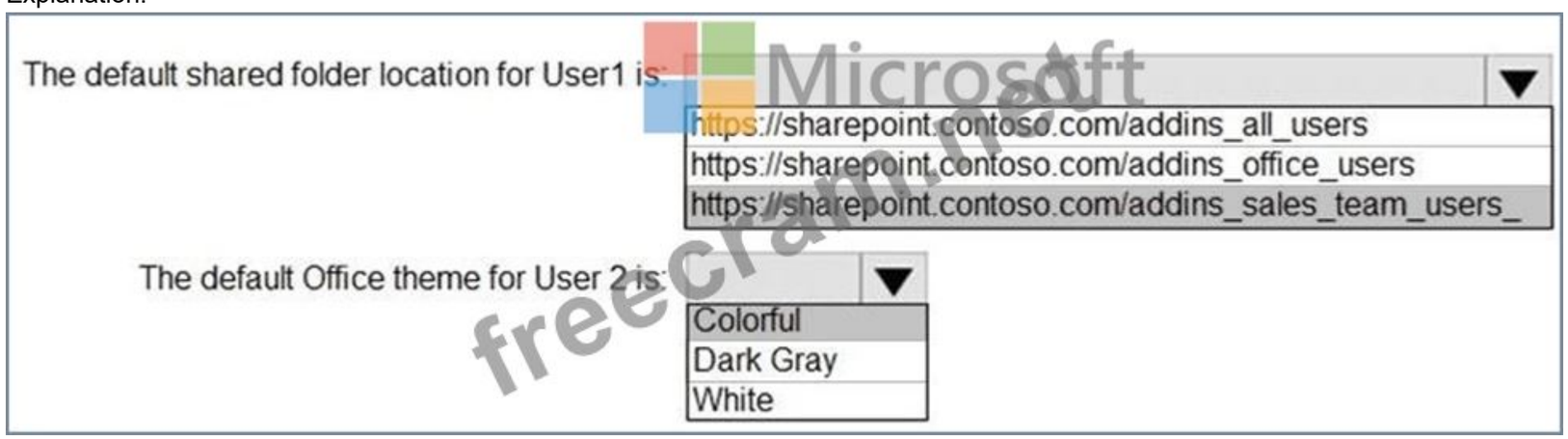
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

NEW QUESTION: 40
You have several devices enrolled in Microsoft Endpoint Manager
You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown In the following table.

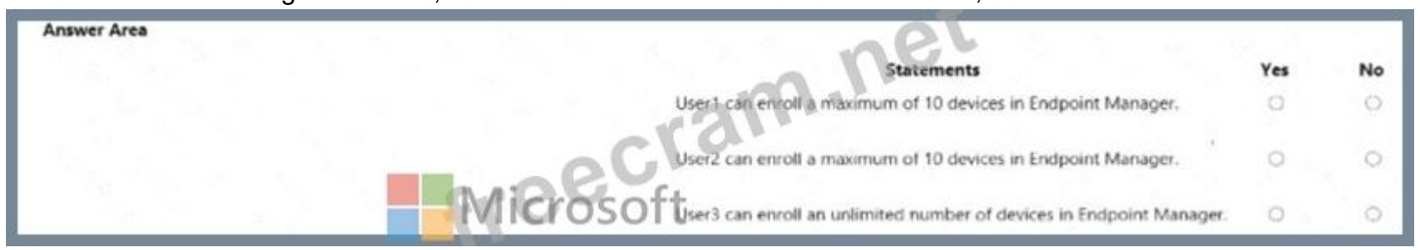
Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	**None**	**None**

The device limit restrictions in Endpoint manager are configured as shown in the following table.

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

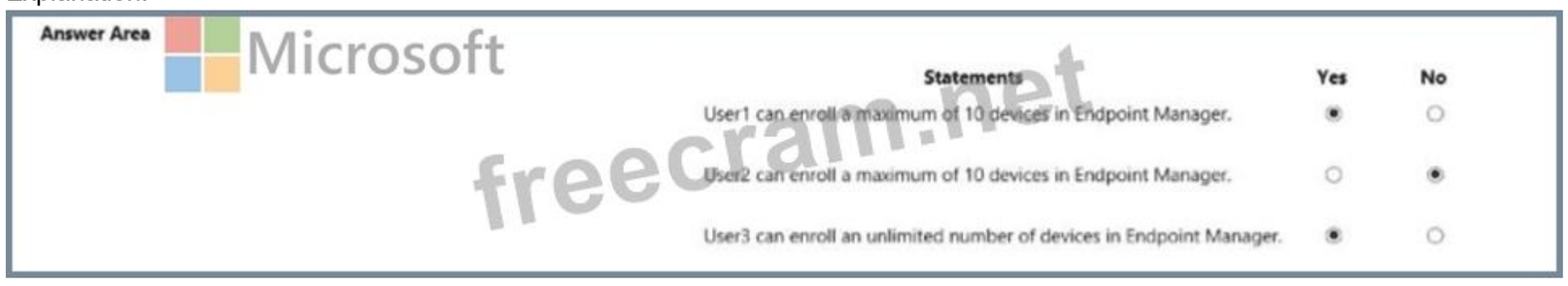
You add user as a device enrollment manager in Endpoint manager

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



Answer:

Explanation:



NEW QUESTION: 41

You have a Microsoft 365 E5 subscription.

Conditional Access is configured to block high-risk sign-ins for all users.

All users are in France and are registered for multi-factor authentication (MFA).

Users in the media department will travel to various countries during the next month.

You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention.

What should you configure?

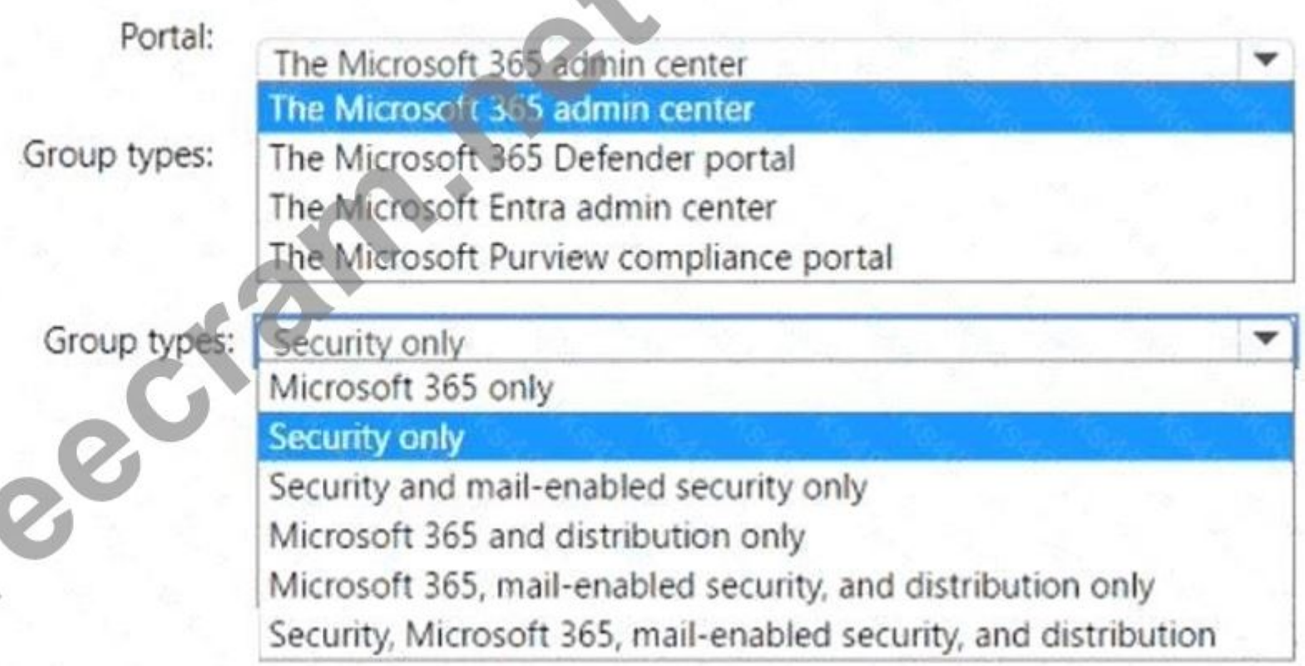
A. an exclusion group

B. the MFA registration policy

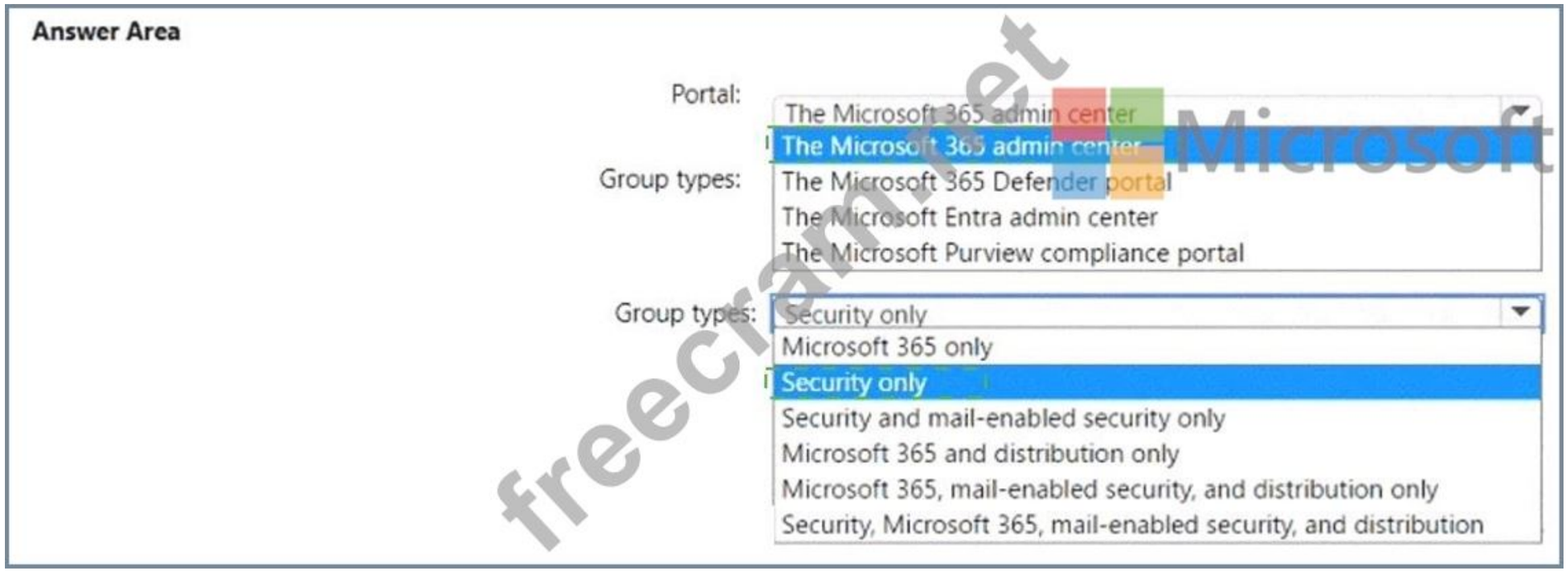
C. named locations
D. self-service password reset (SSPR)
Answer: (SHOW ANSWER)
Self-remediation with self-service password reset
If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock

NEW QUESTION: 42
You have a Microsoft 365 E5 subscription.
You need to configure a group naming policy.
Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

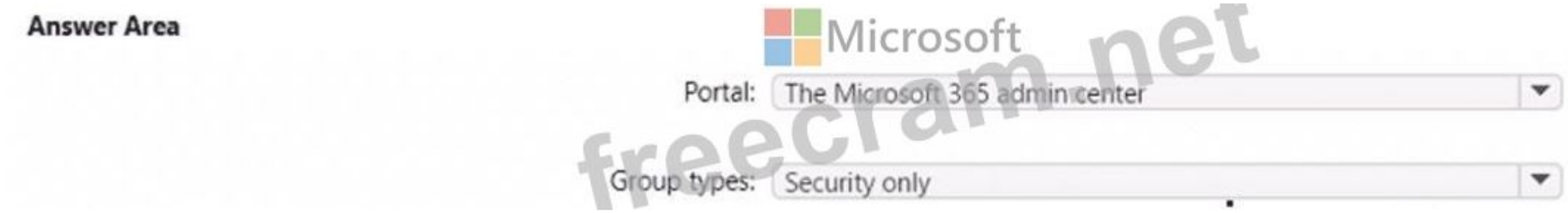
Answer Area



Answer:



Explanation:



NEW QUESTION: 43

(You have a Microsoft 365 E5 subscription that contains 1,000 Windows devices.

You need to review the exposure score of the devices.

Which portal should you use?)

A. the Microsoft Intune admin center

B. the Microsoft Purview portal

C. the Microsoft Defender portal

D. the Microsoft 365 admin center

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation From Exact Extract of Microsoft 365 Admin documents guides:

The correct answer is the Microsoft Defender portal.

Explanation:

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

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

* The Exposure Score helps administrators:

* Understand how vulnerable devices are across the organization
* Track improvements to security posture over time
* Prioritize remediation actions based on risk
* Microsoft explicitly states that Exposure Score is viewed and managed within the Microsoft Defender portal, which serves as the central dashboard for Defender for Endpoint, Defender for Office 365, and related security services.

Why the other options are incorrect

A). the Microsoft Intune admin center

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

B). the Microsoft Purview portal

Microsoft Purview is used for data governance, compliance, insider risk, and information protection. It has no functionality related to endpoint exposure scoring.

D). the Microsoft 365 admin center

The Microsoft 365 admin center is designed for tenant-wide administration such as users, licenses, and services. It does not provide detailed endpoint security metrics like Exposure Score.

NEW QUESTION: 44

You have a Microsoft 365 E5 tenant that contains the resources shown in the following table.

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

To which resources can you apply a sensitivity label by using an auto-labeling policy?

A. Mailbox1 and Site1 only
B. Mailbox1, Account1, and Site1 only
C. Account1 and Site1 only
D. Mailbox1, Account1, Site1, and Channel1
E. Account1, Site1, and Channel1 only

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 45

You have a Microsoft 365 subscription that contains a user named User1.

User1 requires admin access to perform the following tasks:

Manage Microsoft Exchange Online settings.

Create Microsoft 365 groups.

You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.

What should you use?

A. zure AD Identity Protection
B. Microsoft Entra Verified ID
C. Conditional Access
D. Azure AD Privileged Identity Management (PJM)

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

NEW QUESTION: 46
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

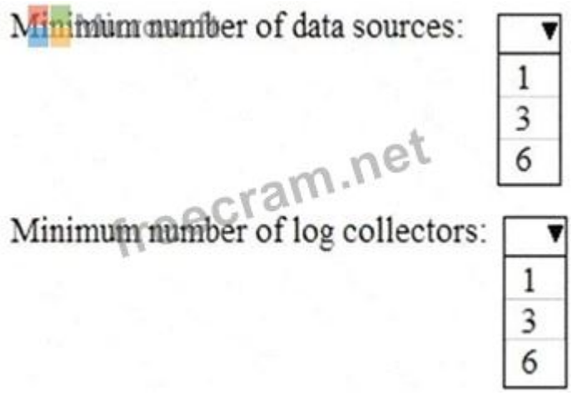
Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to publish a sensitivity label named Label1.
To which groups can you publish Label1?
A. Group1 only
B. Group1 and Group2 only
C. Group1 and Group4 only
D. Group1, Group2, and Group3 only
E. Group1 Group2, Group3, and Group4
Answer: (SHOW ANSWER)
In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites

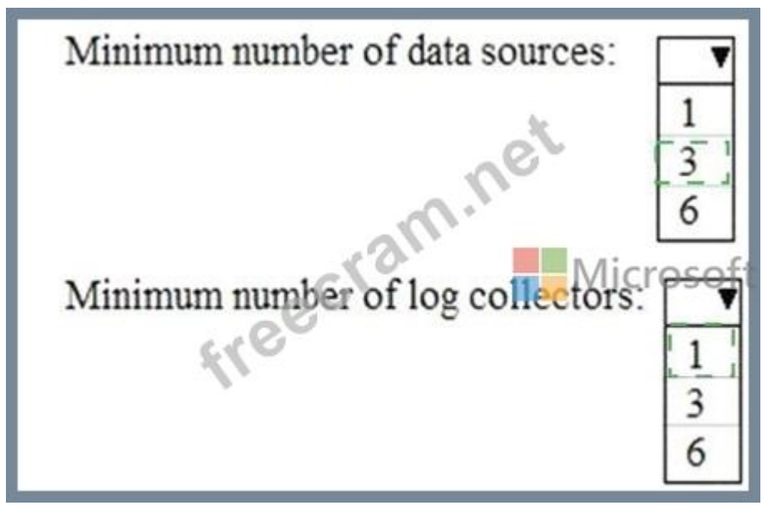
NEW QUESTION: 47
You have a Microsoft 365 E5 tenant.
You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.
You need to export the existing template.
Which file format should you use for the exported template?
A. CSV
B. XLSX
C. JSON
D. XML
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldwide#export-a-template

NEW QUESTION: 48
You have a Microsoft 365 tenant.
You plan to implement device configuration profiles in Microsoft Intune.
Which platform can you manage by using the profiles?
A. macOS
B. Windows 8.1
C. Android Enterprise
D. Ubuntu Linux
Answer: (SHOW ANSWER)

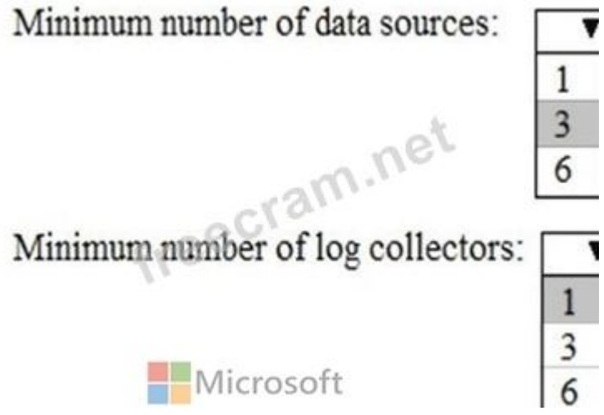
NEW QUESTION: 49
You need to meet the technical requirement for log analysis.
What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



References:

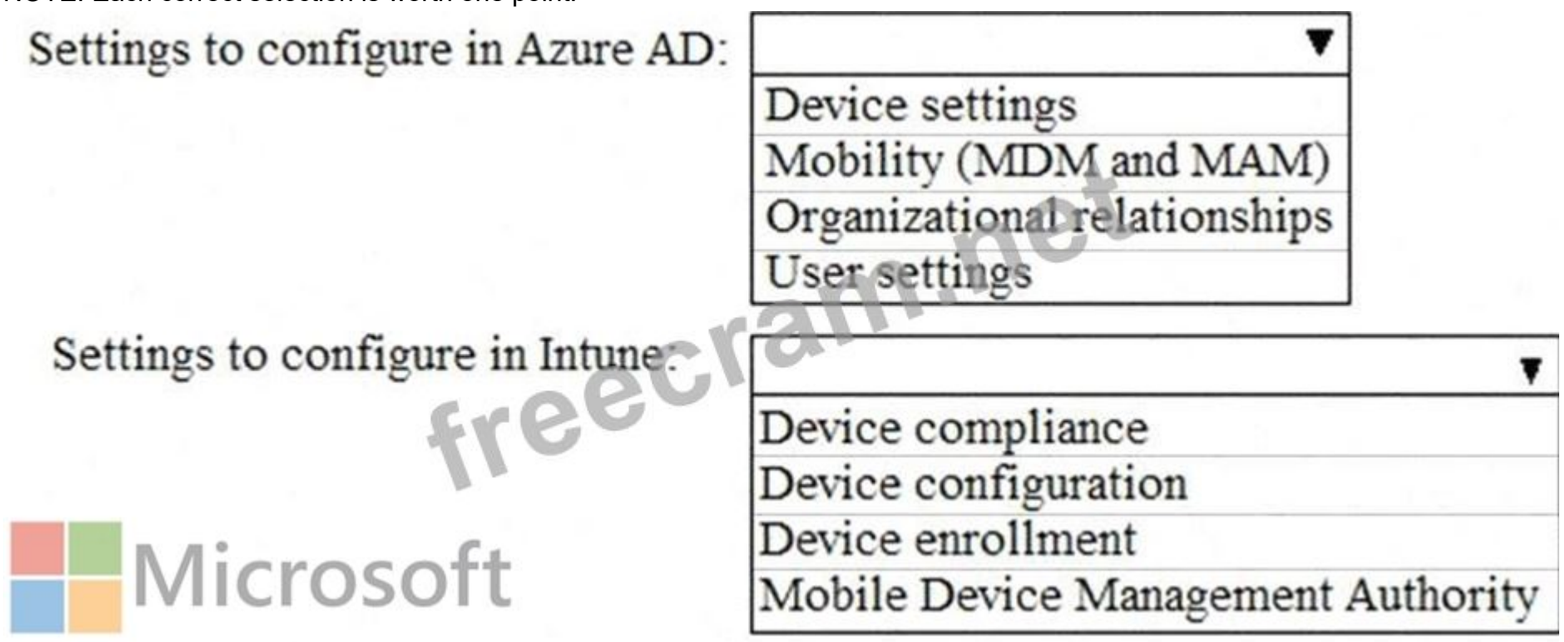
https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

NEW QUESTION: 50

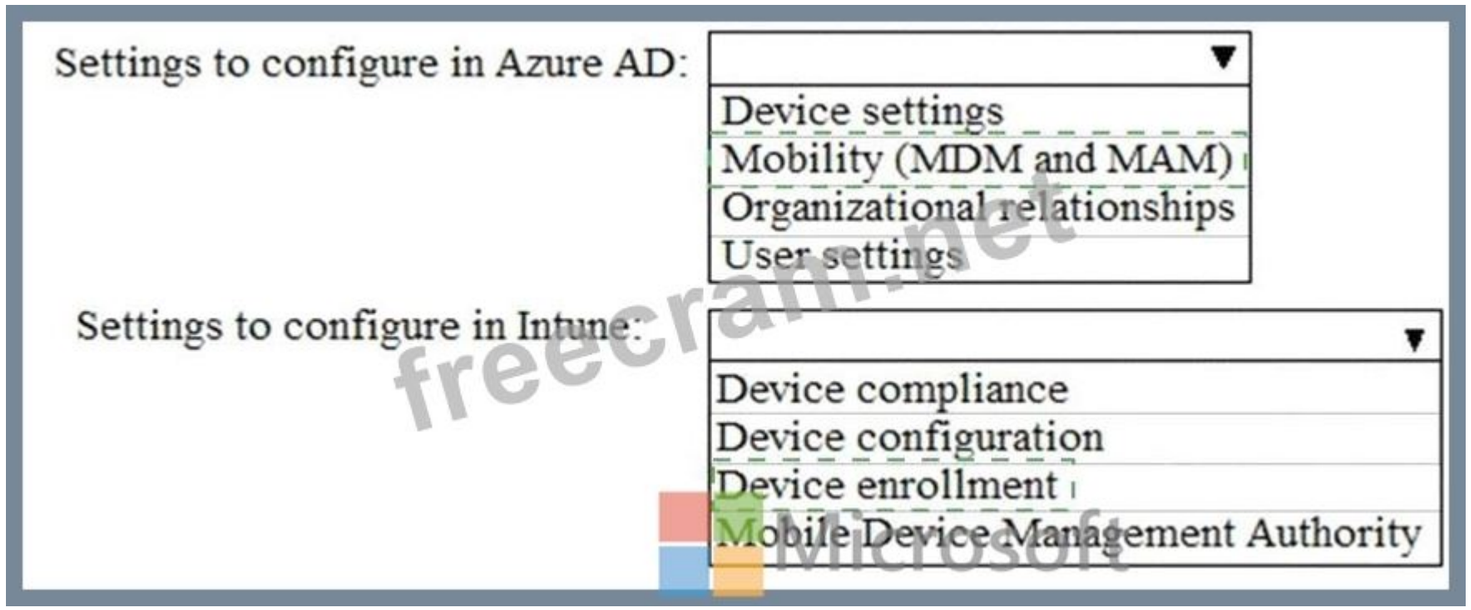
You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.
You need to remove User1 from the Restricted entities list. What should you use?

A. the Exchange admin center
B. the Microsoft 365 admin center
C. the Microsoft Purview portal
D. the Microsoft Entra admin center
E. the Microsoft Defender portal
Answer: (SHOW ANSWER)

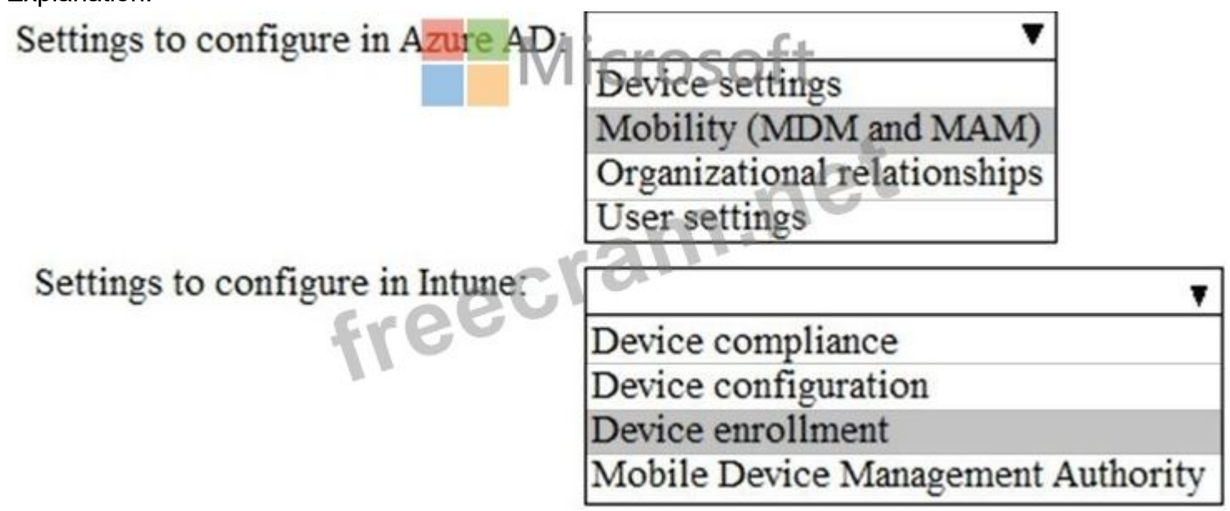
NEW QUESTION: 51
You need to meet the Intune requirements for the Windows 10 devices.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



References:

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

Topic 3, Litware Inc.Case Study

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

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

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

To start the case study

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

Overview

General Overviews

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

Environment

Existing Environment

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

Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

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

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

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

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

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

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

The verified domain is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Audit log search is turned on for the litware.com tenant.

Problem Statements

Litware identifies the following issues:

Users open email attachments that contain malicious content.

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

User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.
Requirements
Planned Changes
Litware plans to implement the following changes:
Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
Implement data loss prevention (DLP) policies to protect confidential information.
Grant User2 permissions to review the audit logs of he litware.com tenant.
Deploy new devices to the Seattle office as shown in the following table.

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

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

NEW QUESTION: 52

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You copy the Group Policy Administrative Templates from a Windows 10 computer to Server1.
Does this meet the goal?
A. yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From Device Manager, you view the computer properties.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

NEW QUESTION: 54
You configure an anti-phishing policy as shown in the following exhibit.

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

Use the drop-down menus to select the answer choke that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

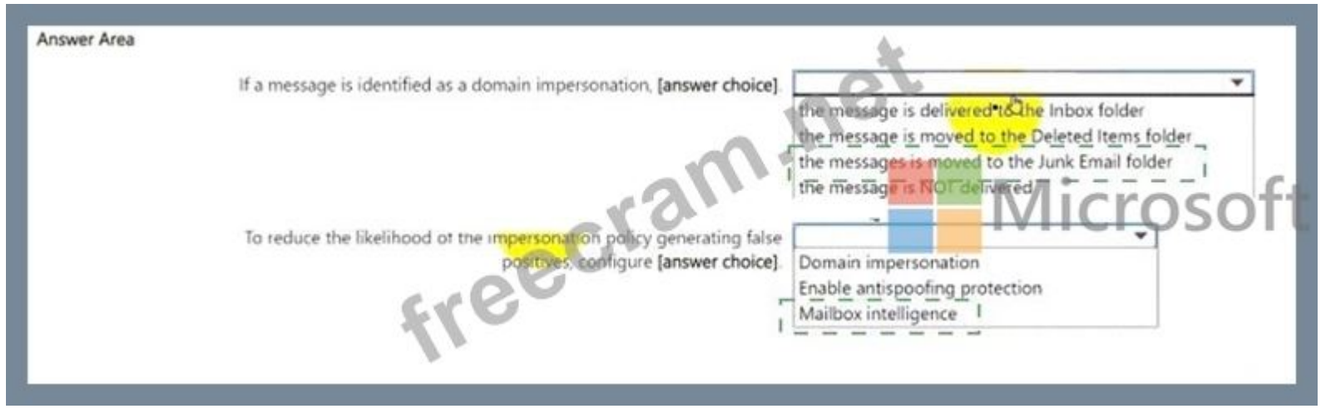
If a message is identified as a domain impersonation, [answer choice]

- 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:



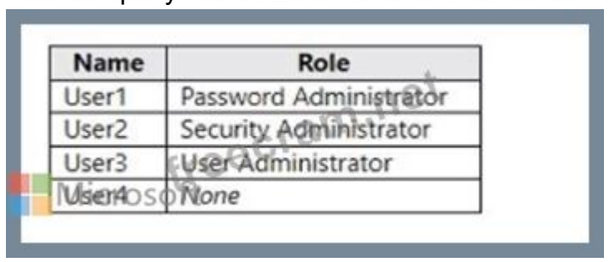
Explanation:

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: 55

Your company has a Azure AD tenant named comoso.onmicrosoft.com that contains the users shown in the following table.



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

You need to identify which users can perform the following administrative tasks:

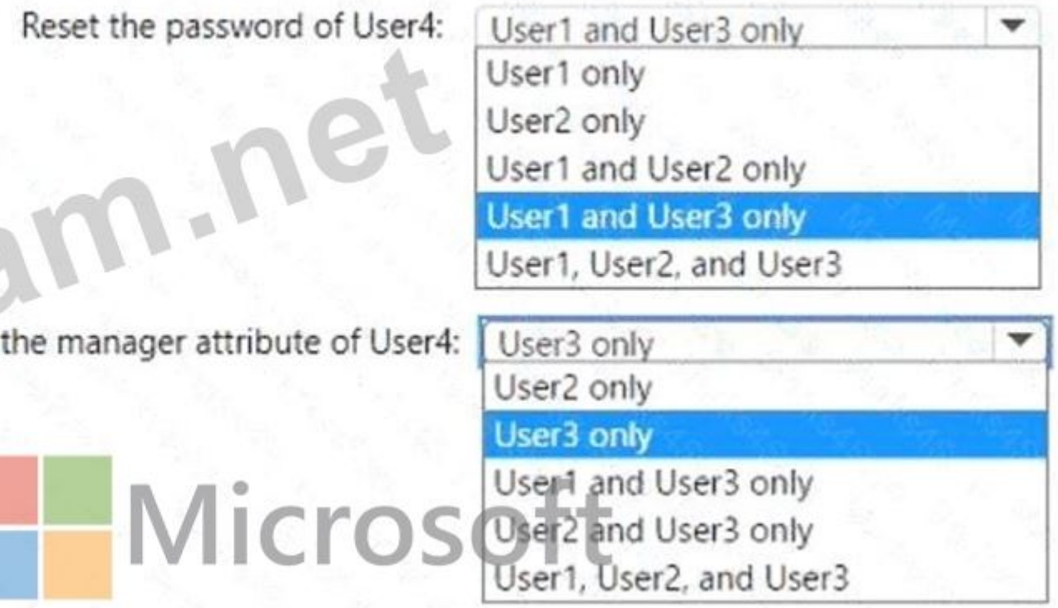
* Reset the password of User4.

* Modify the value for the manager attribute of User4.

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

NEW QUESTION: 56

Your company has a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

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

You create a retention label named Label 1 that has the following configurations:

* Retains content for five years
* Automatically deletes all content that is older than five years

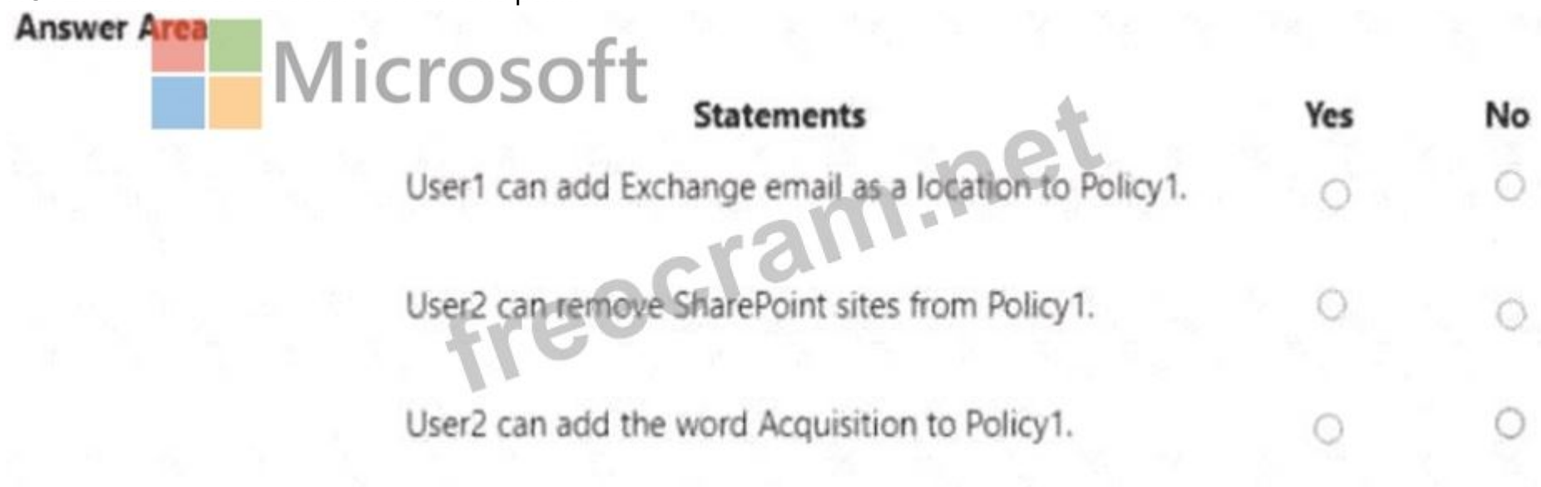
You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

* Applies to content that contains the word Merger
* Specifies the OneDrive accounts and SharePoint sites locations

You run the following command.

Set-RetentionConpliancePolicy Policy1 -RestrictiveRetention Strue -Force For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

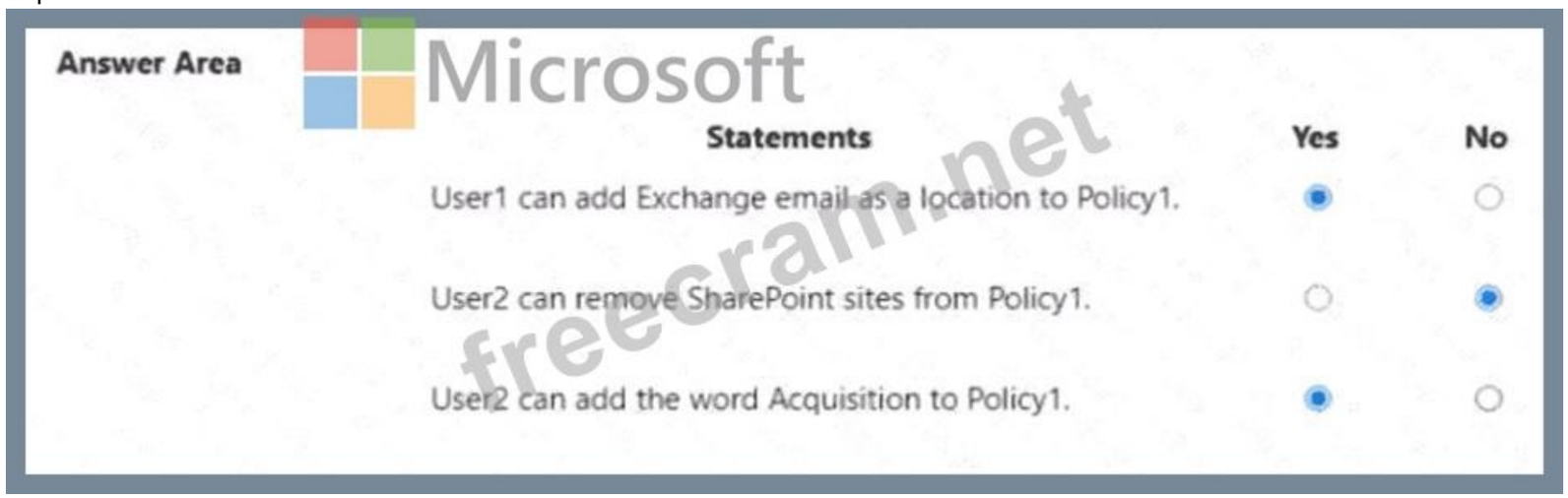


Answer:

Answer Area

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

Explanation:

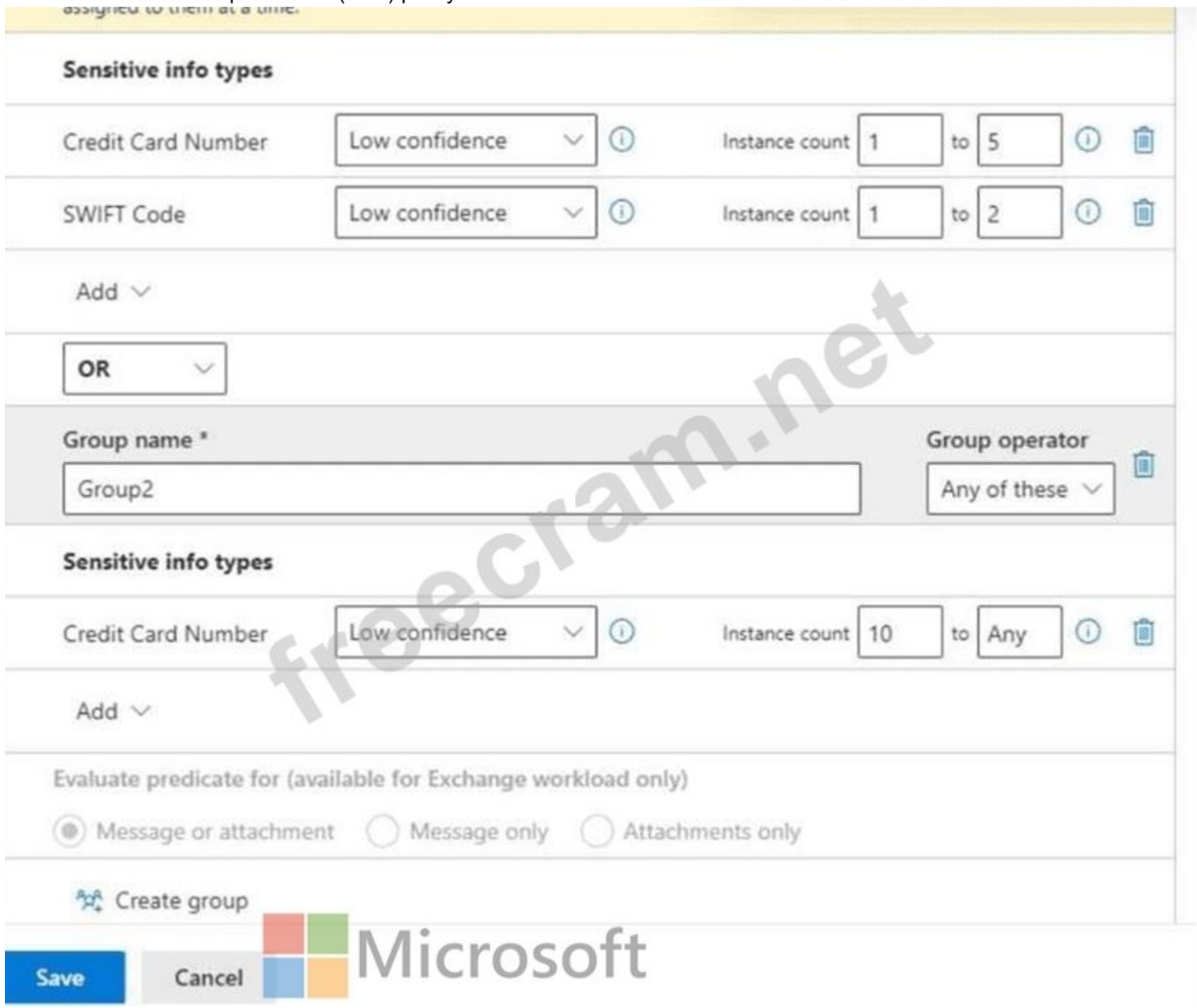


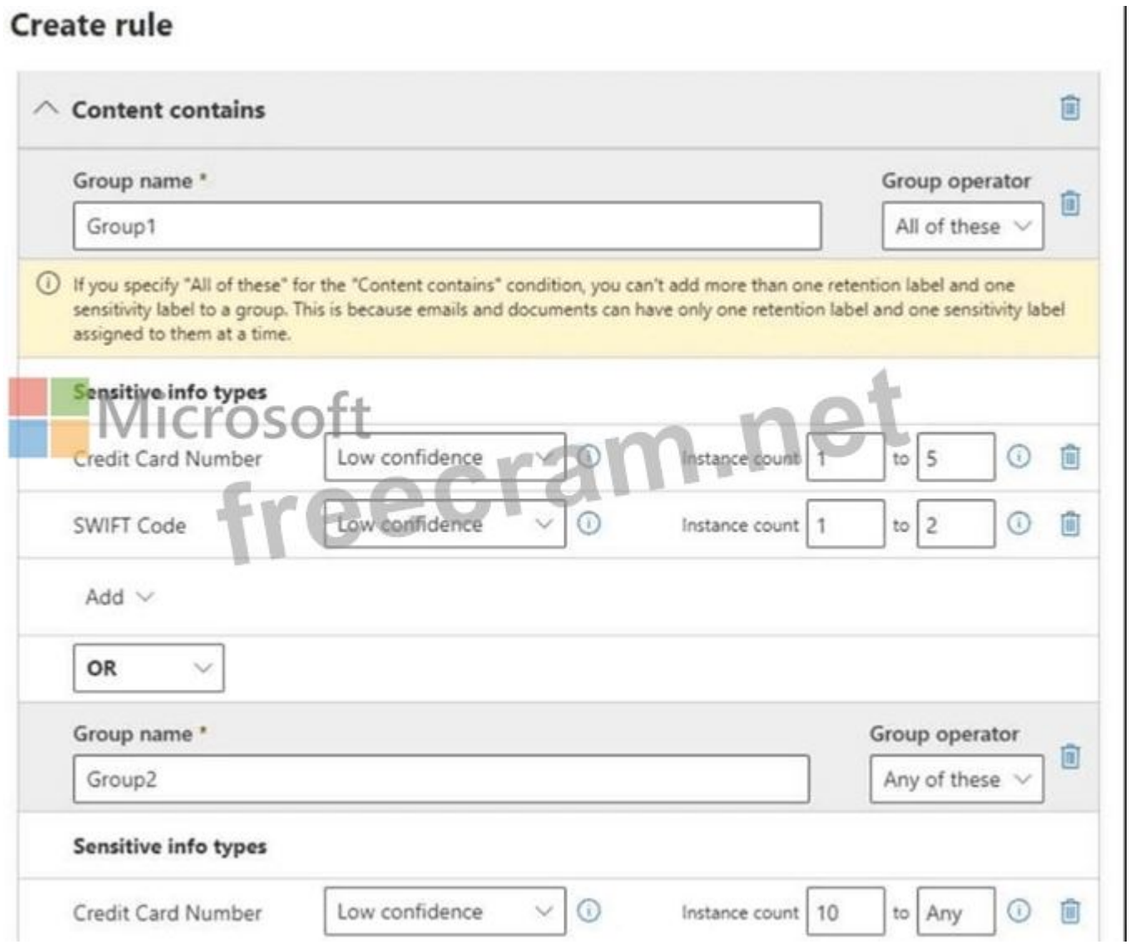
NEW QUESTION: 57
You need to create the DLP policy to meet the technical requirements.
What should you configure first?
A. sensitive info types
B. the Insider risk management settings
C. the event types
D. the sensitivity labels
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

NEW QUESTION: 58
You have a Microsoft 365 E5 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2.
You have the documents shown in the following table.

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

You create a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rule as shown in the exhibit.





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

NOTE: Each correct selection is worth one point.

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

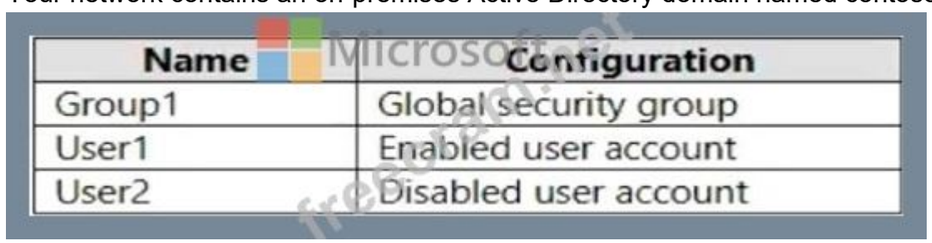
Document1: Credit Card = 3, SWIFT = 3

* 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: 59

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.



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

You configure Azure AD Connect to sync contoso.com to Azure AD.

Which objects will sync to Azure AD?

A. Group1 only

B. User1 and User2 only

C. Group1 and User1 only

D. Group1, User1, and User2

Answer: (SHOW ANSWER)

Disabled accounts

Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.

The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.

Reference:

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

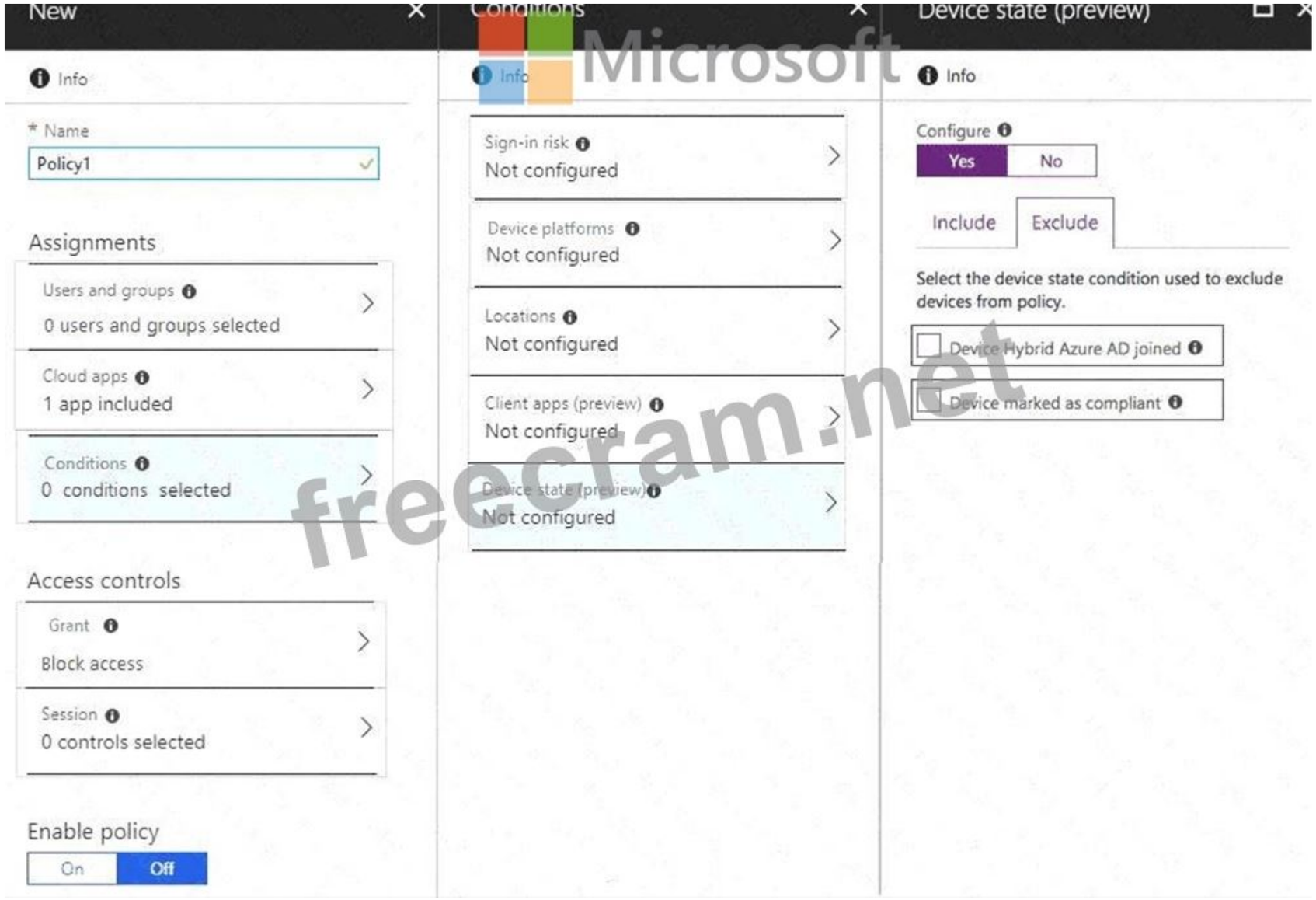
NEW QUESTION: 60

You need to configure a conditional access policy to meet the compliance requirements.

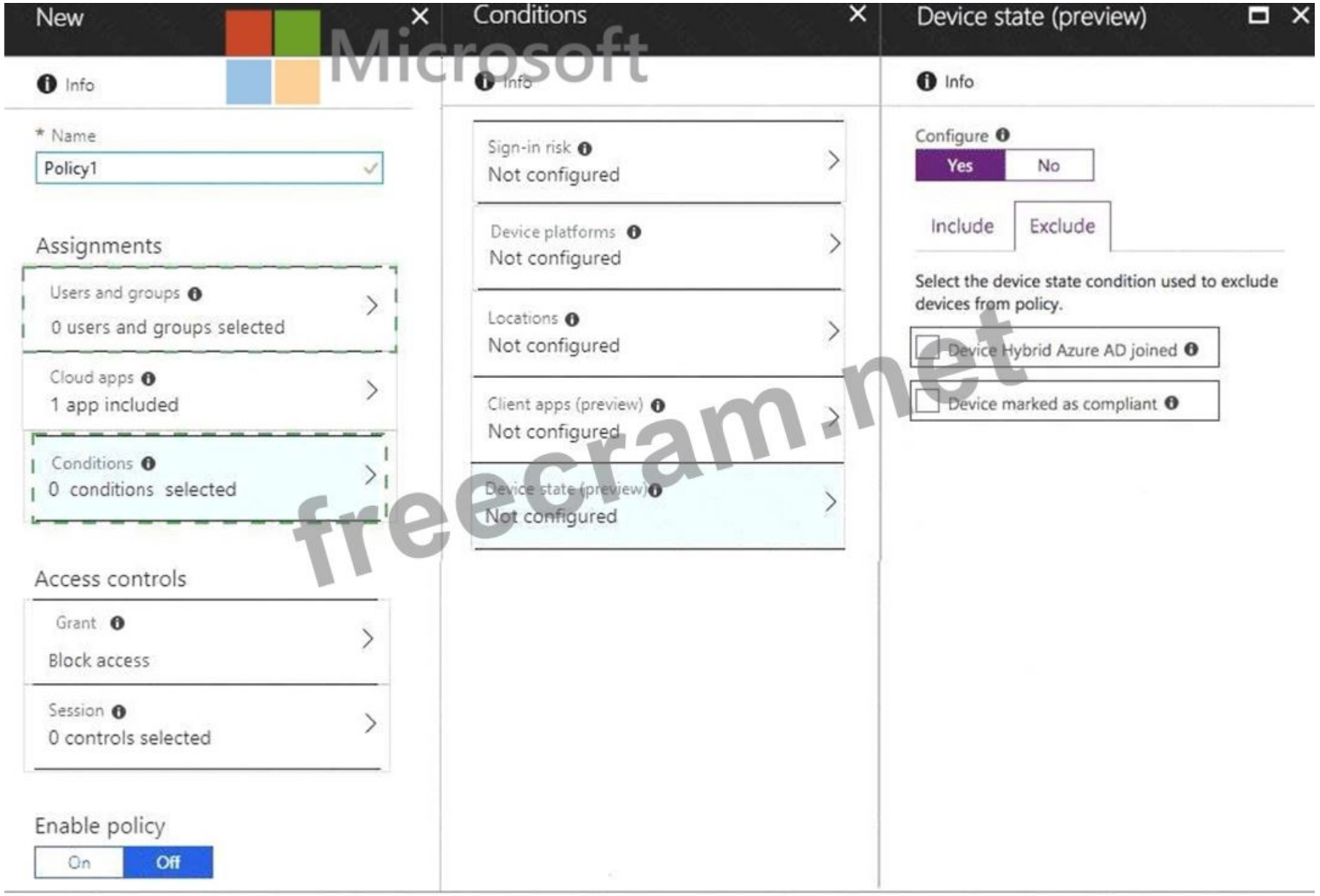
You add Exchange Online as a cloud app.

Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

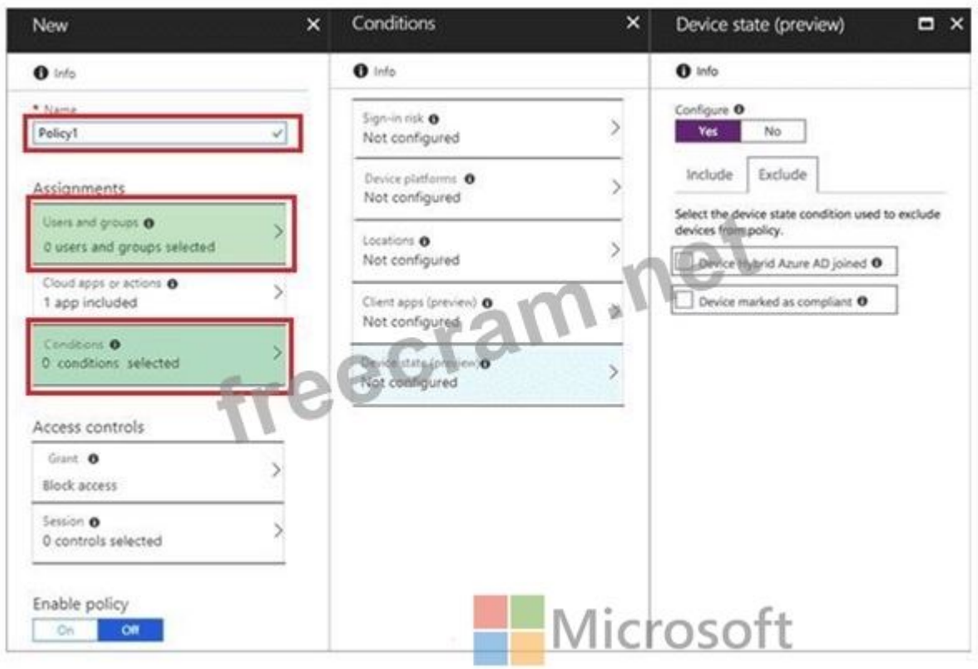


Answer:



Explanation:

Suggested answer:



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

NEW QUESTION: 61

You have a Microsoft 365 tenant that contains the compliance policies shown in the following table.

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

The tenant contains the devices shown in the following table.

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

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

Answer:

Explanation:

NEW QUESTION: 62

You have a Microsoft J65 E5 subscription.

You integrate Microsoft Defender for Endpoint with Microsoft Intune.

You need to ensure that devices automatically onboard to Defender for Endpoint when they are enrolled in Intune.

Solution: You configure a device configuration profile.

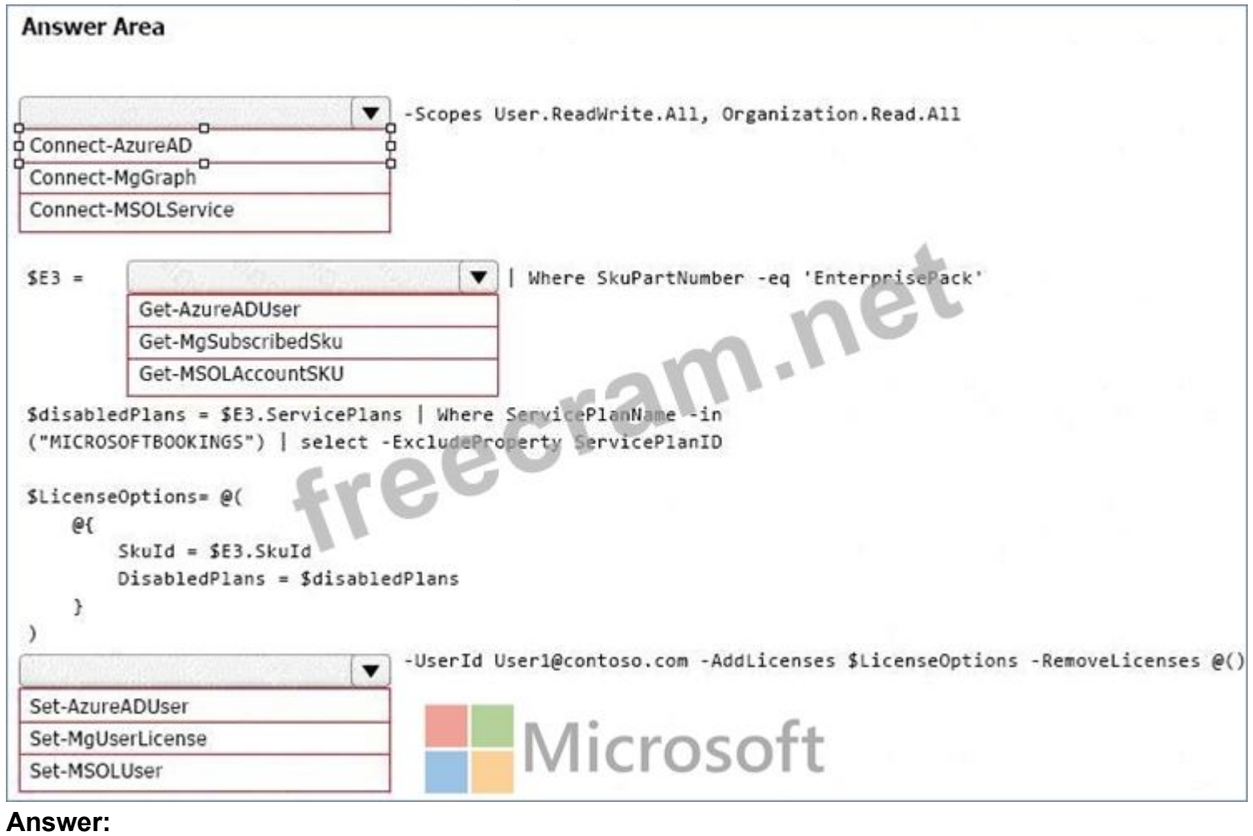
Does this meet the goal?

A. Yes

B. No
Answer: (SHOW ANSWER)

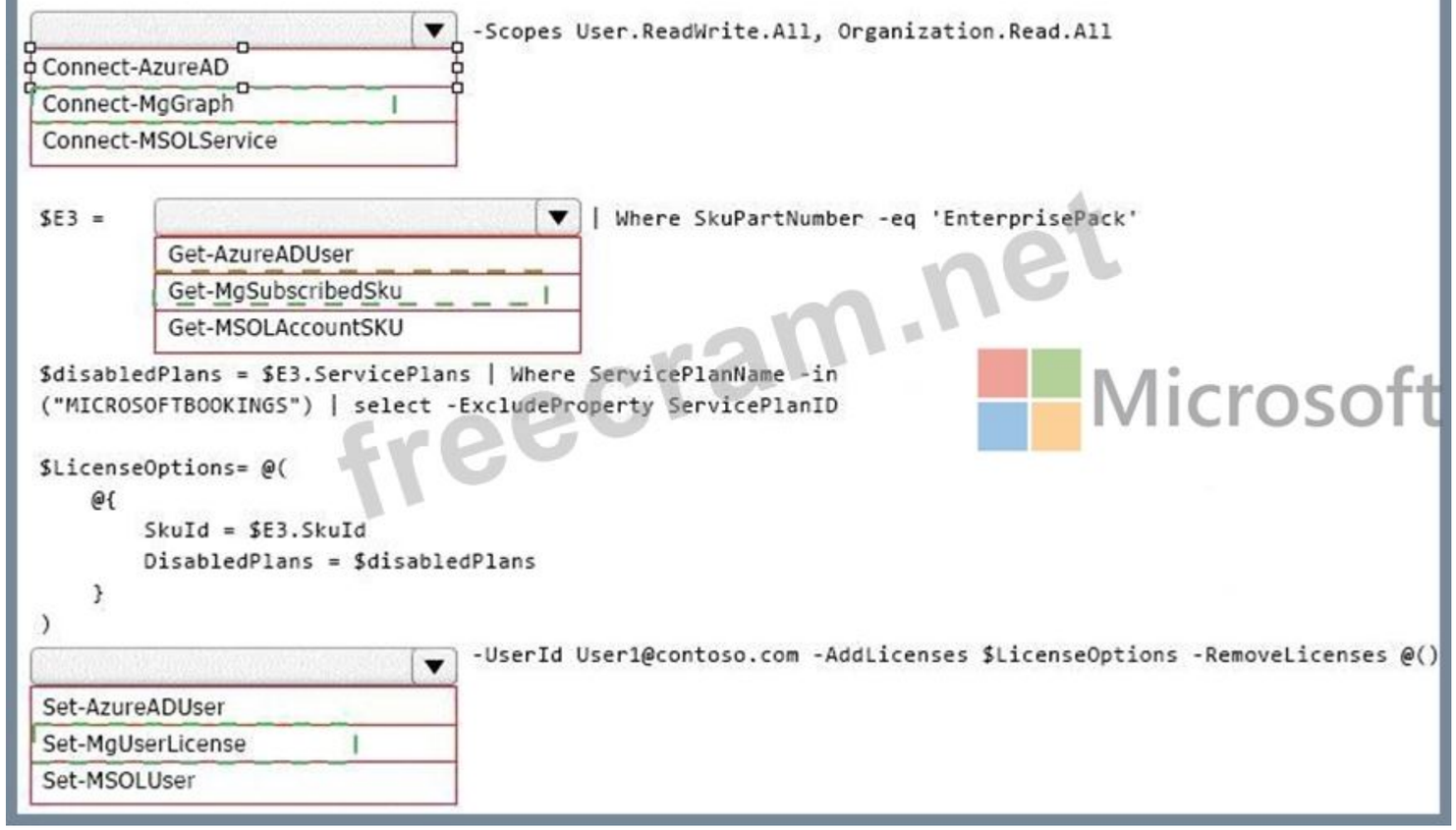
NEW QUESTION: 63
You have a Microsoft 365 subscription.
You need to identify which administrative users performed eDiscovery searches during the past week.
What should you do from the Security & Compliance admin center?
A. Perform a content search
B. Create a supervision policy
C. Perform an audit log search
D. Create an eDiscovery case
Answer: (SHOW ANSWER)

NEW QUESTION: 64
HOTSPOT
You have a Microsoft 365 subscription.
A user named user1@contoso.com was recently provisioned.
You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Answer Area



Explanation:

Answer Area

```
[ ▼ ]  -Scopes User.ReadWrite.All, Organization.Read.All
```

- Connect-AzureAD
- Connect-MgGraph
- Connect-MSOLService

```
$E3 = [ ▼ ] | Where SkuPartNumber -eq 'EnterprisePack'
```

- Get-AzureADUser
- Get-MgSubscribedSku
- Get-MSOLAccountSKU

```
$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$LicenseOptions= @(
    @{
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    }
)
[ ▼ ]  -UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @()
```

- Set-AzureADUser
- Set-MgUserLicense
- Set-MSOLUser

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: 65

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You have devices enrolled in Intune as shown in the following table.

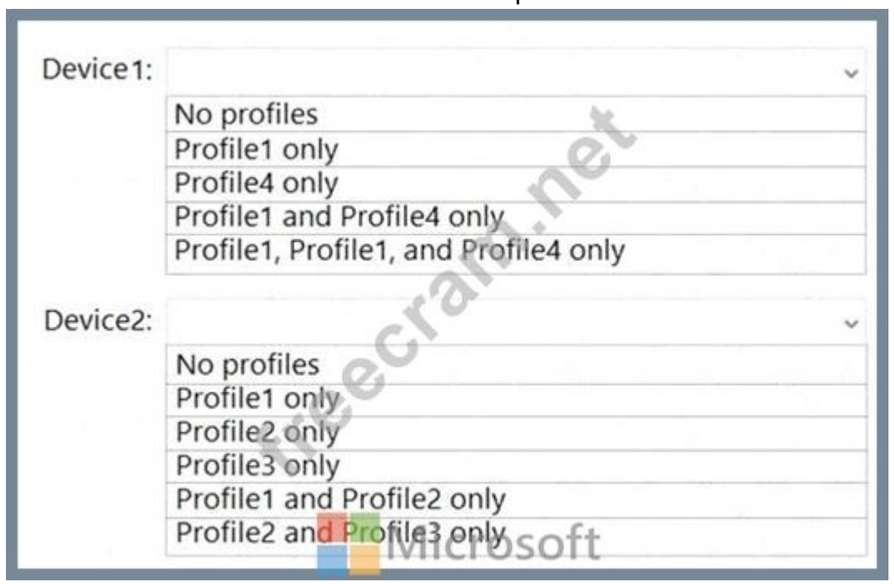
Name	Platform	Member of	Scope (Tags)
Device1	Windows 10	Group1, Group3	Tag1
Device2	Android	Group2	Tag2

You create the device configuration profiles shown in the following table.

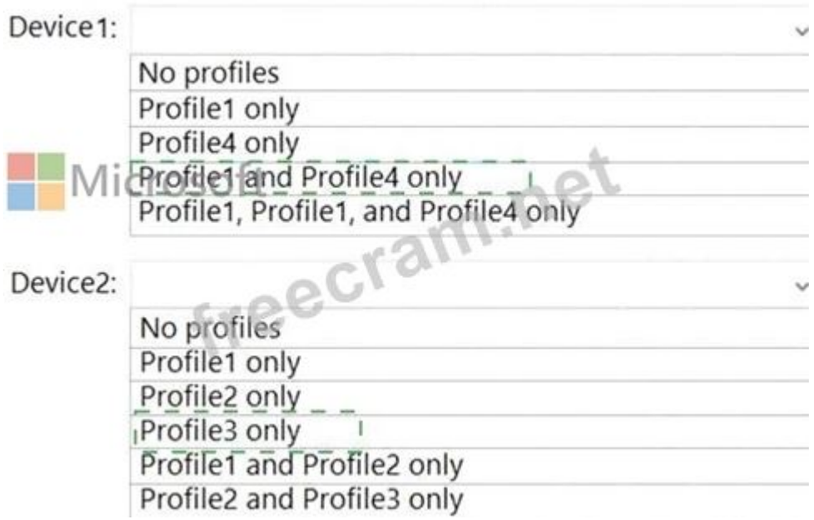
Name	Platform	Assignments: Included groups	Assignments: Excluded groups	Scope tags
Profile1	Windows 10 and later	Group1	Group3	Tag1, Tag2
Profile2	Android Enterprise	All devices	Group2	Tag1, Tag2
Profile3	Android Enterprise	Group2, Group3	Group3	Tag1
Profile4	Windows 10 and later	Group3	None	Default

Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.

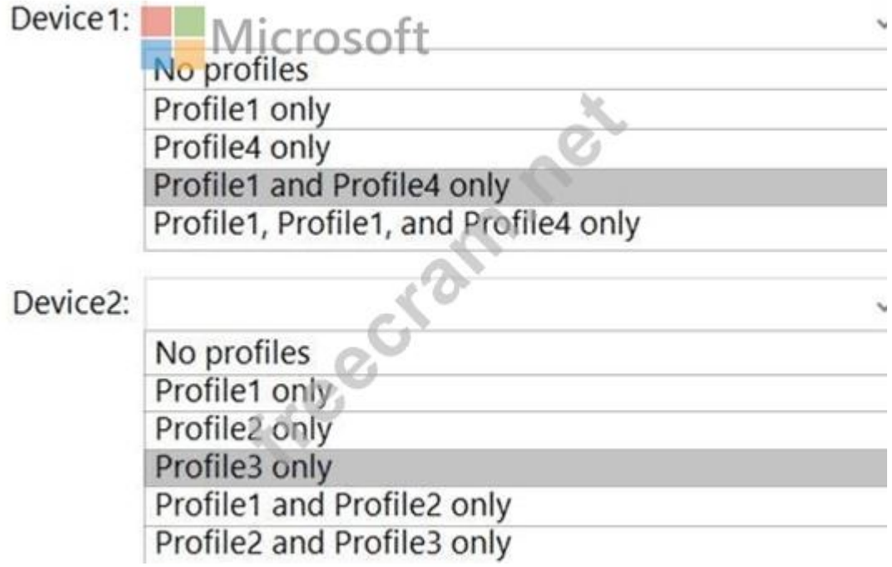
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 66

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 security center.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

A. Microsoft Cloud App Security

B. Azure Sentinel

C. Azure Web Application Firewall

D. Azure Defender

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

NEW QUESTION: 67

You have a Microsoft 365 E5 tenant.

You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege.

Which type of policy should you create and which Microsoft 365 compliance center role is required to create the pokey? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 68

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

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. no settings

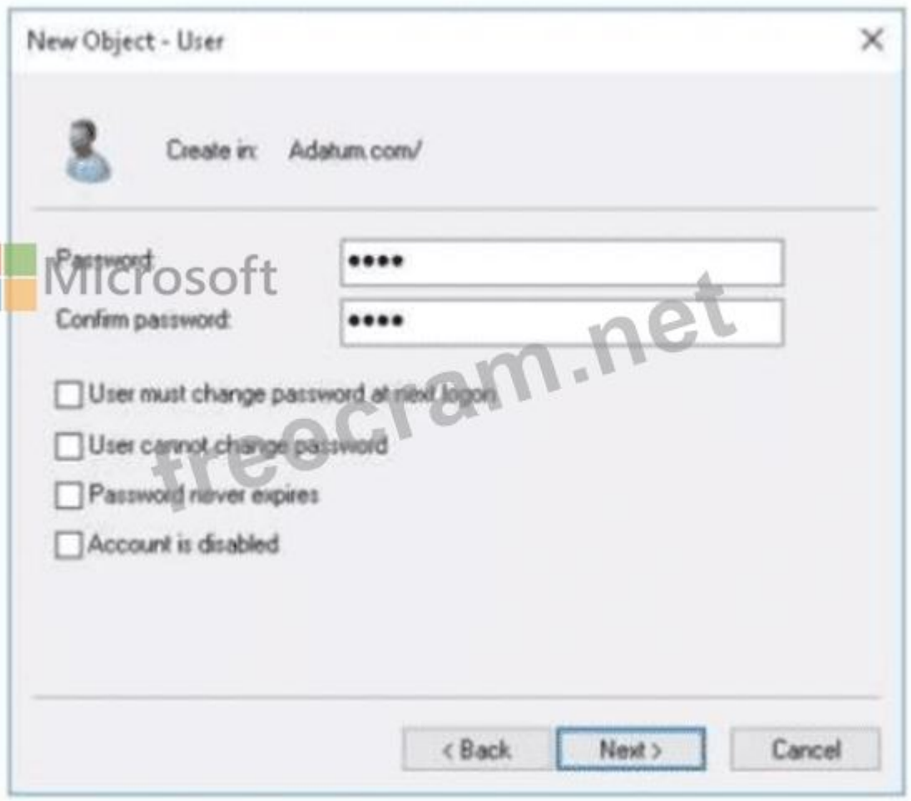
B. only the settings of Policy!

C. only the settings of Policy2

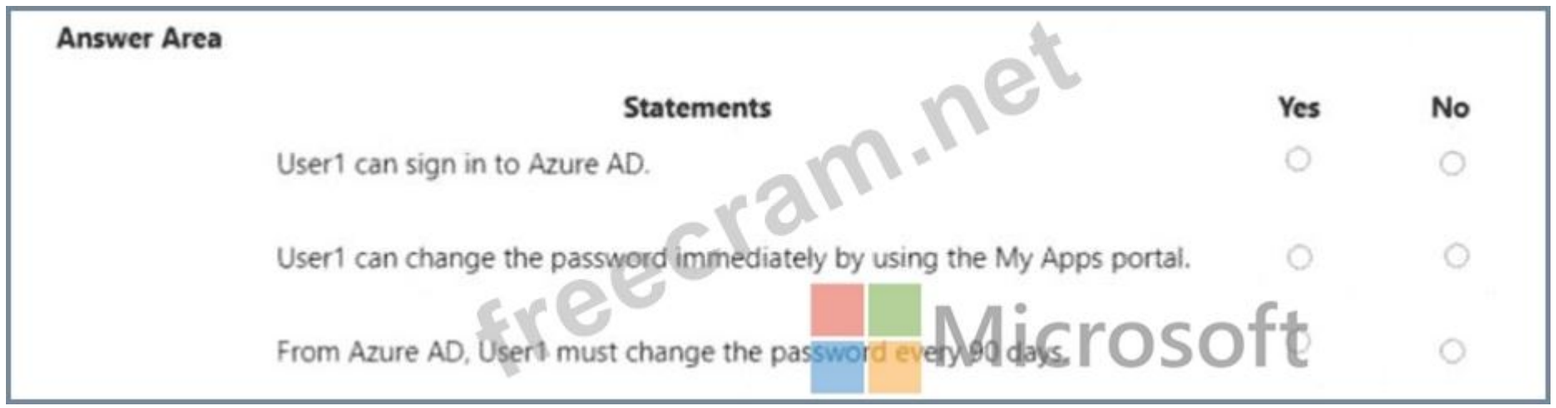
D. only the settings of Policy3

Answer: (SHOW ANSWER)

NEW QUESTION: 69
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure AD by using the Azure AD Connect Express Settings. Password write back is disabled.
You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.



The Azure AD password policy is configured as shown in the following exhibit.
Password policy
Set the password policy for all users in your organization.
Days before passwords expire 90
Days before a user is notified about 14
expiration
You confirm that User1 is synced to Azure AD.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

NEW QUESTION: 70

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You need to ensure that users are prevented from opening or downloading malicious files from Microsoft Teams, OneDrive, or SharePoint Online.
What should you do?

A. Create a newAnti-malware policy

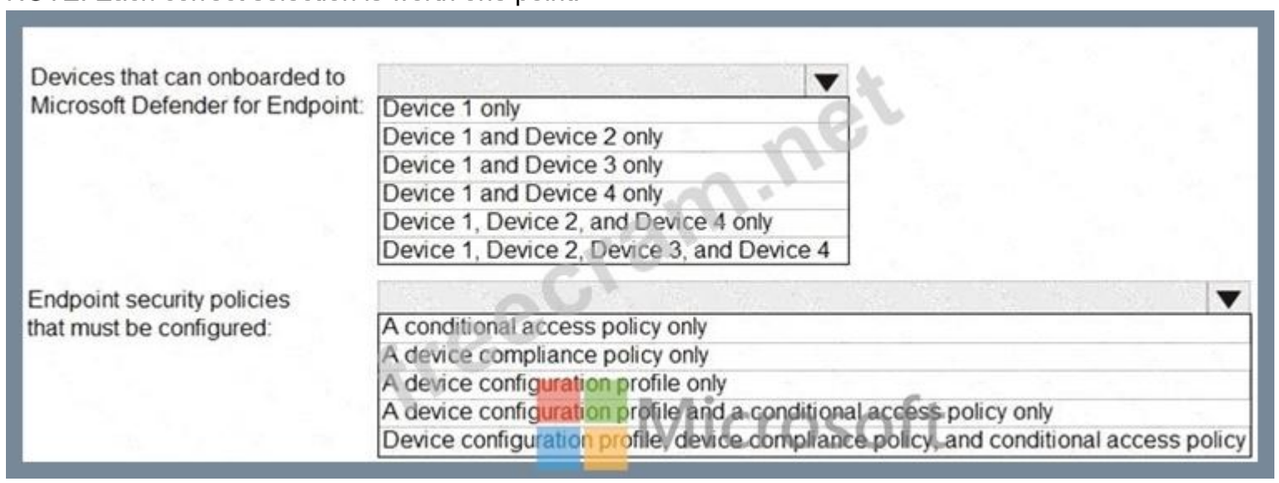
B. Configure the Safe Links global settings.

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

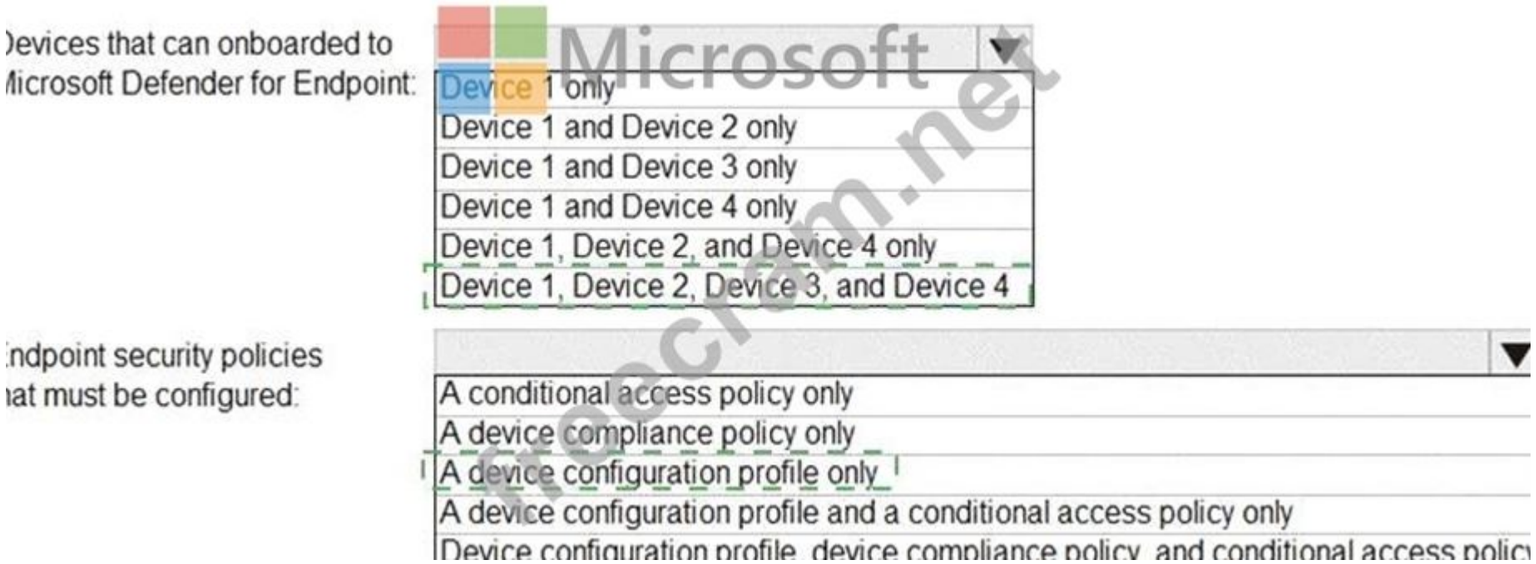
NEW QUESTION: 71
You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.
You have devices enrolled in Microsoft Intune as shown in the following table.

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

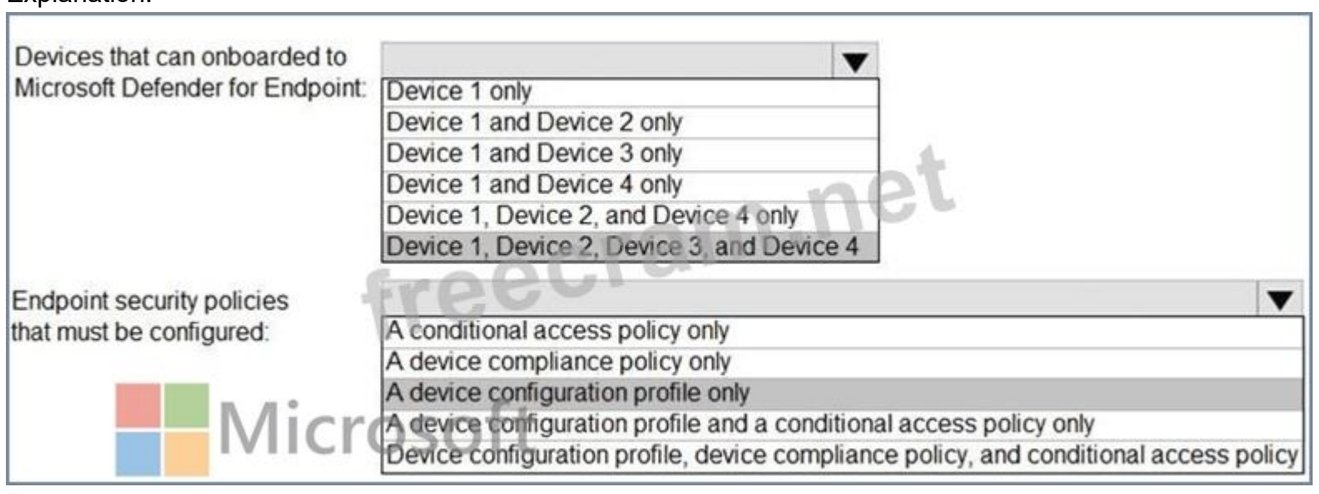
You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant.
Noncompliant devices must be blocked from accessing corporate resources.
You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

NEW QUESTION: 72
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

Which users can review the Adoption Score in the Microsoft 365 admin center?
A. User! and User3 only
B. User1 and User2 only

C. User! only
D. User2onry
E. User1, User2. and User3
Answer: (SHOW ANSWER)

NEW QUESTION: 73
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft Defender XDR. Which Microsoft service source will appear on the Incidents page of the Microsoft Defender portal?
A. Microsoft Defender for Cloud Apps
B. Microsoft Defender for Cloud
C. Azure Arc
D. Azure Information Protection
Answer: (SHOW ANSWER)

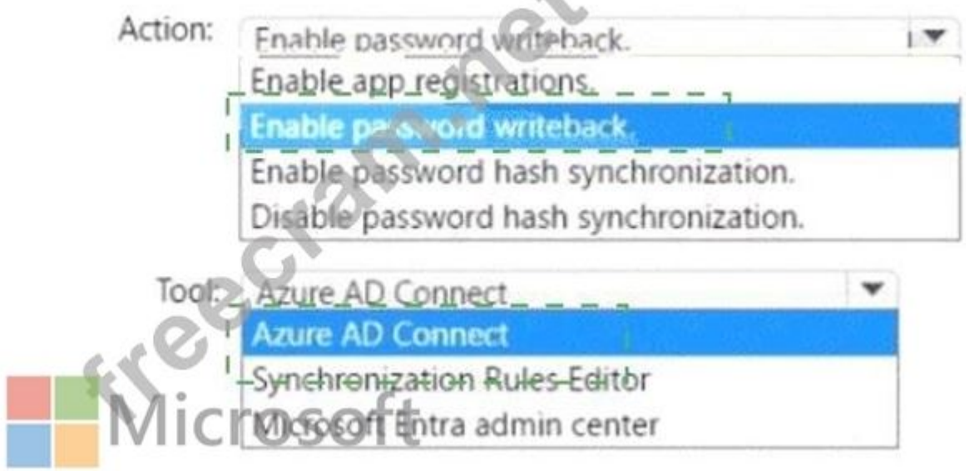
NEW QUESTION: 74
Your company has multiple offices.
You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.
You need to ensure that the local administrators can manage only the devices in their respective office.
What should you use?
A. scope tags
B. configuration profiles
C. device categories
D. conditional access policies
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

NEW QUESTION: 75
You need to ensure that Admin4 can use SSPR.
Which tool should you use. and which action should you perform? To answer, select the appropriate options m the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area



Explanation:

NEW QUESTION: 76

You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management. You need to add the phone number of the help desk to the Company Portal app. What should you do?

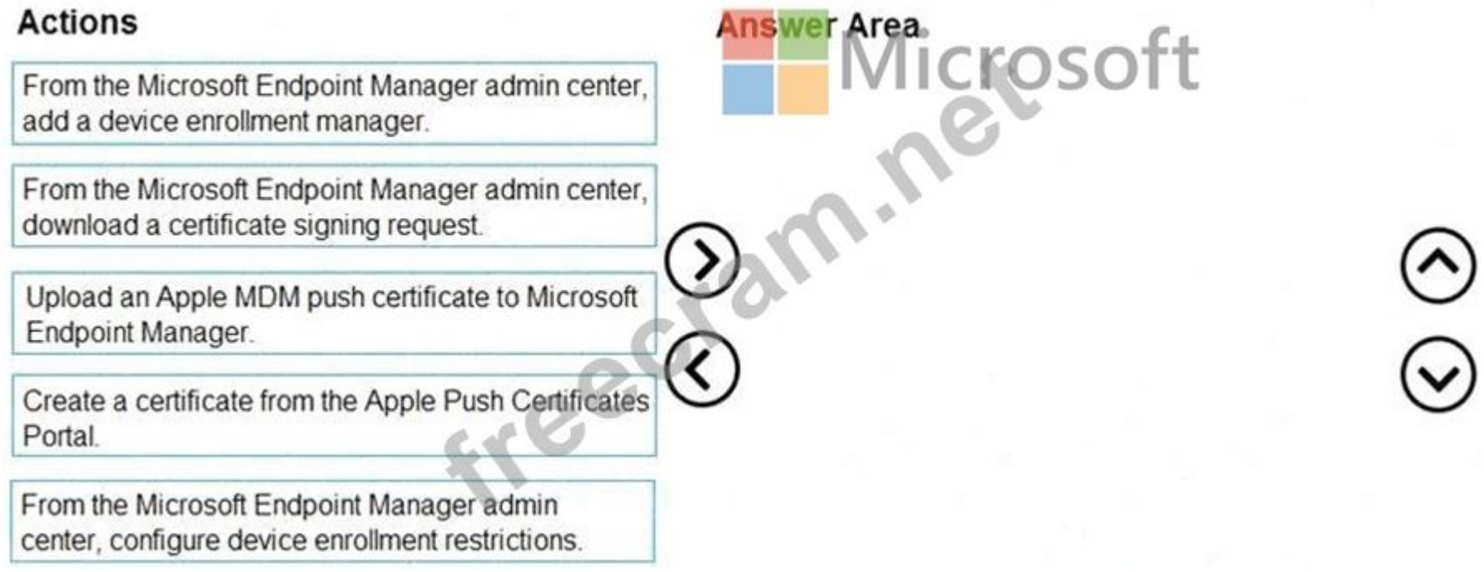
A. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.

B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.

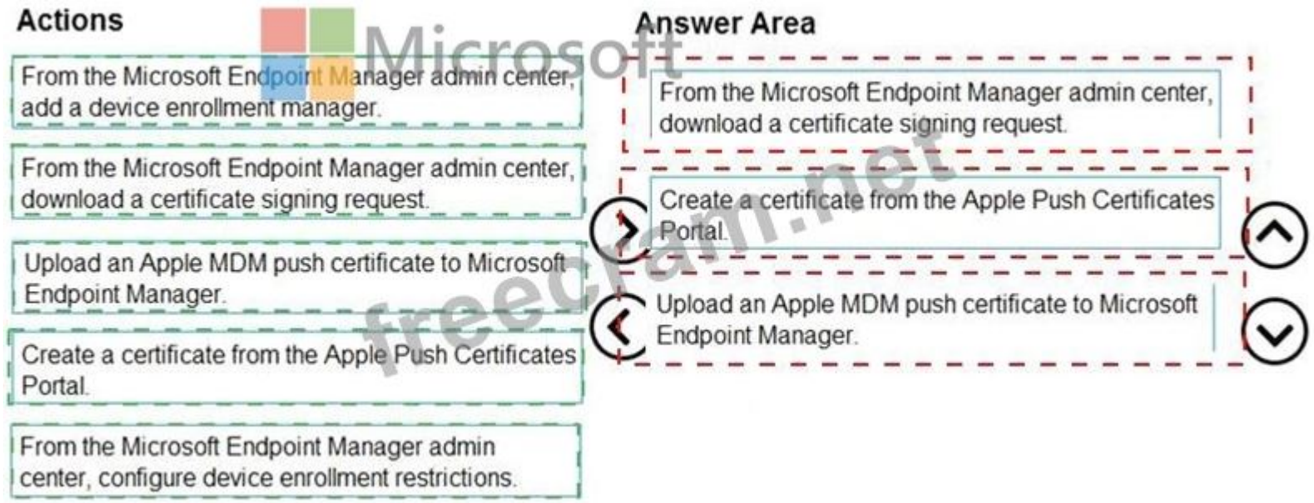
C. From the Microsoft 365 admin center, modify Organization information.

D. From the Microsoft 365 admin center, modify Help desk information.
Answer: (SHOW ANSWER)
Reference:
https://systemcenterdudes.com/intune-company-portal-customization/

NEW QUESTION: 77
You have a Microsoft 365 E5 subscription.
Several users have iOS devices.
You plan to enroll the iOS devices in Microsoft Endpoint Manager.
You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



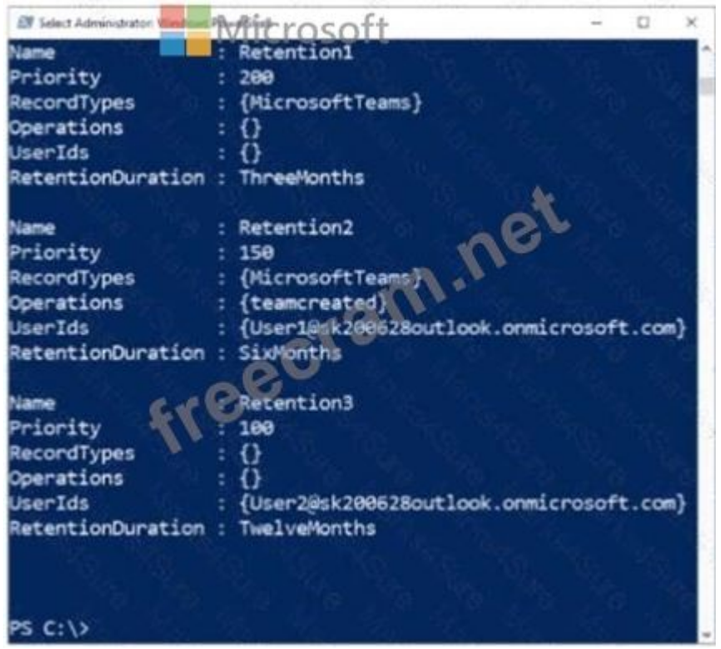
Answer:



Explanation:

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

NEW QUESTION: 78
You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic NOTE Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 79

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

The subscription has the following two anti-spam policies:

* Name: AntiSpam1
* Priority: 0
* Induce these users, groups and domains
o Users: User3
o Groups: Group1
* Exclude these users, groups and domains
o Groups: Group2
* Message limits
o Set a daily message limit 100
* Name: AntiSpam2
* Priority: 1
* Include these users, groups and domains
o Users: User! o Groups: Group2
* Exclude these users, groups and domains
o Users: User3
* Message limits
o Set a daily message limit 50

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	○	○
User2 can send a maximum of 50 email messages per day.	○	○
User3 can send a maximum of 100 email messages per day.	○	○

Answer:

Explanation:

NEW QUESTION: 80

You have a Microsoft 365 E5 subscription. Administrators are issued FID02 security keys.
You need to create a Conditional Access policy that will use a FID02 security key as an authentication method. Which Access controls option should you select for the policy?

A. Require authentication strength
B. Require token protection for sign-in sessions
C. Require approved client app
D. Require multifactor authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 81

On which server should you install the Azure ATP sensor?

A. Server 1
B. Server 2
C. Server 3
D. Server 4
E. Server 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.

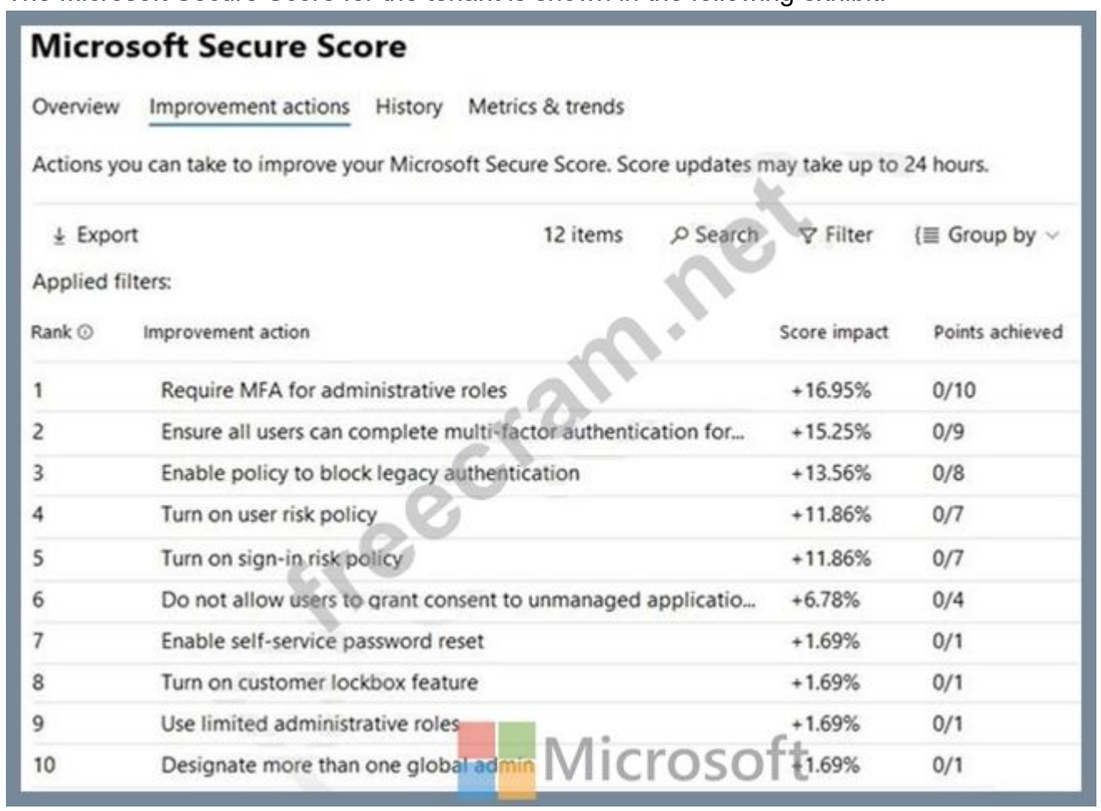
NEW QUESTION: 82
You have a Microsoft 365 E5 subscription.
You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.
Which conditions can you use in the DLP rules of the policy?
A. sensitive info types
B. content search queries
C. keywords
D. sensitivity labels
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: 83
You have a Microsoft 365 E5 subscription.
You plan to ingest syslog data from a supported firewall device to Microsoft Defender for Cloud Apps.
You need to configure automatic log upload.
Which two components should you configure for the log collector? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. the receiver type
B. the host IP address or FQDN
C. a connection string
D. the data source
E. the username and password

Answer: (SHOW ANSWER)

NEW QUESTION: 84
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
A Built-in protection preset security policy is applied to the subscription.
Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. Anti-phishing
B. Anti-spam
C. Safe Links
D. Anti-malware
E. Safe Attachments
Answer: (SHOW ANSWER)

NEW QUESTION: 85
You have a Microsoft 365 E5 tenant.
The Microsoft Secure Score for the tenant is shown in the following exhibit.



You plan to enable Security defaults for Azure Active Directory (Azure AD).
Which three improvement actions will this affect?
A. Require MFA for administrative roles.
B. Ensure all users can complete multi-factor authentication for secure access

C. Enable policy to block legacy authentication
D. Enable self-service password reset
E. Use limited administrative roles
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

NEW QUESTION: 86
You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps. You need to create a file policy named Policy1 that meets the following requirements:
* Inspects files in connected software as a service (SaaS) apps
* Inspects protected files
Which two settings should you configure? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Answer Area

Admin quarantine

Microsoft Information Protection

Azure security

Files

Conditional Access App Control

General Settings

User monitoring

Device identification

App onboarding/maintenance

Edge for Business protection

App governance

Service status

Explanation:

Answer Area

NEW QUESTION: 87

You have a Microsoft 365 subscription that contains the alerts shown in the following table.

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

Which properties of the alerts can you modify?

A. Status only

B. Status and Comment only

C. Status and Severity only

D. Status, Severity, and Comment only

E. Status, Severity, Comment and Category

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365-worldwide#limitations

NEW QUESTION: 88
You have a Microsoft 365 E5 subscription.
You create a user named Admin1.
You need to ensure that Admin1 can view Endpoint security policies from the Microsoft Defender portal. The solution must follow the principle of least privilege.
Which Microsoft Entra role should you assign to Admin1?
A. Security Operator
B. Cloud Device Administrator
C. Security Reader
D. Security Administrator
E. Global Reader
Answer: (SHOW ANSWER)

NEW QUESTION: 89
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

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

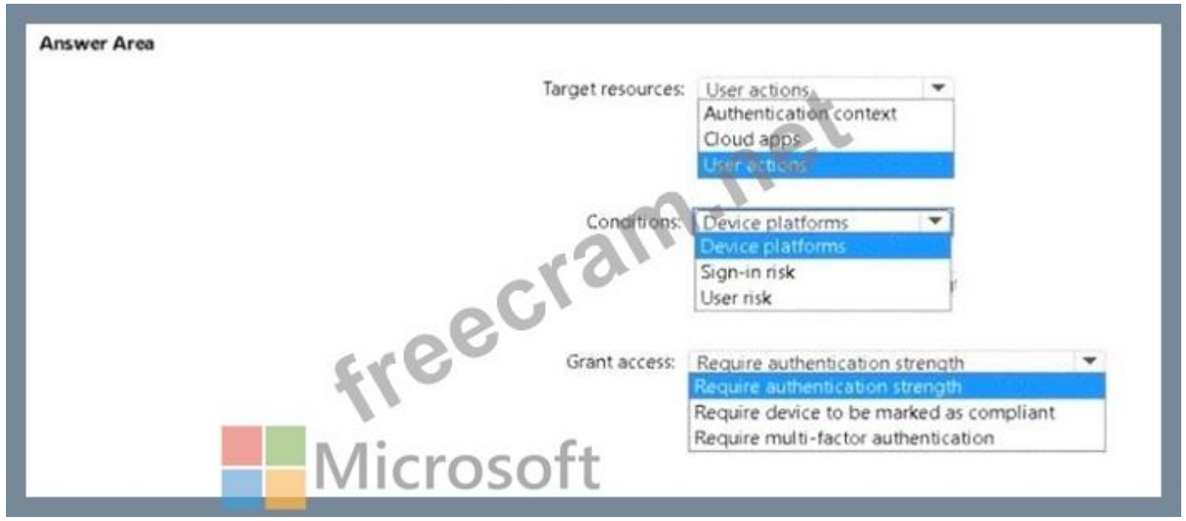
You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?
A. Device 1, Device2, and Device3 only
B. Device3 only
C. Device2 and Device3 only
D. Device1, Device2, Devices and Device4
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements

NEW QUESTION: 90
You need to protect the U.S. PII data to meet the technical requirements.
What should you create?

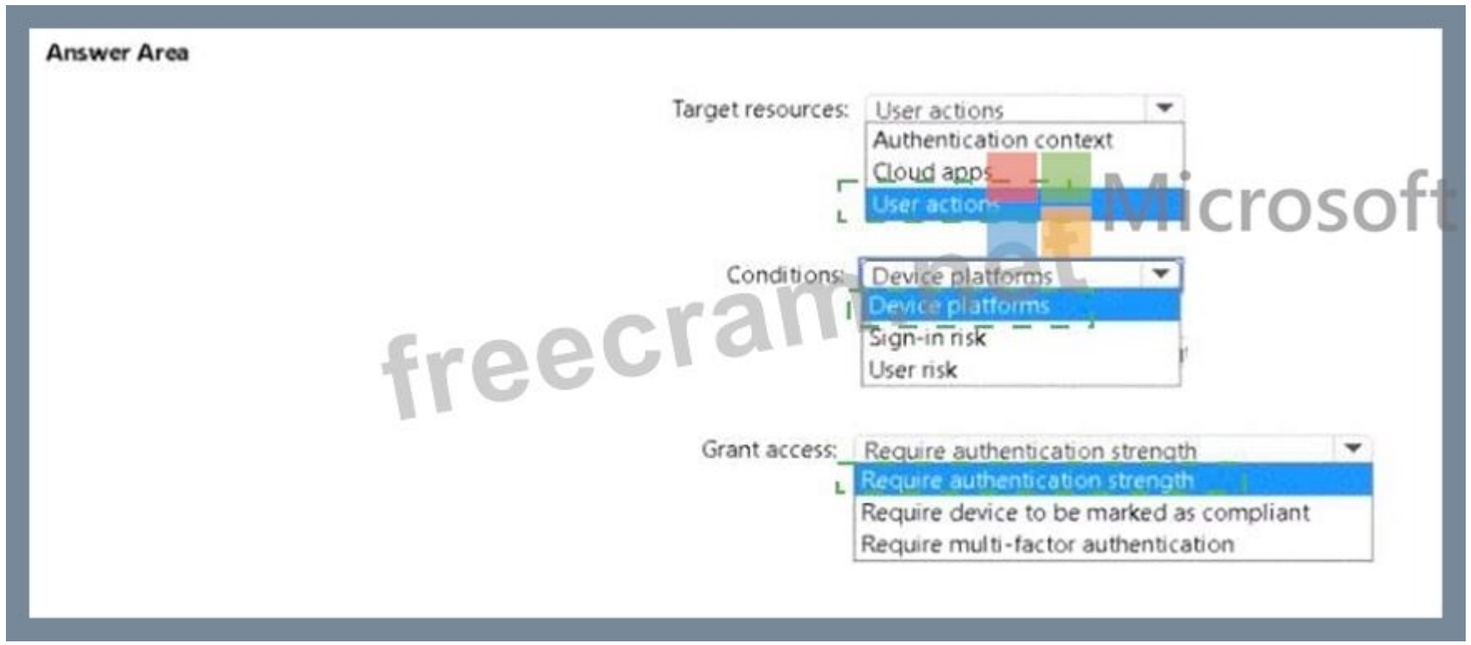
A. a Security & Compliance alert policy that contains an activity
B. a data loss prevention (DLP) policy that contains a domain exception
C. a Security & Compliance retention policy that detects content containing sensitive data
D. a data loss prevention (DLP) policy that contains a user override
Answer: (SHOW ANSWER)

NEW QUESTION: 91
You have a Microsoft 365 E5 subscription.
You need to create a Conditional Access policy that will require the use of FID02 security keys only when users join their Windows devices to Microsoft Entra ID.
How should you configure the policy? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.



Answer:



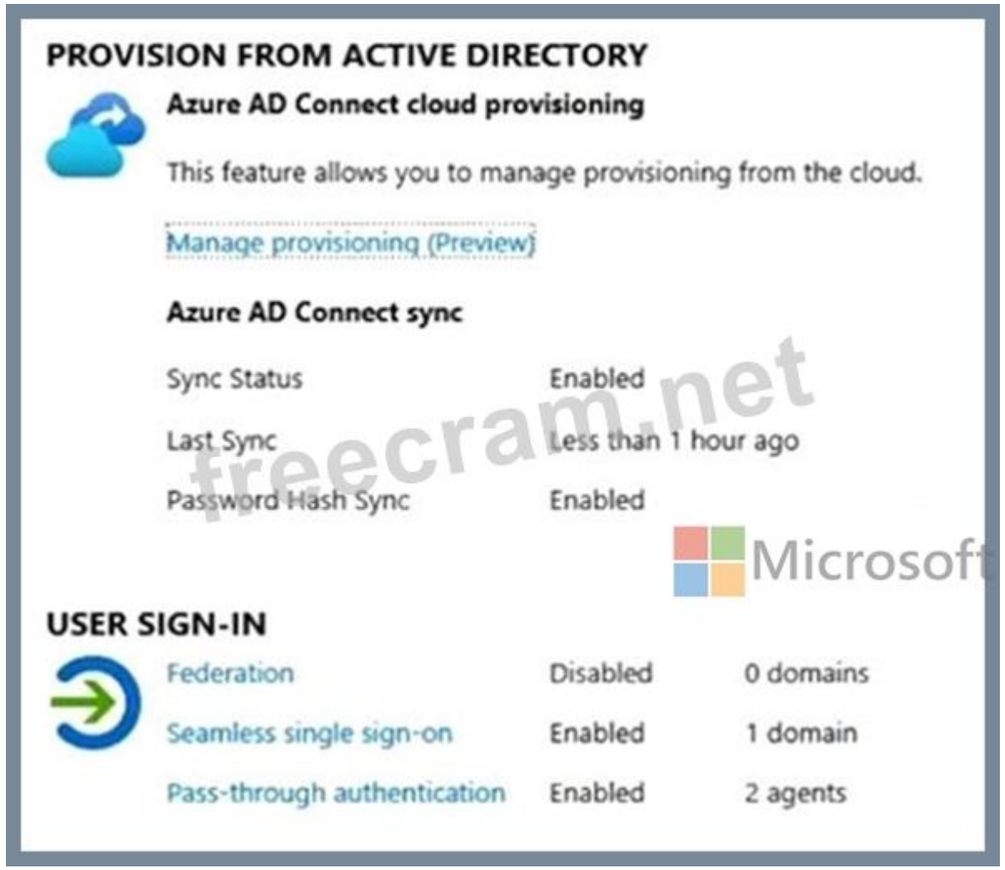
Explanation:

NEW QUESTION: 92
You have a Microsoft 365 subscription.
You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.
What is the maximum number of onmicrosoft.com domains the subscription can contain?
A. 1
B. 2
C. 5
D. 10
Answer: C (LEAVE A REPLY)
You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to create a new one.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq

NEW QUESTION: 93
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet the goal?
A. Yes
B. No
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: 94
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

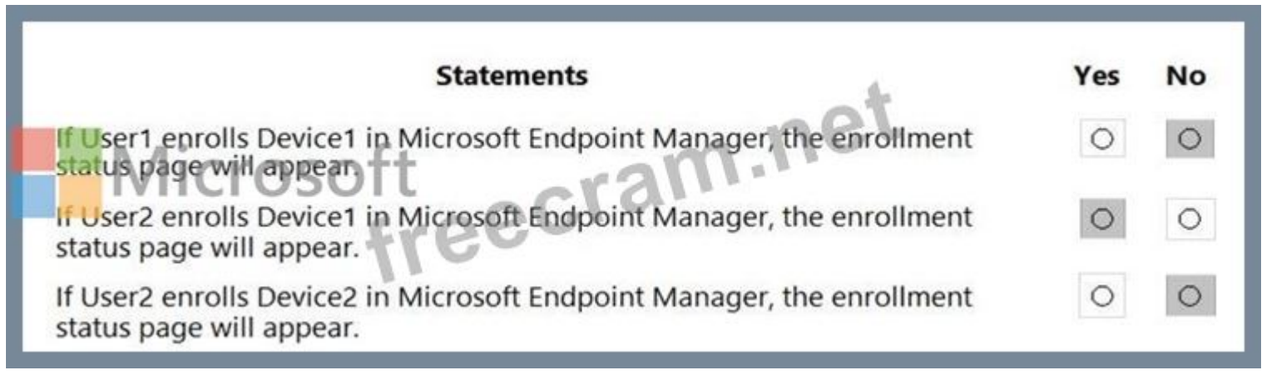
In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:
Show app and profile configuration progress: Yes
Allow users to collect logs about installation errors: Yes
Only show page to devices provisioned by out-of-box experience (OOBE): No Assignments: Group2 For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:



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

NEW QUESTION: 95
You have a Microsoft 365 E5 subscription that contains a group named Group1. The subscription uses Microsoft Defender for Cloud Apps.
You configure cloud discovery.
You need to ensure that you can create a custom report that details shadow IT usage by the members of Group1.
What should you do first?
A. Configure user enrichment.
B. Disable anonymization.
C. Add an app connector.
D. Configure user monitoring.
Answer: (SHOW ANSWER)

NEW QUESTION: 96
You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.
During testing, you discover that a user can share credit card information with external users by using email.
However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint.
You need to prevent the user from sharing the credit card information by using email and SharePoint.
What should you configure?
A. the user overrides of the DLP policy rule
B. the conditions of the DLP policy rule
C. the status of the DLP policy
D. the locations of the DLP policy
Answer: (SHOW ANSWER)

NEW QUESTION: 97
You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps.
You configure a session control policy to block downloads from SharePoint Online sites.
Users report that they can still download files from SharePoint Online sites.
You need to ensure that file download is blocked while still allowing users to browse SharePoint Online sites.
What should you configure?

A. an activity policy
B. a Conditional Access policy
C. an access policy
D. a data loss prevention (DLP) policy
Answer: (SHOW ANSWER)

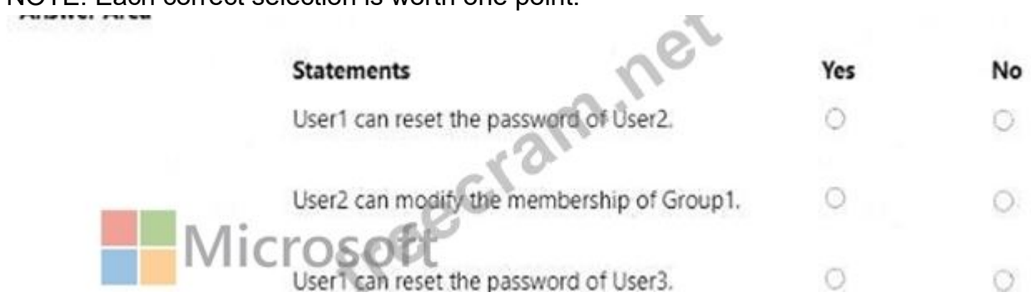
NEW QUESTION: 98
You have a Microsoft 365 subscription That contains two administrative units named AU1 and AU2.
The subscription contains the users shown in the following table.

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

The subscription contains the groups shown in the following table.

Name	Members	Administrative unit
Group1	User3	AU2
Group2	User2 User3	AU1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

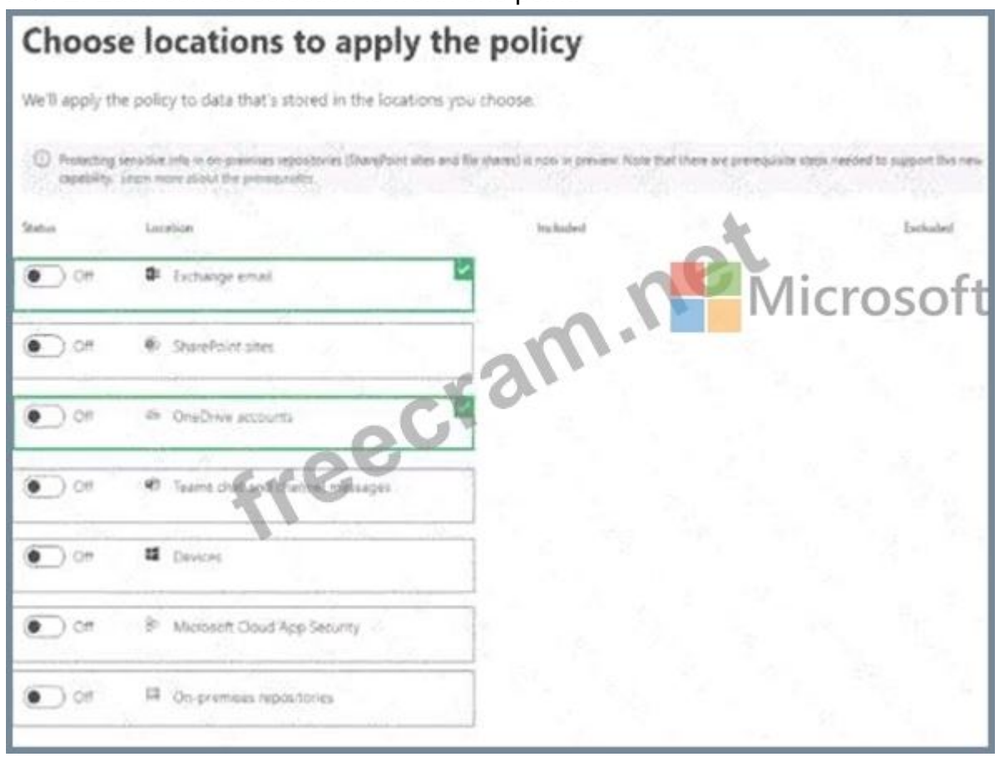
NEW QUESTION: 99
Your company has three main offices and one branch office. The branch office is used for research.
The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.
You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.
What should you include in the recommendation?
A. Azure AD password protection
B. a Microsoft Intune device compliance policy
C. a Microsoft Intune device configuration profile
D. Azure AD conditional access
Answer: (SHOW ANSWER)

NEW QUESTION: 100
You have a Microsoft 365 subscription.
You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.
Which type of group should you use to assign the Reports Reader role and to access App1?

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

https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?
https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy

NEW QUESTION: 101
You have a Microsoft 365 E5 tenant
You create a data toss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.
To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

NEW QUESTION: 102

You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.

Which authentication strategy should you implement for the pilot projects?

A. pass-through authentication

B. pass-through authentication and seamless SSO

C. password hash synchronization and seamless SSO

D. password hash synchronization

Answer: (SHOW ANSWER)

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

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

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

Fabrikam does NOT plan to implement identity federation.

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

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

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

Reference:

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

NEW QUESTION: 103

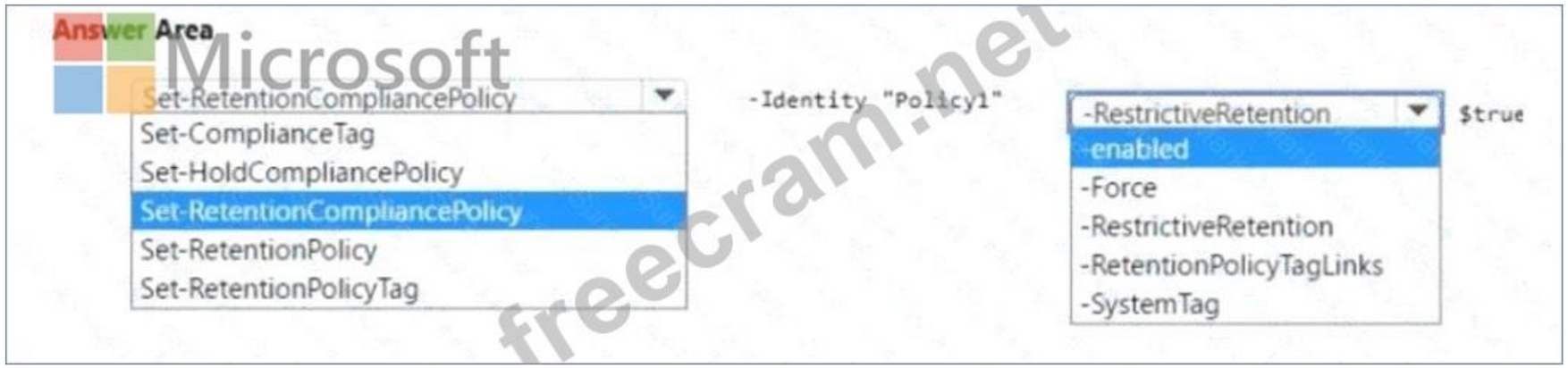
Your company has an Azure AD tenant named contoso.com that includes the users shown in the following table.

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

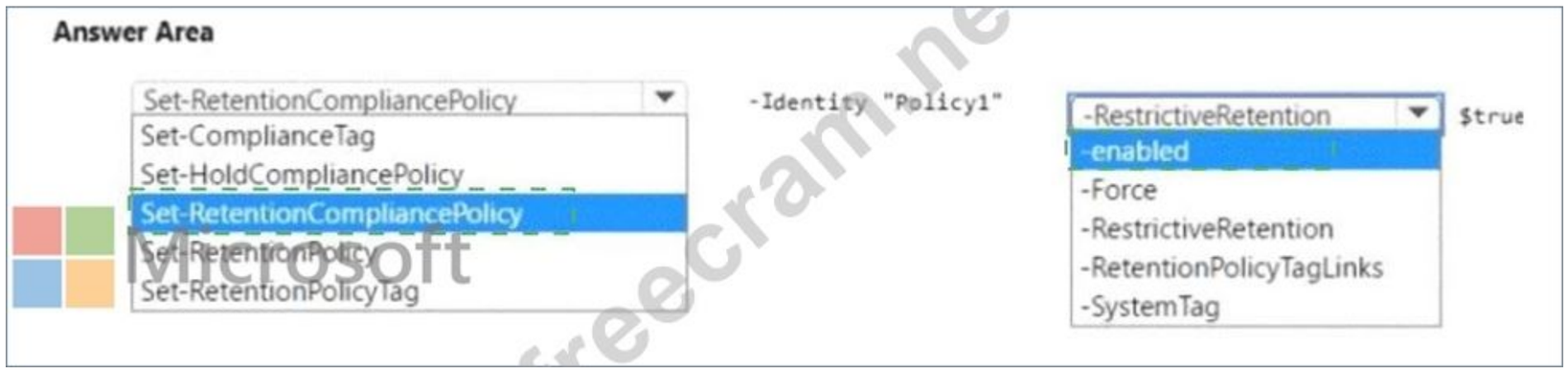
Group2isa member of Group1.
You assign an Office 365 Enterprise E3 license to Group1.
How many Office 365 E3 licenses are assigned?
A. 1
B. 3
C. 4
D. 2
Answer: (SHOW ANSWER)

NEW QUESTION: 104
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it as a result these questions will not appear in the review screen.
Your network contains an Active Directory forest.
You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
* Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
* User passwords must be 10 characters or more.
Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)

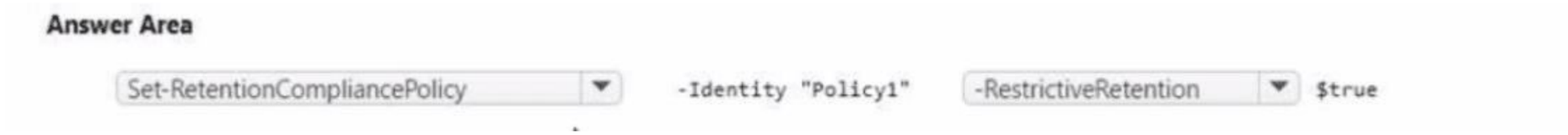
NEW QUESTION: 105
From the Microsoft Purview compliance portal, you create a retention policy named Policy 1.
You need to prevent all users from disabling the policy or reducing the retention period.
How should you configure the Azure PowerShell command? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 106

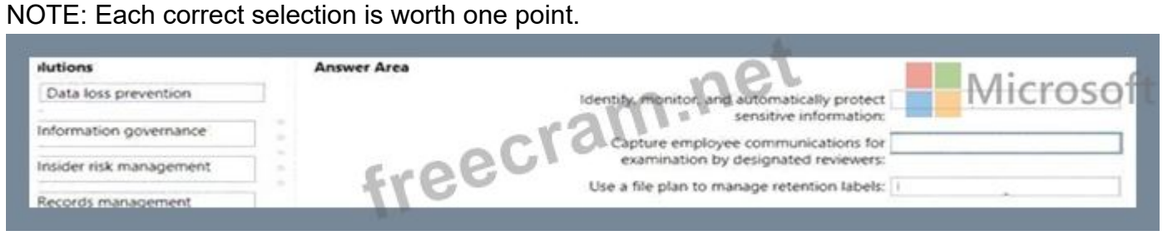
You have a Microsoft 365 E5 tenant.

You need to implement compliance solutions that meet the following requirements:

* Use a file plan to manage retention labels.
* Identify, monitor, and automatically protect sensitive information.
* Capture employee communications for examination by designated reviewers.

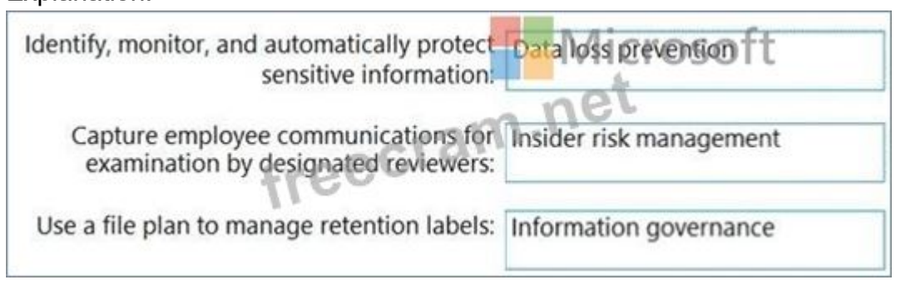
Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



NEW QUESTION: 107

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role.

Does this meet the goal?

A. Yes

B. No

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: 108

You have a Microsoft 365 E5 subscription that contains two sensitivity labels named Label1 and Label2. The subscription contains a Windows device named Device1 that is onboarded to Microsoft Purview. Device1 contains the files shown in the following table.

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

You create a data loss prevention (DLP) policy named Policy1 that has the following configurations:

Answer:

Explanation:

NEW QUESTION: 109

You have a Microsoft 365 E5 subscription.

You need to use Microsoft Defender for Cloud Apps to monitor user mailbox activities. What should you do?

A. Create an access policy.

B. Enable mailbox audit logging.

C. Create an activity policy.

D. Create an app connector for Microsoft 365.

Answer: (SHOW ANSWER)

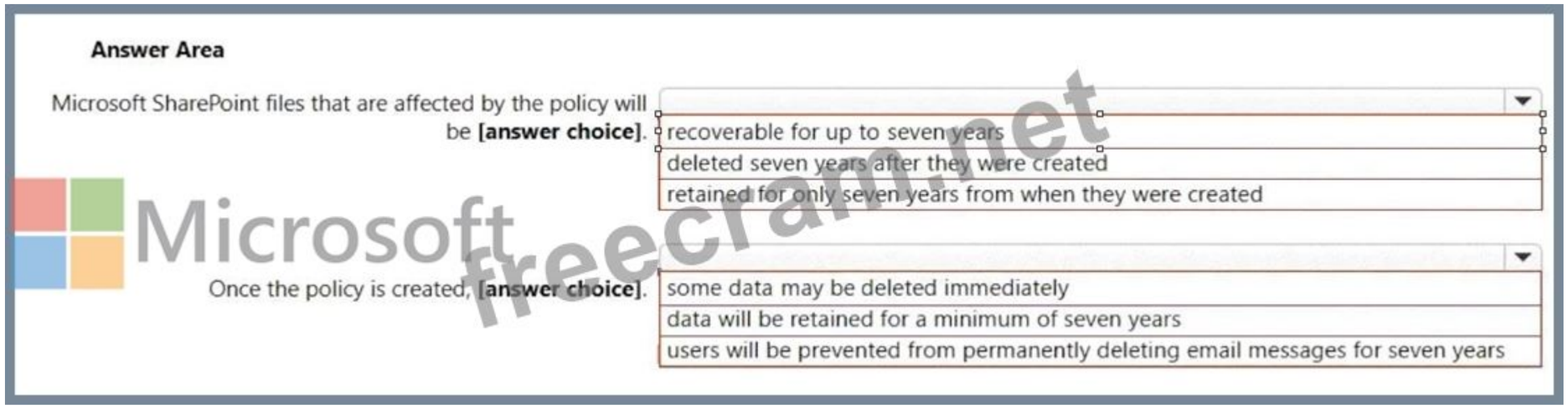
NEW QUESTION: 110

HOTSPOT

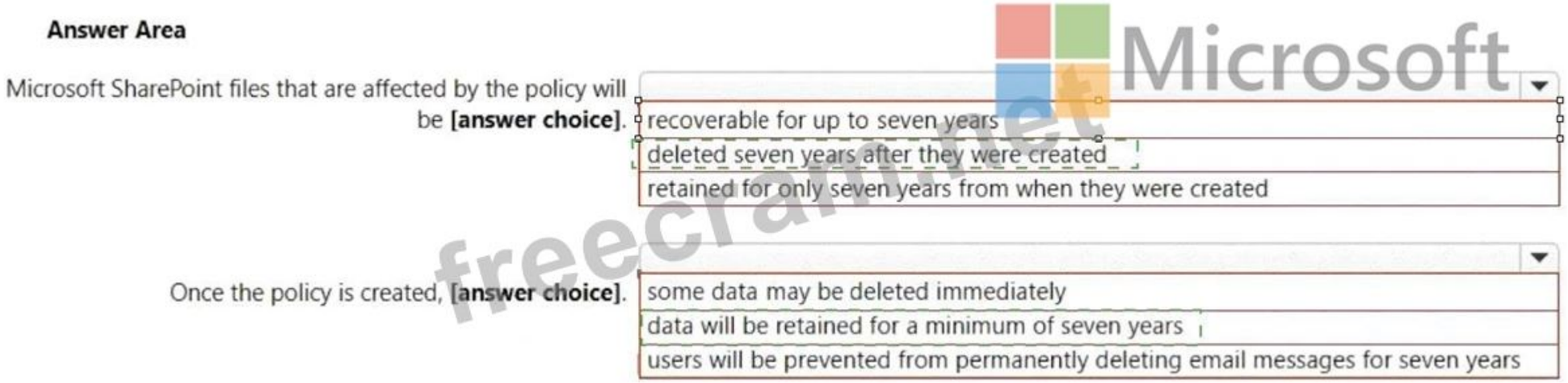
You have a Microsoft 365 tenant.

You plan to create a retention policy as shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

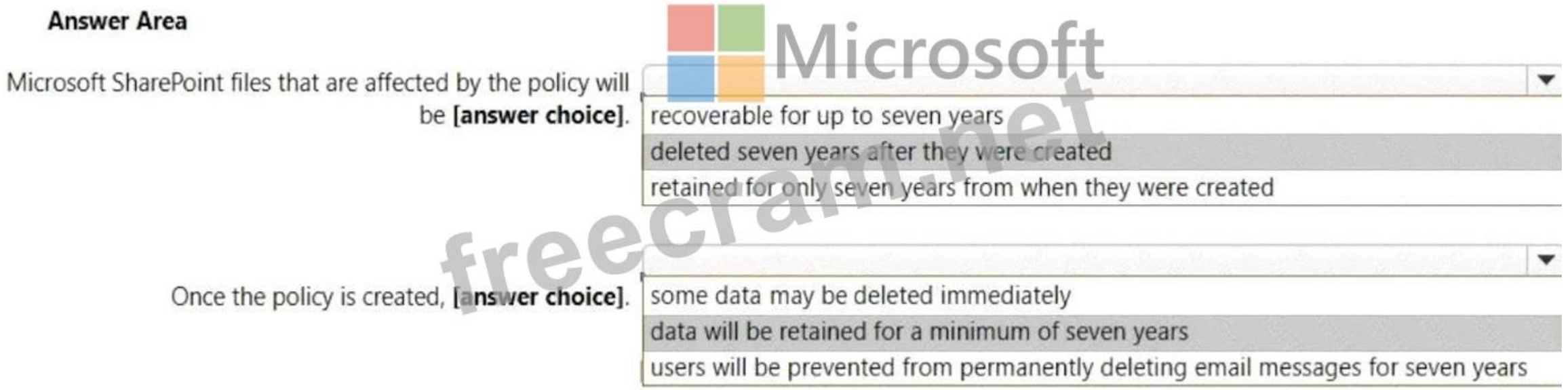


Answer:



Explanation:

Answer Area



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

NEW QUESTION: 111
You have a Microsoft 365 E5 subscription.
From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.
What is the longest time range that can be included in the report?
A. 1 day
B. 7 days
C. 30 days
D. 90 days
Answer: (SHOW ANSWER)
View email security reports in the Microsoft 365 Defender portal
The aggregate view shows data for the last 90 days and the detail view shows data for the last 30 days Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email-security

NEW QUESTION: 112
You have a Microsoft 365 E5 tenant that contains a user named User1.
You plan to implement insider risk management.
You need to ensure that User1 can perform the following tasks:
Review alerts.
Manage cases.
Create notice templates.
Review user emails by using Content explorer.
The solution must use the principle of least privilege.
To which role group should you add User1?
A. Insider Risk Management
B. Insider Risk Management Analysts
C. Insider Risk Management Investigators
D. Insider Risk Management Admin
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide

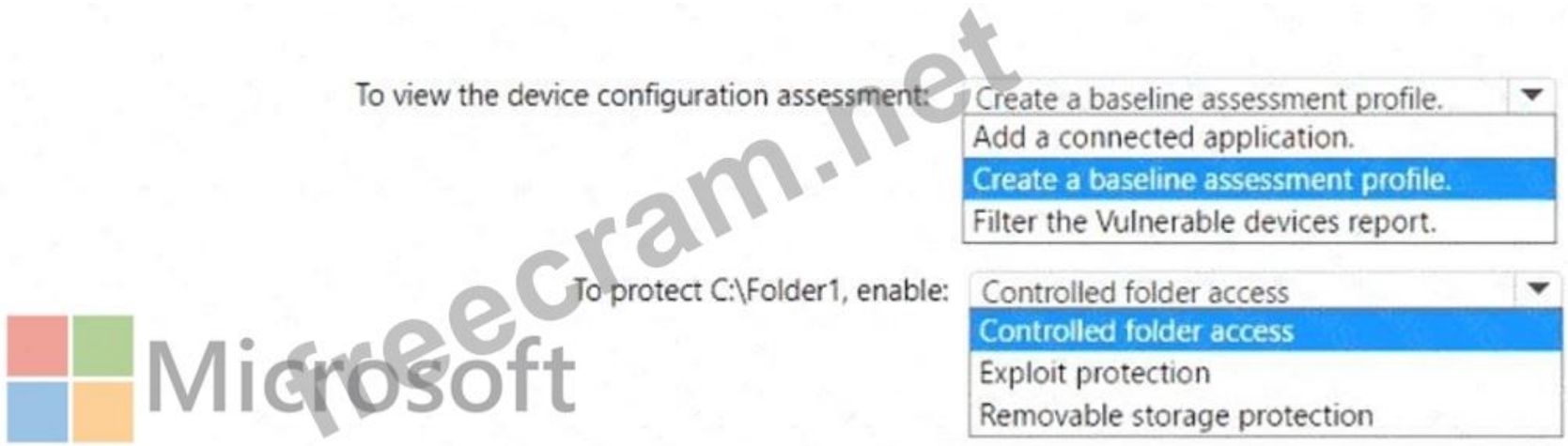
NEW QUESTION: 113
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature.
You need to block users from downloading a file named File1.exe.
What should you use?
A. an indicator
B. a suppression rule
C. a device configuration profile
Answer: (SHOW ANSWER)

NEW QUESTION: 114
You have a Microsoft 365 subscription.
You add a domain named contoso.com.
When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.
com.
You need to change the email address used to verify the domain.
What should you do?
A. Add a TXT record to the DNS zone of the domain.
B. Modify the NS records for the domain.
C. From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription.
D. From the domain registrar, modify the contact information of the domain.
Answer: (SHOW ANSWER)

NEW QUESTION: 115
You have a Microsoft 365 E5 tenant.
You plan to deploy 1.000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.
You need to recommend a Microsoft Intune enrollment option that meets the following requirements:
* Minimizes user interaction
* Minimizes administrative effort
* Automatically installs corporate apps
What should you recommend?
A. Automated Device Enrollment (ADE)
B. bring your own device (BYOD) user and device enrollment
C. Apple Configurator enrollment
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll

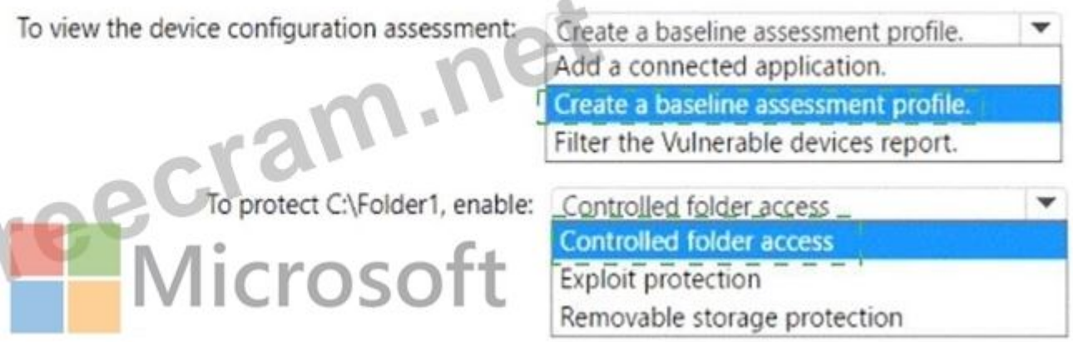
NEW QUESTION: 116
You have a Microsoft 365 E5 subscription.
All corporate Windows 11 devices are managed by using Microsoft Intune and onboarded to Microsoft Defender for Endpoint.
You need to meet the following requirements:
* View an assessment of the device configurations against the Center for Internet Security (CIS) vl.0.0 benchmark.
* Protect a folder named C:\Folder1 from being accessed by untrusted applications on the devices.
What should you do? To answer, select the appropriate options in the answer area.

Answer Area



Answer:

Answer Area



Explanation:

Answer Area

NEW QUESTION: 117

You have a Microsoft 365 is subscription that includes Microsoft Intune.

You manage all iOS devices by using Intune.

You plan to protect corporate-owned iOS devices by using Microsoft Defender for Endpoint. You configure a connection between Intune and Defender for Endpoint.

You need to onboard the devices to Defender for Endpoint.

What should you do?

A. Enable Microsoft Defender for Cloud.

B. Add an app to Intune.

C. Download an onboarding package.

D. Create an app protection policy.

Answer: (SHOW ANSWER)

NEW QUESTION: 118

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.

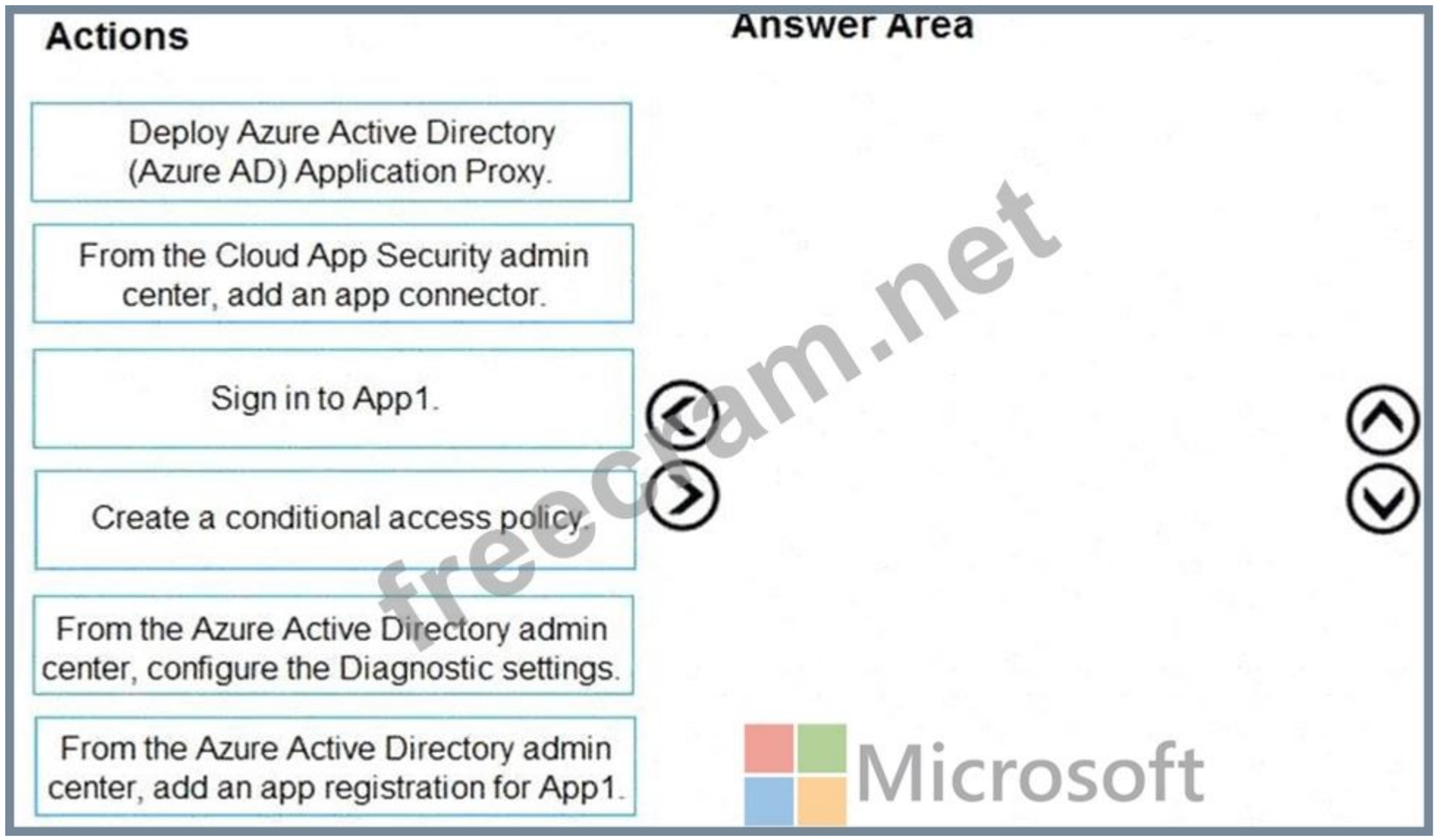
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Security administrator role.

Does this meet the goal?

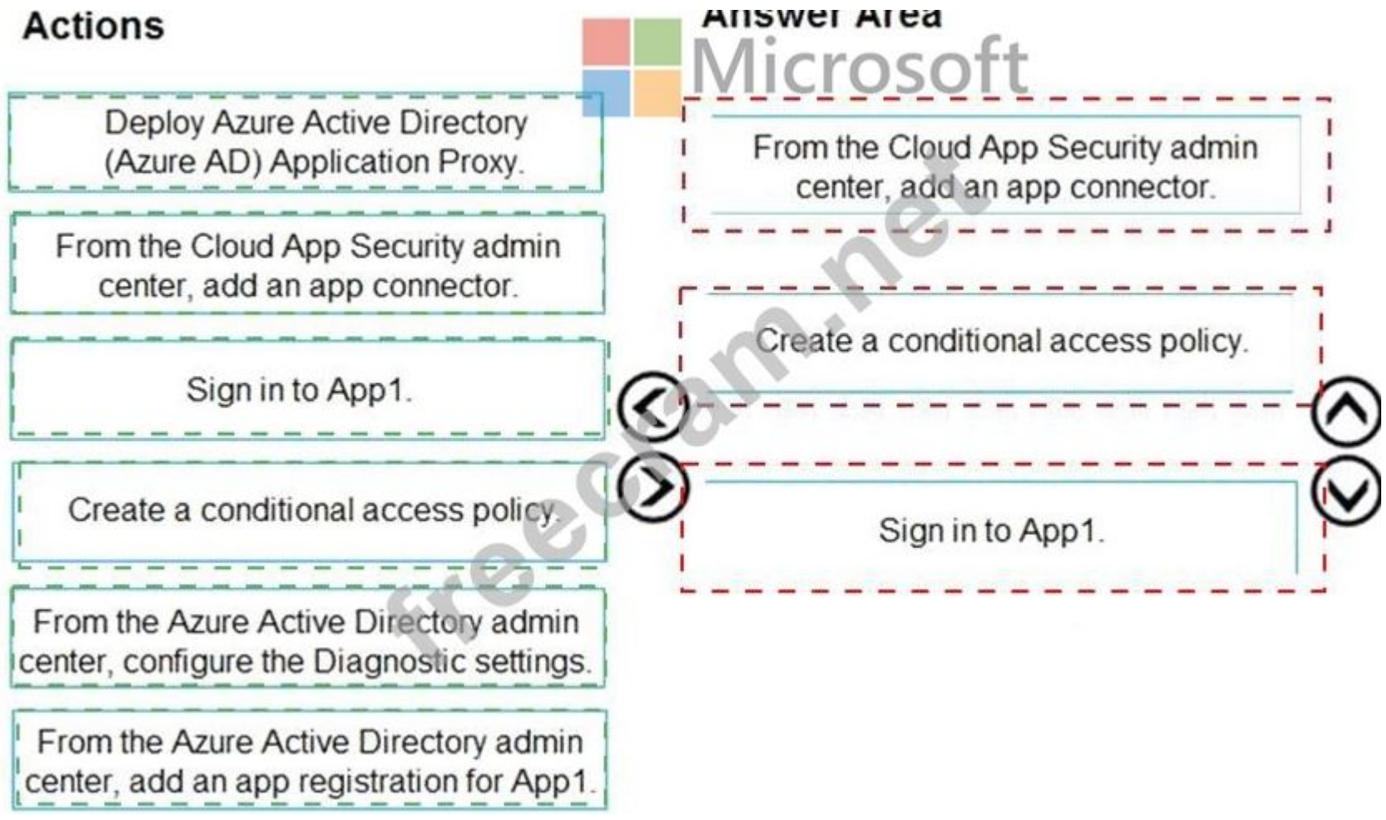
A. Yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 119
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365 and contains a mailbox named Mailbox1.
You plan to use Mailbox1 to collect and analyze unfiltered email messages.
You need to ensure that Defender for Office 365 takes no action on any inbound emails delivered to Mailbox1.
What should you do?
A. Create a mail flow rule.
B. Configure Mailbox! as a SecOps mailbox.
C. Configure a retention policy for Mailbox1.
D. Place a litigation hold on Mailbox1.
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Your company purchases a cloud app named App1.
You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:

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

NEW QUESTION: 121
You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.

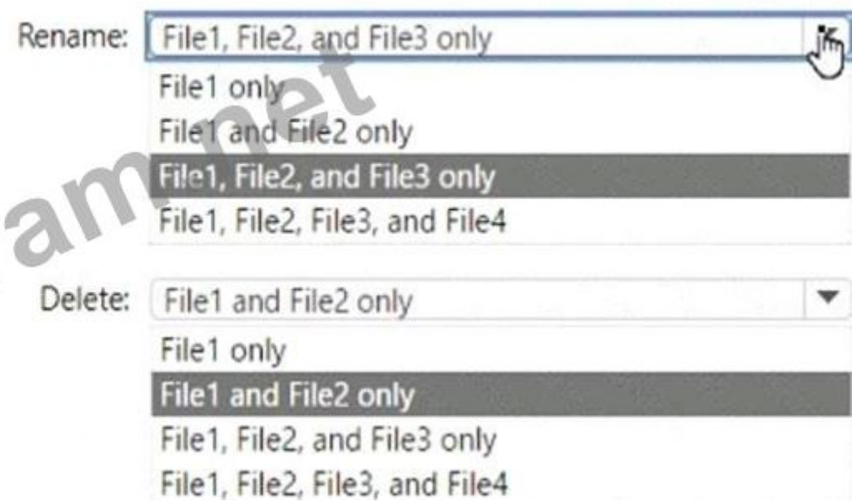
Name	Retention period	During the retention period
Retention1	5 years	Retain items even if users delete
Retention2	5 years	Mark items as a record
Retention3	5 years	Mark items as a regulatory record

Site1 contains the files shown in the following table.

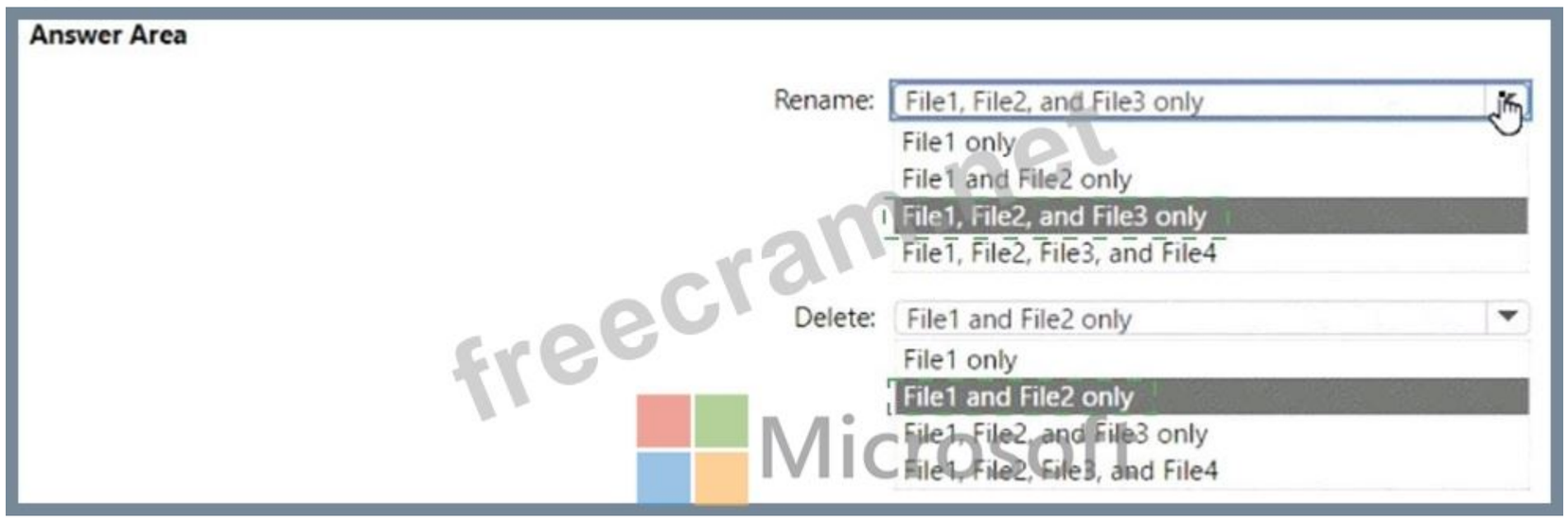
Name	Label
File1	*None*
File2	Retention1
File3	Retention2
File4	Retention3

Which files can User1 rename, and which files can User1 delete? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Answer Area

Rename: File1, File2, and File3 only

Delete: File1 and File2 only

NEW QUESTION: 122

You have a Microsoft 365 subscription that contains the users shown in the following table.

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

You create a new administrative unit named AU1 and configure the following AU1 dynamic membership rule.

The subscription contains the role assignments shown in the following table.

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.	○	○

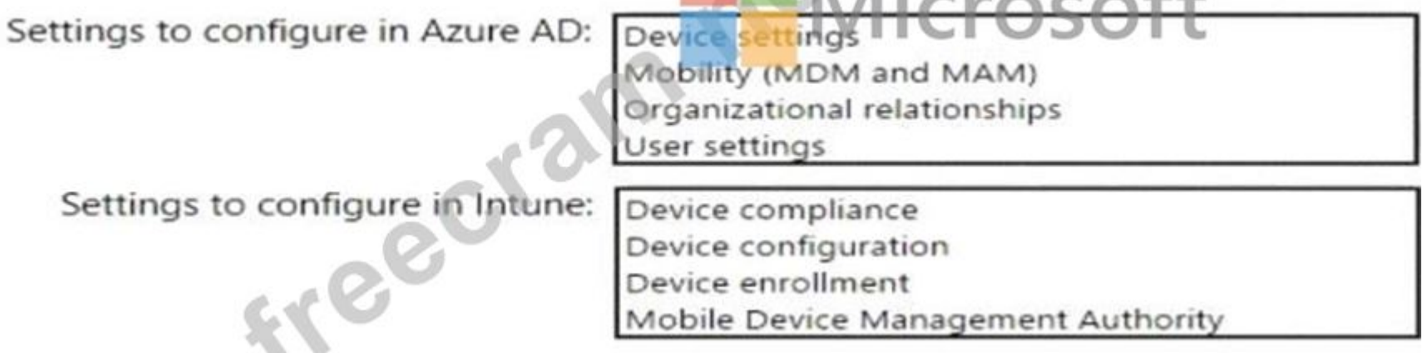
Answer:

Answer Area

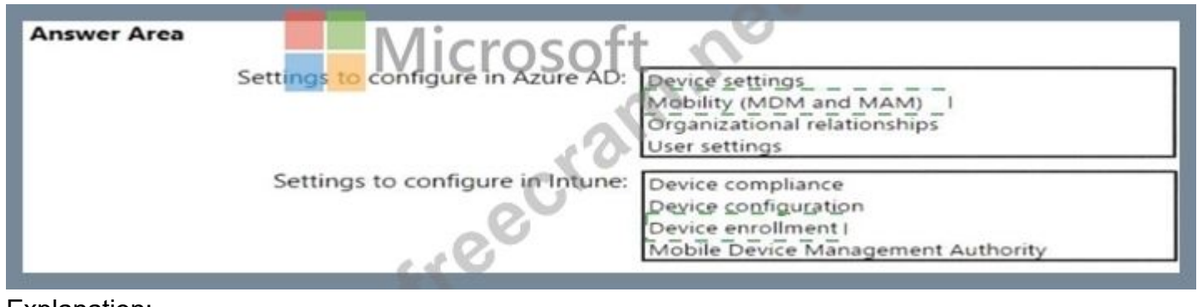
Explanation:
Admin1 can reset the password of User1: Yes
Admin1 has the User Administrator role within AU1. User1 is a member of Group1, which is included in AU1's dynamic membership rule.
Admin1 can reset the password of User2: No
User2 is a member of both Group1 and Group2. However, User2's job title 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: 123
You need to meet the technical requirements and planned changes for Intune.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Explanation:

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

NEW QUESTION: 124
You have a Microsoft 365 E5 subscription and use Microsoft Purview. The subscription contains the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	macOS
Device3	Android
Device4	Linux

All the devices are onboarded to Microsoft Defender for Endpoint. You plan to deploy Endpoint data loss prevention (Endpoint DLP) policies. Which devices can be protected by using the DLP policies?
A. Device1, Device2, Device3, and Device4
B. Device1 and Device2 only
C. Device1, Device2, and Device 3 only
D. Device1 only
E. Device1, Device3, and Device 4 only
Answer: (SHOW ANSWER)

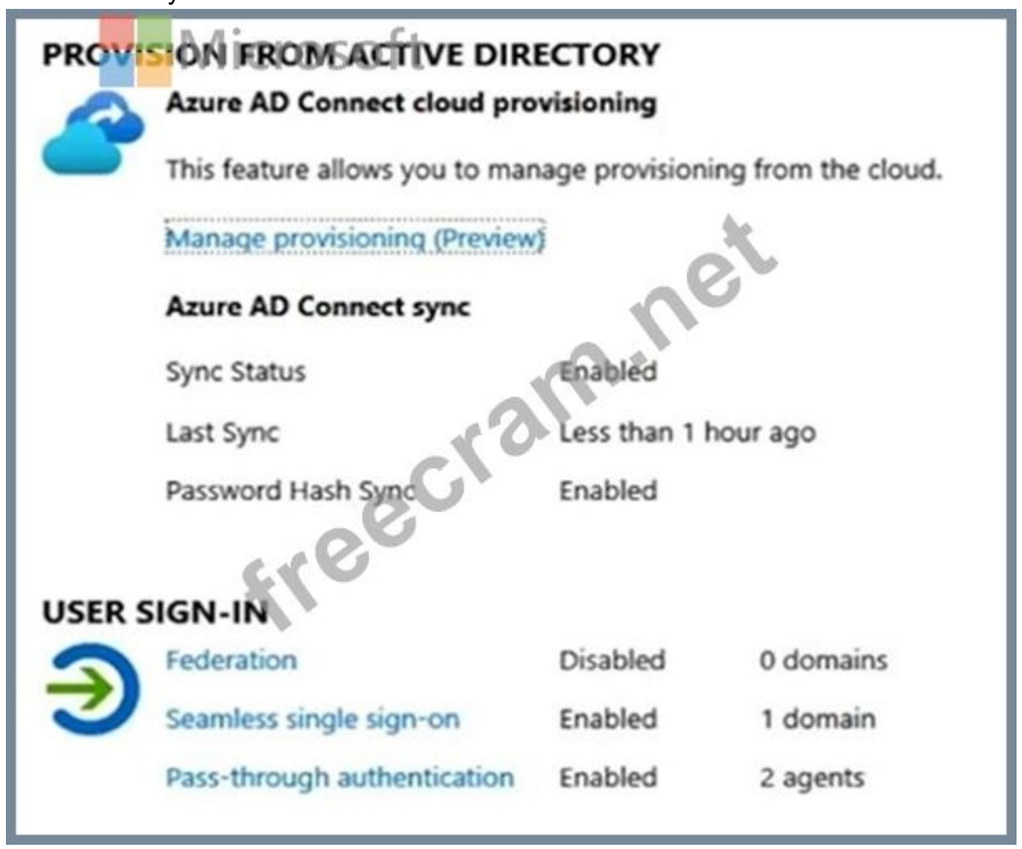
NEW QUESTION: 125
You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs.
What should you do?
A. From PowerShell, run the Add-ADSyncConnectorAttnbuteinclusion cmdlet.
B. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.
C. From PowerShell, run the start-ADSyncSyncCycle cmdlet.
D. From the Microsoft Azure AD Connect wizard, select Manage federation.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
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: 127

You need to recommend a solution for the security administrator. The solution must meet the technical requirements.
What should you include in the recommendation?
A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
B. Microsoft Azure Active Directory (Azure AD) Identity Protection
C. Microsoft Azure Active Directory (Azure AD) conditional access policies
D. Microsoft Azure Active Directory (Azure AD) authentication methods
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
Topic 2, 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 Azure Active Directory (Azure AD) 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 Azure Advanced 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 Azure AD, 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: 128
You have a new Microsoft 365 E5 tenant.
You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.
What should you do first?
A. Enable auditing.
B. Enable Microsoft 365 usage analytics.
C. Create an Insider risk management policy.
D. Create a communication compliance policy.
Answer: (SHOW ANSWER)
Microsoft Purview auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization.
This capability provides visibility into the activities performed across your Microsoft 365 organization.
Note: Permissions alert policies
Example: Elevation of Exchange admin privilege
Generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in Exchange Online.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview
https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies

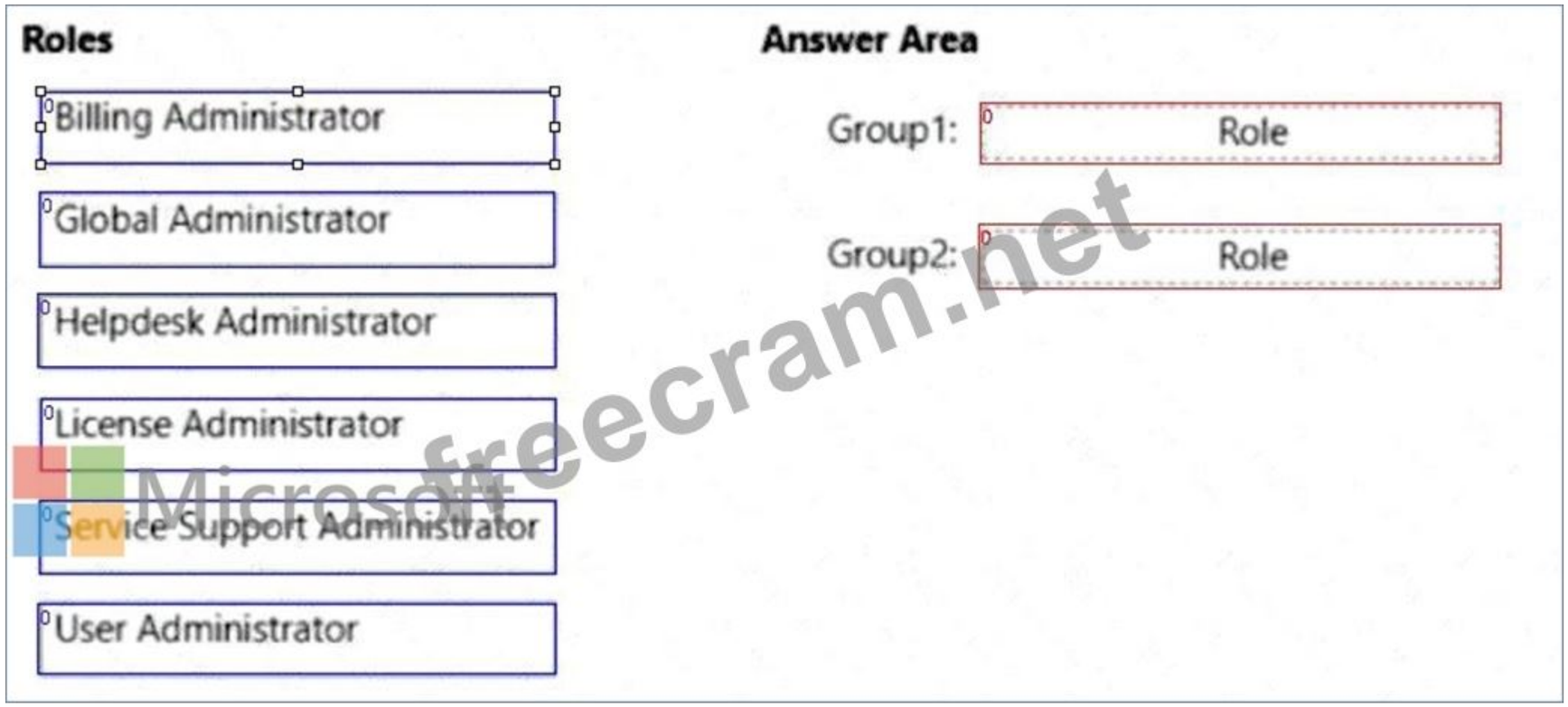
NEW QUESTION: 129
You have a Microsoft 365 E5 subscription that is linked to a Microsoft Entra tenant named contoso.com.
You purchase 100 Microsoft 365 Business Voice add-on licenses.
You need to ensure that the members of a group named Voice are assigned a Microsoft 365 Business Voice add-on license automatically.
What should you do?
A. From the Microsoft 365 admin center, modify the settings of the Voice group.
B. From the Licenses page of the Microsoft 365 admin center, assign the licenses.

C. From the Microsoft Entra admin center, modify the settings of the Voice group.
Answer: (SHOW ANSWER)

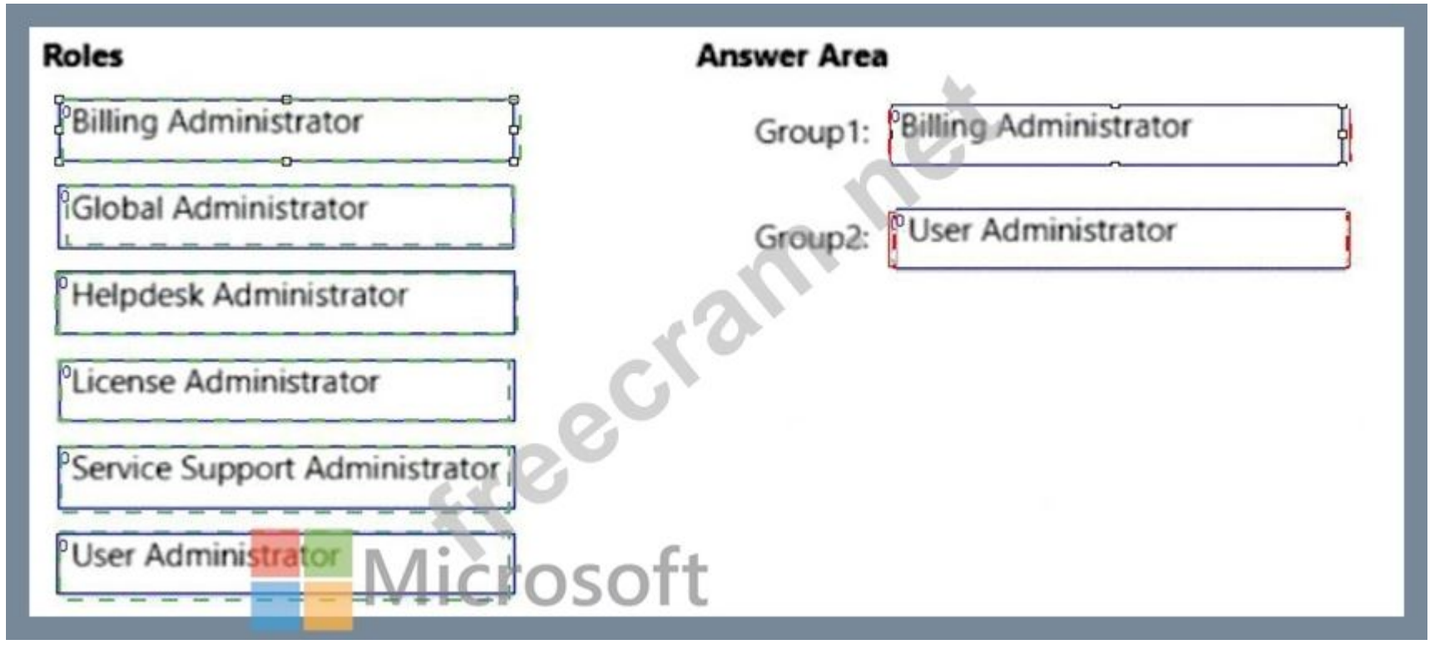
NEW QUESTION: 130
DRAG DROP
You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.
You need to ensure that each group can perform the tasks shown in the following table.

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.

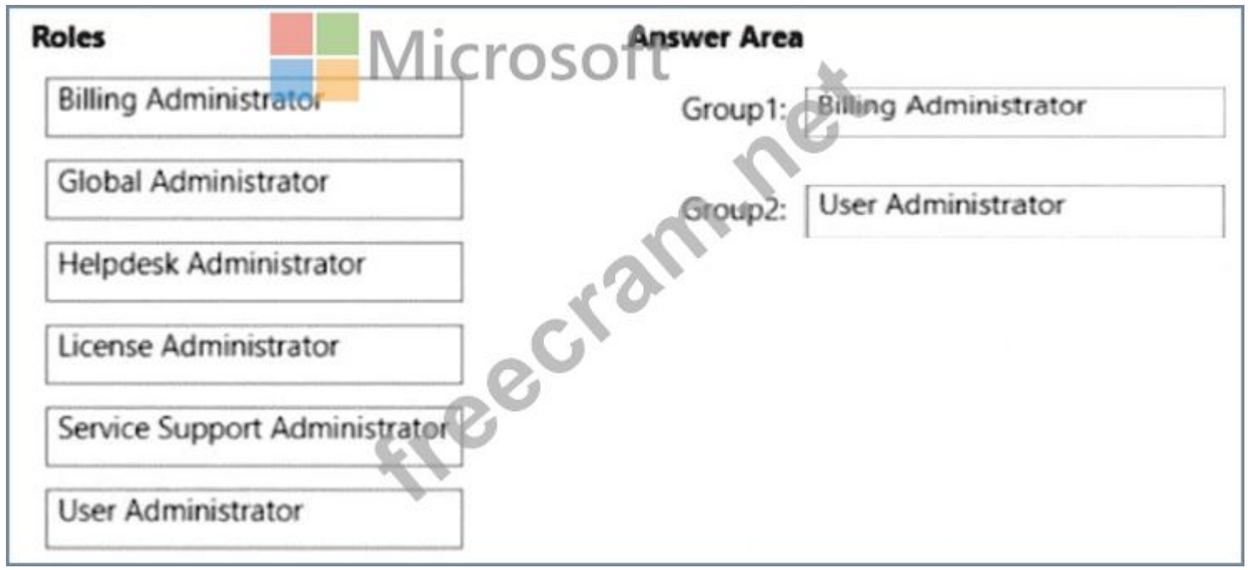
The solution must use the principle of least privilege.
Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



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: 131

You have a Microsoft 365 E5 subscription that contains two users named user1@contoso.com and user2@contoso.com and a Microsoft SharePoint site named Site1.

You create a data loss prevention {DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	User notifications	Priority
Rule1	4 or more IP addresses	User1@contoso.com	0
Rule2	2 or more IP addresses	User1@contoso.com	1
Rule3	3 or more IP addresses	User2@contoso.com	2

DLP1 is applied to Site1.

You have the files shown in the following table.

Name	Number of IP addresses in the file
File1.xlsx	2
File2.doc	3
File3.pptx	4
File4.txt	6

You copy the files to Site1.

low many notifications will each user receive? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:
User1@contoso.com: 2 notifications
User2@contoso.com: 1 notification
User1@contoso.com: 2 notifications
File3.pptx contains 4 IP addresses, which matches Rule1 (4 or more IP addresses), triggering a notification to User1.
File4.txt contains 6 IP addresses, which also matches Rule1, triggering another notification to User1.
Therefore, User1 receives 2 notifications.
User2@contoso.com: 1 notification
File2.doc contains 3 IP addresses, which matches Rule3 (3 or more IP addresses), triggering a notification to User2. Therefore, User2 receives 1 notification.

NEW QUESTION: 132
You have a Microsoft 365 subscription.
You discover that some external users accessed center for a Microsoft SharePoint site.
You modify the sharePoint sharing policy to prevent sharing, outside your organization.
You need to be notified if the SharePoint sharing policy is modified in the future.
Solution: From the Security $ Compliance admin center you create a threat management policy.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 133
You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.
From Microsoft Defender Security Center, you perform a security investigation.

You need to run a PowerShell script on the device to collect forensic information.
Which action should you select on the device page?
A. Initiate Live Response Session
B. Initiate Automated Investigation
C. Collect investigation package
D. Go hunt
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

NEW QUESTION: 134
You have a Microsoft 365 E5 subscription and an Azure AD tenant named contoso.com.
All users have computers that run Windows 11, are joined to contoso.com, and are protected by using BitLocker Drive Encryption (BitLocker).
You plan to create a user named Admin1 that will perform following tasks:
* View BitLocker recovery keys.
* Configure the usage location for the users in contoso.com.
You need to assign roles to Admin1 to meet the requirements. The solution must use the principle of least privilege. Which two roles should you assign? To answer, select the appropriate roles in the answer area.
NOTE: Each correct selection is worth one point

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 ⓘ

Microsoft

Answer:

Answer Area

Devices

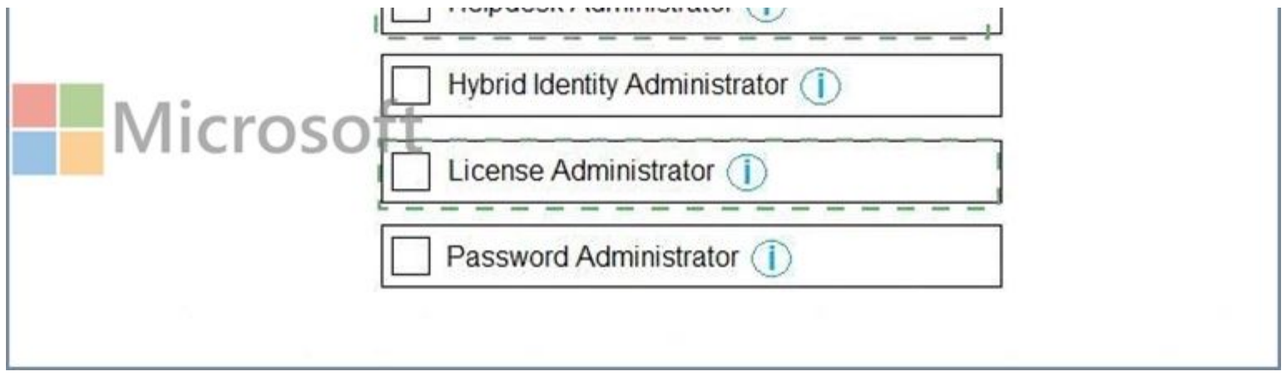
- [ ] Cloud Device Administrator
- [ ] Desktop Analytics Administrator
- [ ] Intune Administrator
- [ ] Printer Administrator
- [ ] Printer Technician
- [ ] Windows 365 Administrator

Global

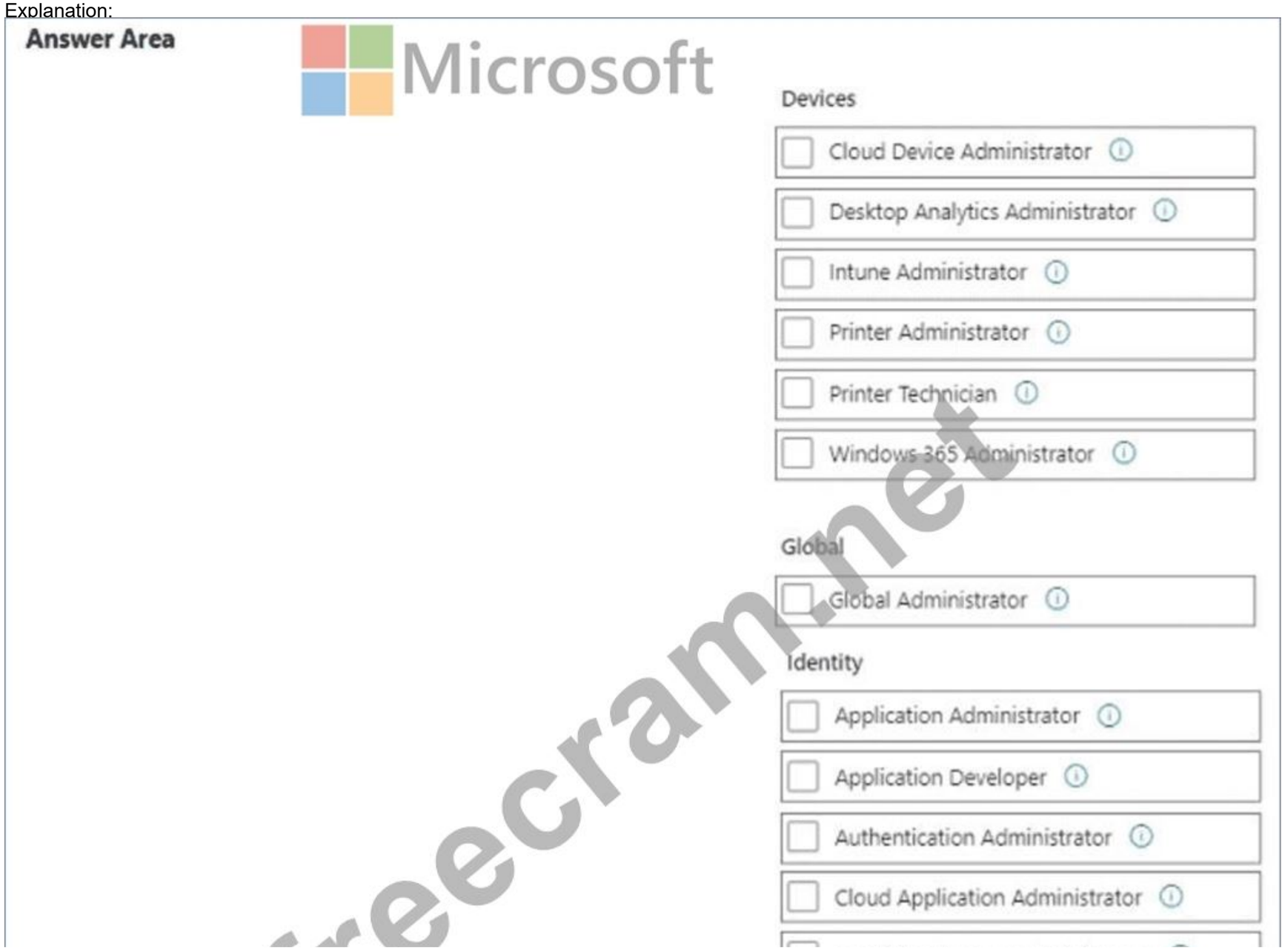
- [ ] Global Administrator

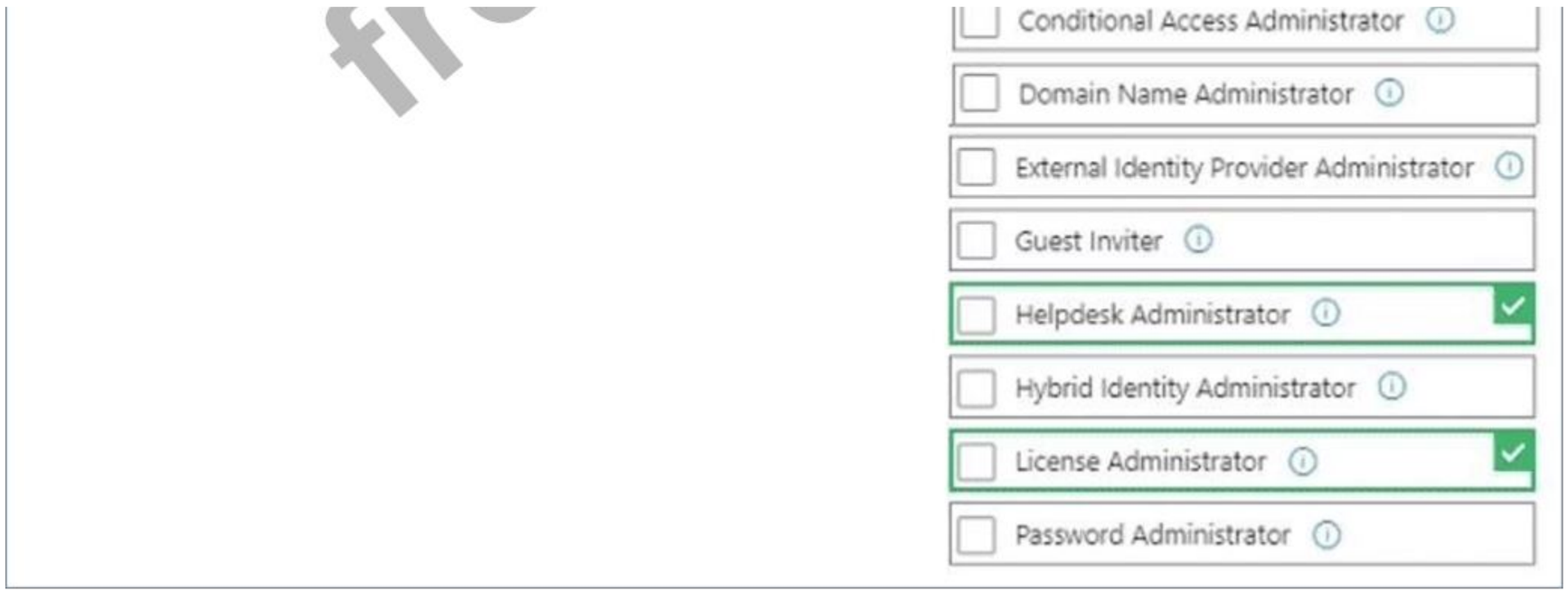
Identity

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



Explanation:

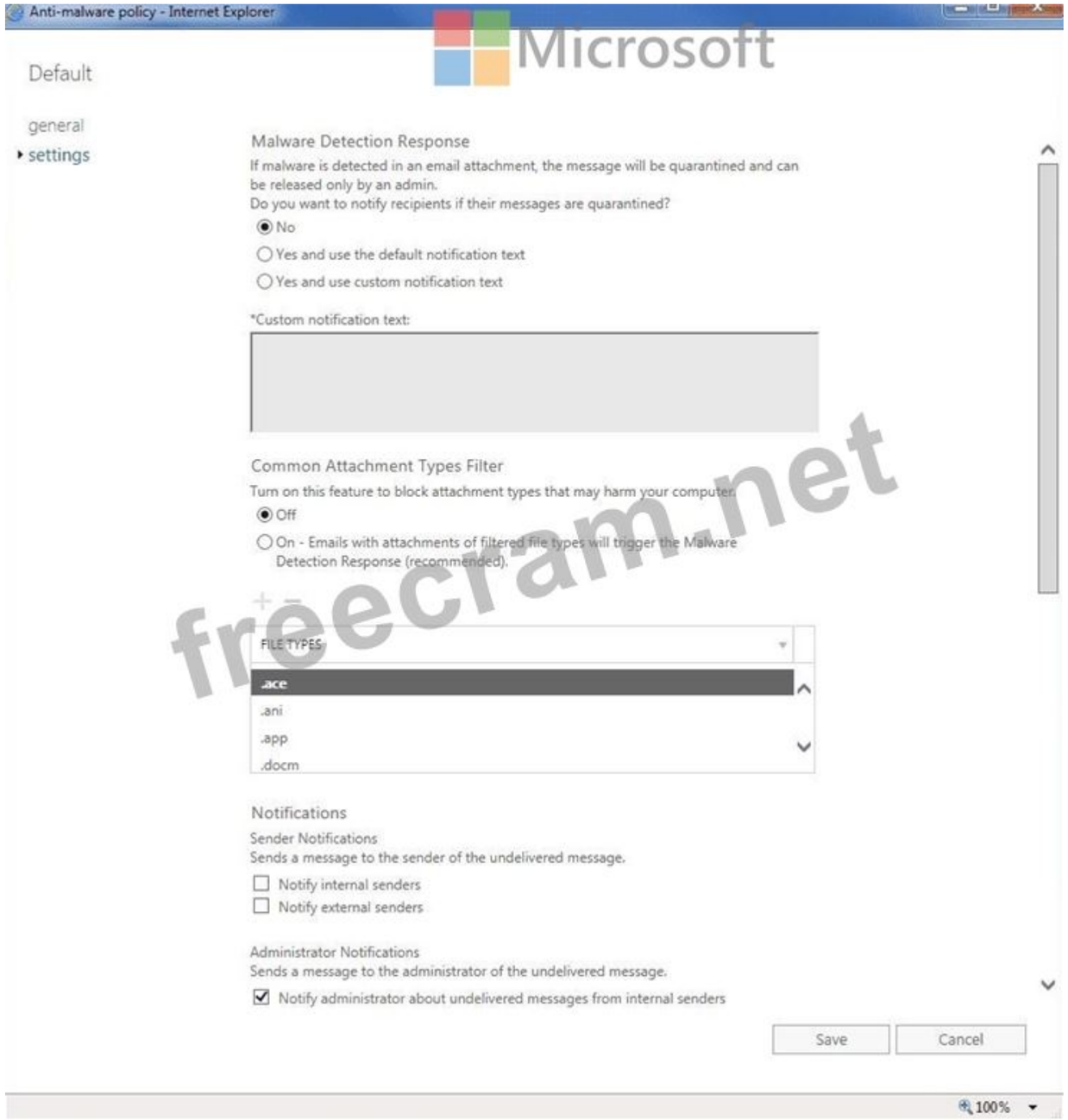




NEW QUESTION: 135

You have a Microsoft 365 E5 subscription that contains a user named User1.

The subscription has a single anti-malware policy as shown in the following exhibit.



An email message that contains text and two attachments is sent to User1. One attachment is infected with malware.

How will the email message and the attachments be processed?

A. Both attachments will be removed. The email message will be quarantined, and Used will receive an email message without any attachments and an email message that includes the following text:
'Malware was removed.'

B. The email message will be quarantined, and the message will remain undelivered.

C. Both attachments will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text:

'Malware was removed."

D. The malware-infected attachment will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies

NEW QUESTION: 136
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

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

Defender for Endpoint has the device groups shown in the following table.

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*

You create an incident email notification rule configured as shown in the following table.

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

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	○
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	○
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	○	○

Answer:

Answer Area

Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	○
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	○
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	○	○

Explanation:

Answer Area

Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	○
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	○
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	○	○

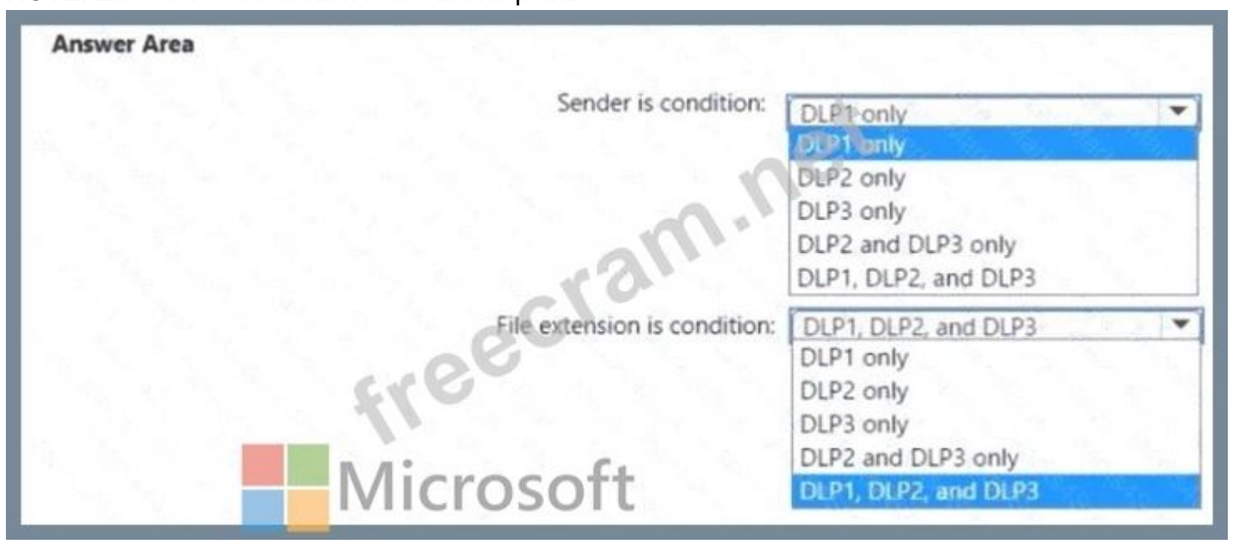
Box 1: No
Device1 is in Group2 as Name starts with Device and Tag contains Inventory.
However, the Group2 has alert severity low.
Box 2: No

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: 137
You have a Microsoft 365 E5 subscription.
You plan to create the data loss prevention (DLP) policies shown in the following table.

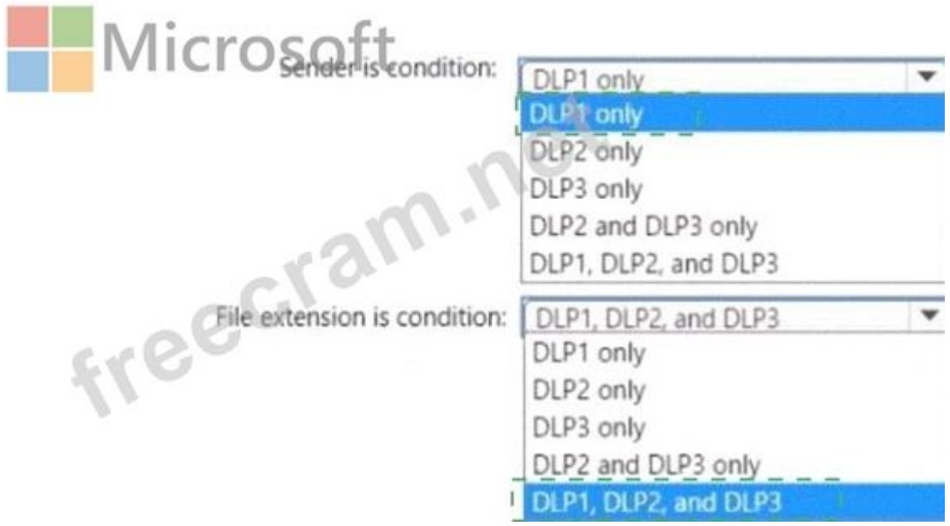
Name	Apply to location
DLP1	Exchange email
DLP2	SharePoint sites
DLP3	OneDrive accounts

You need to create DLP rules for each policy.
Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Answer Area



Explanation:

NEW QUESTION: 138

You have a Microsoft 365 E5 subscription.

You need to create a Conditional Access policy named Policy that meets the following requirements:

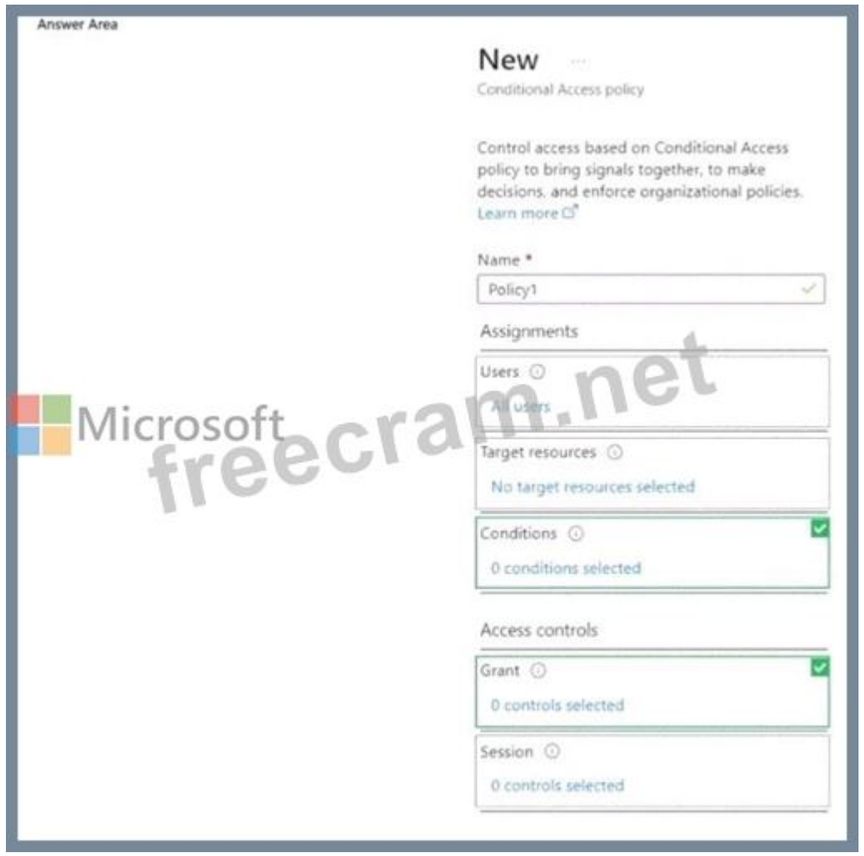
* Applies to high-risk users

* Requires multifactor authentication (MFA)

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

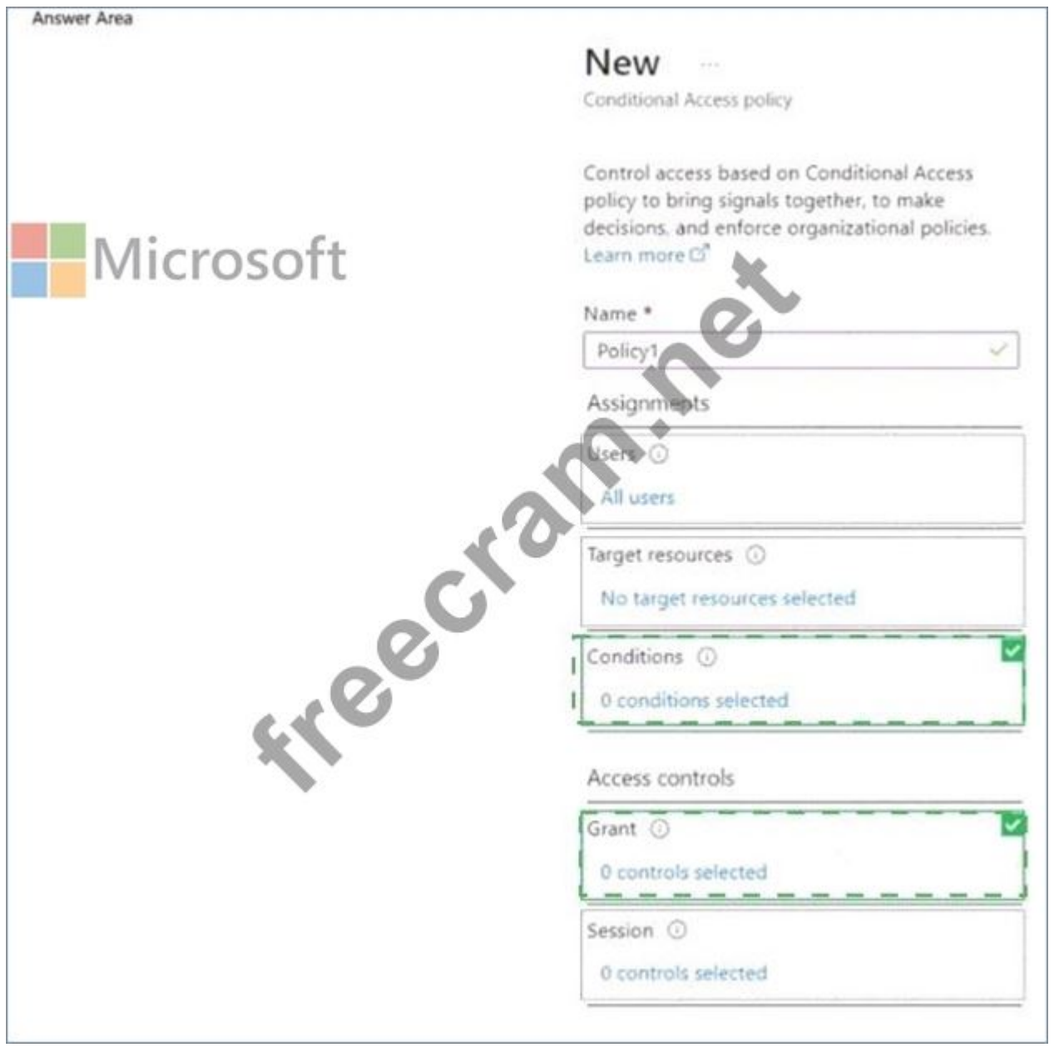
NOTE: Each correct selection is worth one point.

Answer Area

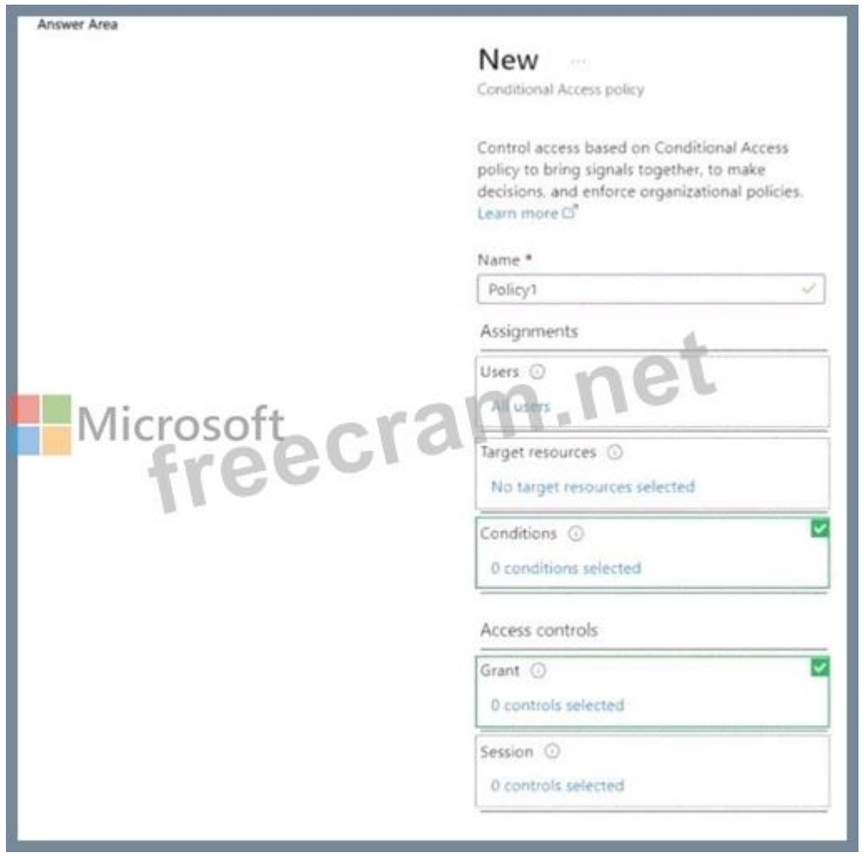


Answer:

Answer Area



Explanation:



NEW QUESTION: 139

You have a Microsoft 365 subscription that contains the users shown in the following table.

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

You create a new administrative unit named AU1 and configure the following AU1 dynamic membership rule.

Answer:

Answer Area

Explanation:

NEW QUESTION: 140

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

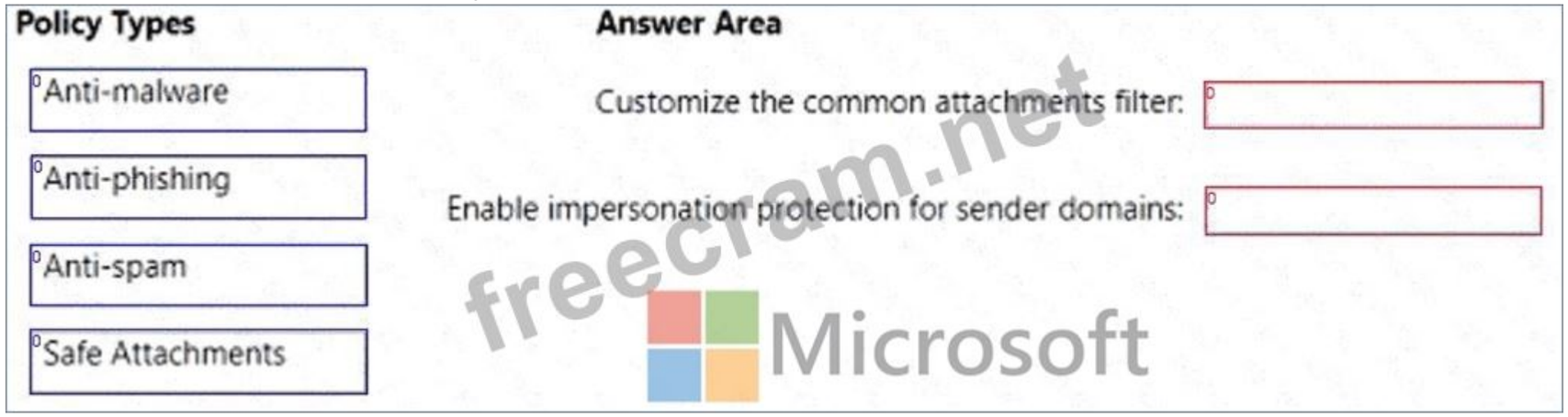
You need to configure policies to meet the following requirements:

Customize the common attachments filter.

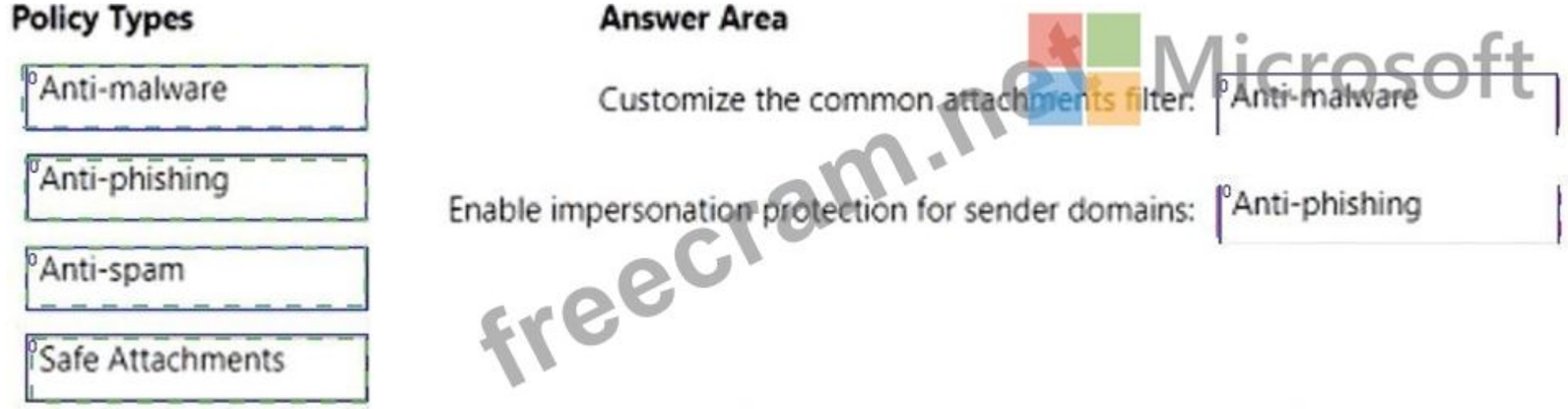
Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

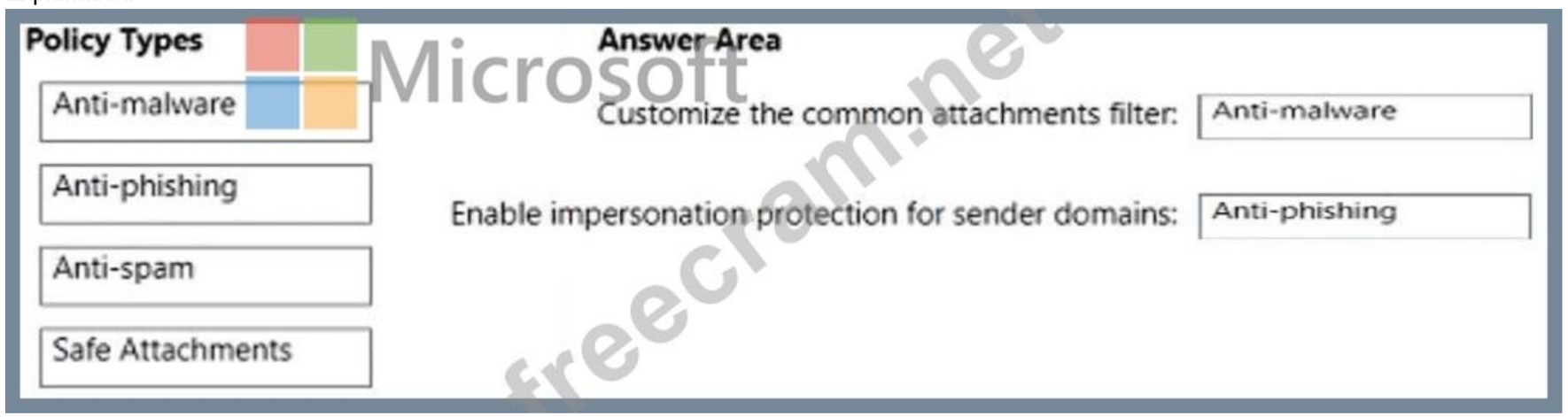
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Box 1: Anti-malware

Customize the common attachments filter.

See step 5 below.

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

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

On the Name your policy page, configure these settings:

Name: Enter a unique, descriptive name for the policy.

Description: Enter an optional description for the policy.

3. When you're finished on the Name your policy page, select Next.

4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions)

5. On the Protection settings page, configure the following settings:

Protection settings section:

Enable the common attachments filter: If you select this option, messages with the specified attachments are treated as malware and are automatically quarantined. You can modify the list by clicking Customize file types and selecting or deselecting values in the list.

6. Etc.

Box 2: Anti-phishing

Enable impersonation protection for sender domains.

Anti-phishing policies in Microsoft 365

The high-level differences between anti-phishing policies in EOP and anti-phishing policies in Defender for Office 365 are described in the following table:

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

Reference:

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

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

NEW QUESTION: 141

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	*None*

The device type restrictions in Endpoint Manager are configured as shown in the following table.

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

Answer Area

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

Answer:

Explanation:

NEW QUESTION: 142

You need to configure the compliance settings to meet the technical requirements.

What should you do in the Microsoft Endpoint Manager admin center?

A. From Compliance policies, modify the Notifications settings.

B. From Locations, create a new location for noncompliant devices.

C. From Retire Noncompliant Devices, select Clear All Devices Retire State.

D. Modify the Compliance policy settings.

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION: 143

You have a Microsoft 365 subscription.

You need to identify which shadow IT apps users connect to by using Cloud Discovery in Microsoft Defender for Cloud Apps. What should you create first?

A. an app discovery policy

B. a Conditional Access policy

C. a session policy

D. a Cloud Discovery snapshot report

Answer: (SHOW ANSWER)

NEW QUESTION: 144

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune.

You plan to use Endpoint analytics to identify hardware issues.

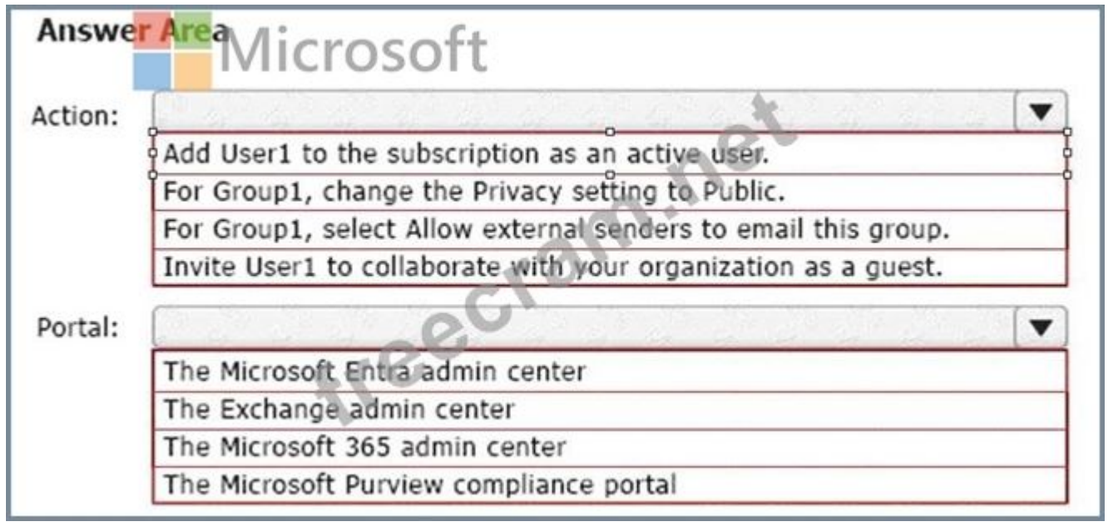
You need to enable Window health monitoring on the devices to support Endpoint analytics What should you do?

A. Create a configuration profile.

B. Create a Windows 10 Security Baseline profile
C. Create a compliance policy.
D. Configure the Endpoint analytics baseline regression threshold.
Answer: (SHOW ANSWER)

NEW QUESTION: 145
HOTSPOT
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.

An external user named User1 has an email address of user1@outlook.com.
You need to add User1 to Group1.
What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

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

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

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

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

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

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

Box 2: The Microsoft Entra admin center

Microsoft Entra admin center unites Azure AD with family of identity and access products Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.

Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).

Reference:

https://stefanos.cloud/kb/how-to-manage-microsoft-365-guest-users

https://m365admin.handsontek.net/microsoft-entra-admin-center-unites-azure-ad-with-family-of-identity-and- access-products

NEW QUESTION: 146

You create the planned DLP policies.

You need to configure notifications to meet the technical requirements.

What should you do?

A. From the Microsoft 365 security center, configure an alert policy.

B. From the Microsoft Endpoint Manager admin center, configure a custom notification.

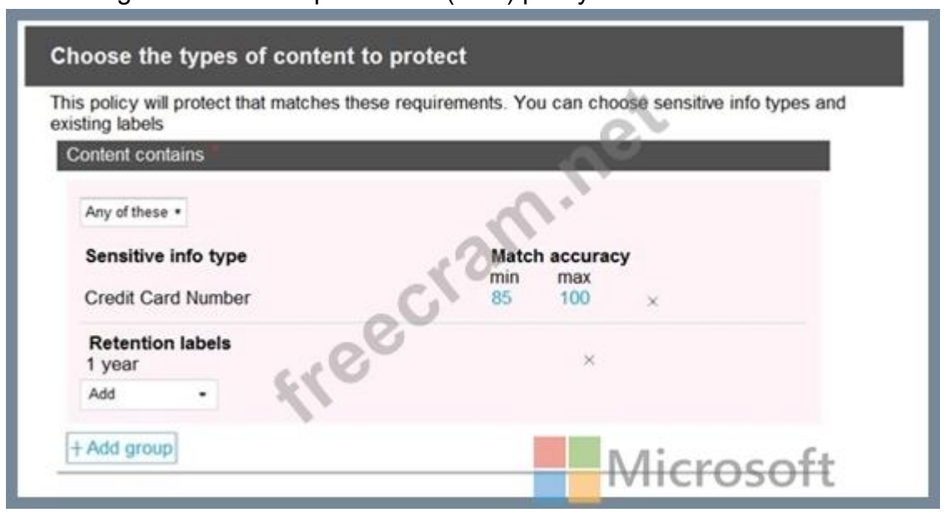
C. From the Microsoft 365 admin center, configure a Briefing email.

D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

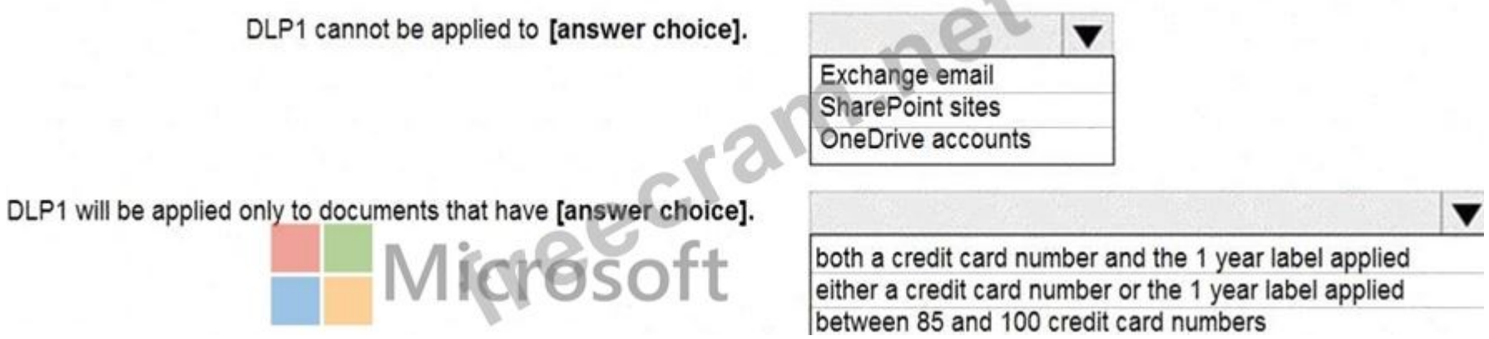
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide

NEW QUESTION: 147
You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:
* Windows 10
* Android
* iOS
On which devices can you configure the Endpoint DLP policies?
A. Windows 10 only
B. Windows 10 and Android only
C. Windows 10 and macO Sonly
D. Windows 10, Android, and iOS
Answer: (SHOW ANSWER)
Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide

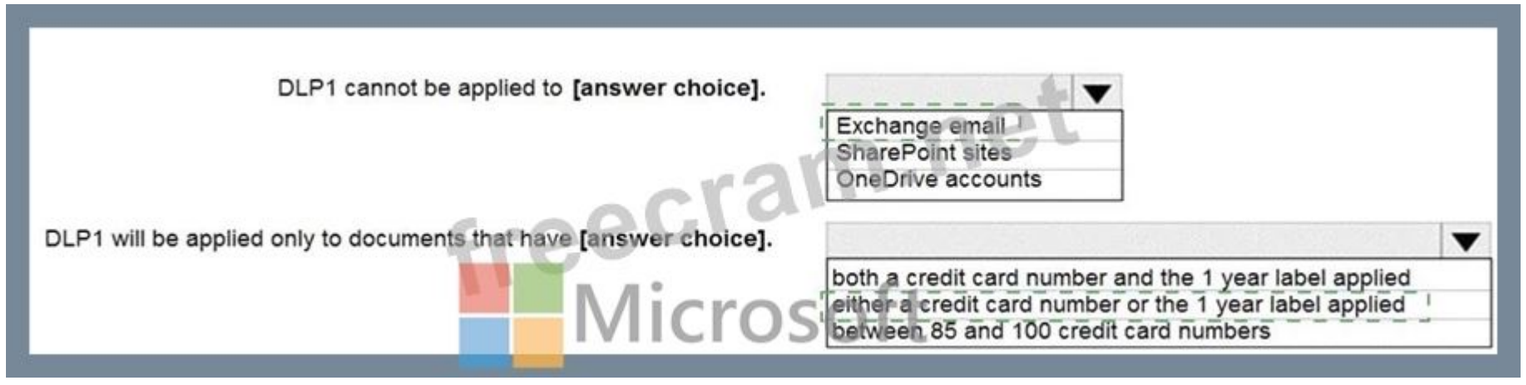
NEW QUESTION: 148
You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.



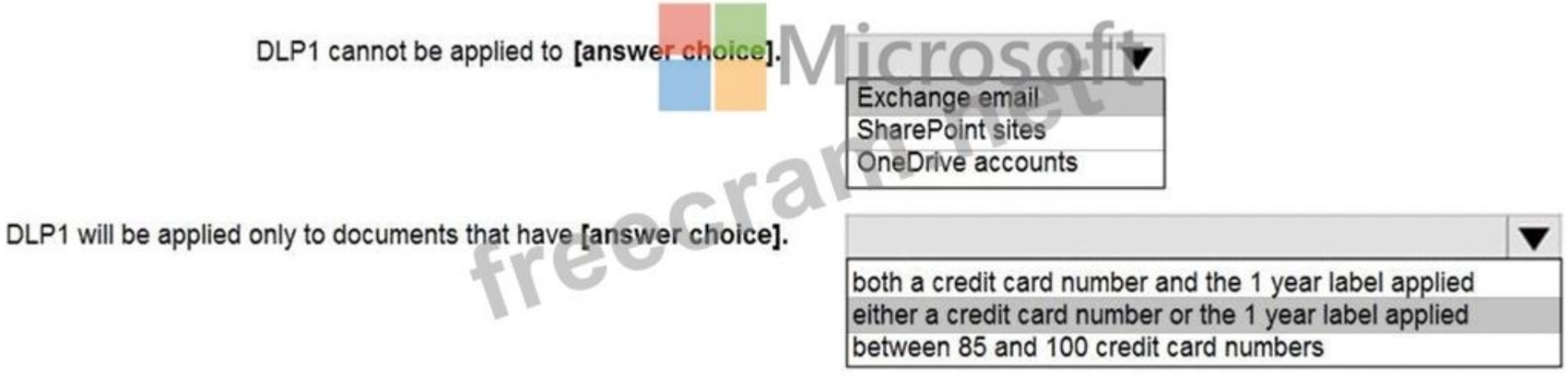
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

nce:

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

NEW QUESTION: 149

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles.

Which platform can you manage by using the profile?

A. Ubuntu Linux

B. macOS

C. iOS
D. Android
Answer: (SHOW ANSWER)
Intune device configuration profiles can be applied to Windows 10 devices and macOS devices Note:
There are several versions of this question in the exam. The question has two possible correct answers:
Windows 10
macOS
Other incorrect answer options you may see on the exam include the following:
Android Enterprise
Windows 8.1
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

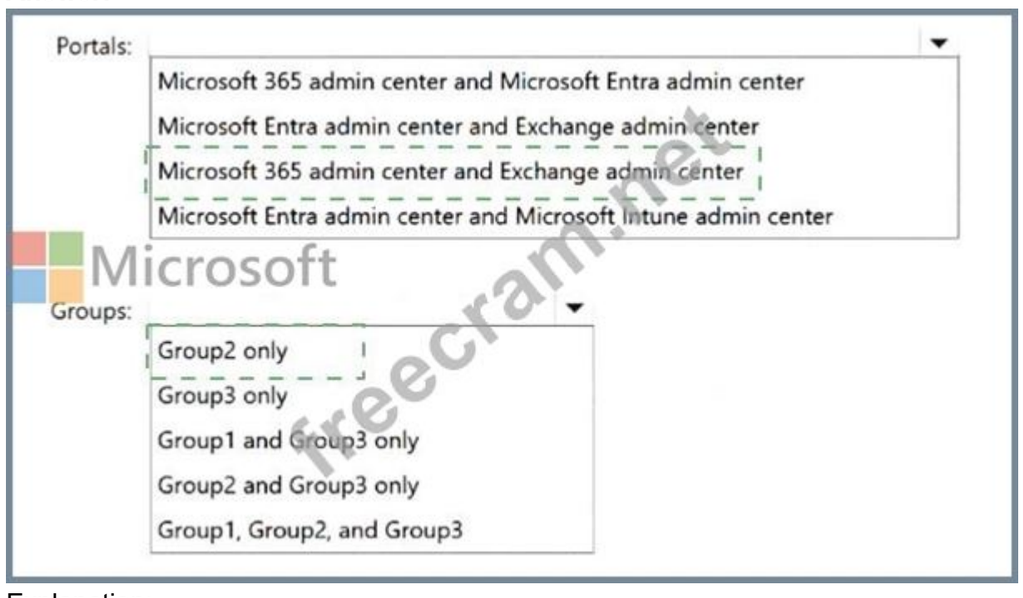
NEW QUESTION: 150
On which server should you use the Defender for Identity sensor?
A. Server1
B. Server2
C. Server3
D. Server4
E. Servers5
Answer: (SHOW ANSWER)
However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct.
BTW, ATP now known as Defender for Identity.

NEW QUESTION: 151
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365

You need to create a contact named Contact1 and add Contact1 to a group.
Which two portals can you use to create Contact1, and to which groups can you add Contact1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:



Explanation:

Portals: Microsoft 365 admin center and Exchange admin center

Groups: Group2 only

Creating a contact (mail contact)

A contact (also called a mail contact) is an Exchange object. Microsoft documentation states that mail contacts are created and managed using Exchange-related admin experiences.

* The Exchange admin center explicitly supports creating and managing mail contacts.
* The Microsoft 365 admin center provides a simplified interface that also allows admins to create contacts (which are stored in Exchange Online).

Therefore, the two correct portals that can be used to create Contact1 are:

* Microsoft 365 admin center

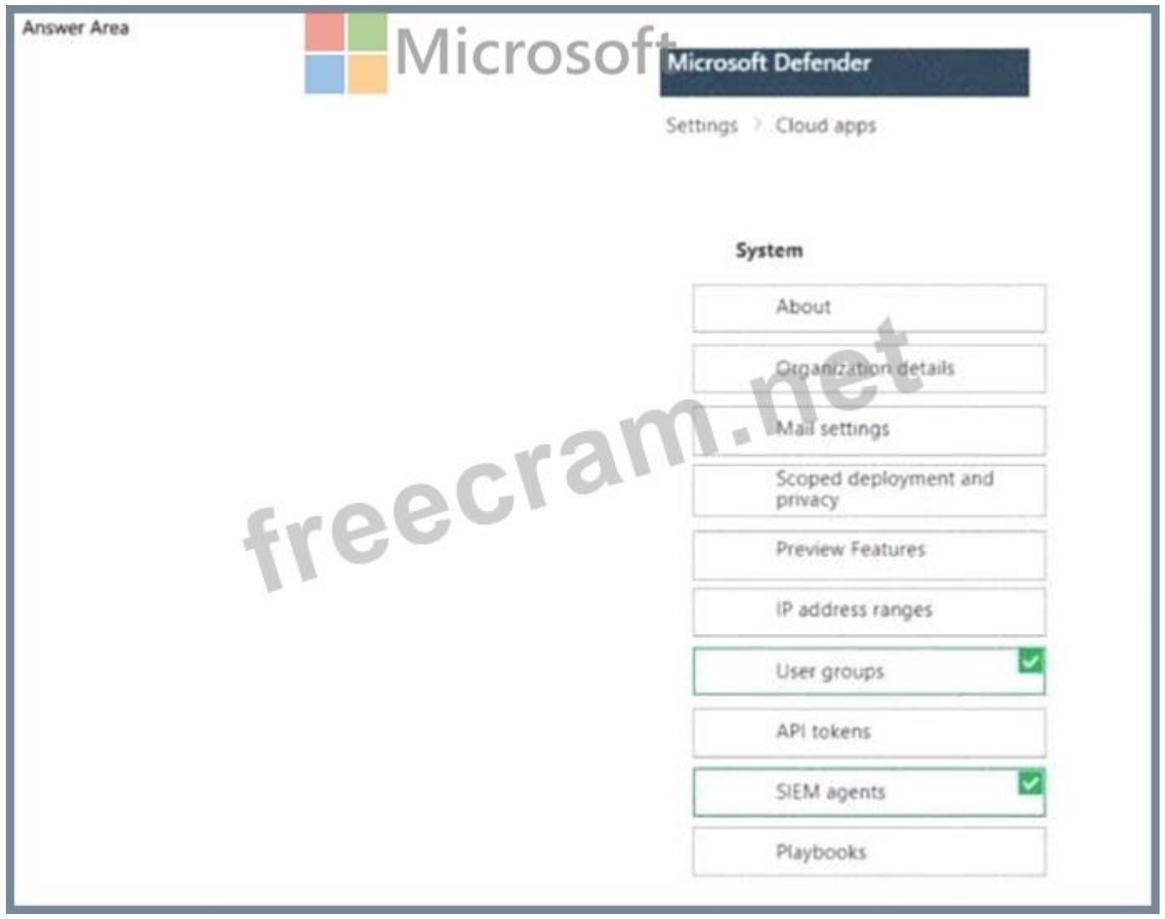
* Exchange admin center
Other portals are incorrect:
* Microsoft Entra admin center manages users, groups, and devices, but does not support creating mail contacts.
* Microsoft Intune admin center is for device and app management only.
Adding a contact to a group
Microsoft documentation clearly differentiates which group types can contain contacts:
* Distribution groups support adding mail-enabled objects, including:
* Mail users
* Mail contacts
* Security groups do not support mail contacts.
* Microsoft 365 groups only support user mailboxes and do not support contacts.

NEW QUESTION: 152
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Service Administrator role.
Does this meet the goal?
A. Yes
B. No
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?view=o365-worldwide

NEW QUESTION: 153
You have a Microsoft 365 E5 subscription. You plan to use Microsoft Entra ID Protection.
You need to ensure that account passwords must be changed if account credential. What should you configure?
A. self-service password reset (SSPR)
B. a sign-in risk policy
C. a user risk policy
D. Password protection

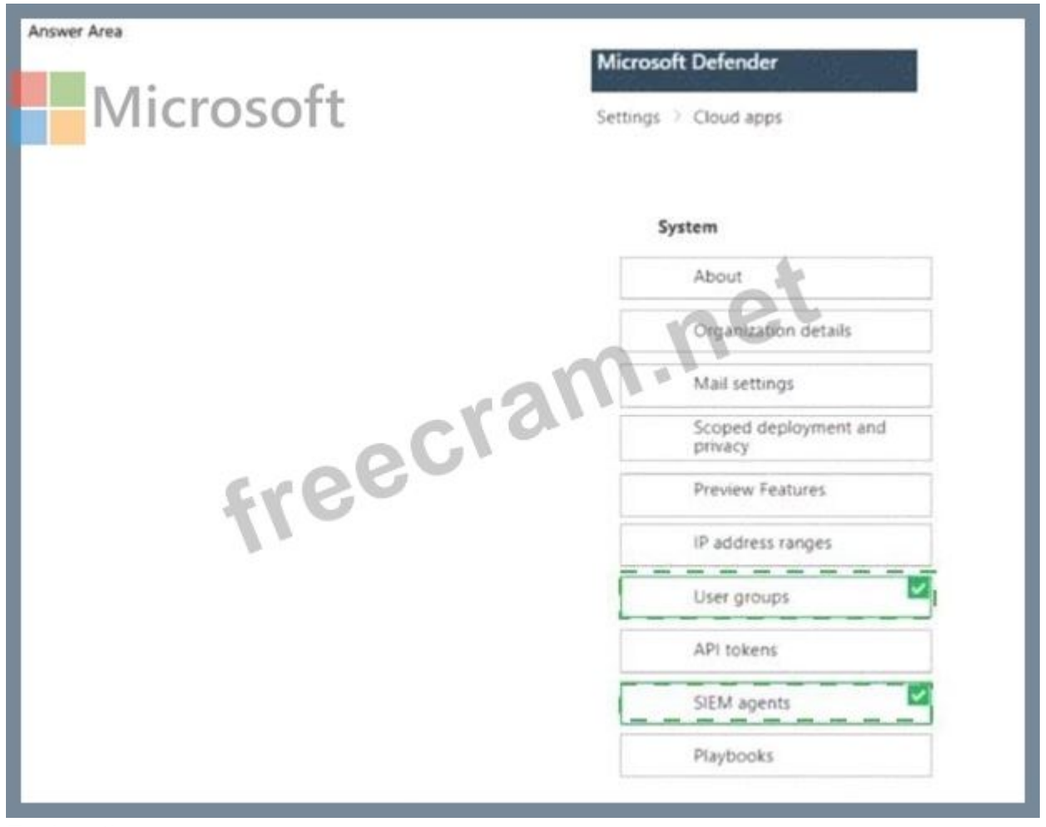
Answer: (SHOW ANSWER)

NEW QUESTION: 154
You have a Microsoft 36S E5 subscription.
You connect a cloud app that contains a group named Group1 to Microsoft Defender tor Cloud Apps.
You need to configure the Cloud apps settings to monitor all activities performed by the members of Group1.
Which two settings should you configure? to answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



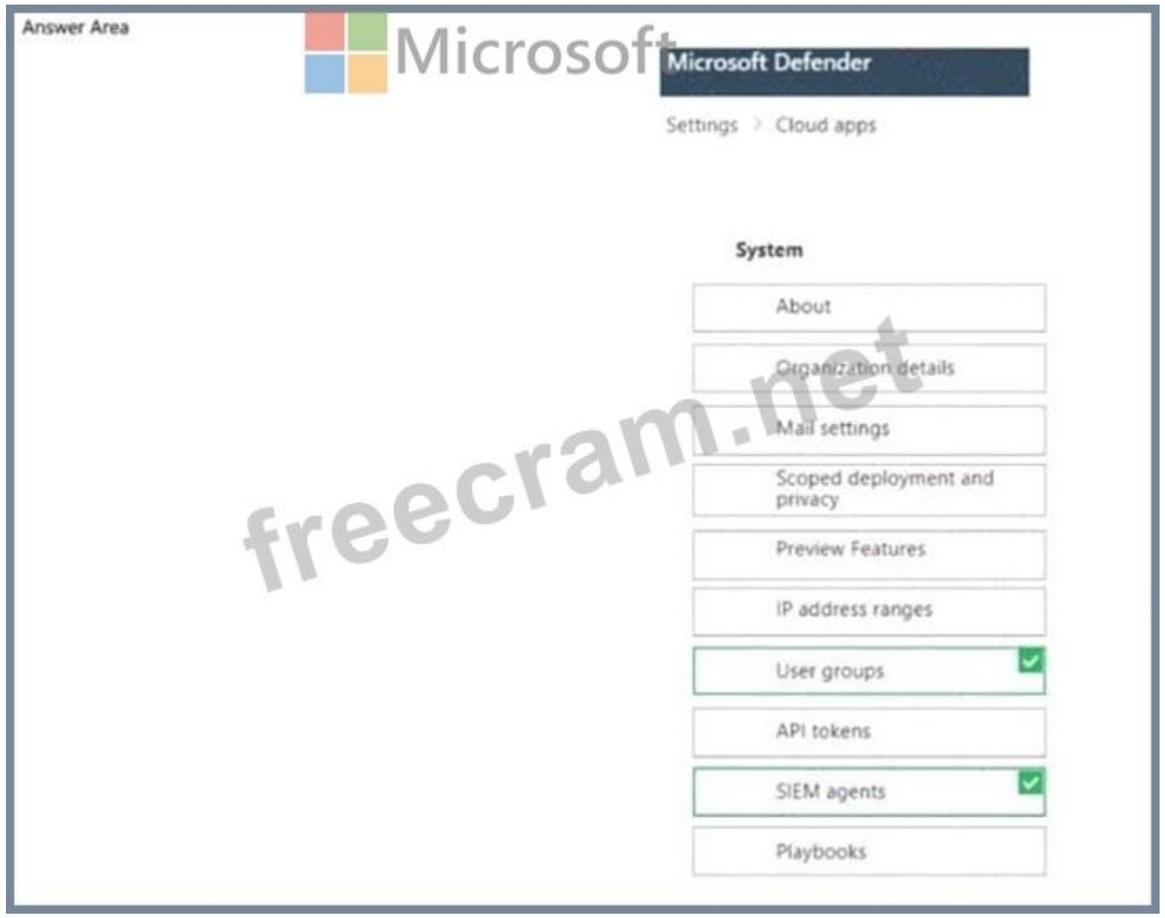
Answer:

Answer Area



Explanation:

Answer Area



NEW QUESTION: 155
Your network contains an on-premises Active Directory domain named contoso.com.
For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.
You plan to sync contoso.com to an Azure AD tenant.
You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.
What should you include in the recommendation?
A. pass-through authentication
B. conditional access policies
C. password synchronization
D. Azure AD Identity Protection policies
Answer: (SHOW ANSWER)
Reference:
https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

NEW QUESTION: 156
You have a Microsoft 365 E5 subscription that contains the following user:
Name: User1

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

NEW QUESTION: 157
You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

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

You plan to implement Microsoft Defender for Endpoint.
You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.
You need to identify which user can view security incidents from the Microsoft 365 Defender portal.
Which user should you identify?
A. User2
B. User1
C. User4
D. User3
Answer: (SHOW ANSWER)

NEW QUESTION: 158
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

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

All the policies are configured to send malicious email messages to quarantine. Which policies support a customized quarantine retention period?

A. Policy1 and Policy2 only

B. Policy2 and Policy4 only

C. Policy1 and Policy3only

D. Policy3 and Policy4 only

Answer: (SHOW ANSWER)

NEW QUESTION: 159

You have a Microsoft 365 E5 subscription.

You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:

* Support KQL for querying data.

* Retain report data for at least one year.

What should you include in the recommendation?

A. a security report in Microsoft 365 Defender

B. Azure Monitor workbooks

C. Microsoft 365 usage analytics

D. End point analytics

Answer: (SHOW ANSWER)

NEW QUESTION: 160

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

You plan to provide User4 with early access to Microsoft 365 feature and service updates.

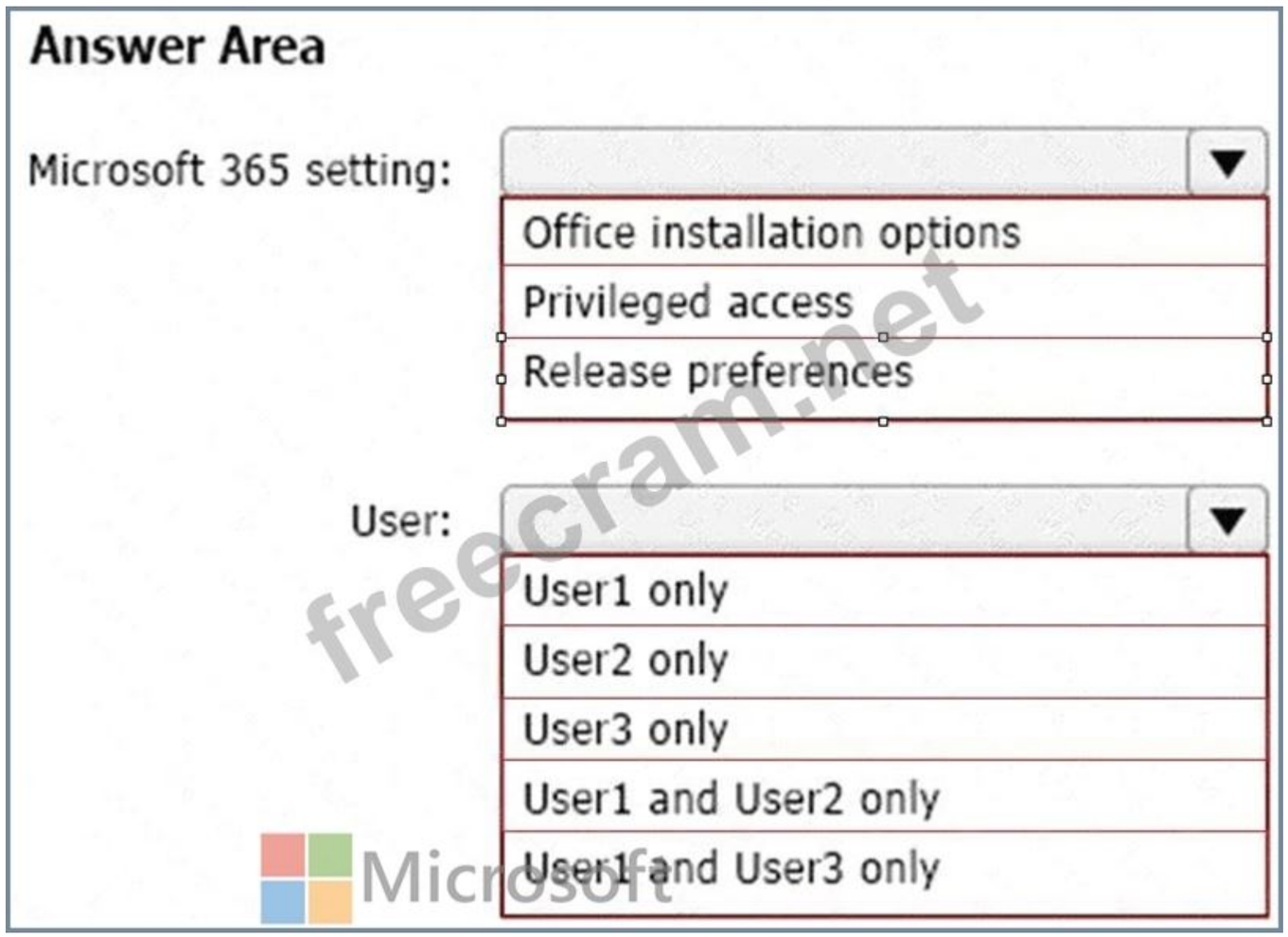
You need to identify which Microsoft 365 setting must be configured, and which user can modify the setting.

The solution must use the principle of least privilege.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area

Microsoft

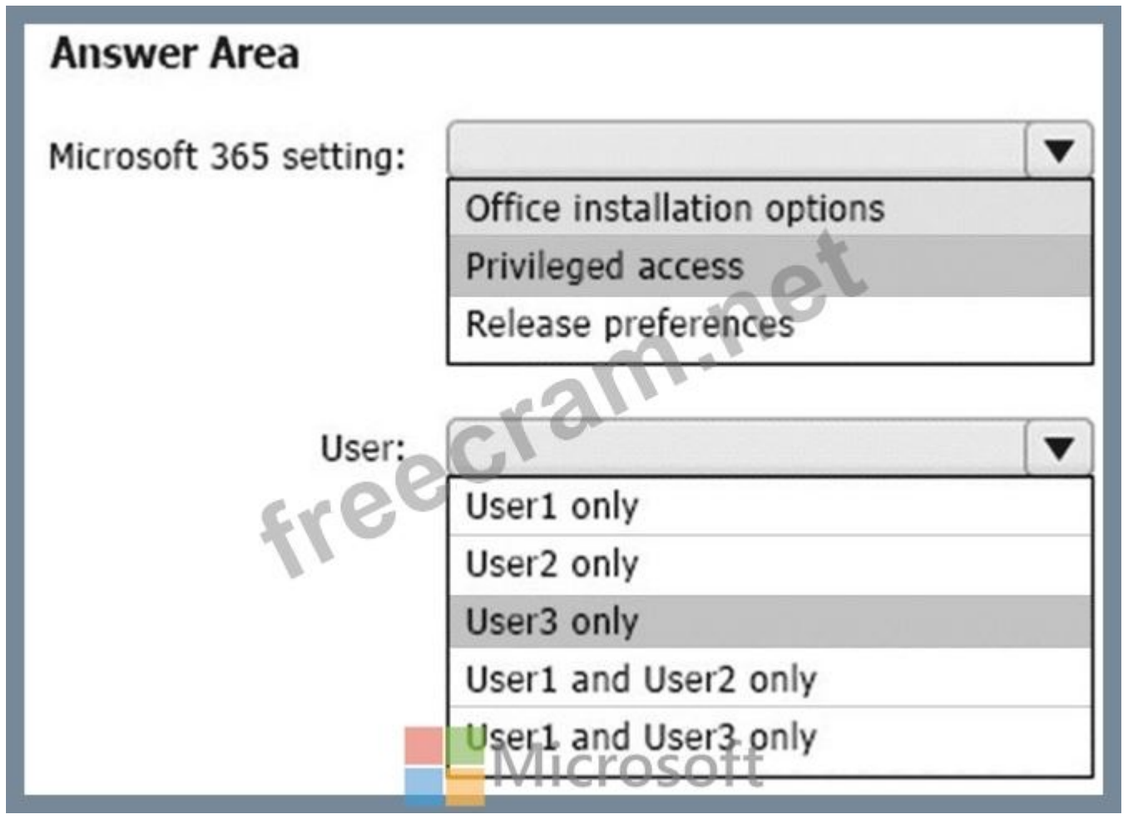
Microsoft 365 setting:

- Office installation options
- Privileged access
- Release preferences

User:

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

Explanation:



NEW QUESTION: 161
You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps.
You plan to perform a security audit of all the apps detected by Cloud Discovery.
You need to track which apps were audited. The solution must ensure that the list of audited apps can be displayed in the cloud app catalog.
A. Generate a Cloud Discovery snapshot report.
B. Define each app as a critical asset.
C. Enable app governance.
D. Deploy Conditional Access App Control.
E. Apply a custom app tag to each app.
Answer: (SHOW ANSWER)

NEW QUESTION: 162
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to a Microsoft Entra tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.) User2 fails to authenticate to the Microsoft Entra tenant when signing in as usef2@fabfikam.com You need to ensure that User2 can access the resources in Microsoft Entra ID.
Solution: From the Microsoft Entra admin center, you add <abrlkam.com as a custom domain You insttud User2 to sign in as user2@fabrikam.com Does this meet the goal?
A. Yes

B. No

Answer: (SHOW ANSWER)

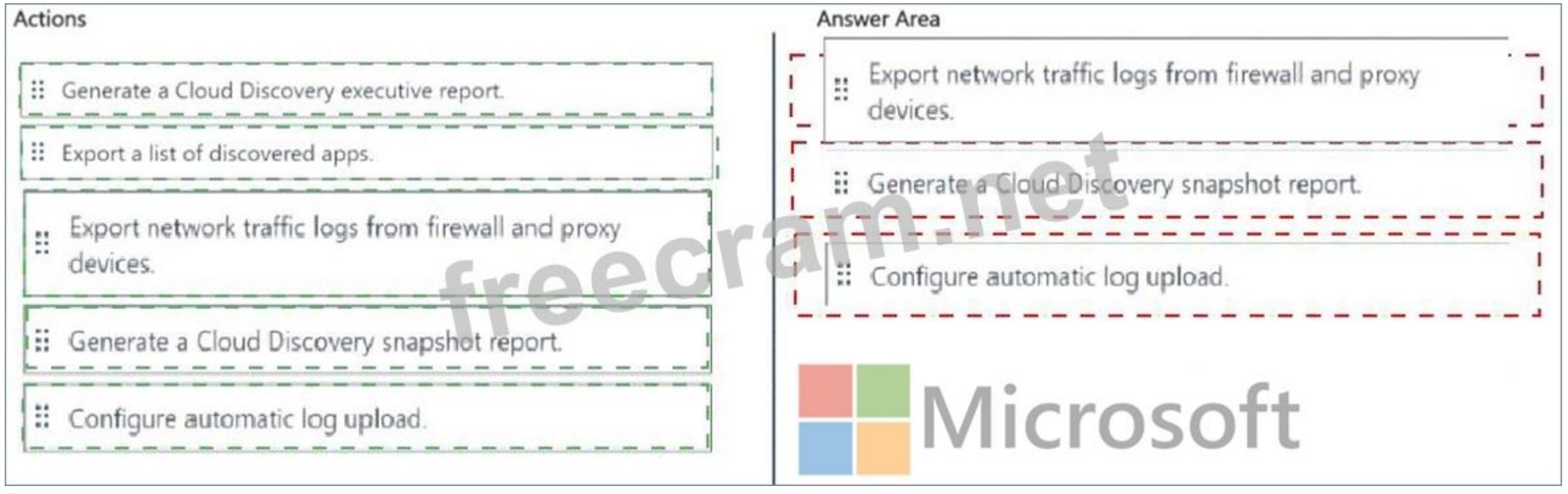
NEW QUESTION: 163

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps.

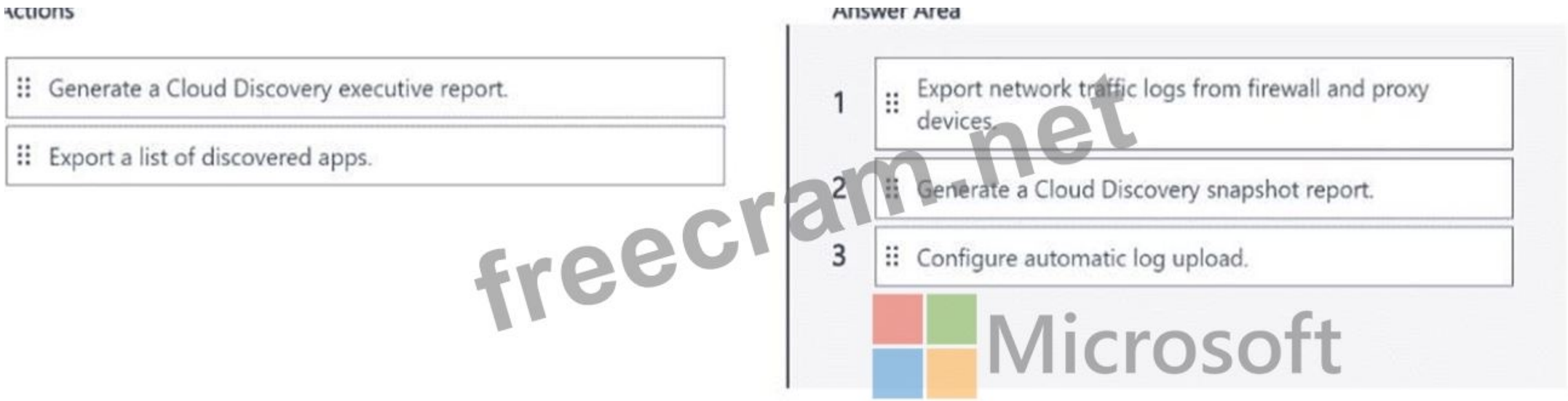
You need to configure Cloud Discovery to generate a report that identifies top potential risks and provides a workflow to mitigate and manage the risks.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer:



Explanation:



NEW QUESTION: 164

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals.

More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Office 365.

You need to implement a threat policy that will apply a balanced baseline protection profile to protect against spam, phishing, and malware.

Solution: You create an anti-malware policy.

Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

NEW QUESTION: 165

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Linux
Device3	MacOS

You plan to create an Endpoint security policy by using the Defender Update controls template. To which device can you apply the policy?

A. Devke1 and Device3 only

B. Device1 and Devke2 only

C. Device1 only

D. Devke1, Device2. and Devke3

Answer: (SHOW ANSWER)

NEW QUESTION: 166

You have a Microsoft 365 subscription.
You have a data loss prevention (DLP) policy that blocks sensitive data from being shared in email messages.
You need to modify the policy so that when an email message containing sensitive data is sent to both external and internal recipients, the message is only prevented from being delivered to the external recipients.
What should you modify?
A. the policy rule actions
B. the policy rule exceptions
C. the policy rule conditions
D. the DLP policy locations
Answer: (SHOW ANSWER)

NEW QUESTION: 167
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview policies to meet the following requirements:
Identify documents that are stored in Microsoft Teams and SharePoint that contain Personally Identifiable Information (PII).
Report on shared documents that contain PII.
What should you create?
A. a data loss prevention (DLP) policy
B. a retention policy
C. an alert policy
D. a Microsoft Defender for Cloud Apps policy
Answer: (SHOW ANSWER)
Demonstrate data protection
Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities.
With DLP policies, you can automatically protect sensitive information across Microsoft 365.
There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.
In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.
From the Security & Compliance tab of your browser, click Home.
Click Data loss prevention > Policy.
Click + Create a policy.
In Start with a template or create a custom policy, click Custom > Custom policy > Next.
In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b.
Description: Protect the personally identifiable information of European citizens Etc.

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

NEW QUESTION: 168
You have a Microsoft 365 subscription that contains the administrative units shown in the following table.

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

The groups contain the members shown in the following table.

Name	Members
Group1	User1
Group2	User2, User4

The users are assigned the roles shown in the following table.

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

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE; Each correct selection is worth one point.
Answer Area

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

Answer:

Explanation:

NEW QUESTION: 169

HOTSPOT

You have a Microsoft 365 E5 subscription.

All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.

You need to configure Defender for Endpoint to meet the following requirements:

Block a vulnerable app until the app is updated.

Block an application executable based on a file hash.

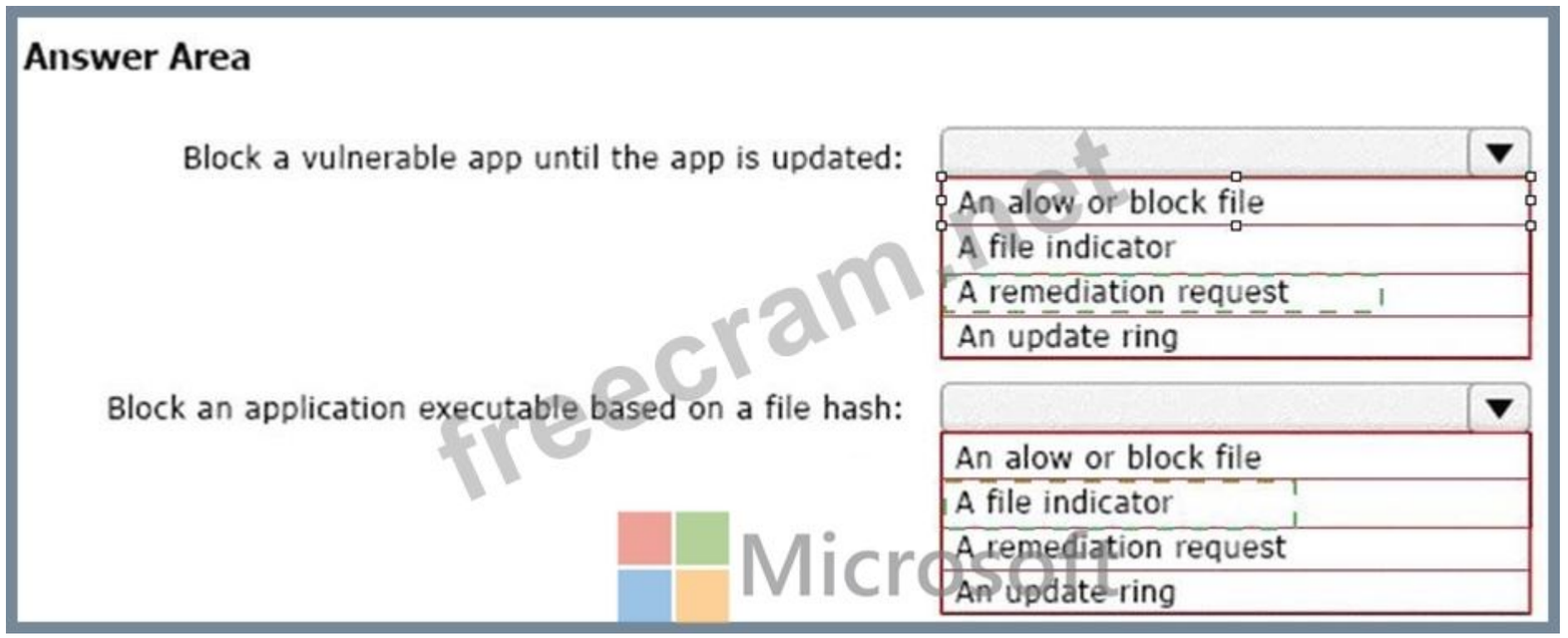
The solution must minimize administrative effort.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

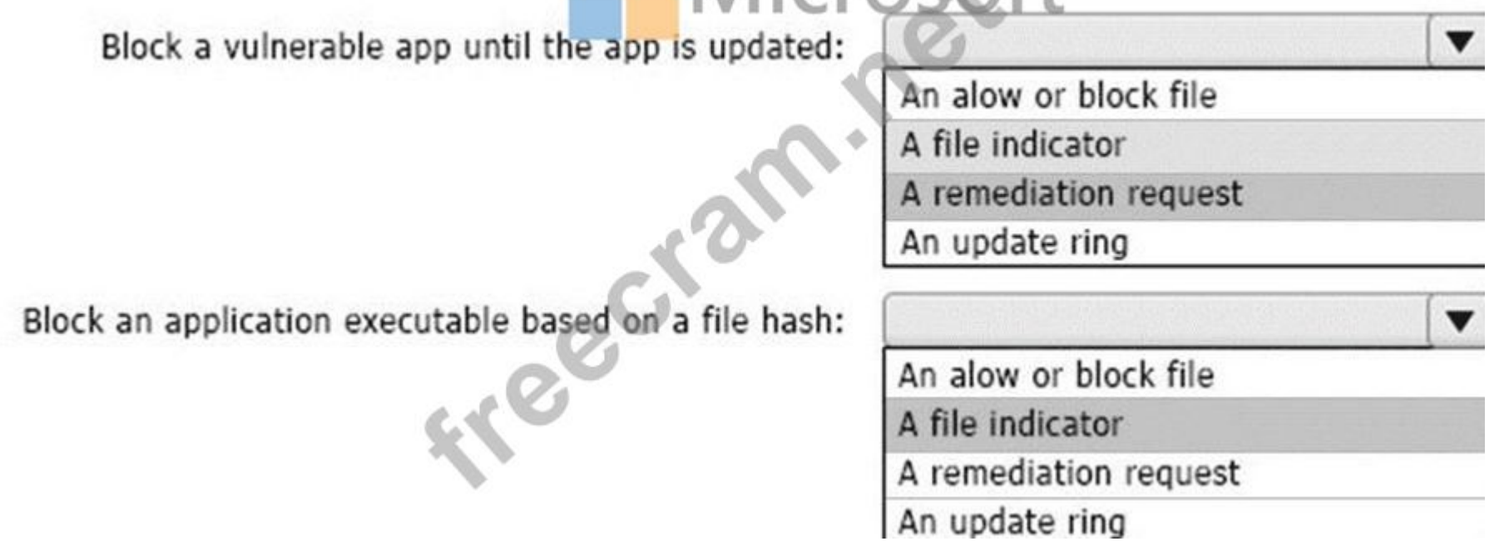
Answer Area

Answer:



Explanation:

Answer Area



Box 1: A remediation request

Block a vulnerable app until the app is updated.

Block vulnerable applications

How to block vulnerable applications

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

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

Select Request remediation.

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

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

Pick a Remediation due date and select Next.

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

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

Box 2: A file indicator

Block an application executable based on a file hash.

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

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

Reference:

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

NEW QUESTION: 170

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

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

You plan to review device startup performance issues by using Endpoint analytics.
Which devices can you monitor by using Endpoint analytics?
A. Device1 only
B. Device1 and Device2 only
C. Device1, Device2, and Device3 only
D. Device1, Device2, and Device4 only
E. Device1, Device2, Device3, and Device4
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/analytics/overview

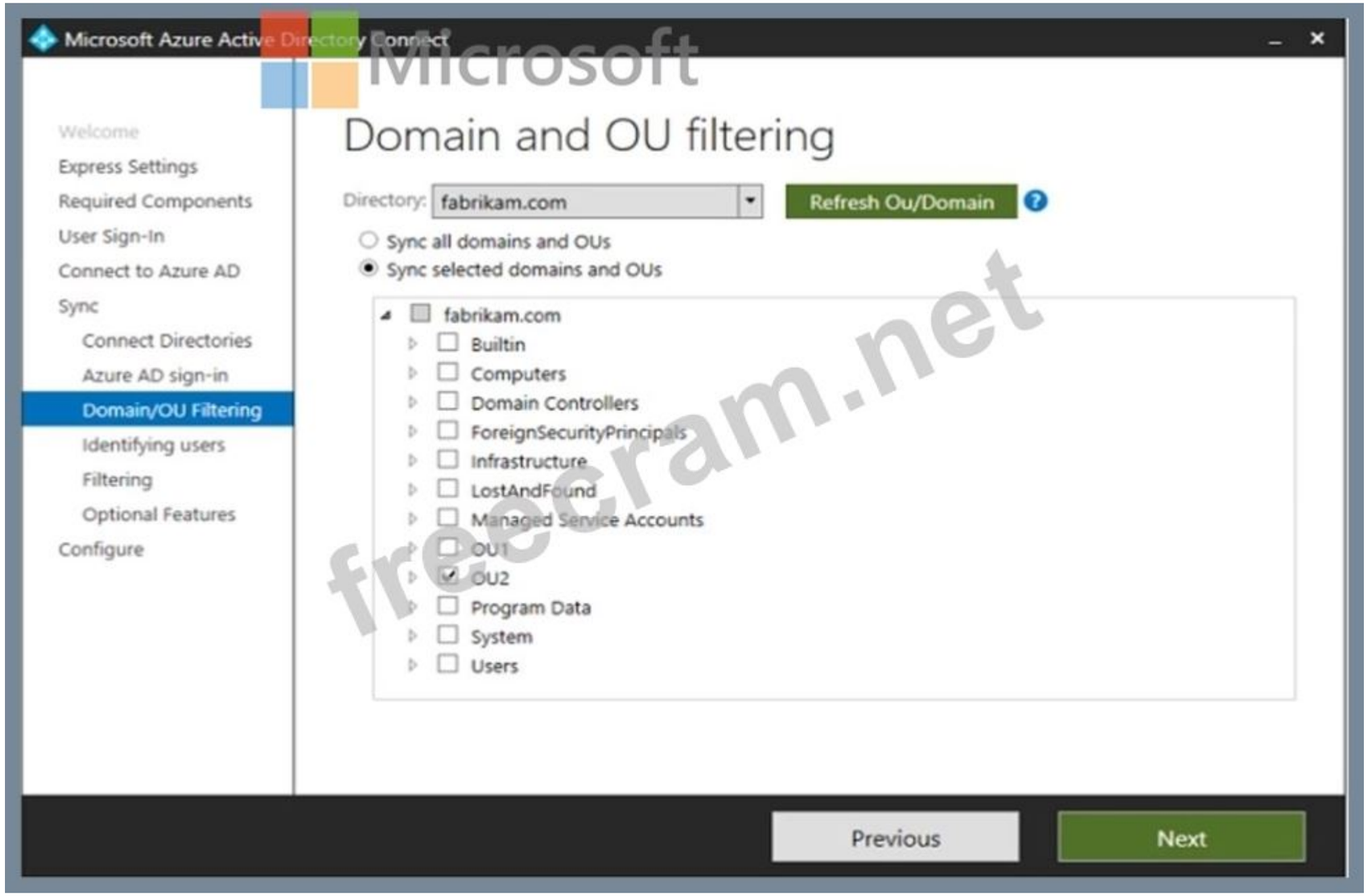
NEW QUESTION: 171
HOTSPOT
Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

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

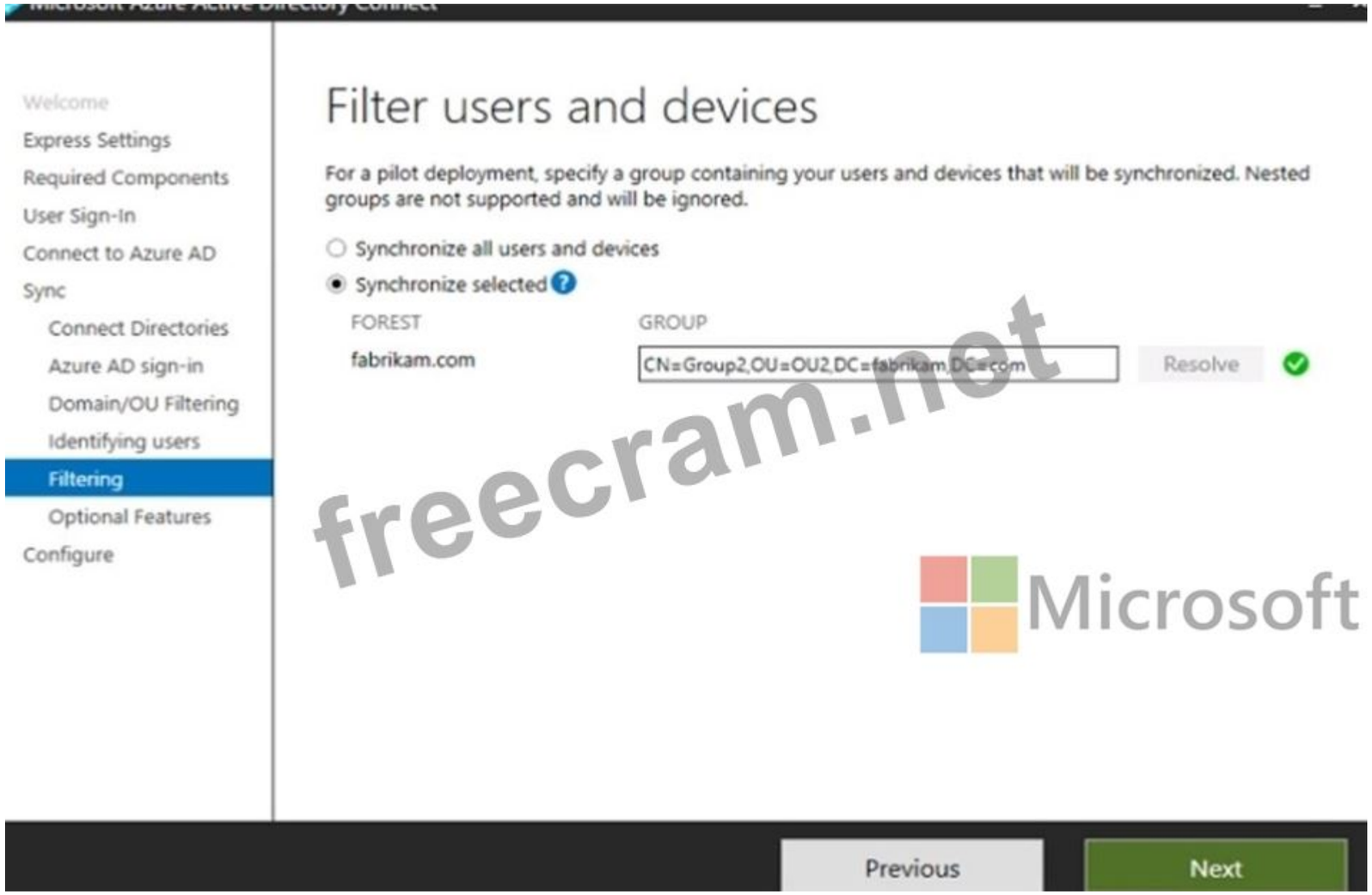
The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.
You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)



You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)



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

NOTE: Each correct selection is worth one point.

Answer:

Answer Area

Explanation:

Answer Area

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

Box 1: No

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

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

Box 2: Yes

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

Box 3: Yes

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

Reference:

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

NEW QUESTION: 172

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. Site!
contains the files shown in the following table.

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

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

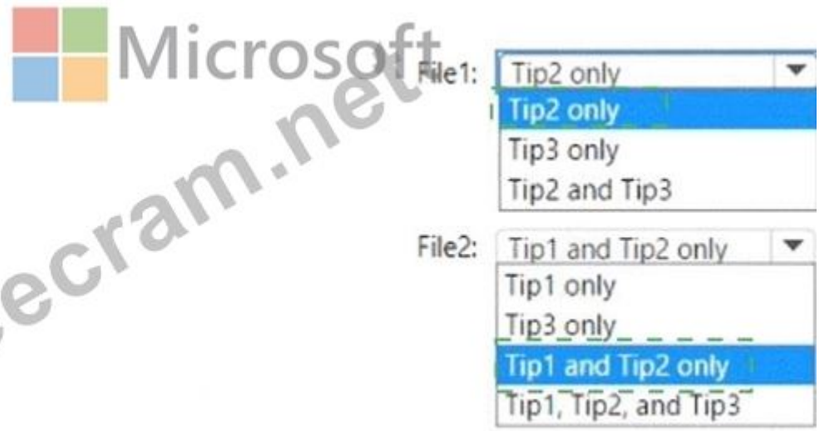
Name	Content contains	Policy tip	If there is a match, stop processing	Priority
Rule1	3 or more IP addresses	Tip1	No	0
Rule2	1 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

You apply DLP1 to Site1.

Which policy tip is displayed for each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:

NEW QUESTION: 173

You have a Microsoft 365 subscription.

You need to add additional domains with the onmicrosoft.com suffix to the subscription. The additional domains must be assignable as email addresses for users.

What is the maximum number of onmicrosoft.com domains the subscription can contain?

A. 10

B. 5

C. 2

D. 1

Answer: D (LEAVE A REPLY)

NEW QUESTION: 174
You have a Microsoft 365 subscription.
You create a retention label named Retention1 as shown in the following exhibit.

You apply Retention! to all the Microsoft OneDrive content.
On January 1, 2020, a user stores a file named File1 in OneDrive.
On January 10, 2020, the user modifies File1.
On February 1, 2020, the user deletes File1.
When will File1 be removed permanently and unrecoverable from OneDrive?
A. February 1, 2020
B. July 10, 2020
C. August 1, 2020
D. July 1.2020
Answer: (SHOW ANSWER)

NEW QUESTION: 175
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

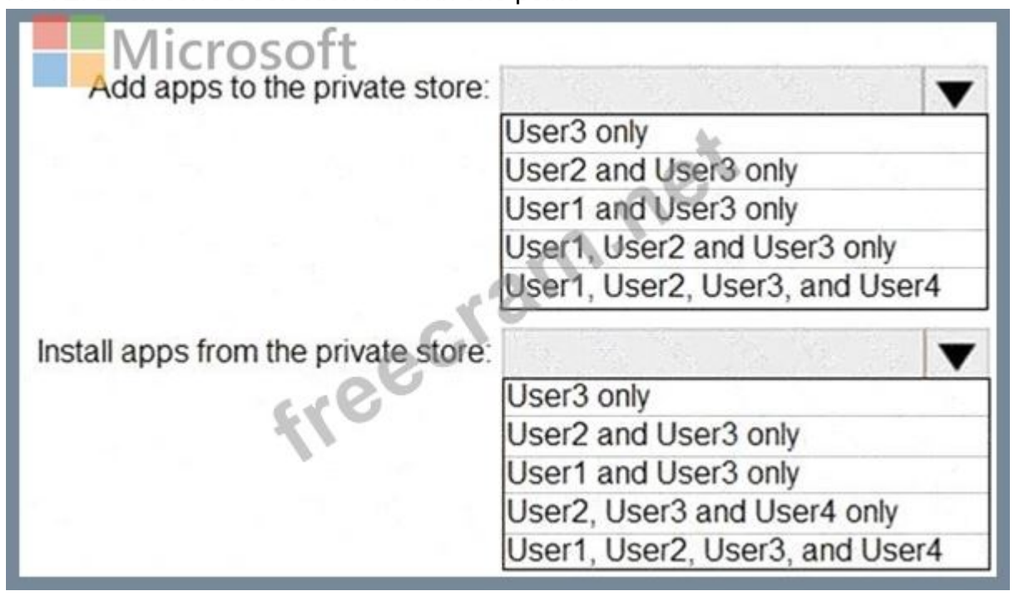
Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	None

Users are assigned Microsoft Store for Business roles as shown in the following table.

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

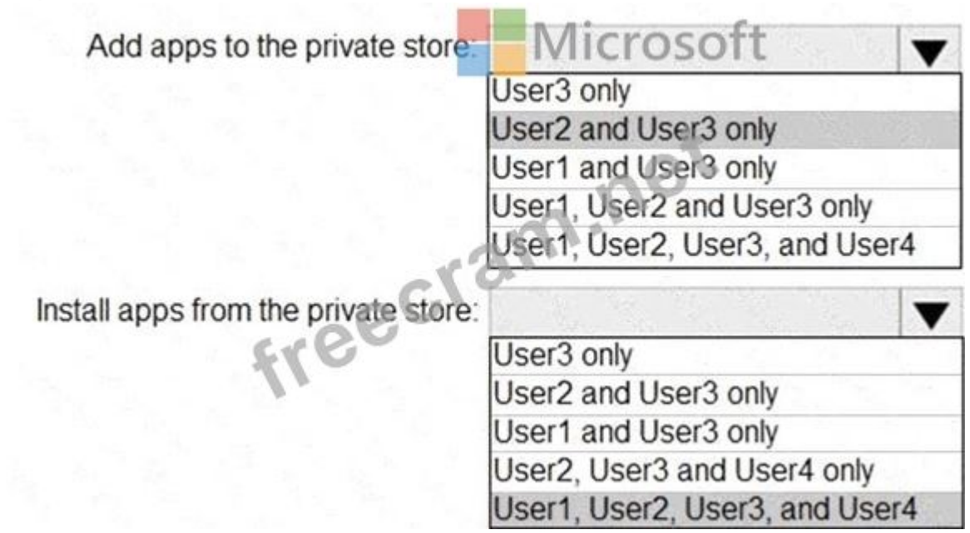
Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



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

NEW QUESTION: 176
You need to create the Microsoft Store for Business. Which user can create the store?
A. User2
B. User3
C. User4
D. User5
Answer: (SHOW ANSWER)

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

NEW QUESTION: 177
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

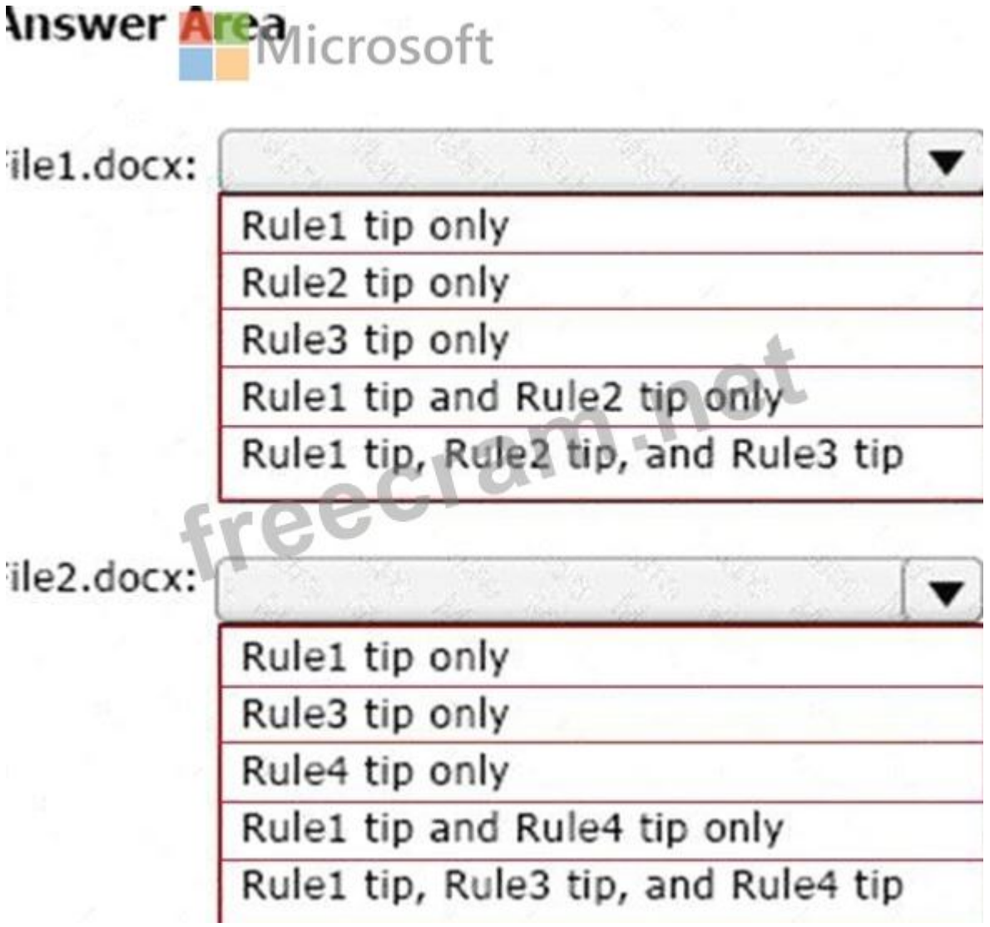
Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users 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 contains the files shown in the following table.

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

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area

File1.docx:

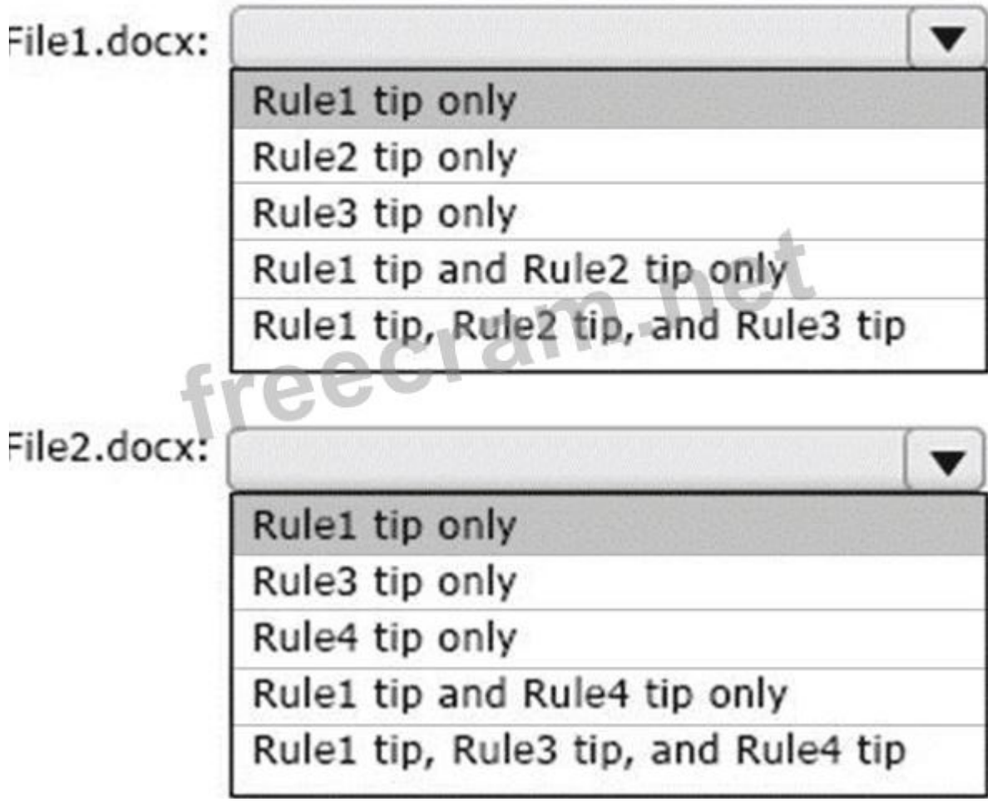
- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

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

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: 178

You enable the Azure AD Identity Protection weekly digest email.

You create the users shown in the following table.

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

Which users will receive the weekly digest email automatically?

A. Admin2, Admin3, and Admin4 only

B. Admin1, Admin2, Admin3, and Admin4

C. Admin2 and Admin3 only

D. Admin3 only

E. Admin1 and Admin3 only

Answer: (SHOW ANSWER)

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: 179

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select System, and then you select About to view information about the system.

Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

Reference:

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

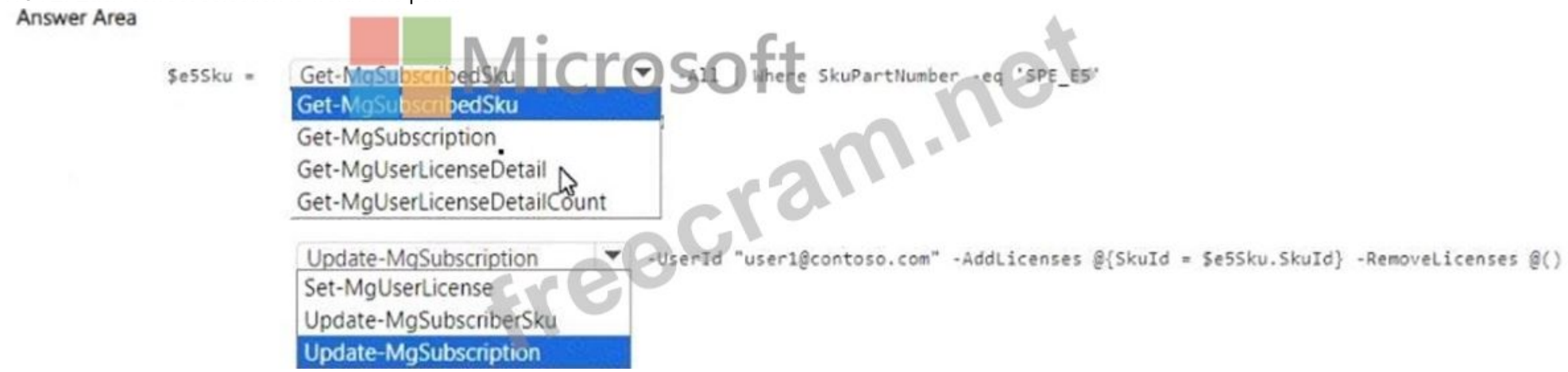
NEW QUESTION: 180

You have a Microsoft 365 E5 subscription.

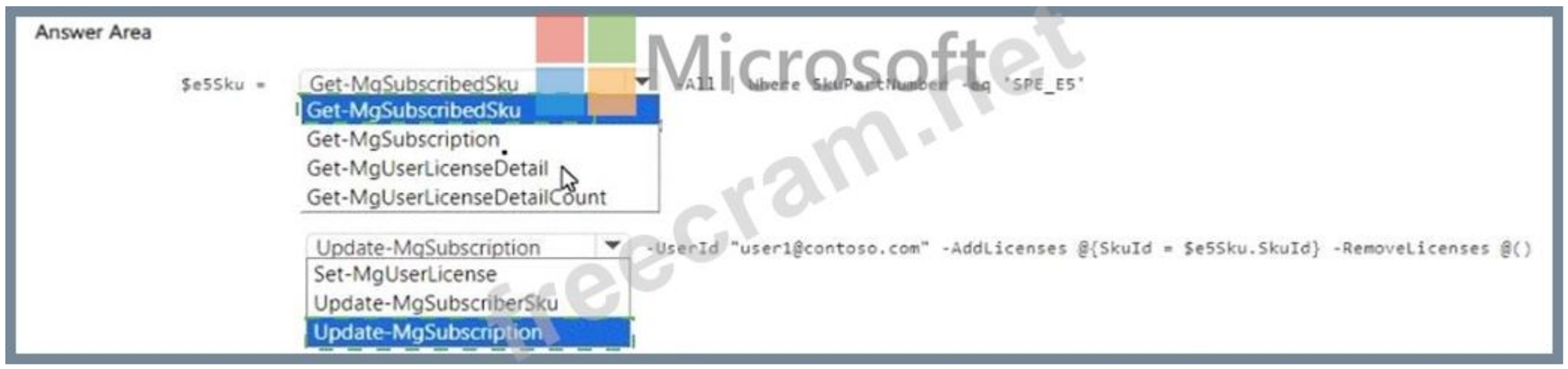
You need to use Microsoft Graph PowerShell to assign a Microsoft 365 E5 license to a new user named user1@contoso.com.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

NEW QUESTION: 181

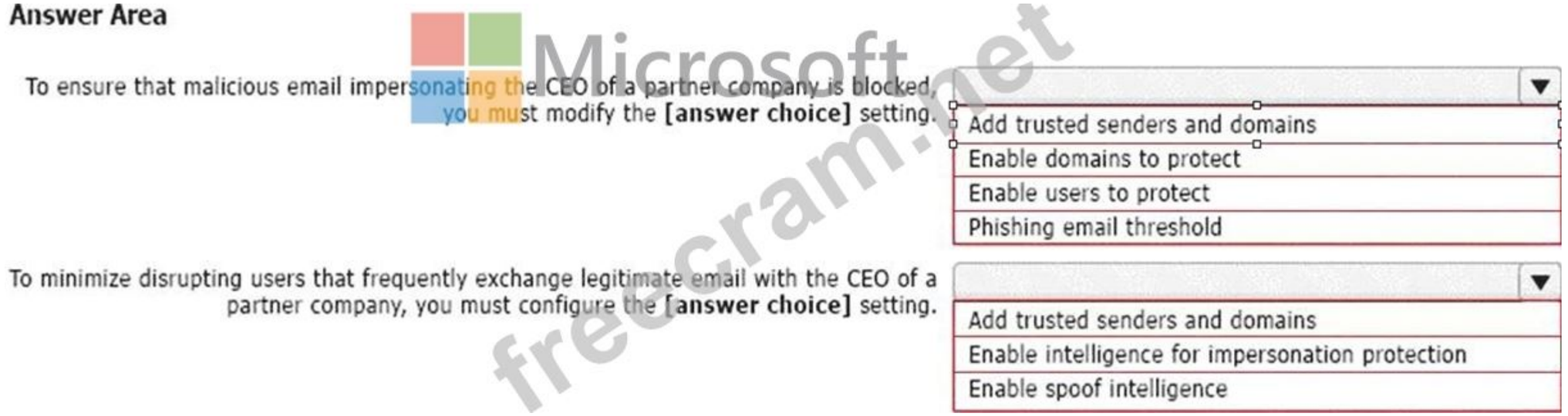
HOTSPOT

You have a Microsoft 365 subscription.

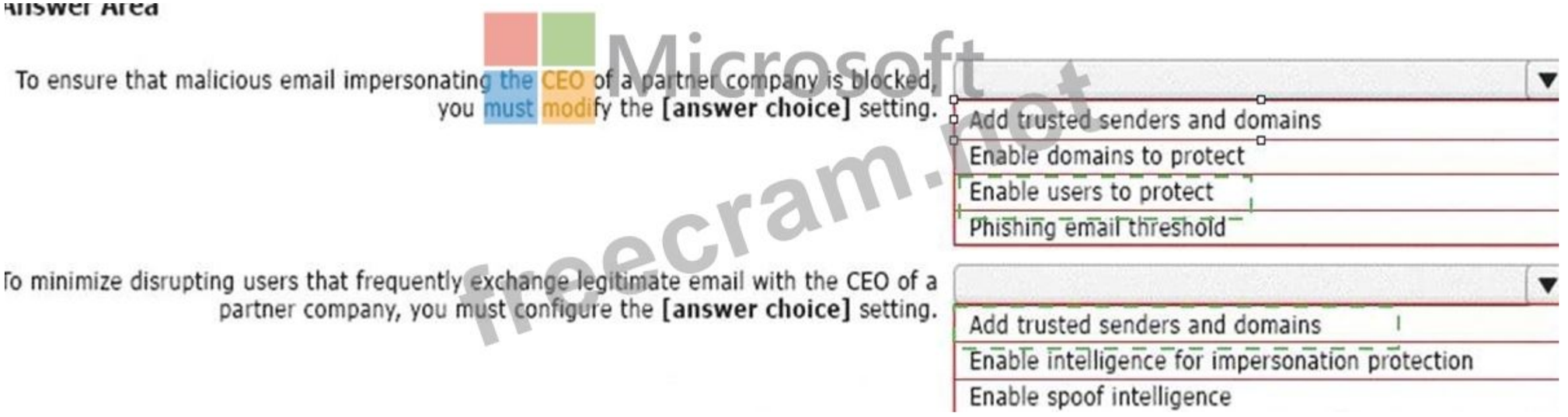
You deploy the anti-phishing policy shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

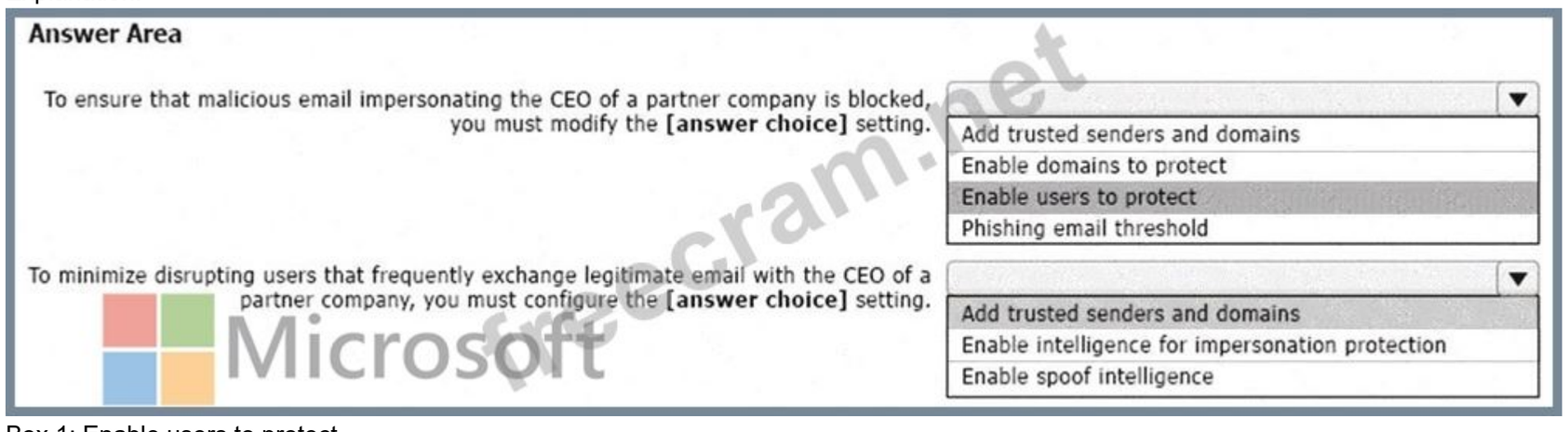
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Box 1: Enable users to protect

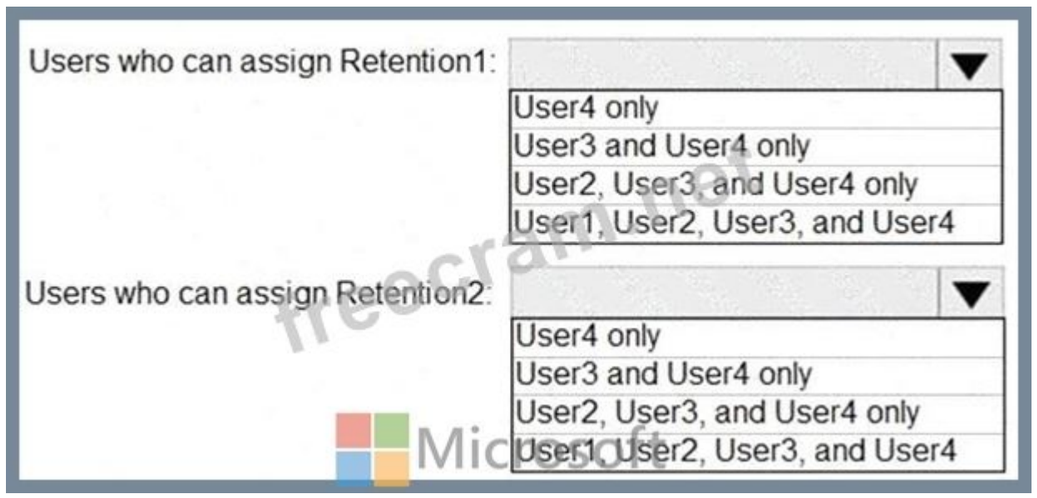
Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation

protection.
User impersonation protection
User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.
You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).
When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender's email address, the action for impersonated users is applied to the message.
Box 2: Add trusted senders and domains
Trusted senders and domains
Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren't applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about

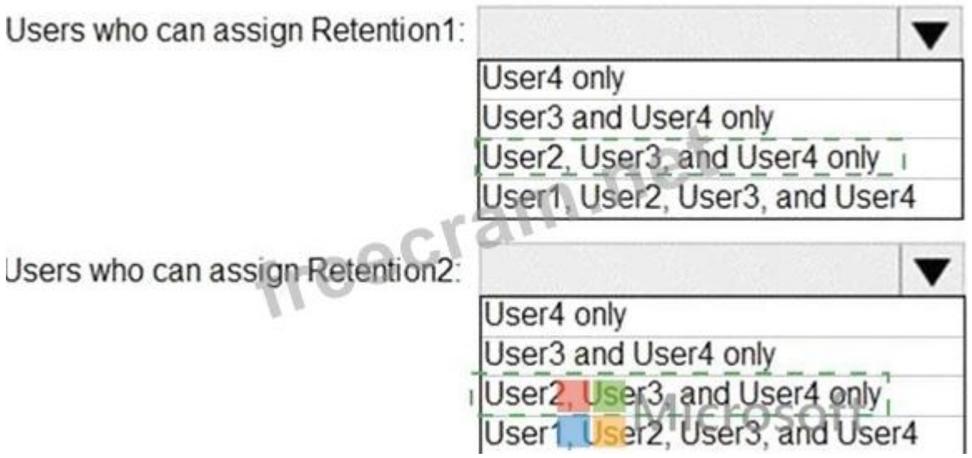
NEW QUESTION: 182
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

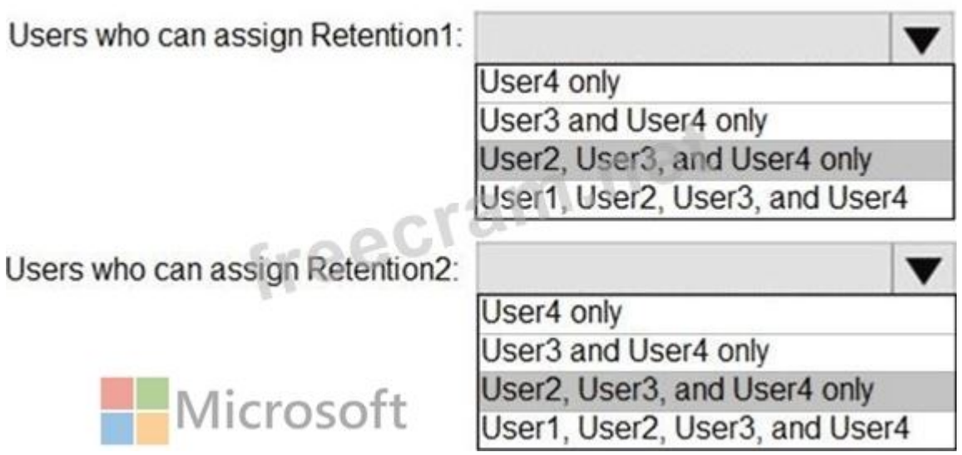
You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email.
You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2.
Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Reference:

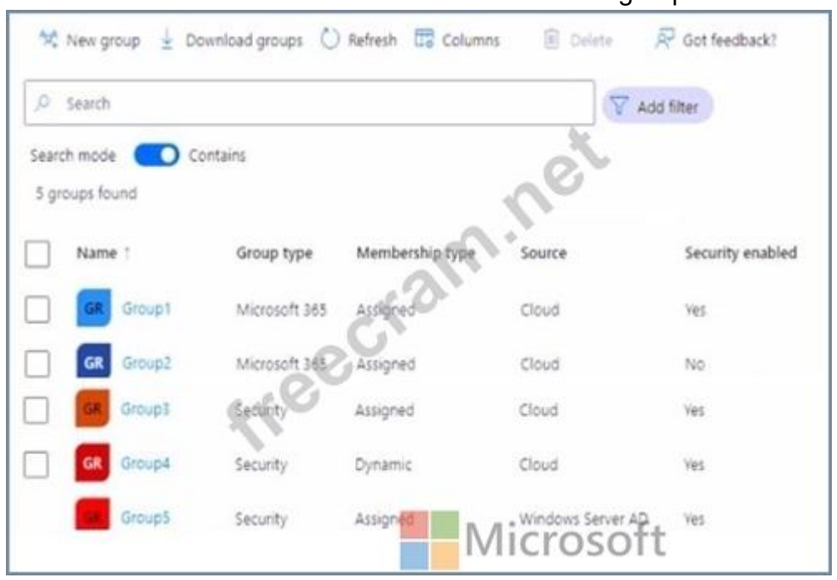
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-exchange?view=o365- worldwide

NEW QUESTION: 183

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might

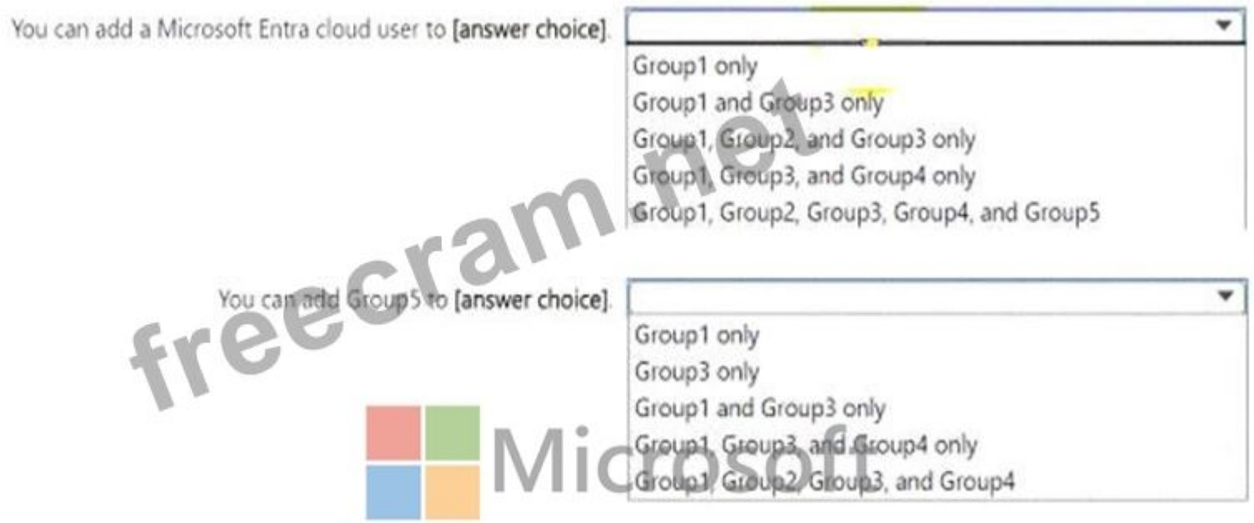
have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it As a result these questions will not appear in the review screen.
Your network contains an Active Directory forest.
You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
* Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
* User passwords must be 10 characters or more.
Solution: implement password hash synchronization and configure password protection in the Azure AD tenant.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 184
You have a Microsoft Entra tenant that contains the groups shown in the following exhibit.

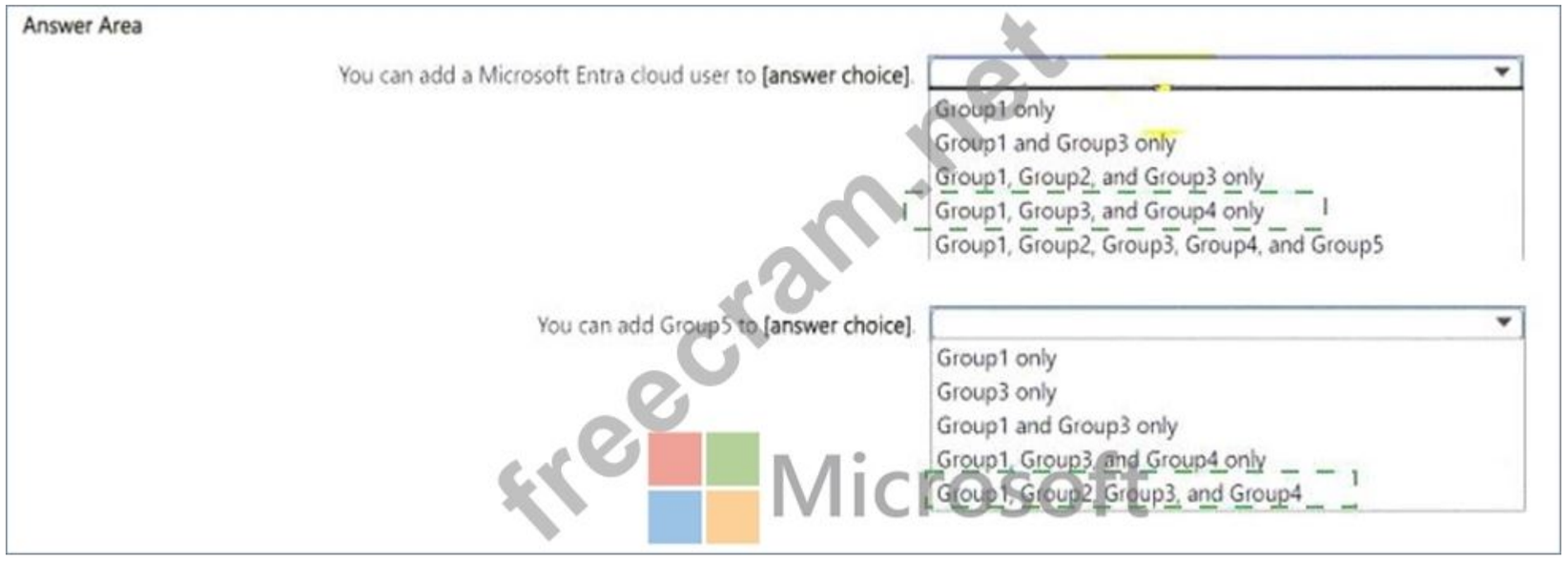


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each cont'd selection is worth one point.

Answer Area



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: 185

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Endpoint. The subscription contains Windows 11 devices.

You need to create a policy to restrict users from accessing the Device security settings and the Account protection settings in Windows Defender Security Center on the devices.
Which type of policy should you create, and which template should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 186
You have a Microsoft 365 E5 subscription that contains the security groups shown in the following table.

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

The subscription contains the users shown in the following table.

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

You have a Conditional Access policy that has the following settings:

* Assignments

o Users

Include: Group1

Exclude: Group2. Group3

o Target resources

Cloud apps

App1

Access controls

Grant

Block access

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

Explanation:

NEW QUESTION: 187

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange admin role.

Does this meet the goal?

A. Yes

B. No

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?view=o365-worldwide

NEW QUESTION: 188

You have an Azure AD tenant.

You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD.

You purchase a Microsoft 365 E3 subscription.

You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort.

What should you do?
A. From the Azure Active Directory admin center, create a security group that has dynamic device membership. Assign licenses to the group and instruct users to sign in to their computer.
B. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online site. Instruct users to run the provisioning package from SharePoint Online.
C. From the Microsoft Endpoinf Manager admin center, create a Windows Autopilot deployment profile.
Assign the profile to all the computers. Instruct users to restart their computer and perform a network restart.
D. Enroll the computers in Microsoft Intune. Create a configuration profile by using the Edition upgrade and mode switch template. From the Microsoft Endpoint Manager admin center, assign the profile to all the computers and instruct users to restart their computer.
Answer: (SHOW ANSWER)

NEW QUESTION: 189
You have a Microsoft 365 E5 subscription.
You create an account tor a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.
Does this meet the goal?
A. no
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 190
You have an Azure subscription and a Microsoft 365 E5 subscription.
You are licensed to use Microsoft Defender XDR
You need to monitor activities from suspicious IP addresses and unusual administrative activities in Azure.
What should you use to monitor the activities, and what should you use to integrate Azure with Microsoft Defender XDR? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area

Answer:

Explanation:

NEW QUESTION: 191
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.
Where can you store data from the LinkedIn connector?
A. a Microsoft OneDrive for Business folder
B. a Microsoft SharePoint Online document library
C. a Microsoft 365 mailbox
D. Azure Files
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin-data?view=o365-worldwide

NEW QUESTION: 192
You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?
A. Microsoft Store for Business
B. Apple Business Manager
C. Apple iTunes Store
D. Apple Configurator
Answer: (SHOW ANSWER)

Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios

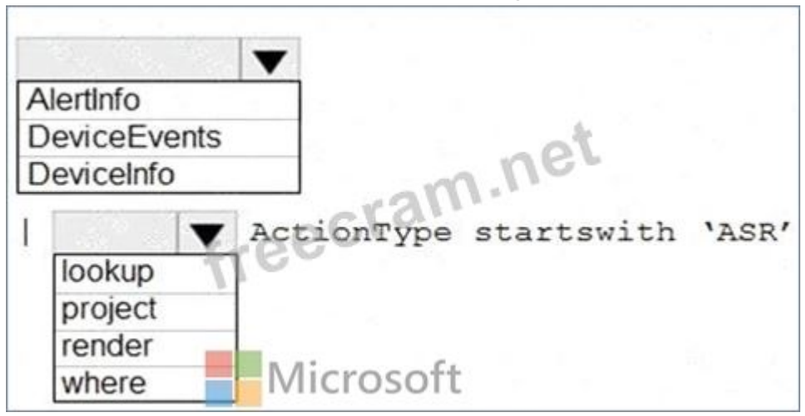
NEW QUESTION: 193
You have a Microsoft 365 tenant that contains two users named User1 and User2. You create the alert policy shown in the following exhibit.

User2 runs a script that modifies a file in a Microsoft SharePoint Online library once every four minutes and runs for a period of two hours.
How many alerts will User1 receive?
A. 10
B. 25
C. 2
D. 5
Answer: (SHOW ANSWER)

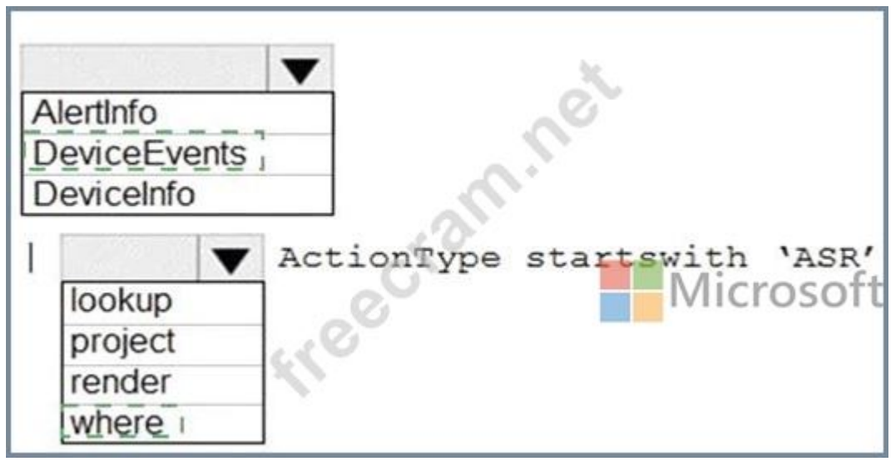
NEW QUESTION: 194
You use Microsoft Defender for Office 365.
You plan to automate an attack simulation campaign.
Any users that fail the simulation must take additional training based on the simulation results.
What is the maximum number of days the training will be available to the users after the simulation?
A. 15

B. 7
C. 30
D. 45
Answer: (SHOW ANSWER)

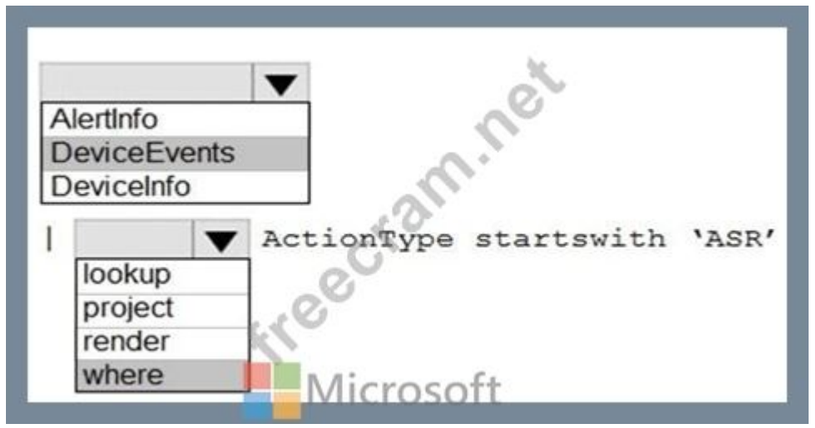
NEW QUESTION: 195
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.
You plan to attack surface reduction (ASR) rules for the Windows 10 devices.
You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.
You need to find the ASR rules that match the activities on the devices.
How should you complete the Kusto query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



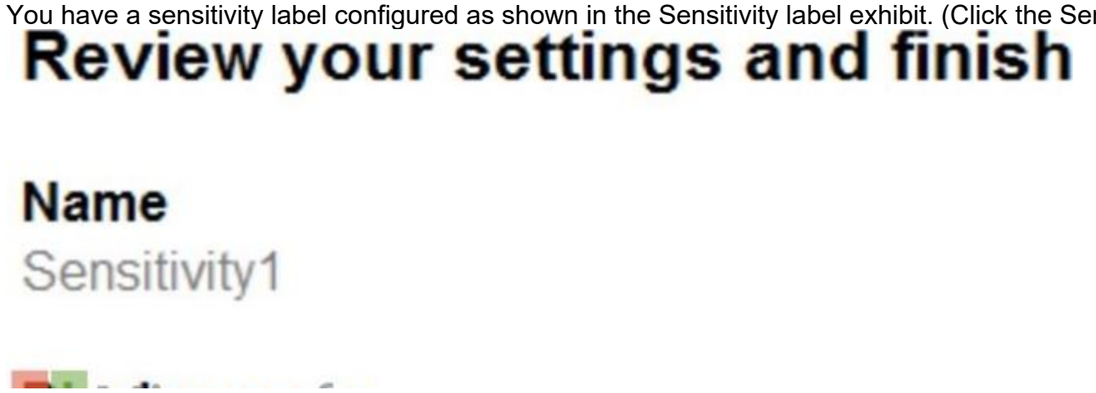
Explanation:



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

NEW QUESTION: 196
You have a Microsoft 365 ES subscription.
You integrate Microsoft Defender for Endpoint with Microsoft Intune.
You need to ensure that devices automatically onboard to Defender for Endpoint when they are enrolled In Intune.
Solution: You create an endpoint detection and response (EDR) policy.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 197
You have a Microsoft 365 E5 tenant.
You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)



Display name
Sensitivity1

Description for users
Sensitivity1

Scope
File.Email

Encryption

Content marking
Watermark: Watermark
Header: Header

Auto-labeling

Group settings

Site settings

Auto-labeling for database columns
None

You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)

Auto-labeling policy

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

Rules for auto-applying this label
Exchange email 1 rule

Mode

On

Comment

A user sends an email that contains the components shown in the following table.

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

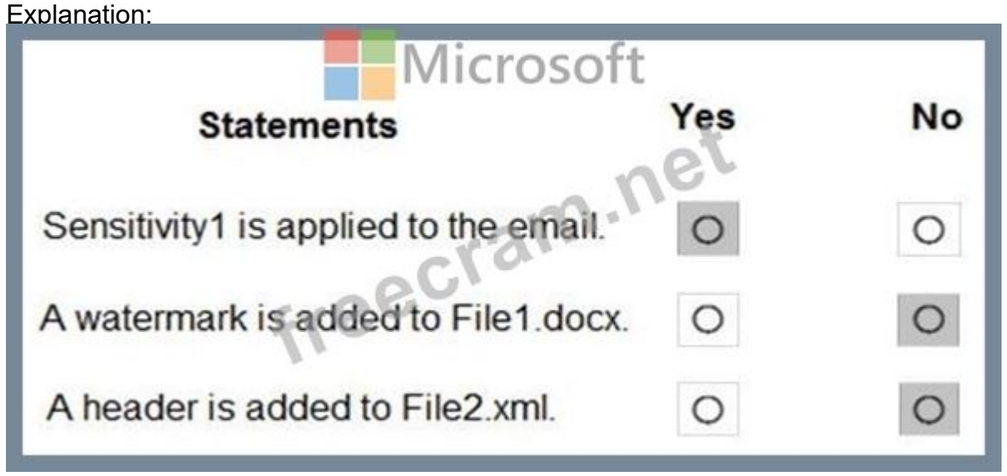
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

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: 198

You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

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

Per-user multifactor authentication is configured to use 131.107.5.0/24 as trusted IPs.

The tenant contains the named locations shown in the following table.

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

You create a conditional access policy that has the following configurations:

* Users: All users
* Target resources assignment: App1
* Conditions: Include all trusted locations
* Grant access: Require multi-factor authentication

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

NOTE: Each correct selection is worth one point.

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:

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.	○	◉

NEW QUESTION: 199

You have a Microsoft 365 subscription that contains more than 2,000 guest users.

You need to ensure that when guest users are added to Microsoft 365 groups in the subscription, their membership is validated by the group owner every 30 days.

What should you configure?

A. retention policies
B. group expiration policies
C. Conditional Access policies
D. access reviews
Answer: (SHOW ANSWER)

NEW QUESTION: 200
You are evaluating the use of multi-factor authentication (MFA).
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	◉	○
Users must use the Microsoft Authenticator app to complete MFA.	○	◉
After registering, users must use MFA for every sign-in.	○	◉

NEW QUESTION: 201
HOTSPOT
You have a Microsoft 365 E3 subscription.
You plan to launch Attack simulation training for all users.
Which social engineering technique and training experience will be available? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

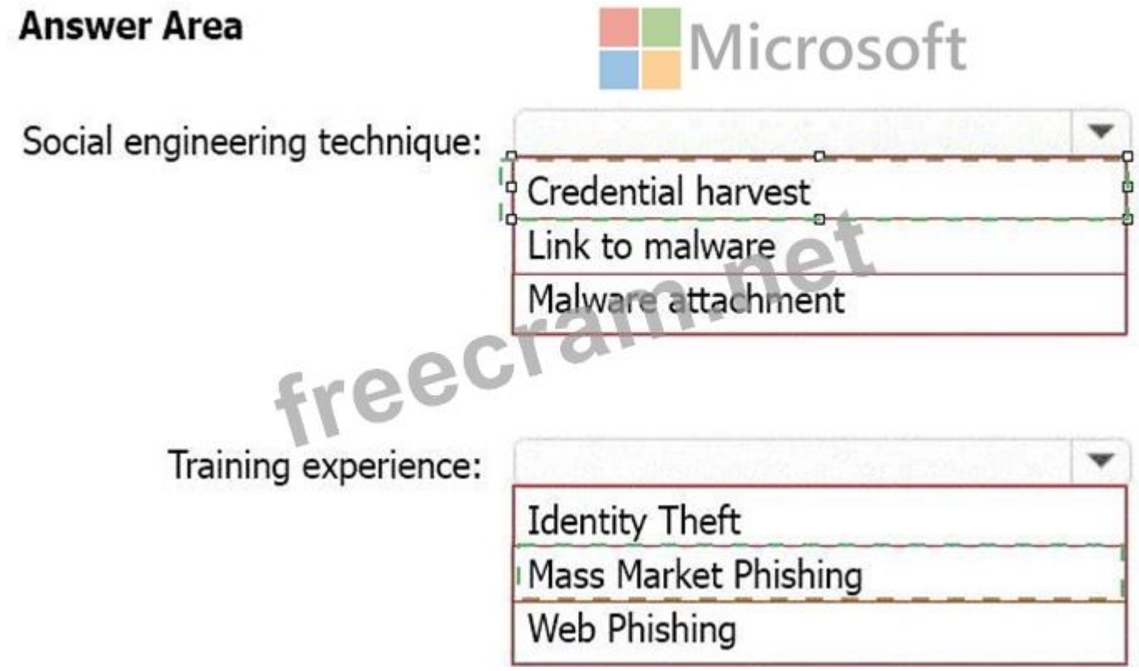
Answer Area

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

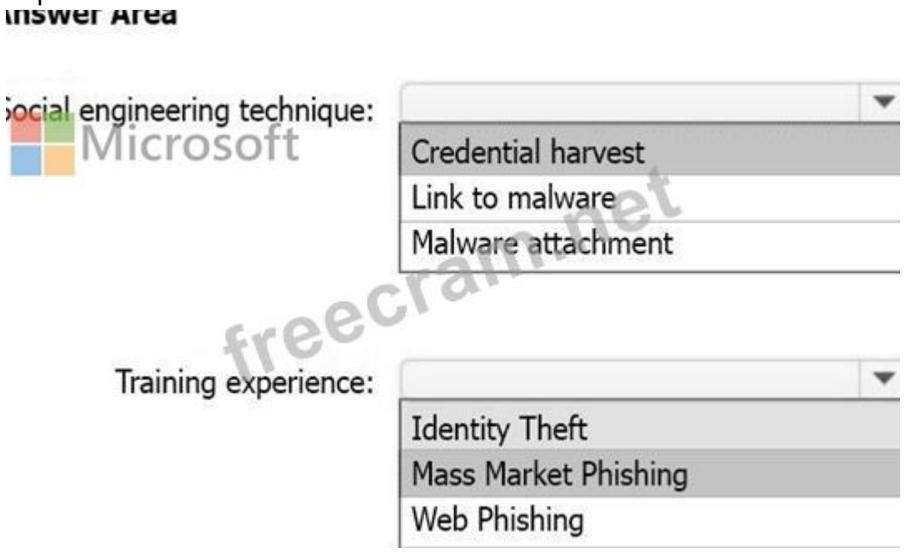
Training experience:
- Identity Theft
- Mass Market Phishing
- Web Phishing

Answer:

Answer Area



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: 202

You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).

The tenant has two Compliance Manager assessments as shown in the following table.

Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Regulations
Establish a threat intelligence program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline
Establish and document a configuration management program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline

You perform the following actions:

For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.

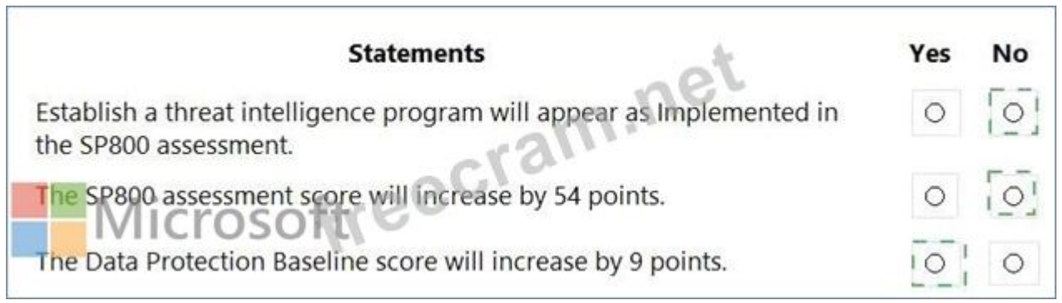
Enable multi-factor authentication (MFA) for all users.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

Answer:



Explanation:

Reference:

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

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

NEW QUESTION: 203

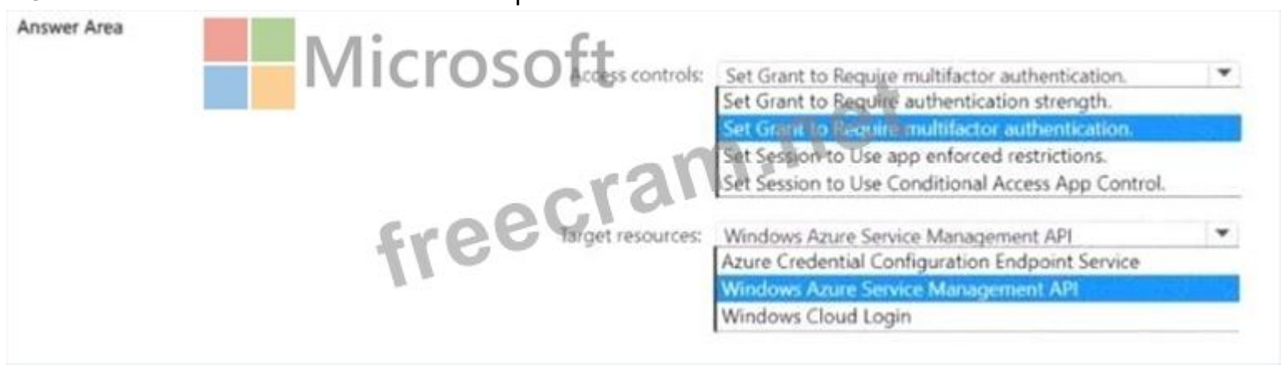
You have a Microsoft 365 E5 subscription.

You plan to create a Conditional Access policy named Policy.

You need to ensure that only Passwordless MFA authentication methods are used when administrators attempt to access the Azure portal. Azure PowerShell. or Azure Command-Line Interlace (CU).

How should you configure Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



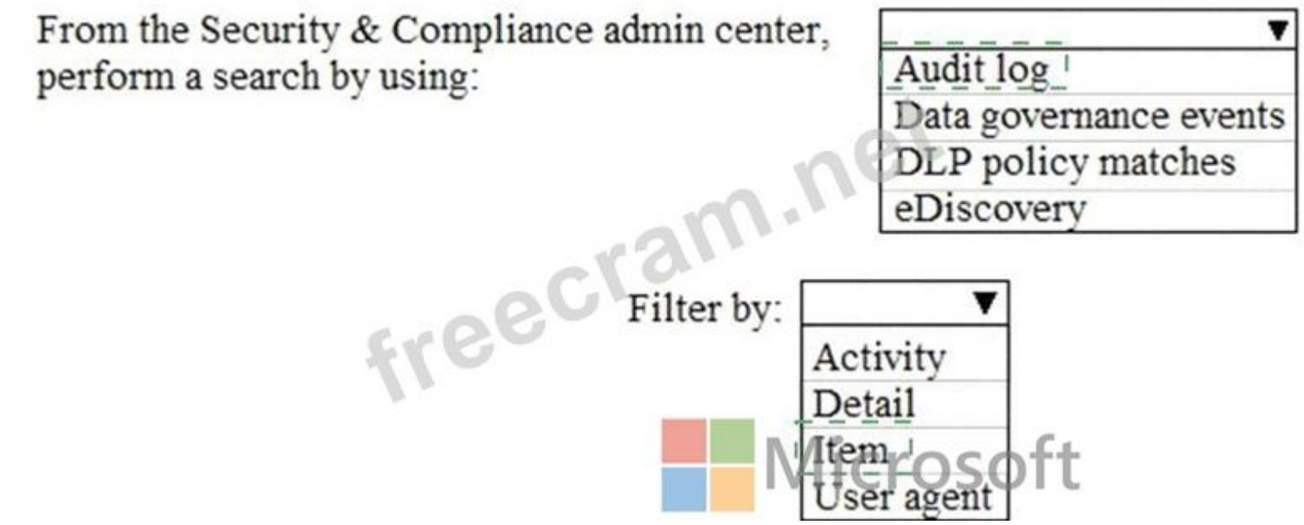
Answer:

Explanation:

NEW QUESTION: 204

You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

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: 205
You have a Microsoft 365 E5 tenant.
You configure sensitivity labels.
Users report that the Sensitivity button is unavailability in Microsoft Word for the web. The sensitivity button is available in Word for Microsoft 365.
You need to ensure that the users can apply the sensitivity labels when they use Word for the web.
What should you do?
A. Create an auto-labeling policy
B. Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive.
C. Copy policies from Azure information Protection to the Microsoft 365 Compliance center
D. Publish the sensitivity labels.

Answer: (SHOW ANSWER)

NEW QUESTION: 206

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

You have labels in Microsoft 365 as shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

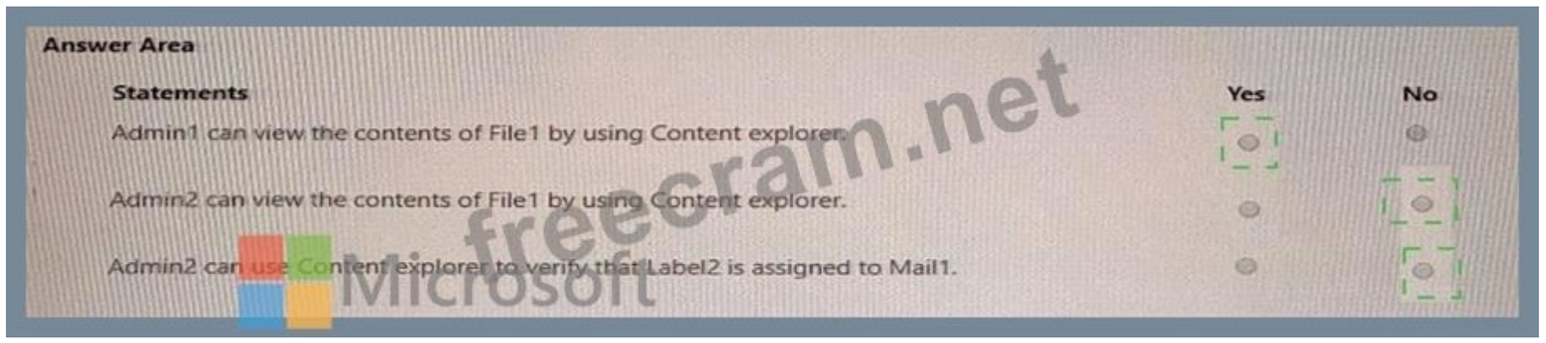
The content in Microsoft 365 is assigned labels as shown in the following table.

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

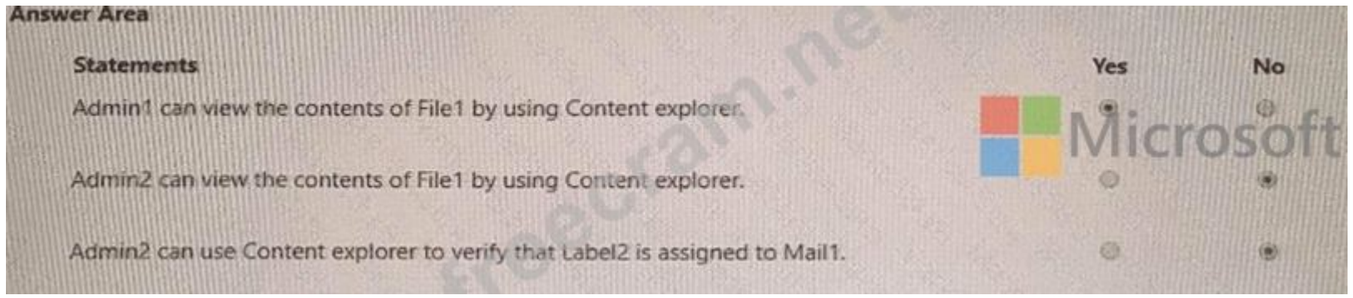
You have labels In Microsoft 365 as shown in the following table.

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

Answer:



Explanation:



NEW QUESTION: 207

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

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

The devices are managed by using Microsoft Intune.

You plan to use a configuration profile to assign the Delivery Optimization settings.

Which devices will support the settings?

A. Device1, Device3, and Device4

B. Device1 only

C. Device1 and Device4

D. Device1, Device2, Device3, and Device4

Answer: (SHOW ANSWER)

NEW QUESTION: 208

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.

Does this meet the goal?

A. Yes

B. No

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: 209
You have a Microsoft 365 subscription.
You suspect that several Microsoft Office 365 applications or services were recently updated.
You need to identify which applications or services were recently updated.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. From the Microsoft 365 admin center review the Service health blade
B. From the Microsoft 365 admin center, review the Message center blade.
C. From the Microsoft 365 admin center review the Products blade.
D. From the Microsoft 365 Admin mobile agg, review the messages.
Answer: (SHOW ANSWER)
The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where Microsoft posts official messages with information including new and changed features, planned maintenance, or other important announcements.
The messages displayed in the Message center can also be viewed by using the Office 365 Admin mobile app.
Reference:
https://docs.microsoft.com/en-us/office365/admin/manage/message-center
https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app

NEW QUESTION: 210
Your company has a Microsoft 365 subscription.
you implement sensitivity Doris for your company.
You need to automatically protect email messages that contain the word Confidential m the subject line.
What should you create?

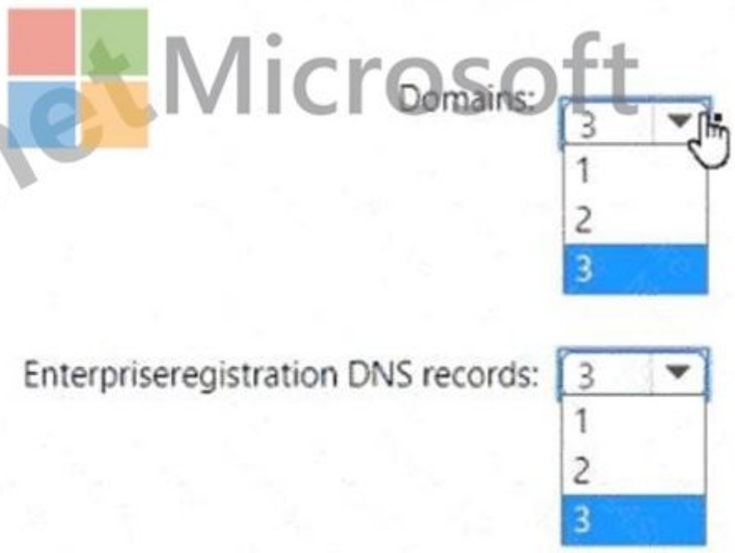
A. a message Dace from the Microsoft 365 security center
B. a sharing policy from the Exchange admin center
C. a mail flow rule from the Exchange admin center
D. a data loss prevention (DLP) policy from the Microsoft 365 compliance center
Answer: (SHOW ANSWER)

NEW QUESTION: 211
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
You plan to perform device discovery and authenticated scans of network devices.
You install and register the network scanner on a device named Device1.
What should you do next?
A. Connect Defender for Endpoint to Microsoft Intune.
B. Download and run an onboarding package.
C. Create an assessment job.
D. Apply for Microsoft Threat Experts - Targeted Attack Notifications.
Answer: (SHOW ANSWER)

NEW QUESTION: 212
You have a Microsoft 365 subscription that uses a third-party multifactor authentication (MFA) product.
While reviewing Microsoft Secure Score, you discover that there are no points listed for the Ensure multifactor authentication is enabled for all users recommendation.
You need to ensure that you receive all the points for the recommendation. The solution must minimize administrative effort.
What should you do?
A. Modify the status of the recommendation.
B. Deploy a Microsoft Defender for Identity sensor.
C. Modify the recommendation tags.
D. Configure a data connector.
Answer: (SHOW ANSWER)

NEW QUESTION: 213
You work at a company named Contoso, Ltd.
Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.
Contoso purchases a company named Fabrikam, Inc.
Contoso plans to add the following domains to the Microsoft 365 subscription:
* fabrikam.com
* east.fabrikam.com
* west.contoso.com
You need to ensure that the devices in the new domains can register by using Autodiscover.
How many domains should you verify, and what is the minimum number of enterprise registration DNS records you should add? To answer, select the appropriate options in the answer area.

Answer Area

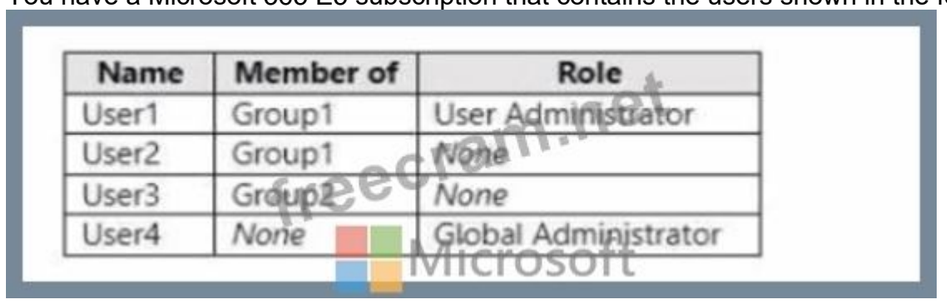


Answer:

Explanation:

NEW QUESTION: 214

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



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

You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.

Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.

NOTE; Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 215

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the departments Microsoft SharePoint Online site. What should you do?

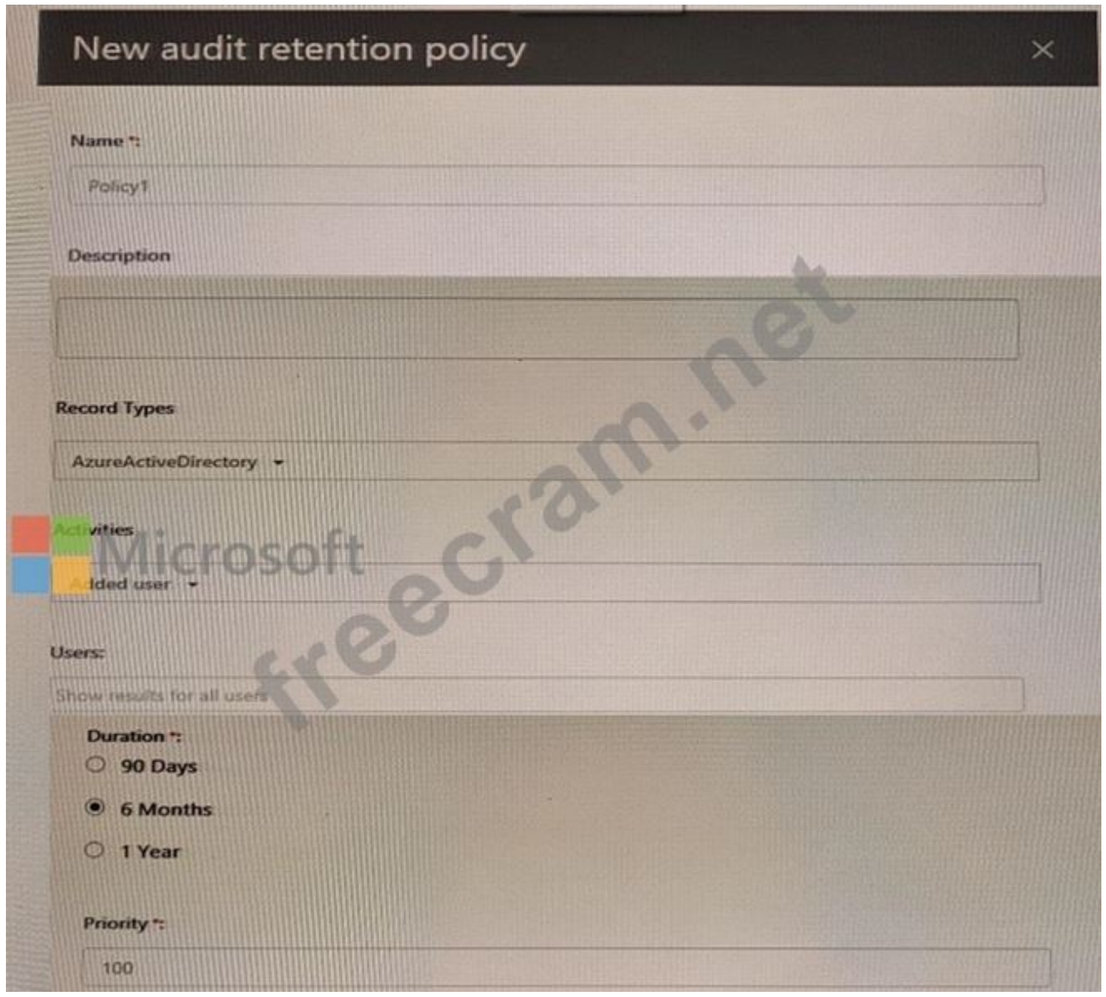
A. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
B. From the SharePoint Online site, create an alert.
C. From the Microsoft 365 Defender portal, create an alert policy.
D. From the SharePoint Online admin center, modify the sharing settings.
Answer: (SHOW ANSWER)

NEW QUESTION: 216
You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.
You need to remove User1 from the Restricted entities list.
What should you use?

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

NEW QUESTION: 217
You have a Microsoft 365 E5 subscription that has auditing turned on. The subscription contains the users shown in the following table.

Name	License
Admin1	Microsoft Office 365 E5
Admin2	*None*



You plan to create a new user named User1.

How long will the user creation audit event be available if Admin1 or Admin2 creates User1? To answer, select the appropriate options in the answer area.

Each correct selection is worth one point.

Answer:

NEW QUESTION: 218

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

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

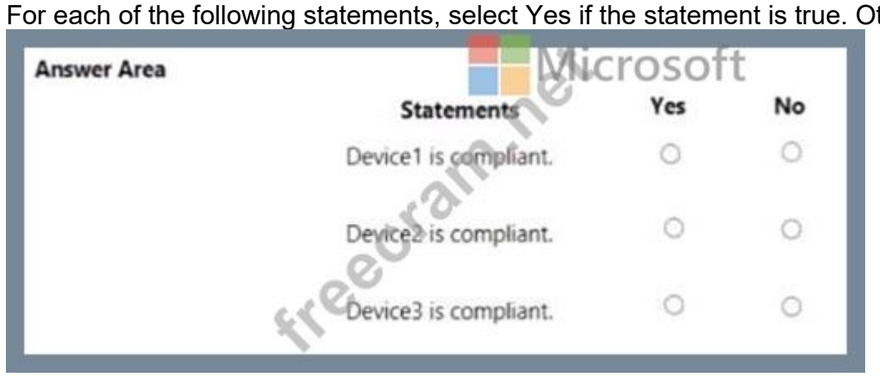
The device compliance policies in Endpoint Manager are configured as shown in the following table.

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

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group3
Policy2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

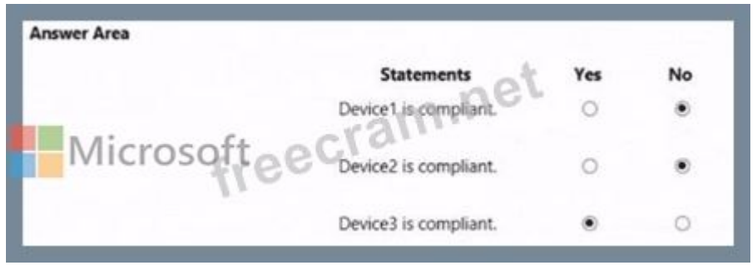


Answer:

Answer Area

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

Explanation:



NEW QUESTION: 219

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

You plan to create a Conditional Access policy that will use GPS-based named locations.

Which users can the policy protect?

A. Userl1 only

B. User1 and User3 only

C. User2 and User4 only

D. User1, User2, User3, and User4

Answer: (SHOW ANSWER)

NEW QUESTION: 220

You have a Microsoft 365 E5 subscription that contains two users named Admin1 and Admin2.

All users are assigned a Microsoft 365 Enterprise E5 license and auditing is turned on.

You create the audit retention policy shown in the exhibit. (Click the Exhibit tab.)

After Policy1 is created, the following actions are performed:

Admin1 creates a user named User1.

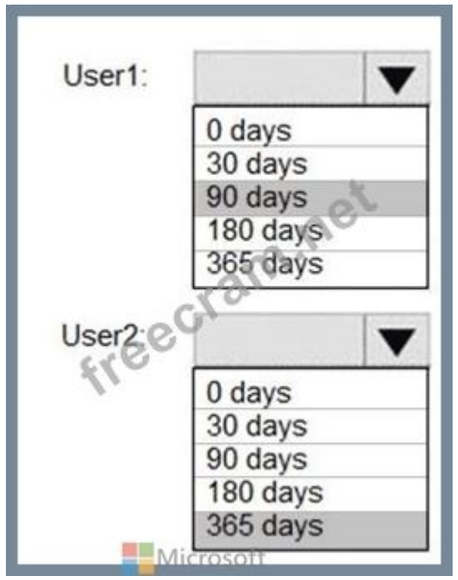
Admin2 creates a user named User2.

How long will the audit events for the creation of User1 and User2 be retained? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:



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

NEW QUESTION: 221
You have a Microsoft 365 E5 subscription.
You plan to implement records management and enable users to designate documents as regulatory records.
You need to ensure that the option to mark content as a regulatory record is visible when you create retention labels.
What should you do first?
A. Configure custom detection rules.
B. Create an Exact Data Match (EDM) schema.
C. Run the Sec-RegulacoryComplianceUI cmdlet.
D. Run the Sec-LabelPolicy cmdlet.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide

NEW QUESTION: 222
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

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 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
This is not a permissions issue so you do not need to assign the Security Reader role.
The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

NEW QUESTION: 223
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert occurs only on a Windows 10 device. The solution must minimize administrative effort.
What should you do first?

A. From the Microsoft 365 admin center, create a mail-enabled security group.
B. From the Microsoft 365 Defender portal, create a device group.
C. From the Microsoft Endpoint Manager admin center, create a device category.
D. From the Azure Active Directory admin center, create a dynamic device group.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 224

You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.
In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

In Azure Active Directory (Azure AD), the Device settings are configured as shown in the following exhibit.

From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).
For each of the following statement, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 225

You have a Microsoft 365 E5 subscription.

You need to create a mail-enabled contact.

Which portal should you use?

A. the SharePoint admin center

B. the Microsoft 365 admin center

C. the Microsoft Purview compliance portal

D. the Microsoft Entra admin center

Answer: (SHOW ANSWER)

NEW QUESTION: 226

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

All the devices in your organization are onboarded to Microsoft Defender for Endpoint.

You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.

What should you do?

A. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.

B. From Alerts queue, create a suppression rule and assign an alert.

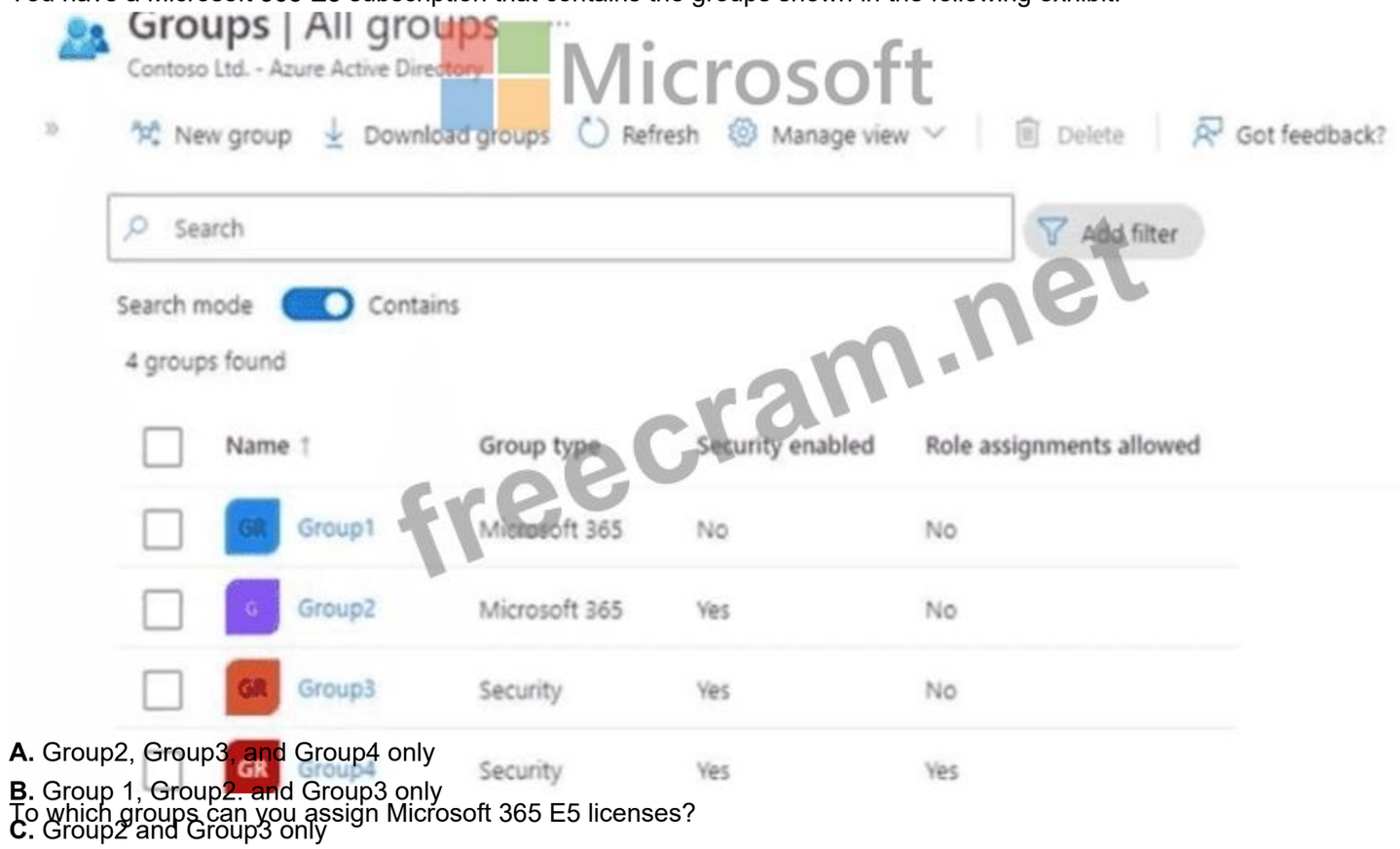
C. From Advanced hunting, create a query and a detection rule.

D. From the Microsoft Purview compliance portal, create an audit log search.

Answer: (SHOW ANSWER)

NEW QUESTION: 227
You have a Microsoft 365 E5 subscription.
You plan to create an anti-malware policy named Policy1.
You need to ensure that Policy1 can detect malicious email messages that were already delivered to a user's mailbox.
What should you do in the Microsoft Defender portal?
A. Configure a quarantine policy.
B. Enable zero-hour auto purge (ZAP).
C. Enable enhanced filtering.
D. Modify the common attachments filter.
Answer: (SHOW ANSWER)

NEW QUESTION: 228
You have a Microsoft 365 E5 subscription that contains the groups shown in the following exhibit.



To which groups can you assign Microsoft 365 E5 licenses?
A. Group2, Group3, and Group4 only
B. Group 1, Group2. and Group3 only
C. Group2 and Group3 only

D. Group! and Group2 only
E. Group3 and Group4 only
Answer: (SHOW ANSWER)

NEW QUESTION: 229
You have a Microsoft 365 subscription.
You register two applications named App1 and App2 to Azure AD.
You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?
A. From the Microsoft Entra admin center, create a conditional access policy
B. From the Microsoft 365 admin center, configure the Modem authentication settings.
C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.
D. From Multi-Factor Authentication, configure the service settings.
Answer: (SHOW ANSWER)
Use Conditional Access policies
If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication

NEW QUESTION: 230
You need to configure the information governance settings to meet the technical requirements.
Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 231

You need to configure Microsoft Entra Connect Sync to support the planned changes for the Montreal Users and Seattle Users OUs.

What should you do?

A. From PowerShell, run the Start-ADSyncSyncCycle cmdlet.

B. From the Microsoft Entra Connect wizard, select Customize synchronization options.

C. From the Microsoft Entra Connect wizard, select Manage federation.

D. From PowerShell, run the Add-ADSyncConnectorAttributeInclusion cmdlet.

Answer: (SHOW ANSWER)

NEW QUESTION: 232

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2. You plan to configure a data loss prevention (DLP) strategy that meets the following requirements:

* Members of Group1 must be prevented from sharing documents that contain credit card numbers.

* Members of Group2 must be prevented from sharing documents that are classified as internal by Microsoft Purview Information Protection.

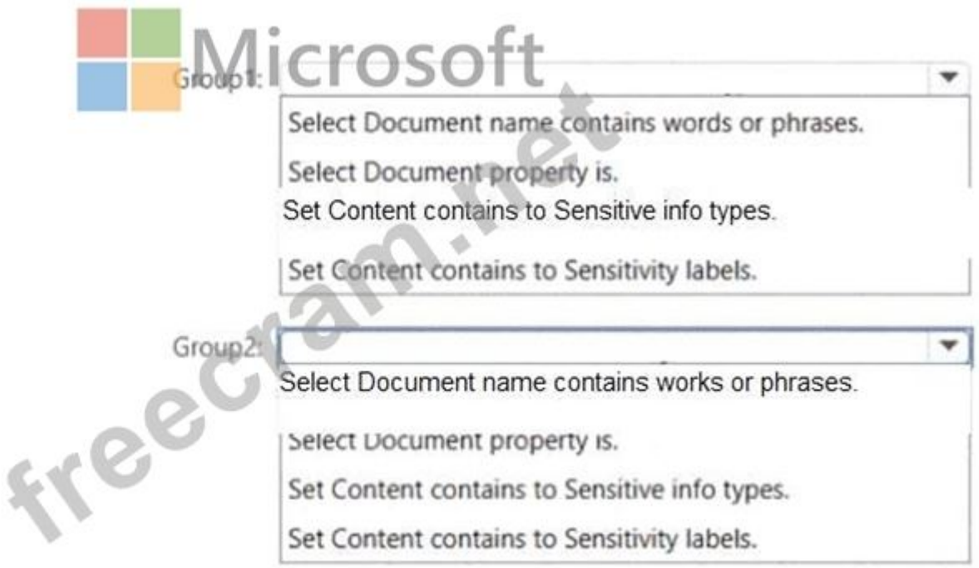
* The solution must minimize administrative effort

You need to create a DLP policy for each group.

Which condition should you add to each DLP policy rule for each group? To answer, select the appropriate options in the answer area.

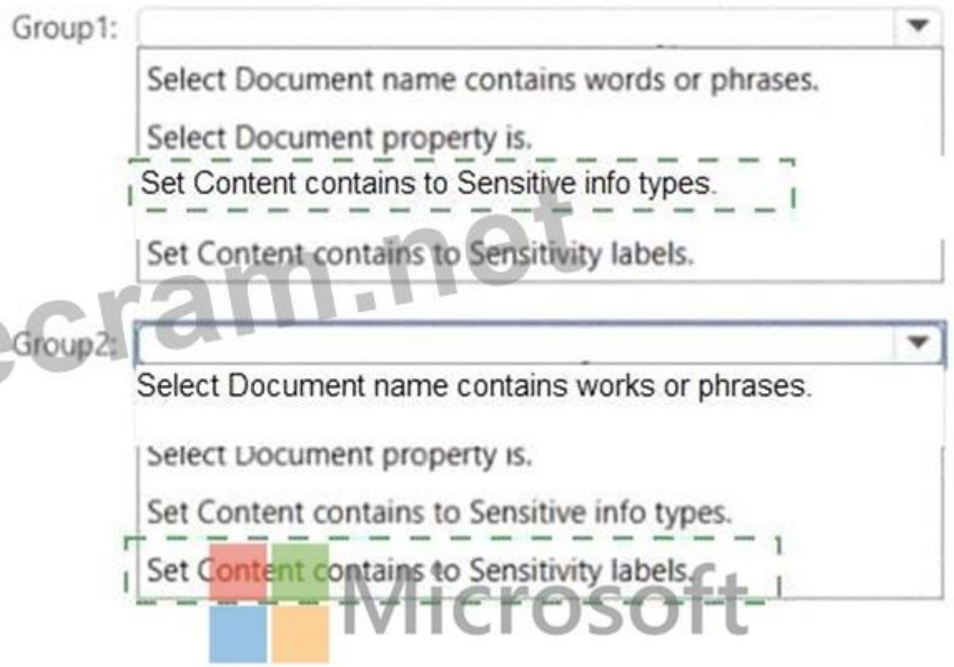
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

Answer Area

NEW QUESTION: 233
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
A Built-in protection preset security policy is applied to the subscription.
Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. Safe Links
B. Anti-malware
C. Anti-spam
D. Safe Attachments
E. Anti-phishing
Answer: (SHOW ANSWER)

NEW QUESTION: 234
You have a Microsoft 365 E5 subscription that uses Endpoint security.
You need to create a group and assign the Endpoint Security Manager role to the group.
Which type of group can you use?
A. security only
B. mail-enabled security, Microsoft 365, and security only
C. Microsoft 365 only
D. distribution, mail-enabled security, Microsoft 365, and security
E. mail-enabled security and security only
Answer: (SHOW ANSWER)

NEW QUESTION: 235
Your network contains an Active Directory forest.
You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
* Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
* User passwords must be 10 characters or more.
Solution: Implement pass-through authentication and configure Microsoft Entra Password protection. Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

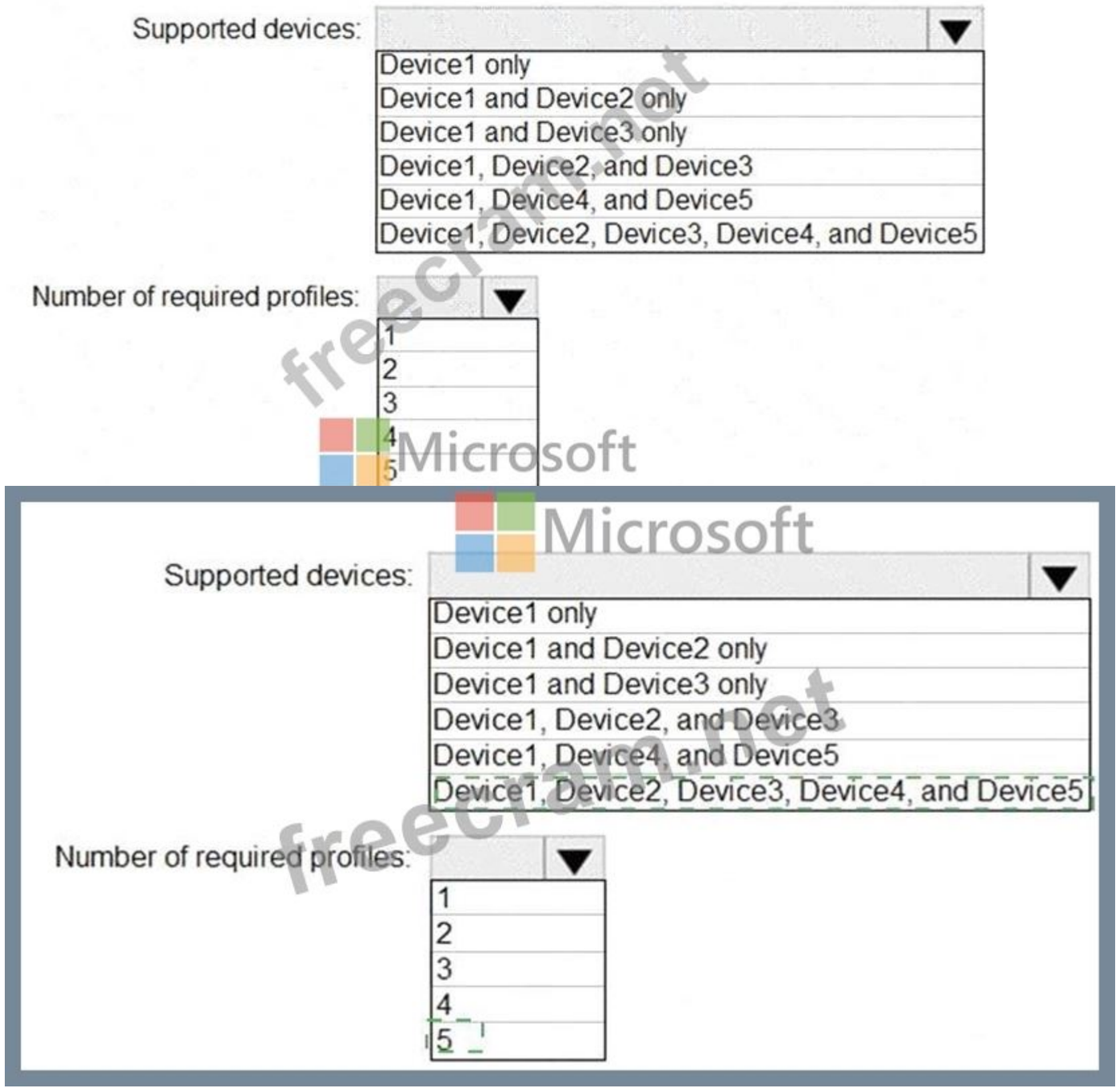
NEW QUESTION: 236

You plan to implement the endpoint protection device configuration profiles to support the planned changes.

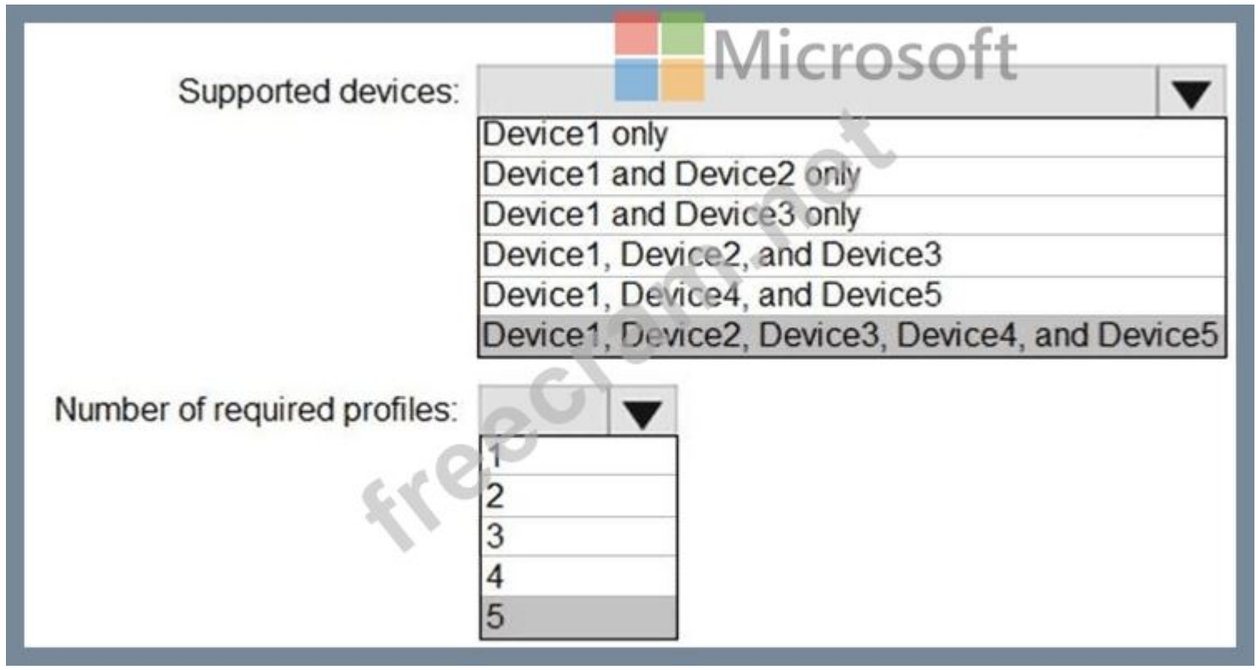
You need to identify which devices will be supported, and how many profiles you should implement.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Explanation:



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

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: 237
You have a Microsoft 365 E5 subscription.
You plan to configure Privileged Identity Management (PIM) for the User Administrator role in Microsoft Entra, You need to ensure that a user can make a role assignment request for the User Administrator role only during the next six months. How should you configure the assignment?
A. Set Allow permanent active to assignment Yes
B. Set Assignment type to Eligible
C. Set Assignment type to Active.
D. Set Allow permanent eligible assignment to Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 238
You have a Microsoft 365 E5 subscription that contains devices onboarded to Microsoft Defender for Endpoint. You integrate Microsoft Defender for Cloud Apps with Defender for Endpoint. You need identify which cloud apps and services were used most during the last 30 days What should you do?
A. Generate a Cloud Discovery snapshot report.
B. Create a threat analytics alert notification.
C. Generate a monthly security summary report
D. Generate a Cloud Discovery executive report
Answer: (SHOW ANSWER)

NEW QUESTION: 239
You have a Microsoft 365 E5 subscription.

Users have the devices shown in the following table.

Name	Platform	Owner	Enrolled in Microsoft Endpoint Manager
Device1	Android	User1	Yes
Device2	Android	User1	No
Device3	iOS	User1	No
Device4	Windows 10	User2	Yes
Device5	Windows 10	User2	No
Device6	iOS	User2	Yes

On which devices can you manage apps by using app configuration policies in Microsoft Endpoint Manager?

A. Device1, Device4, and Device6

B. Device2, Device3, and Device5

C. Device1, Device2, Device3, and Device6

D. Device1, Device2, Device4, and Device5

Answer: C (LEAVE A REPLY)

You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

NEW QUESTION: 240

You have a Microsoft 365 E5 subscription.

You are evaluating Microsoft Defender for Cloud Apps.

Which two types of policy rely on Conditional Access App Control? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. activity policy

B. access policy

C. app discovery policy

D. file policy

E. session policy

F. OAuth app policy

Answer: (SHOW ANSWER)

NEW QUESTION: 241

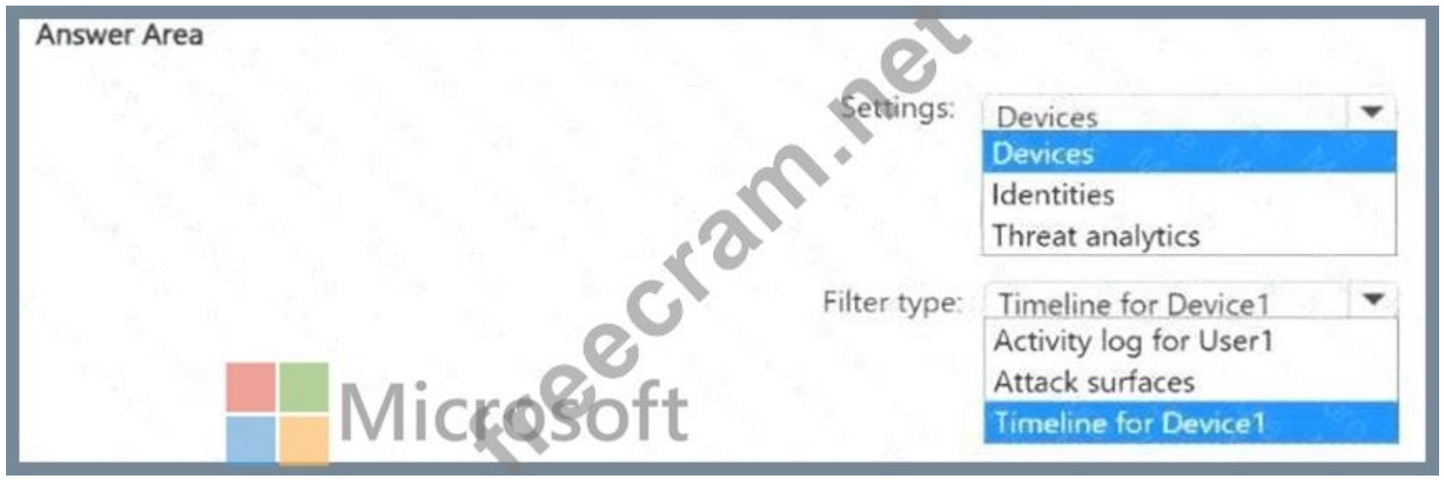
You have a Microsoft 365 E5 subscription that contains a user named User1. User1 has a Windows 11 device named Device1 that is onboarded to Microsoft Defender for Endpoint.

User1 reports that various files were deleted from Device1.

You need to create a filter to identify which service deleted the files.

Which settings should you configure, and which type of filter should you create in the Microsoft Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

NEW QUESTION: 242

You have a Microsoft 365 E5 subscription.

Your company s Microsoft Secure Score recommends the actions shown in the following exhibit.

You select Create Safe Links policies for email messages and change Status to Risk accepted in the Status & action plan settings.

How does the change affect the Secure Score?

A. decreases by 9 points

B. increases by 9 points

C. decreases by 1 point

D. increases by 1 point

E. remains the same

Answer: (SHOW ANSWER)

NEW QUESTION: 243
You have a Microsoft 365 E5 subscription that contains Windows 11 devices. All the devices are onboarded to Microsoft Defender for Endpoint.
You need to compare the configuration of the devices against industry standard benchmarks. What should you use?
A. Attack surface map
B. Events
C. Initiatives
D. Security baselines assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 244
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.

Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer:

Explanation:

Box 1: Yes

User1 is member of Group1.

User1 has MFA registered method of Microsoft Authenticater app (push notification) The Microsoft Authenticator authentication method policy is configured for Group1, registration is optional,

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

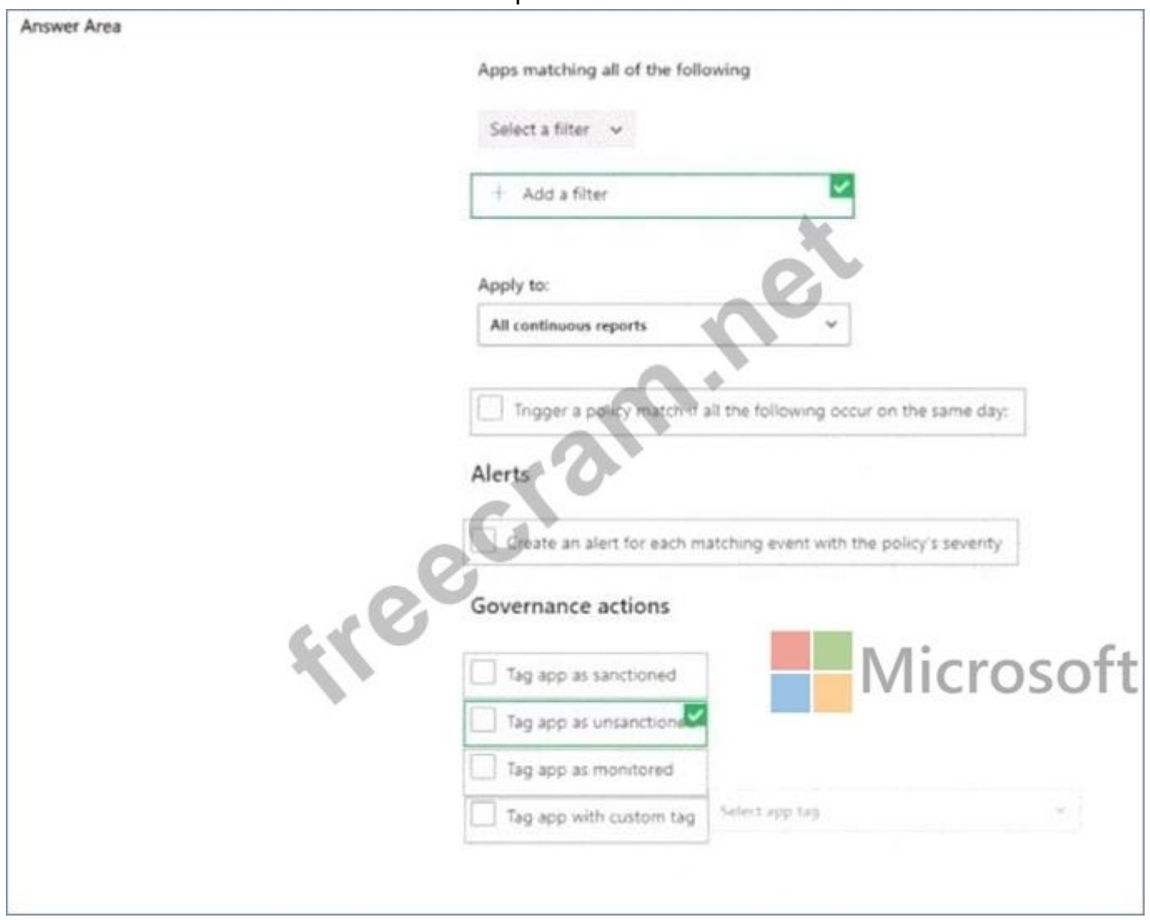
NEW QUESTION: 245
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Department
User1	Human resources
User2	Research
User3	Human resources
User4	Marketing

You need to configure group-based licensing to meet the following requirements:
To all users, deploy an Office 365 E3 license without the Power Automate license option.
To all users, deploy an Enterprise Mobility + Security E5 license.
To the users in the research department only, deploy a Power BI Pro license.
To the users in the marketing department only, deploy a Visio Plan 2 license.
What is the minimum number of deployment groups required?
A. 1
B. 2
C. 3
D. 4
E. 5
Answer: (SHOW ANSWER)
One for all users, one for the research department, and one for the marketing department.
Note: What are Deployment Groups?
With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers on-premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.
Reference:

https://devblogs.microsoft.com/devops/deployment-groups-is-now-generally-available-sharing-of-targets-and-more

NEW QUESTION: 246
You have a Microsoft 365 subscription.
You integrate Microsoft Defender for Cloud Apps with Microsoft Defender for Endpoint.
You need to create a policy to block users from accessing discovered apps that have a risk score of 4 or lower.
Which two settings should you configure? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area