Microsoft.MS-102.v2024-01-23.q169

Exam Code:	MS-102
Exam Name:	Microsoft 365 Administrator
Certification Provider:	Microsoft
Free Question Number:	169
Version:	v2024-01-23
# of views:	564
# of Questions views:	15771
https://www.freecram.net/torrent/Microsoft.MS-102.v2024-01-23.q169.html	

NEW QUESTION: 1
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant.
The tenant contains a group named Group1 and the users shown in the following table:

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

The tenant has a conditional access policy that has the following configurations:
Name: Policy1
Assignments:
- Users and groups: Group1
- Cloud aps or actions: All cloud apps
Access controls:
Grant, require multi-factor authentication
Enable policy: Report-only
You set Enabled Security defaults to Yes for the tenant.
For each of the following settings select Yes, if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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

Answer:

Explanation

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

Conditional Access policies can be enabled in report-only mode.

During sign-in, policies in report-only mode are evaluated but not enforced.

Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.

Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-onl

NEW QUESTION: 2

You have a Microsoft 365 E5 tenant.

You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.

Which two policies can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. a Microsoft Cloud App Security file policy

B. a data loss prevention (DLP) policy

C. a communication compliance policy

D. a sensitivity label policy

E. a retention label policy

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 3

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

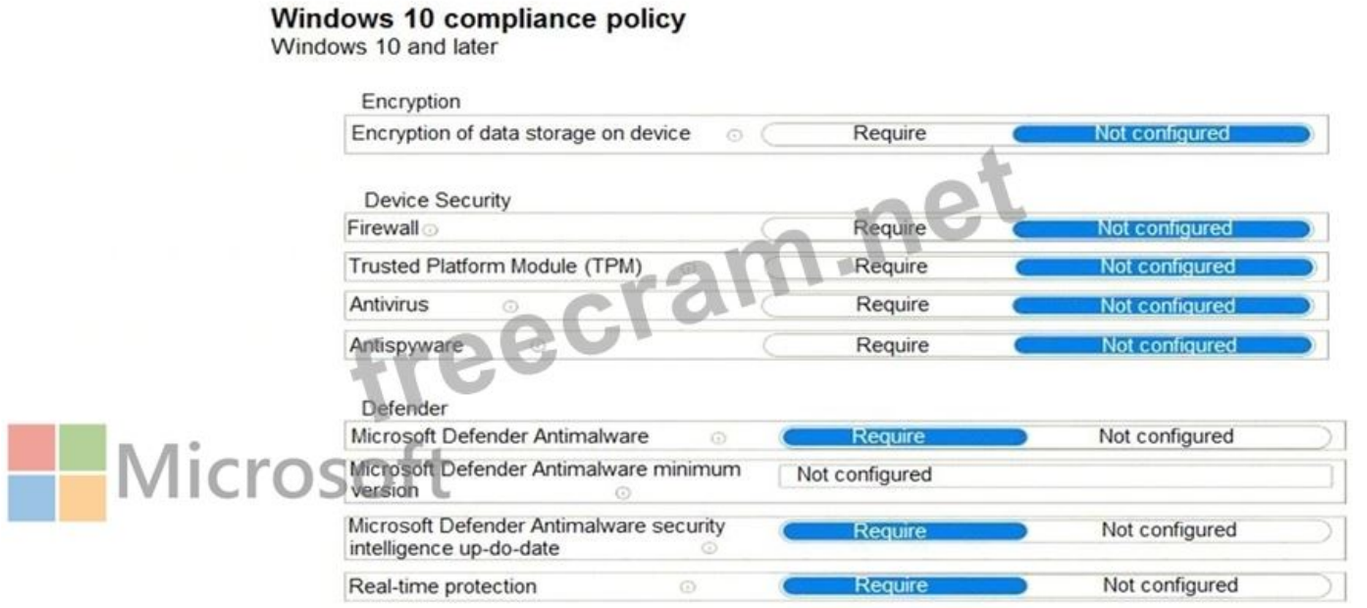
You deploy a third-party antivirus solution to the devices.

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

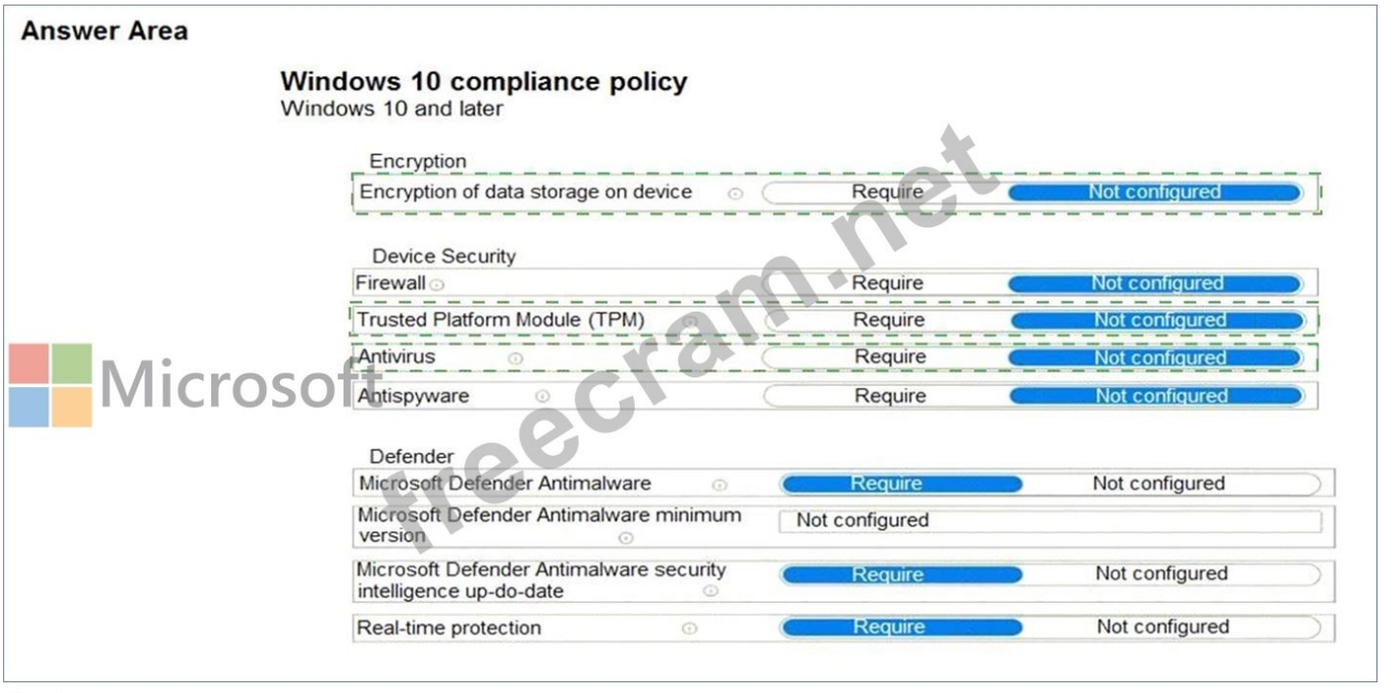
Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

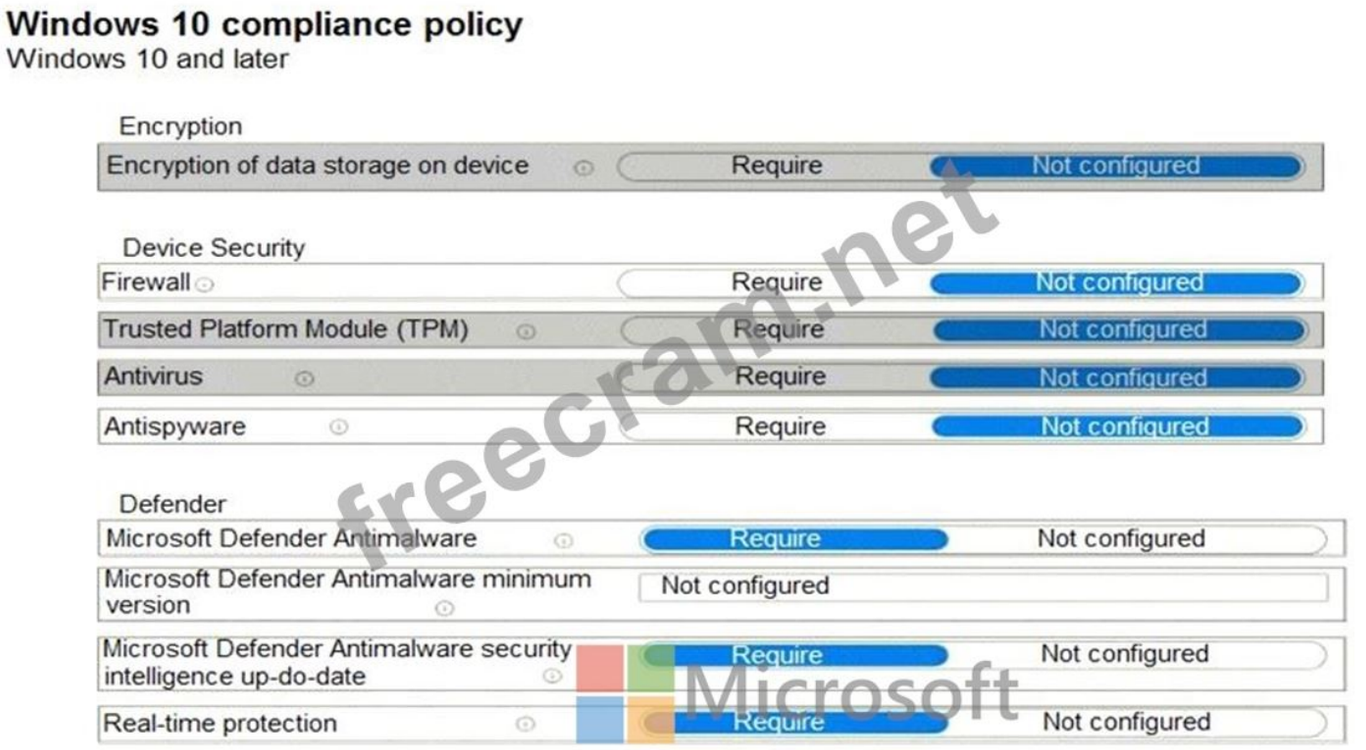


Answer:



Explanation

Graphical user interface Description automatically generated



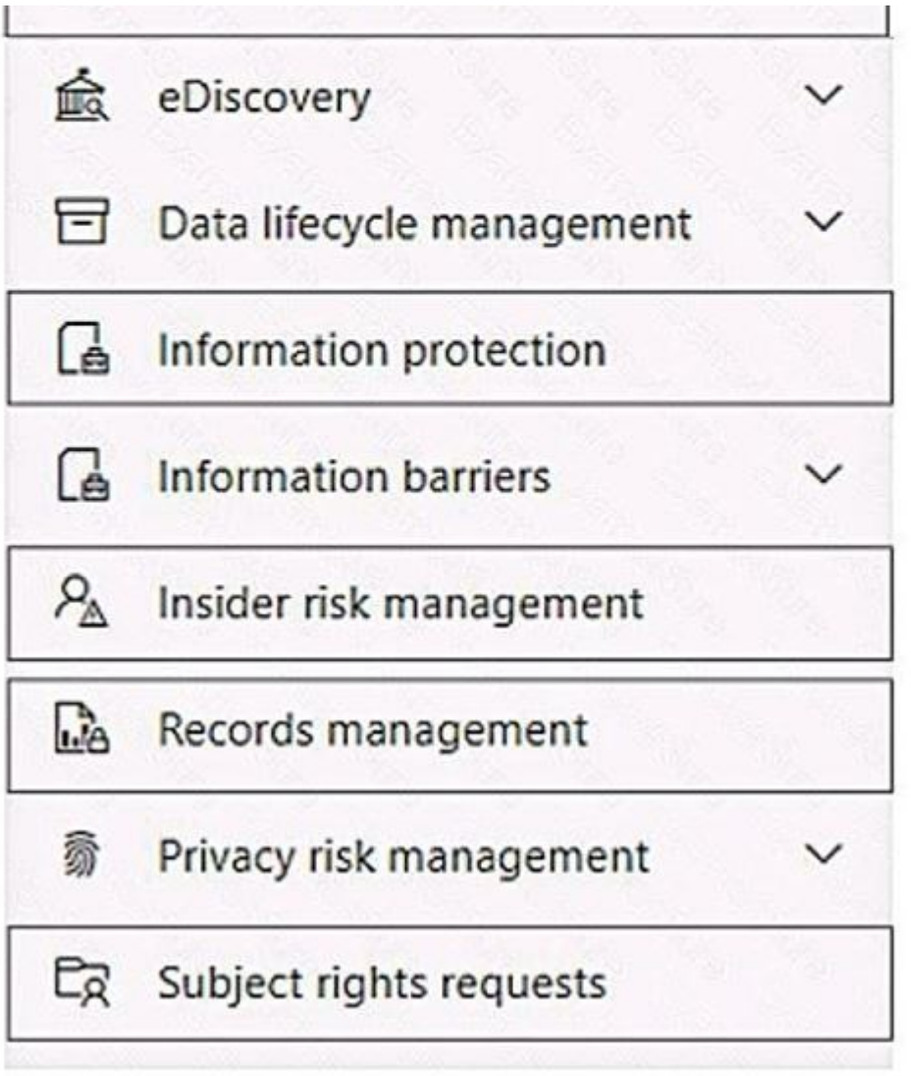
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

NEW QUESTION: 4
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 domain.
You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD.
Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
Explanation

The question states that "all the user account synchronizations completed successfully". Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

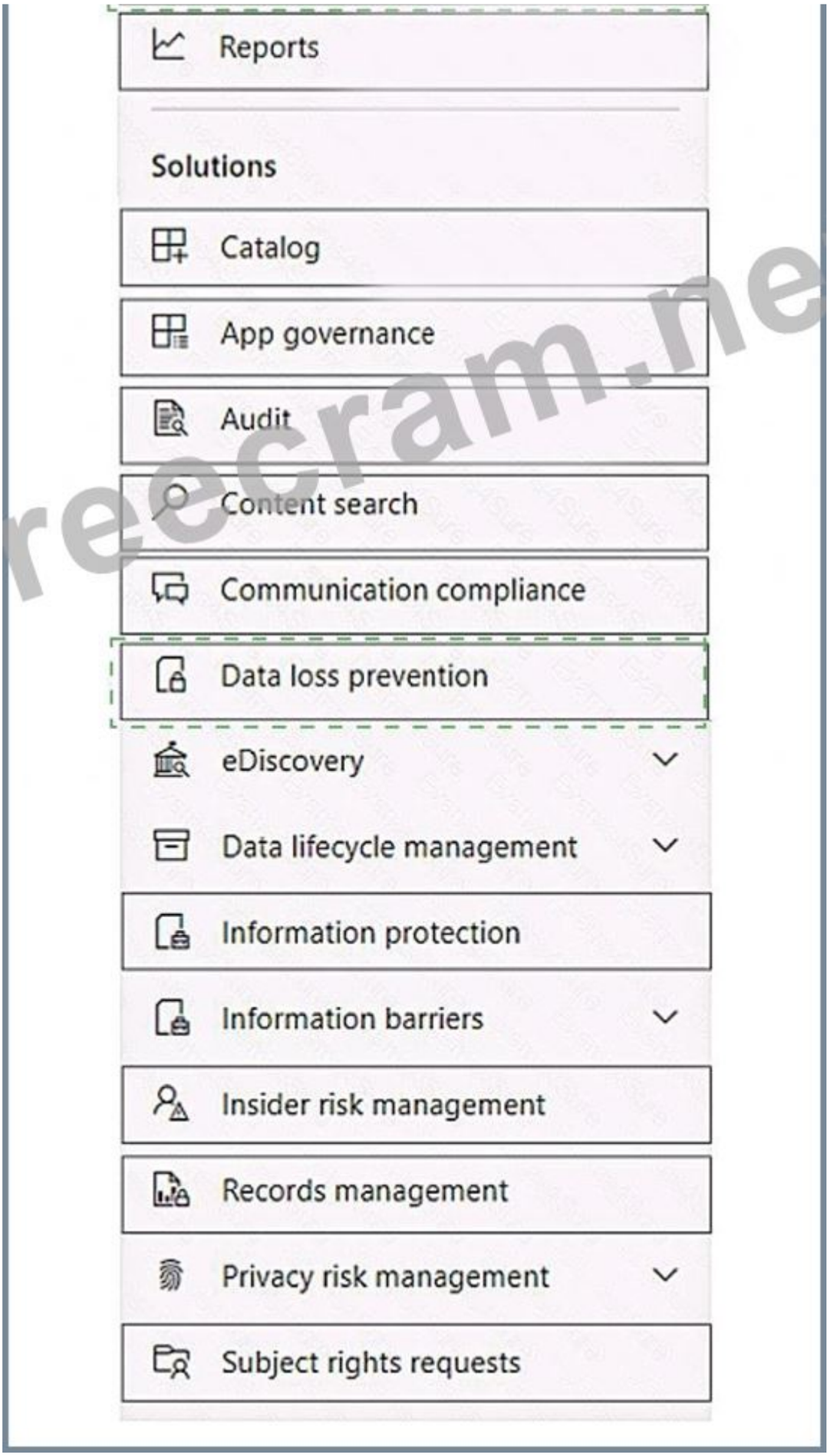
NEW QUESTION: 5
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel.
You need to perform the following tasks:
* Create a sensitive info type named SIT1 based on a regular expression.
* Add a watermark to all new documents that are matched by SIT1.
Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area


eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

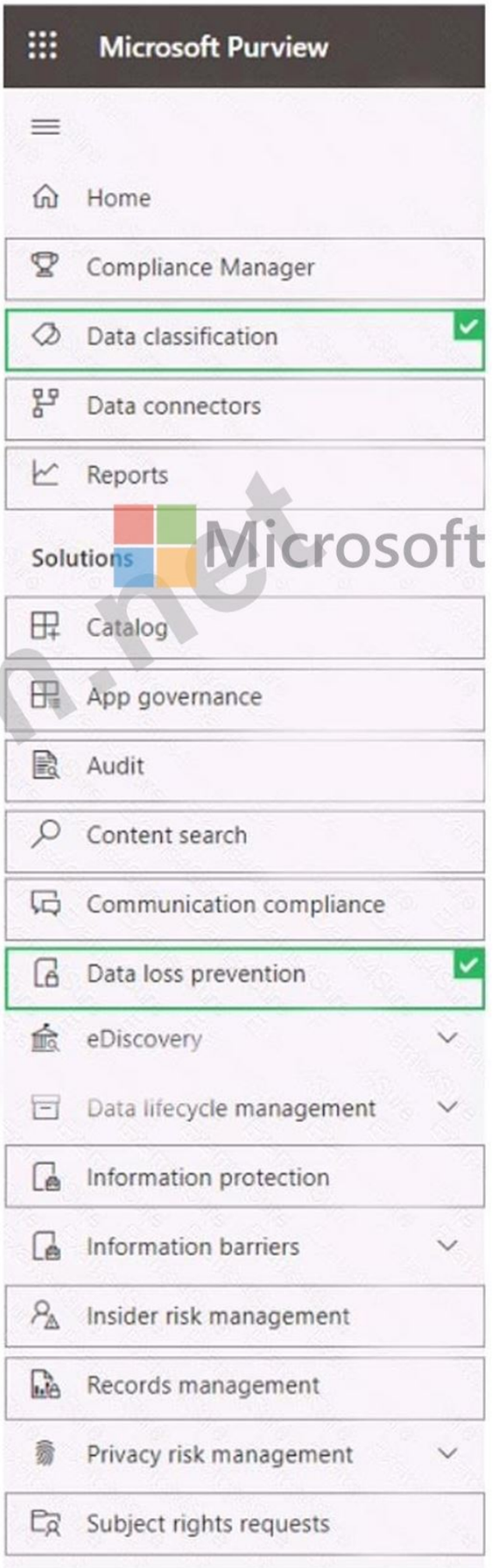
Answer:


Answer Area
Microsoft Purview
Home
Compliance Manager
Data classification
Data connectors
Microsoft



Explanation

Answer Area



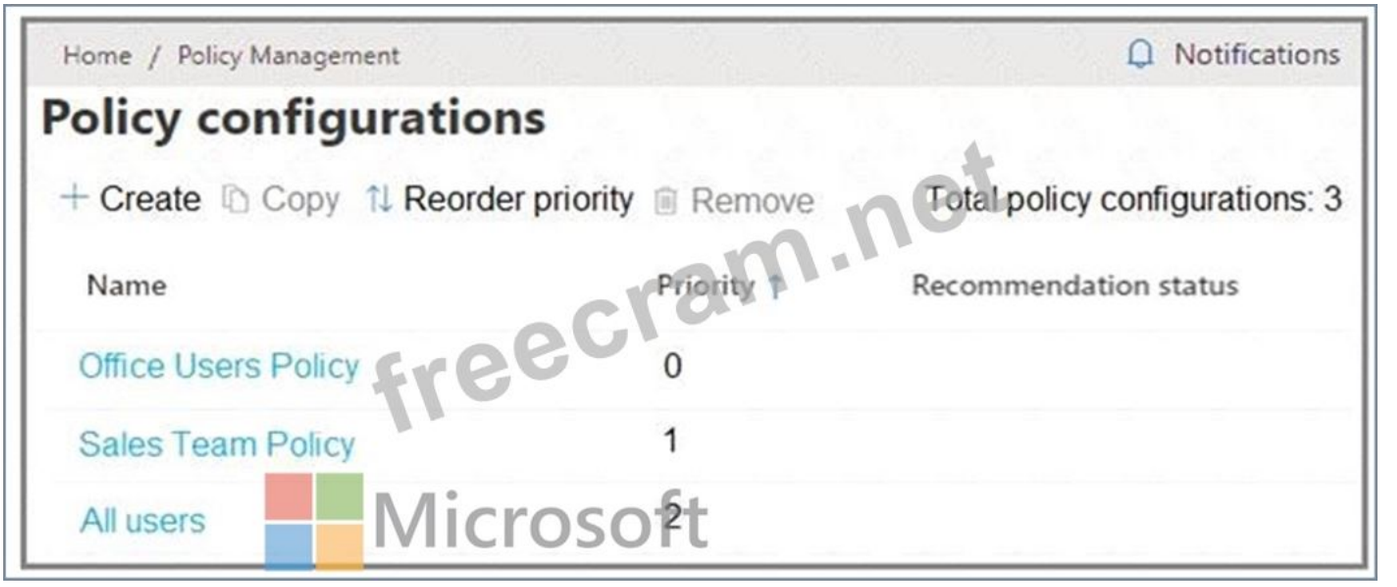
NEW QUESTION: 6
Your network contains three Active Directory forests. There are forests trust relationships between the forests.
You create an Azure AD tenant.
You plan to sync the on-premises Active Directory to Azure AD.
You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.
What should you include in the recommendation?
A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode
B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode
C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode
D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode
Answer: (SHOW ANSWER)
Explanation
Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

NEW QUESTION: 7
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 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-628bec

NEW QUESTION: 8
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.

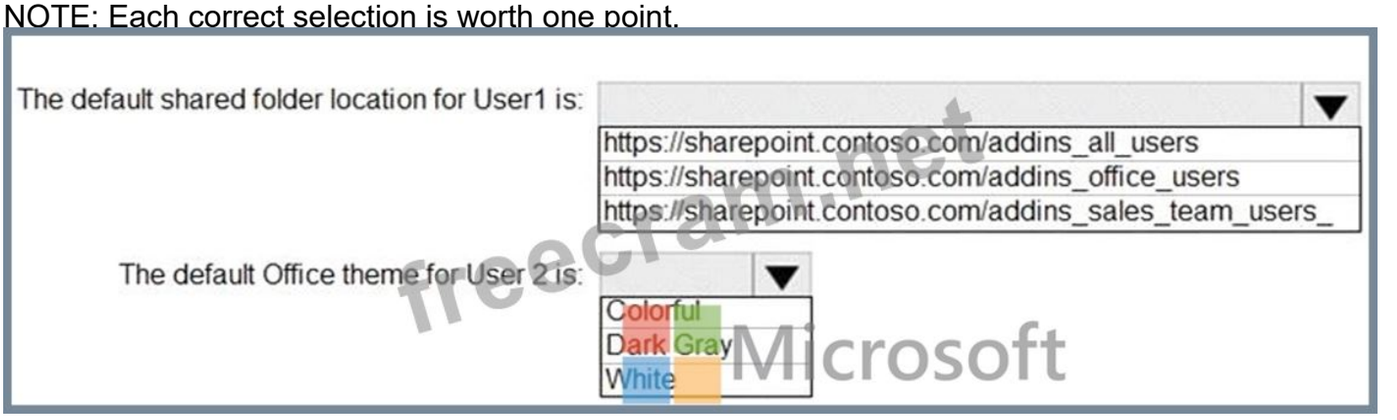


The policies use the settings shown in the following table.

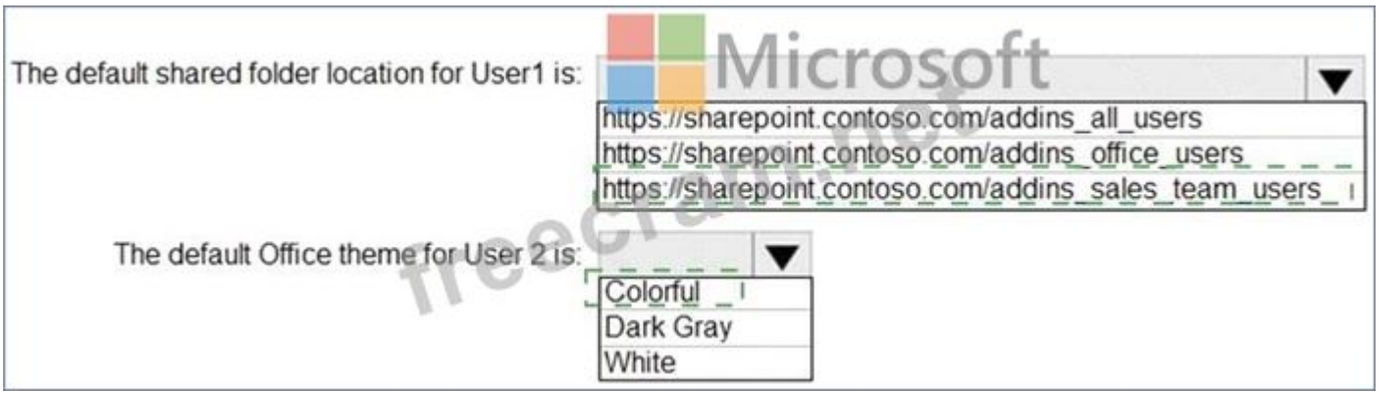
Policy	Default Shared Folder Location	Default Office Theme
All users	https://sharepoint.contoso.com/addins_all_users	Colorful
Office Users Policy	https://sharepoint.contoso.com/addins_office_users	White
Sales Team Policy	https://sharepoint.contoso.com/addins_sales_team_users_	Dark Gray

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.

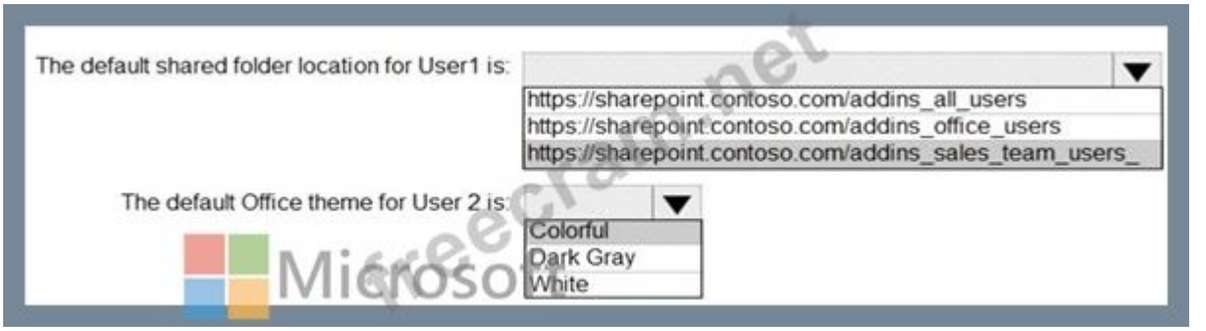


Answer:



Explanation

Table Description automatically generated



Reference:

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

NEW QUESTION: 9

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. User1 and User3 only

B. User2 and User4 only

C. Userl1 only

D. User1, User2. User3. and User4

Answer: (SHOW ANSWER)

NEW QUESTION: 10

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#

NEW QUESTION: 11

You have Windows 10 devices that are managed by using Microsoft Endpoint Manager.

You need to configure the security settings in Microsoft Edge.

What should you create in Microsoft Endpoint Manager?

A. an app configuration policy

B. an app

C. a device configuration profile

D. a device compliance policy

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

NEW QUESTION: 12

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. an activity policy

C. a file policy

D. an anomaly detection policy

Answer: D (LEAVE A REPLY)

NEW QUESTION: 13

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com.

You create a Microsoft Defender for identity instance Contoso.

The tenant contains the users shown in the following table.

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

You need to modify the configuration of the Defender for identify sensors.

Solutions: You instruct User4 to modify the Defender for identity sensor configuration.

Does this meet the goal?

A. No

B. Yes

Answer: (SHOW ANSWER)

NEW QUESTION: 14

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

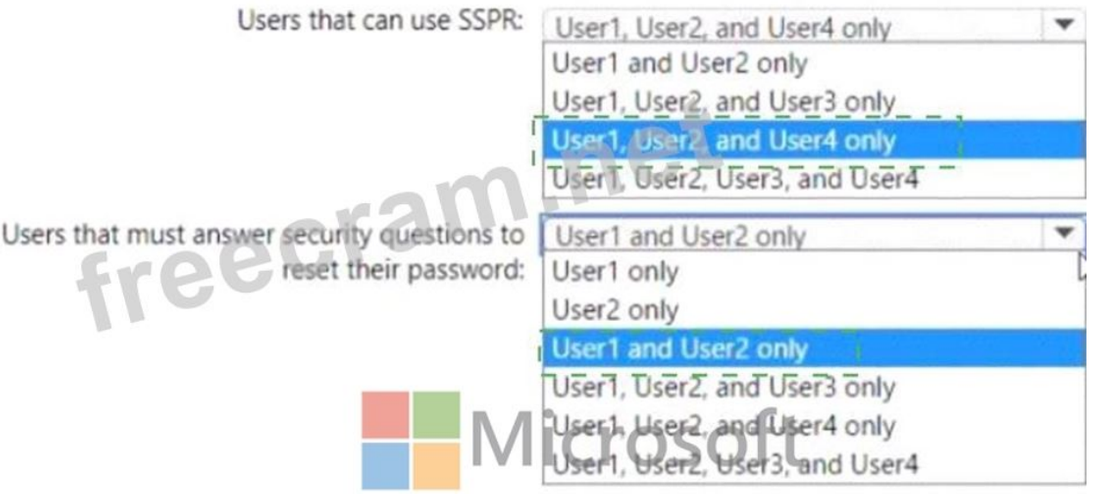
You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.

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:

Answer Area

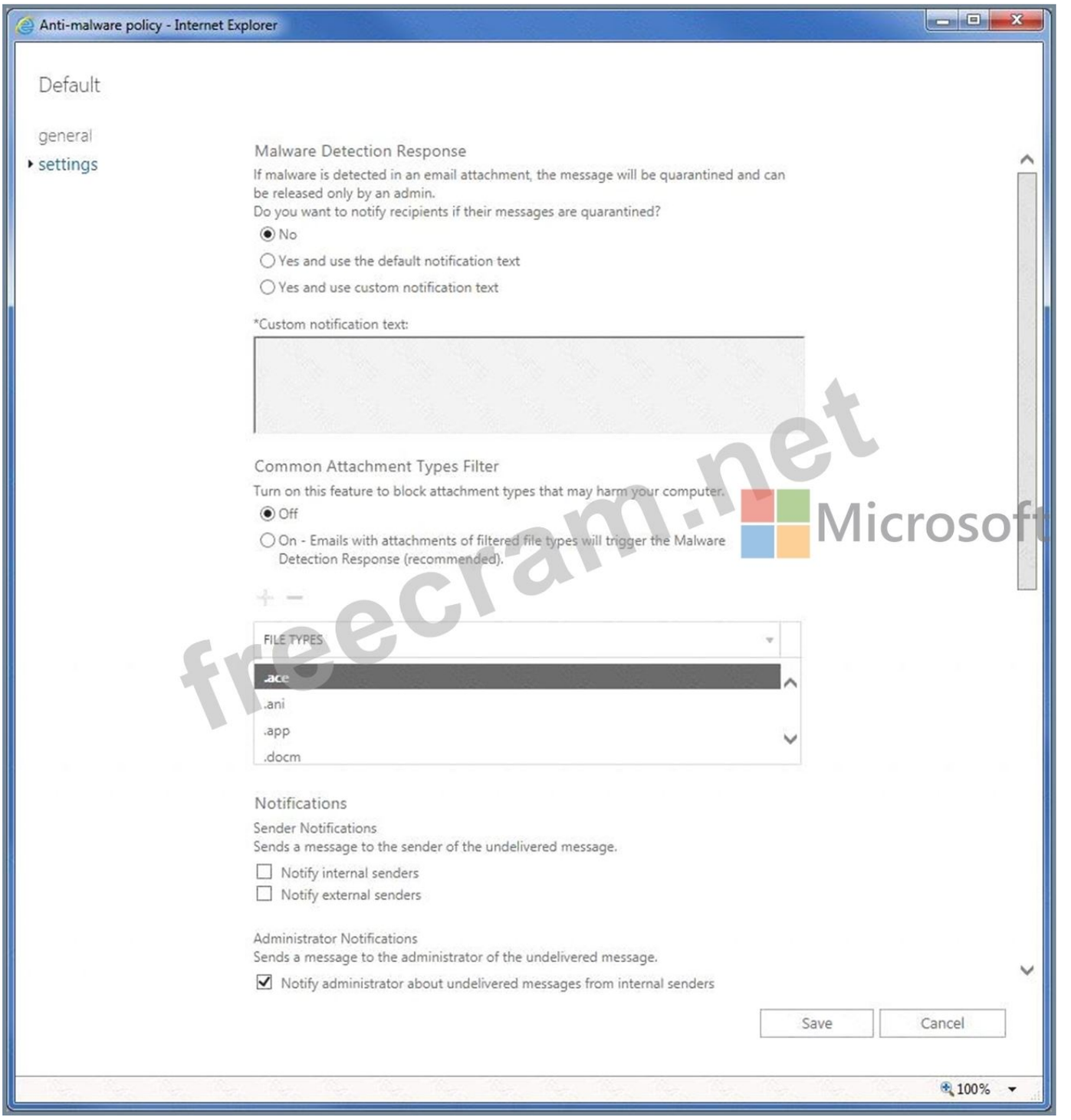


Explanation

NEW QUESTION: 15

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: C (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365

NEW QUESTION: 16

You have a Microsoft 365 tenant that has Enable Security defaults set to 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.

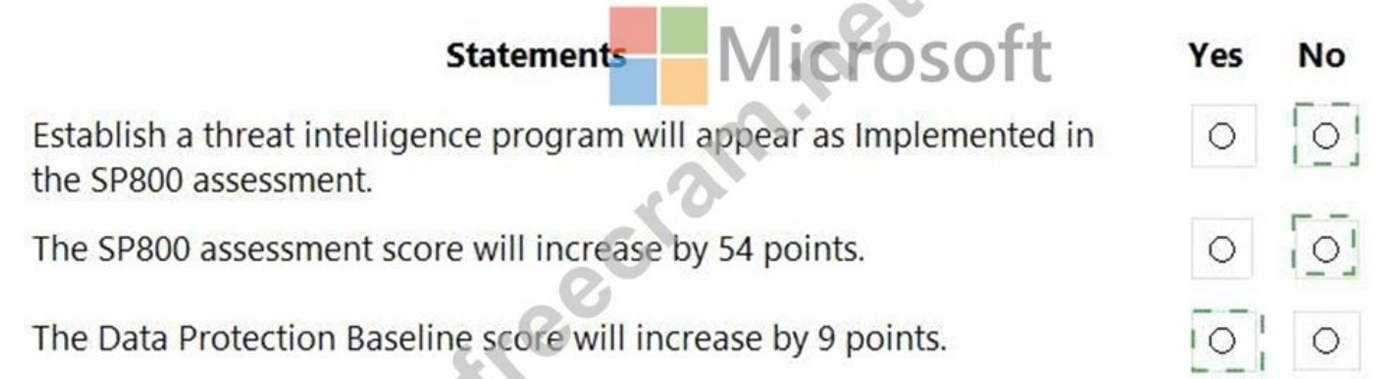
Enable multi-factor authentication (MFA) for all users.

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

NOTE: Each correct selection is worth one point.

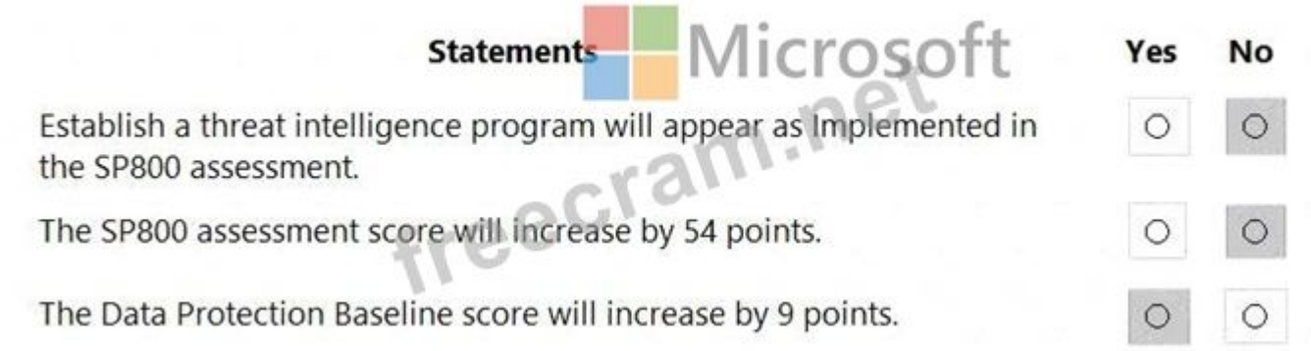
Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

Answer:



Explanation

Graphical user interface, text Description automatically generated



Reference:

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

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwid

NEW QUESTION: 17

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

* Retention period 7 years

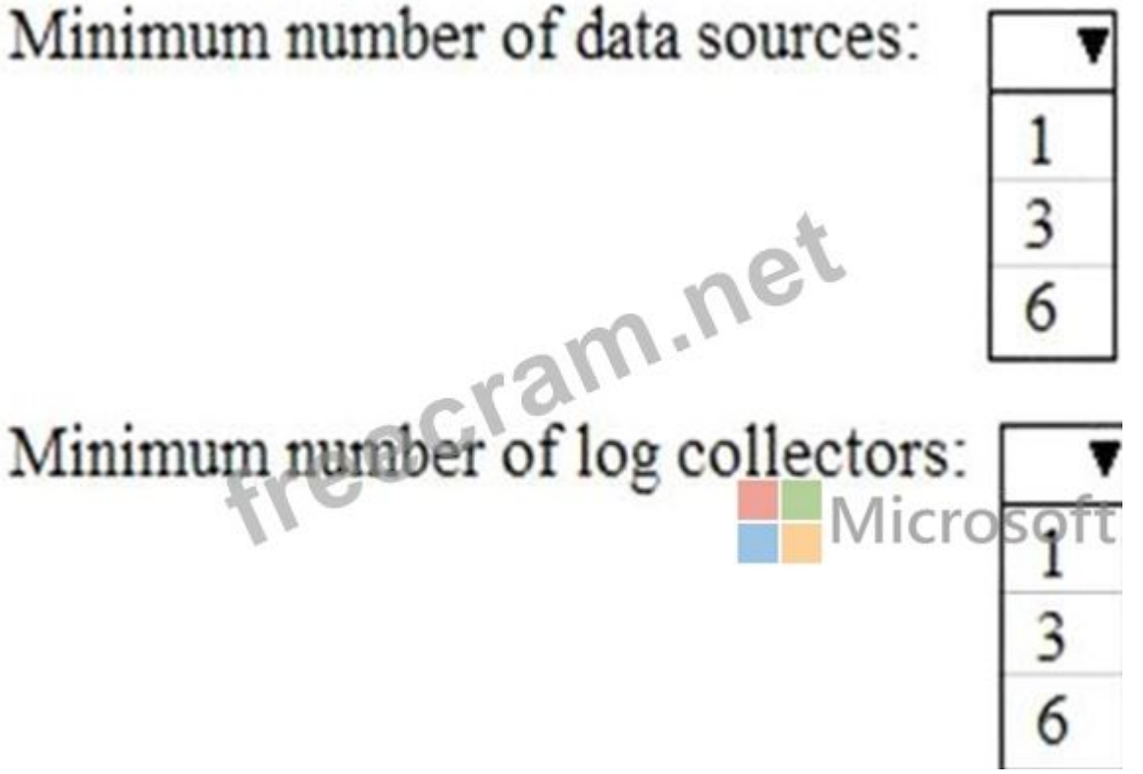
* Start the retention period bated on: When items were created

You need to prevent the removal of the label once the label K applied to a lie What should you select in the retention label settings?

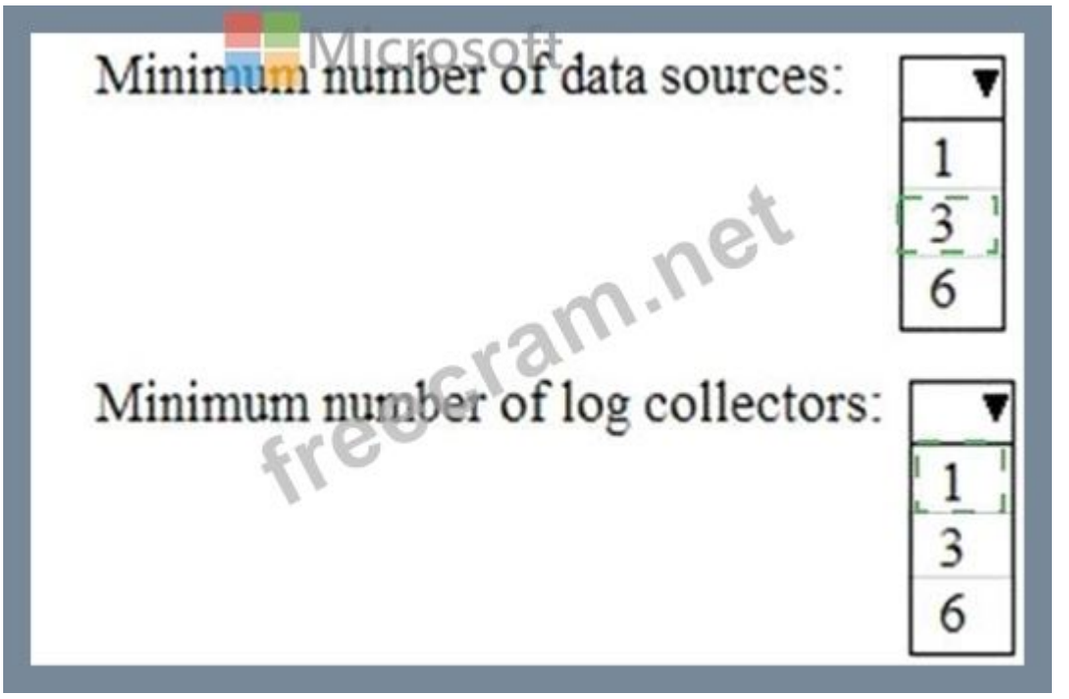
A. Mark items as a regulatory record

B. Retain items forever
C. Mark items as a record
D. Retain items even If users delete
Answer: (SHOW ANSWER)

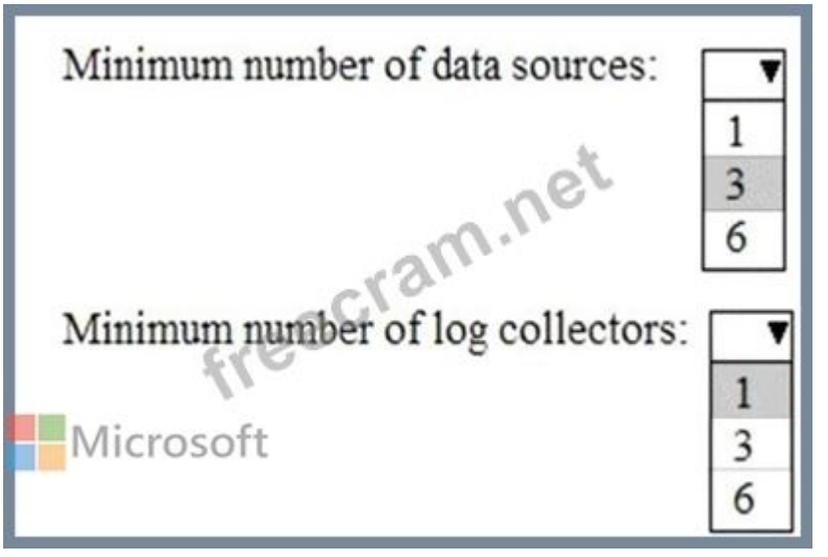
NEW QUESTION: 18
You need to meet the technical requirement for log analysis.
What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



References:

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

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 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 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

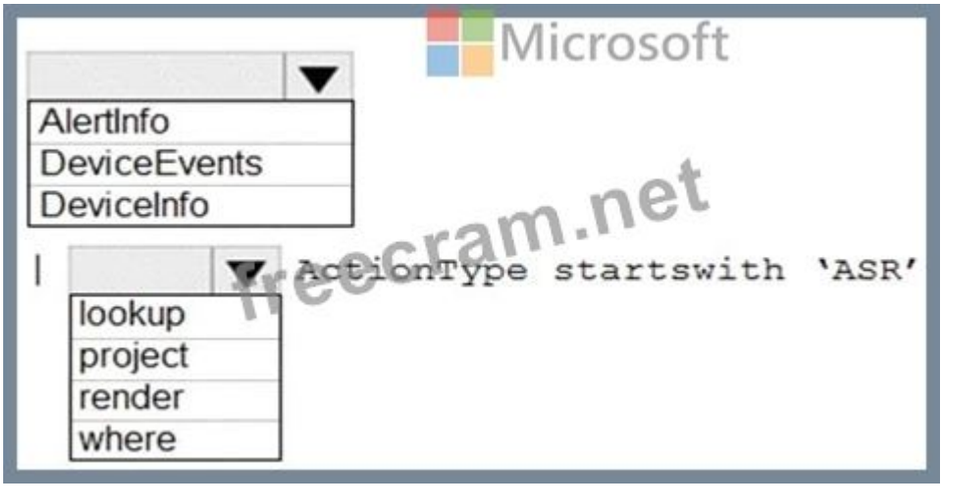
Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.
The verified domain is linked to an Azure Active Directory (Azure AD) tenant named litware.com.
Audit log search is turned on for the litware.com tenant.
Problem Statements
Litware identifies the following issues:
Users open 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

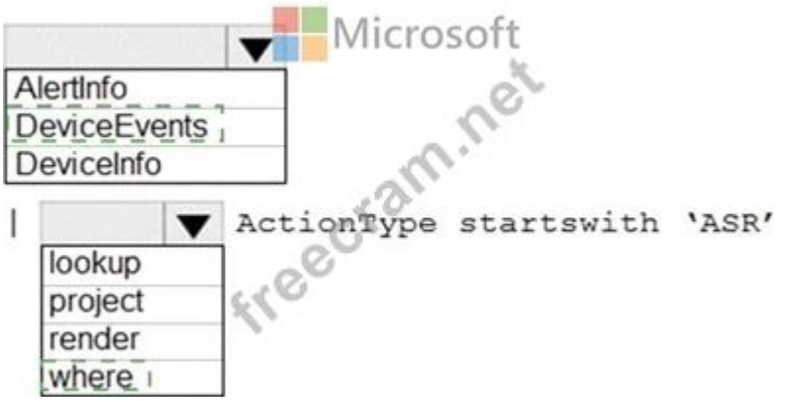
Implement a notification system for when DLP policies are triggered.
Configure a Safe Attachments policy for the litware.com tenant.
Technical Requirements
Litware identifies the following technical requirements:
Retention settings must be applied automatically to all the data stored in SharePoint Online 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: 19
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.

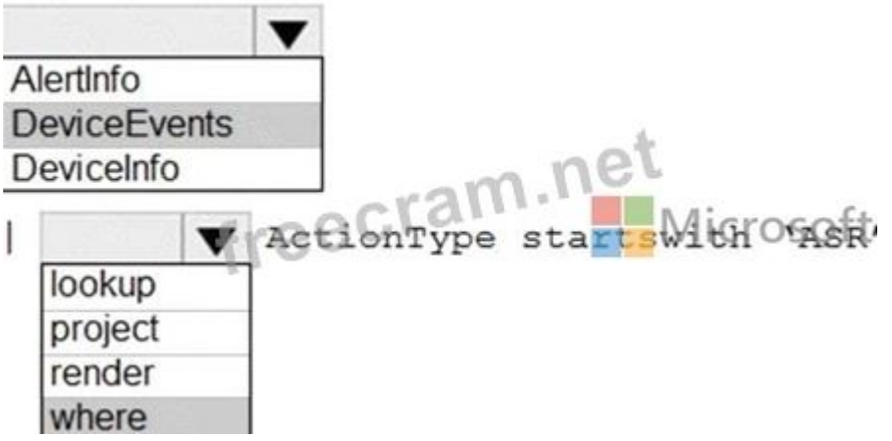


Answer:



Explanation

Graphical user interface, application Description automatically generated



Reference:

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction-

NEW QUESTION: 20

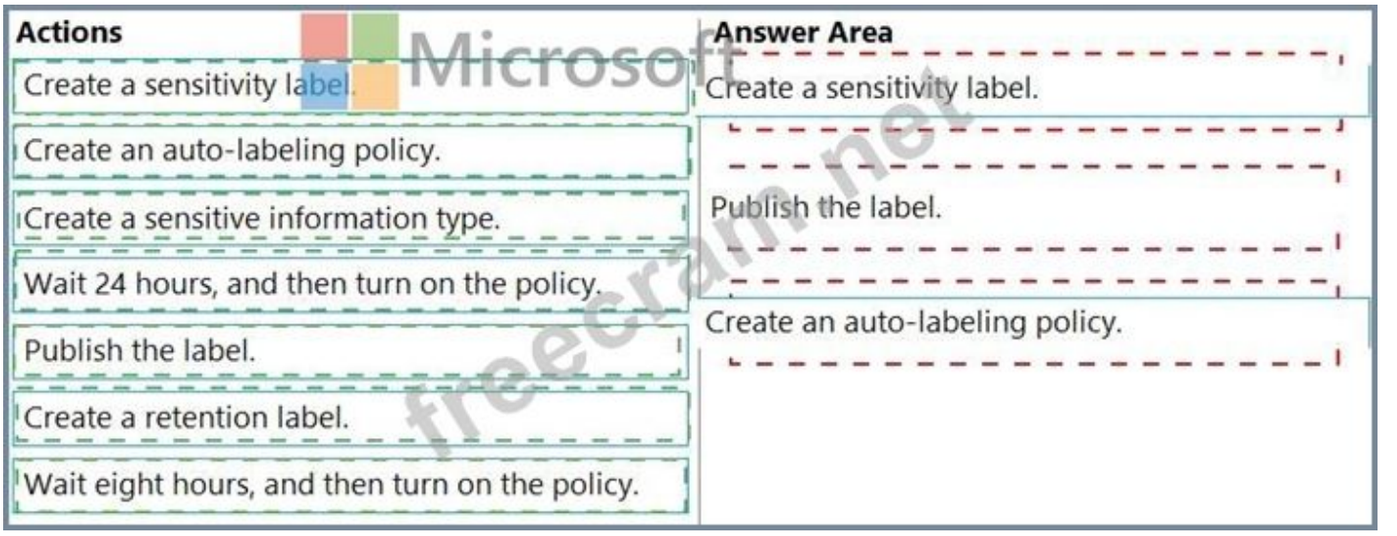
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to automatically label the documents on Site1 that contain credit card numbers.

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.

Actions	Answer Area
Create a sensitivity label.	
Create an auto-labeling policy.	
Create a sensitive information type.	
Wait 24 hours, and then turn on the policy.	
Publish the label.	
Create a retention label.	
Wait eight hours, and then turn on the policy.	

Answer:



Explanation

Graphical user interface, text, application, email Description automatically generated

Reference:

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

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

NEW QUESTION: 21

You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.

Company policy requires that the devices have the following configurations:

* Require complex passwords.
* Require the encryption of removable data storage devices.
* Have Microsoft Defender Antivirus real-time protection enabled.

You need to configure the devices to meet the requirements.

What should you use?

A. an app configuration policy

B. a compliance policy

C a security baseline profile

D a conditional access policy

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 22
You have a Microsoft 365 subscription that uses Security & Compliance retention policies.
You implement a preservation lock on a retention policy that is assigned to all executive users.
Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point?
A. Reduce the duration of policy
B. Disable the policy
C. Extend the duration of the policy
D. Add locations to the policy
E. Remove locations from the policy
Answer: (SHOW ANSWER)

NEW QUESTION: 23
You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

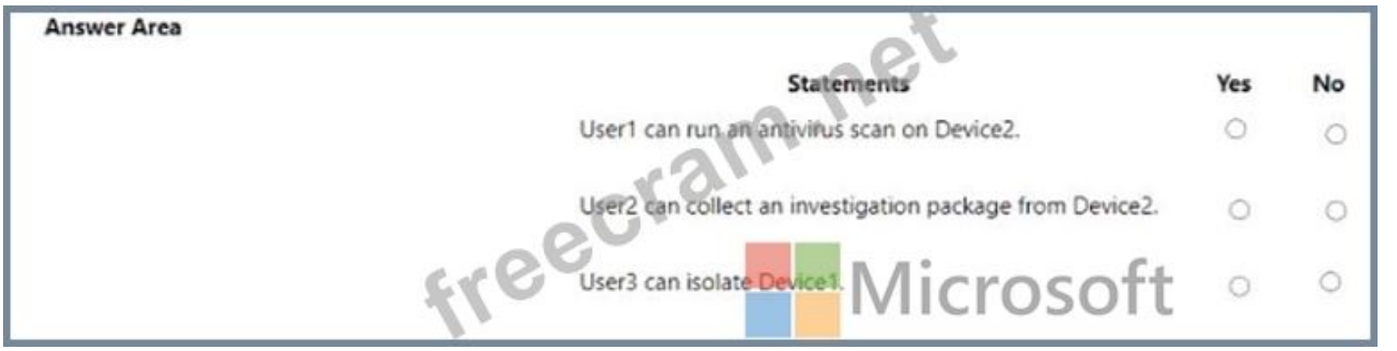
Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

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

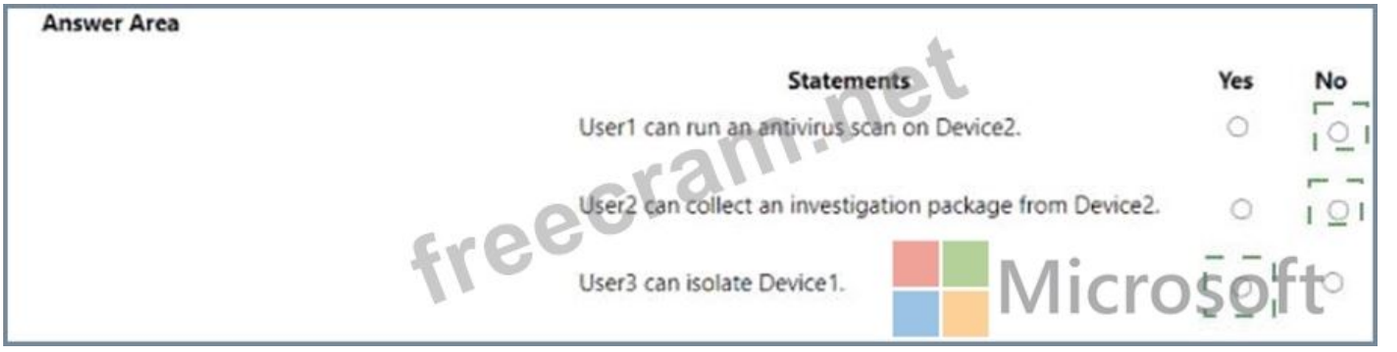
Microsoft Defender for Endpoint contains the device groups shown in the following table.

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



Explanation

NEW QUESTION: 24

Your company has on-premises servers and an Azure AD tenant.

Several months ago, the Azure AD Connect Hearth agent was installed on all the servers.

You review the health status of all the servers regularly.

Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect Servers list.

You suspect that another administrator removed Server1 from the list.

You need to ensure that you can view the health status of Server1.

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 Server1, reinstall the Azure AD Connect Health agent

B. From Azure Cloud shell, run the Connect-Azure AD cmdlet.

C. From Server1, change the Azure AD Connect Health Services Startup type to Automatic

D. From Windows PowerShell, run the Rejister-ArureADConnectHealthsyncAgent cmdlet.

E. From Server1, change the Azure AD Connect Health Services Startup type to Automatic (Delayed Start)

Answer: (SHOW ANSWER)

NEW QUESTION: 25

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: A (LEAVE A REPLY)

Explanation

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: 26

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

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

You have the apps shown in the following table.

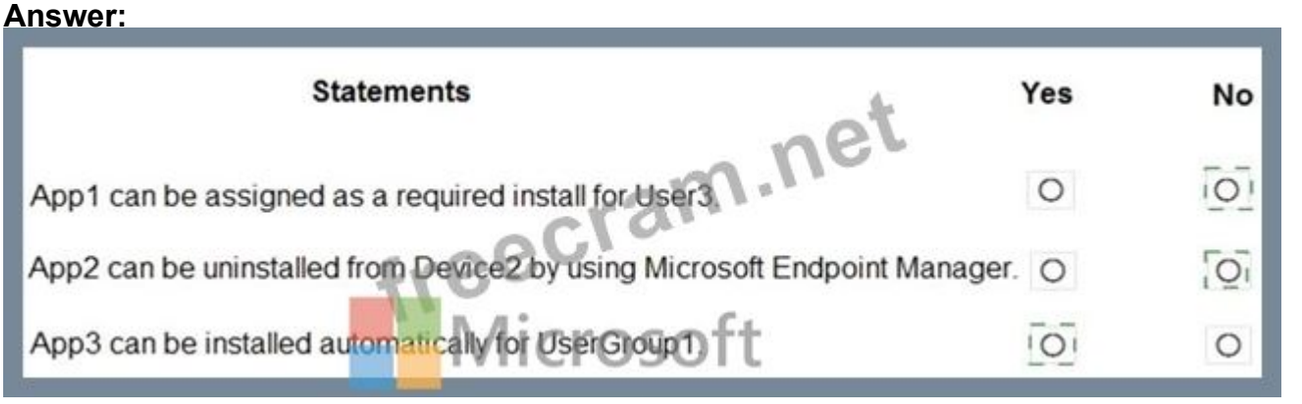
Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the 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.

Answer:



Explanation

Graphical user interface, text, application Description automatically generated

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy

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

NEW QUESTION: 27

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: At a command prompt, you run the winver.exe command.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec

NEW QUESTION: 28
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: 29
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.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Endpoint Management admin center, you create a device configuration profile.
Does this meet the goal?
A. Yes

B. No

Answer: (SHOW ANSWER)

Explanation

You need to create a trusted location and a conditional access policy.

NEW QUESTION: 30

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 that contains a user named User1.

You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 admin center, you assign User1 the Compliance admin role.

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

Reference:

https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/pe

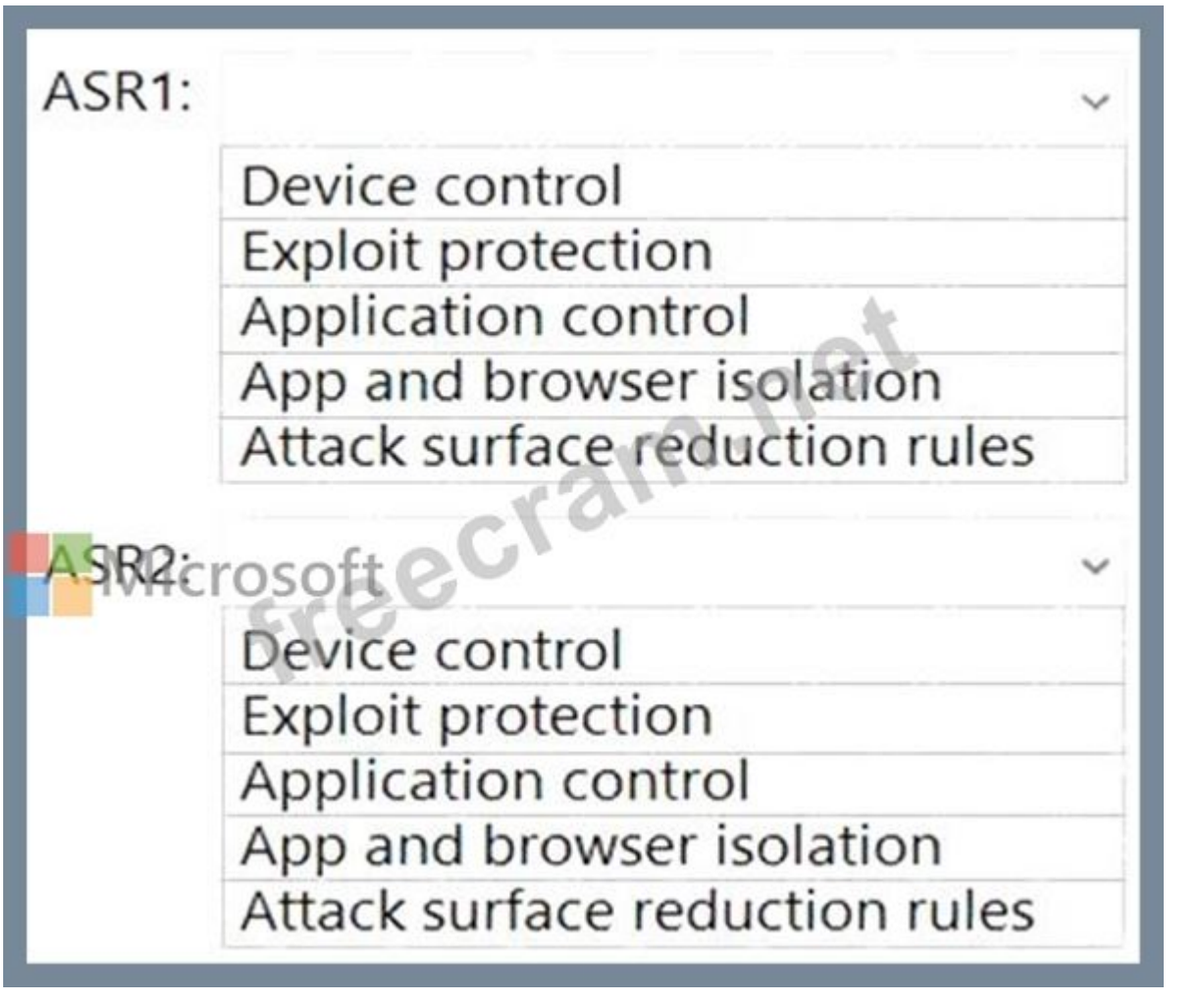
NEW QUESTION: 31

You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.

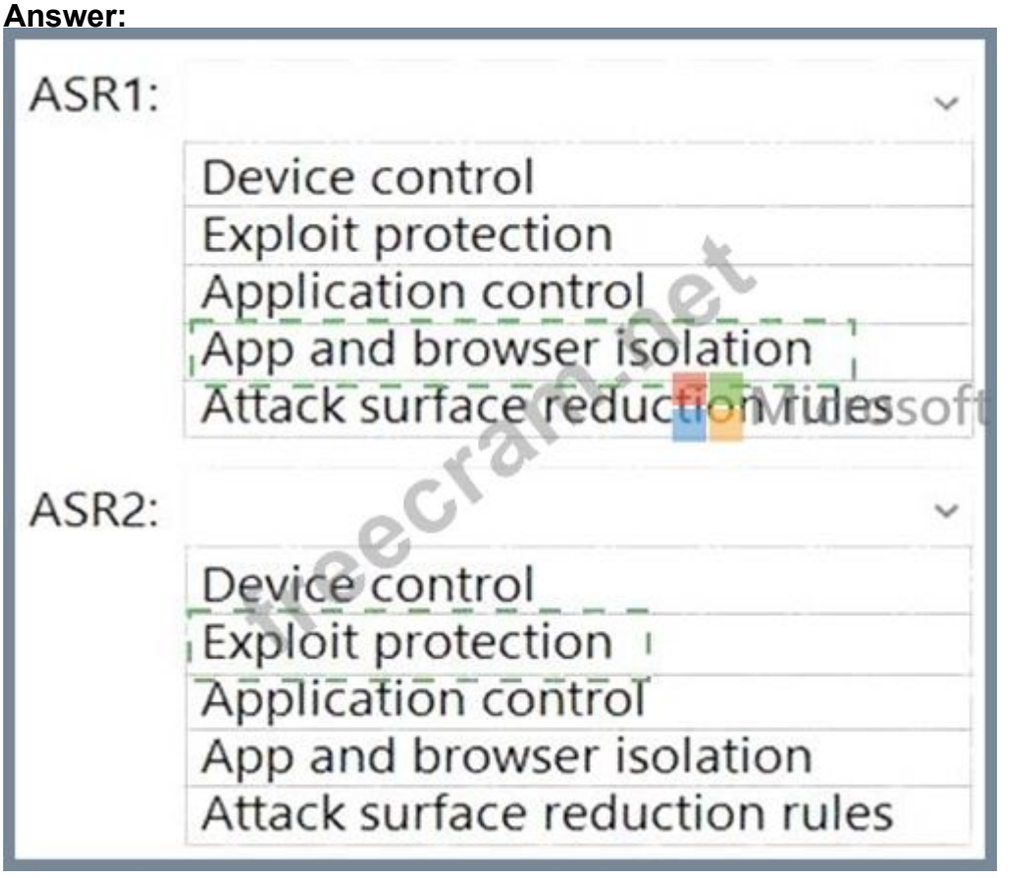
You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard. ASR2 will be used to configure Microsoft Defender SmartScreen.

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.

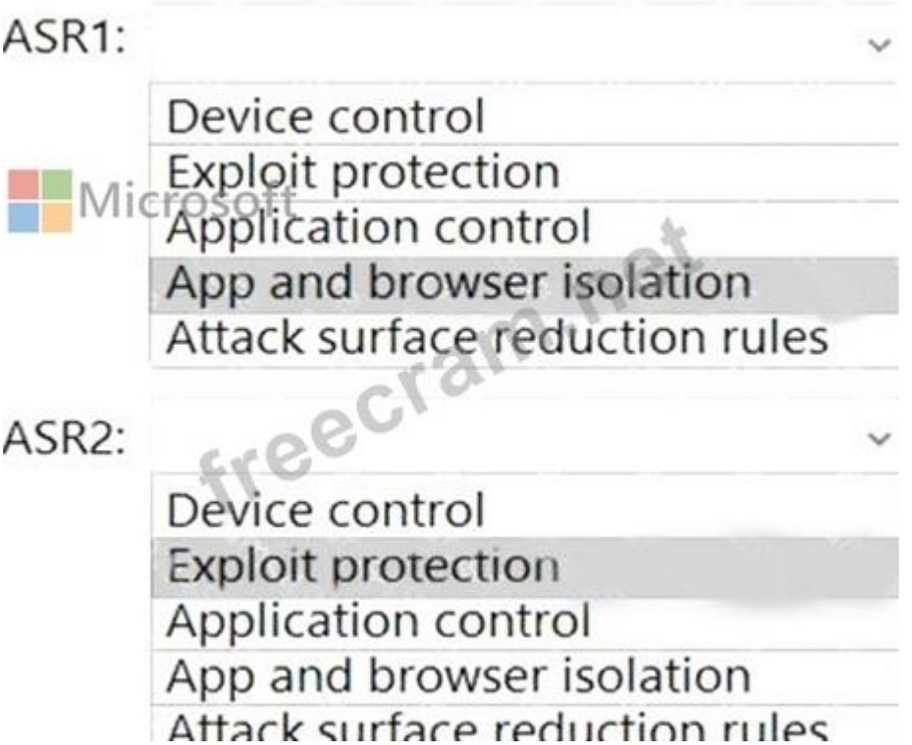


Answer:



Explanation

Graphical user interface, text, application, chat or text message Description automatically generated



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

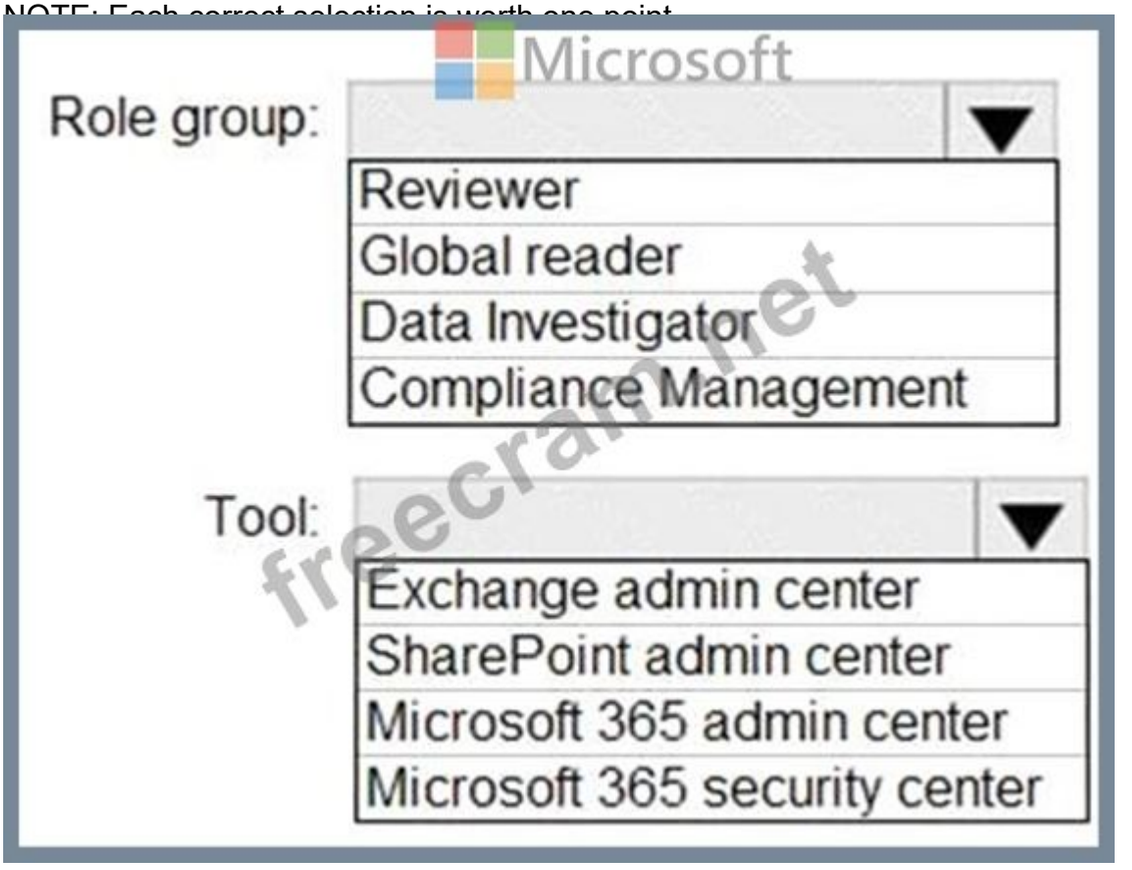
NEW QUESTION: 32
You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.
You need to prevent the members or Group1 from communicating with the members of Group2 by using Microsoft Teams. The solution must comply with regulatory requirements and must not affect other user in the tenant.
What should you use?
A. moderated distribution groups
B. administrator units in Azure Active Directory (Azure AD)
C. communication compliance policies
D. information barriers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 33

You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements.

To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation

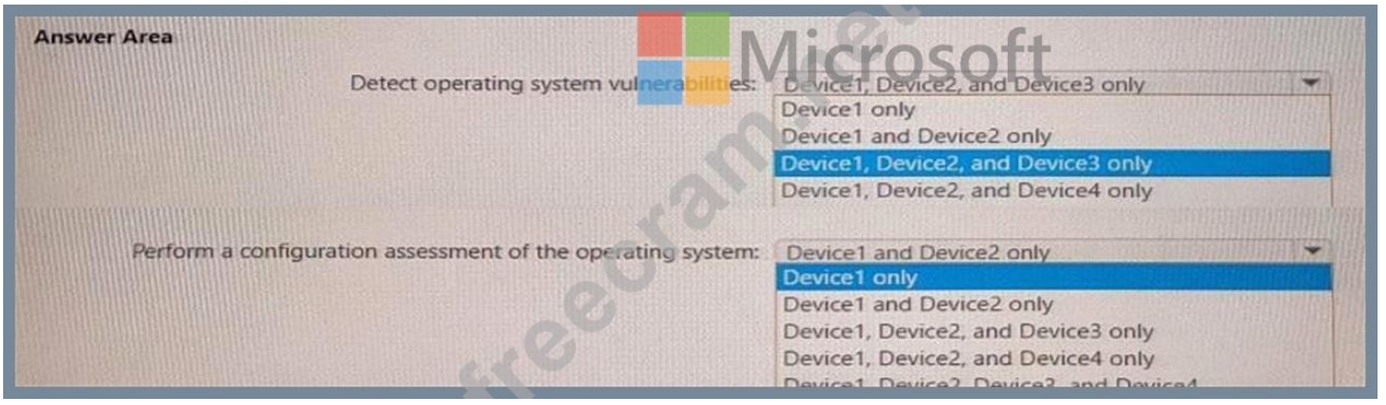
Graphical user interface, text Description automatically generated

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

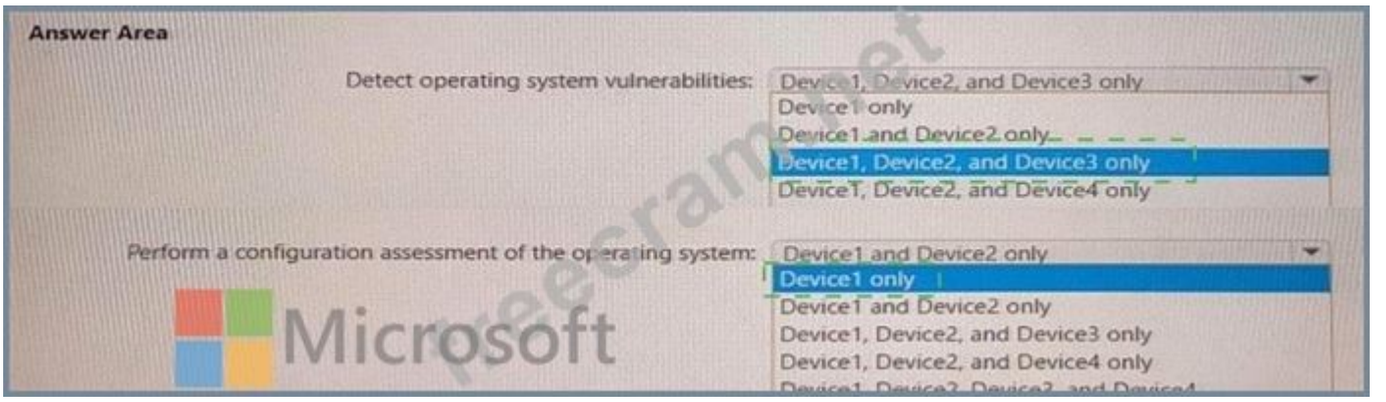
NEW QUESTION: 34
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

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

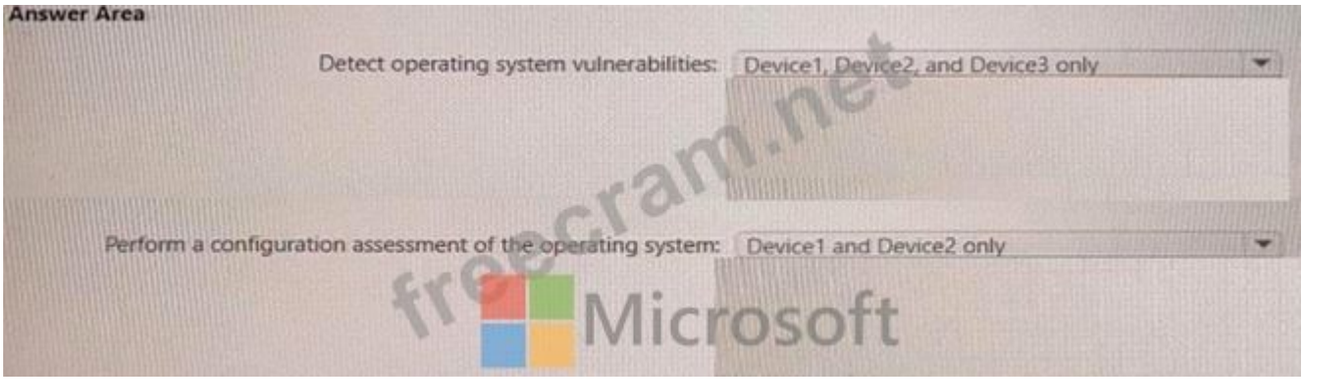
All the devices are onboarded To Microsoft Defender for Endpoint
You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:
* Detect operating system vulnerabilities.



Answer:



Explanation



NEW QUESTION: 35

You need to configure just in time access to meet the technical requirements.

What should you use?

A. entitlement management

B. Azure AD Identity Protection

C. Azure AD Privileged Identity Management (PIM)

D. access reviews

Answer: (SHOW ANSWER)

NEW QUESTION: 36

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: (SHOW ANSWER)

Explanation

References:

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

NEW QUESTION: 37

You have a Microsoft 365 E5 subscription that uses Microsoft intune.
in the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices,
You enable device clean-up rules What can you configure as the minimum number of days before a device a removed automatically?

A. 45
B. 90
C. 10
D. 30
Answer: (SHOW ANSWER)

NEW QUESTION: 38
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 only
B. Device1 and Device4
C. Device1, Device3, and Device4
D. Device1, Device2, Device3, and Device4
Answer: (SHOW ANSWER)

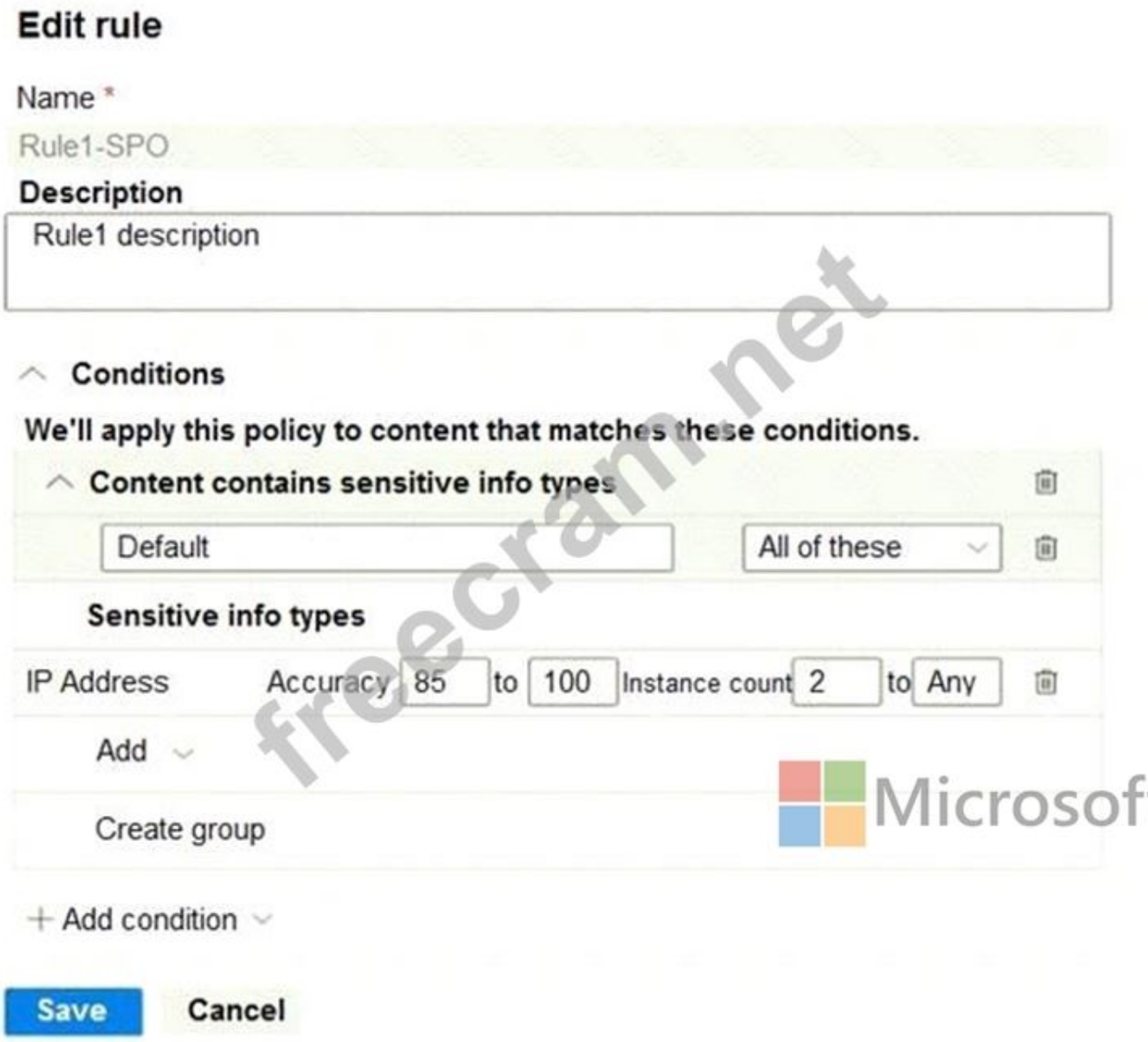
NEW QUESTION: 39
You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.

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

You create a sensitivity label named Sensitivity1 and an auto-label policy that has the following configurations:

Name: AutoLabel1
Label to auto-apply: Sensitivity1
Rules for SharePoint Online sites: Rule1-SPO

Choose locations where you want to apply the label: Site1
Rule1-SPO is configured as shown in the following exhibit.

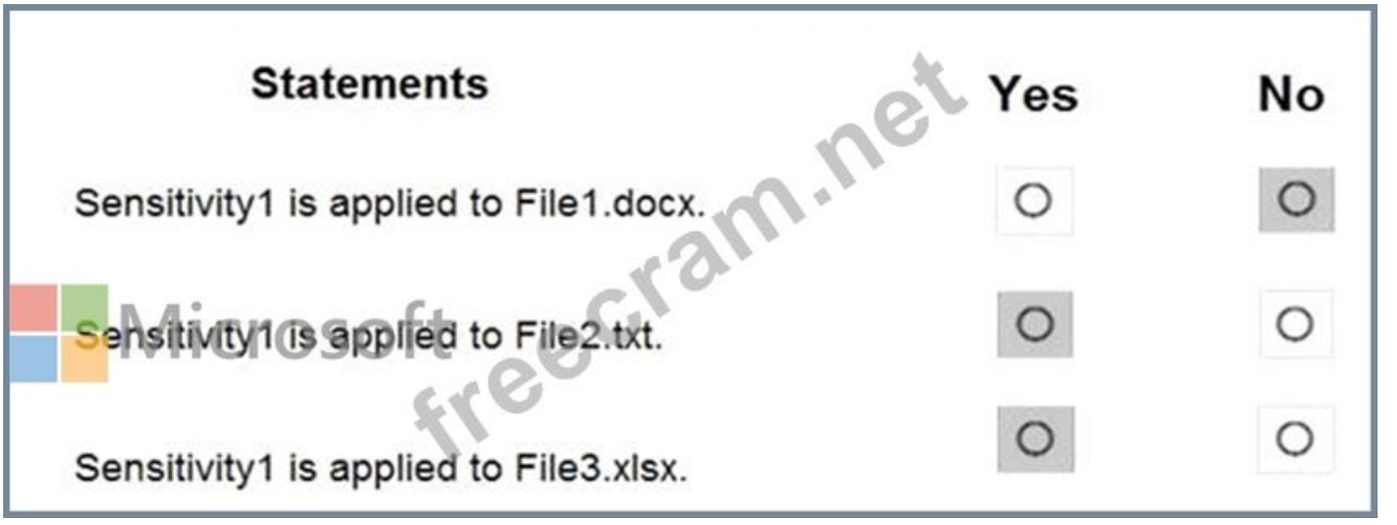


For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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

Answer:

Explanation



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

NEW QUESTION: 40

You need to create the Safe Attachments policy to meet the technical requirements.
Which option should you select?

A. Replace
B. Enable redirect
C. Block
D. Dynamic Delivery

Answer: (SHOW ANSWER)

Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/saf

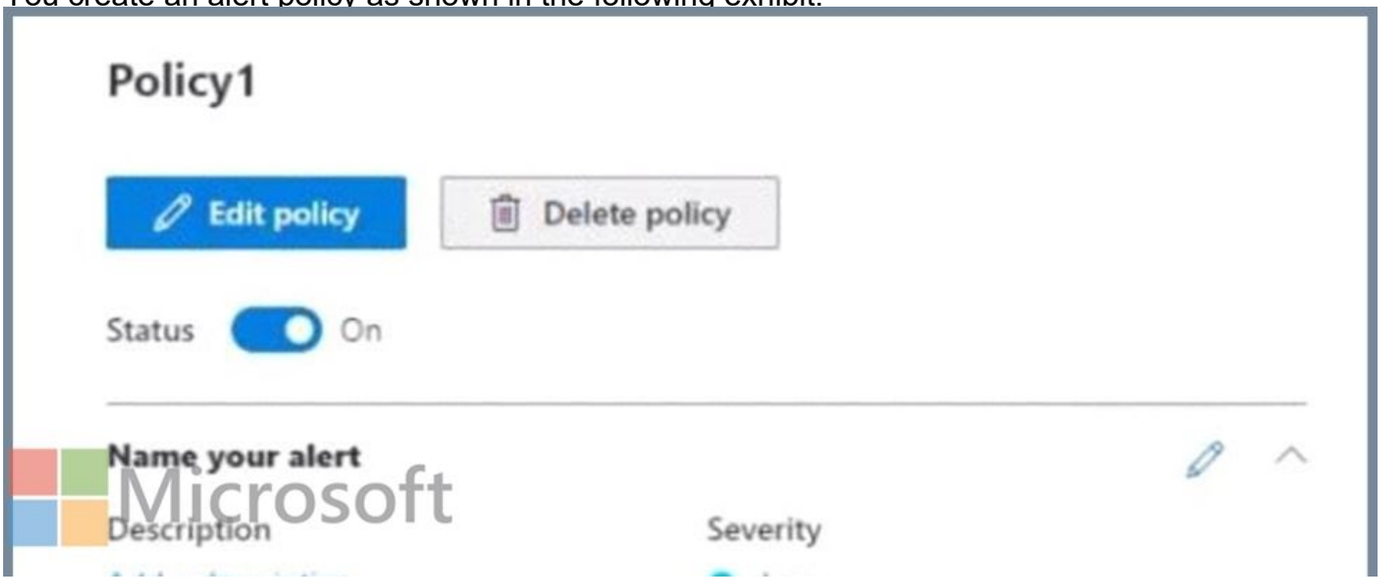
NEW QUESTION: 41

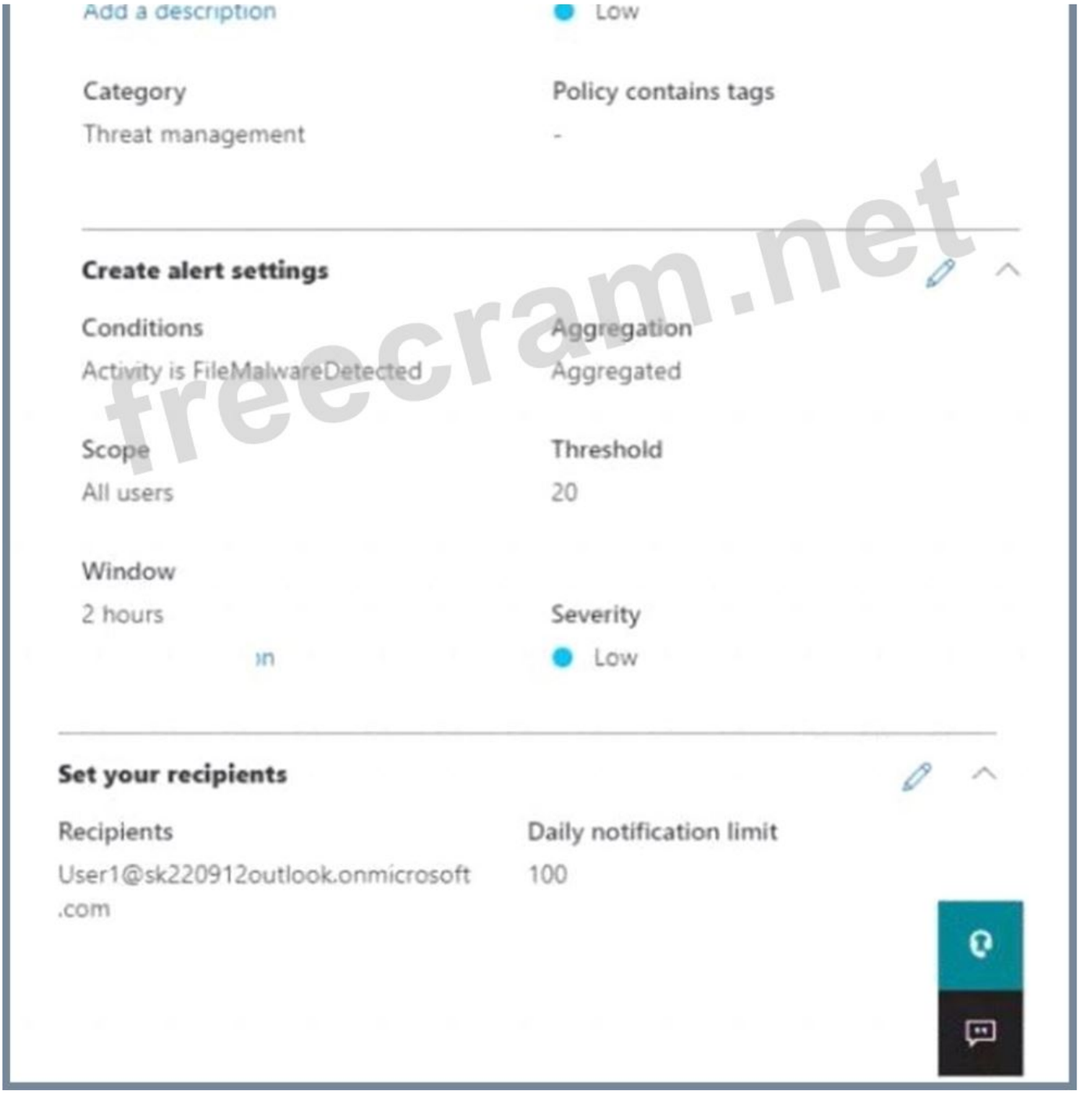
Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD)
Password hash synchronization is disabled.
You plan to implement co-management.
You need to configure Azure AD Connect and the domain to support co-management.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

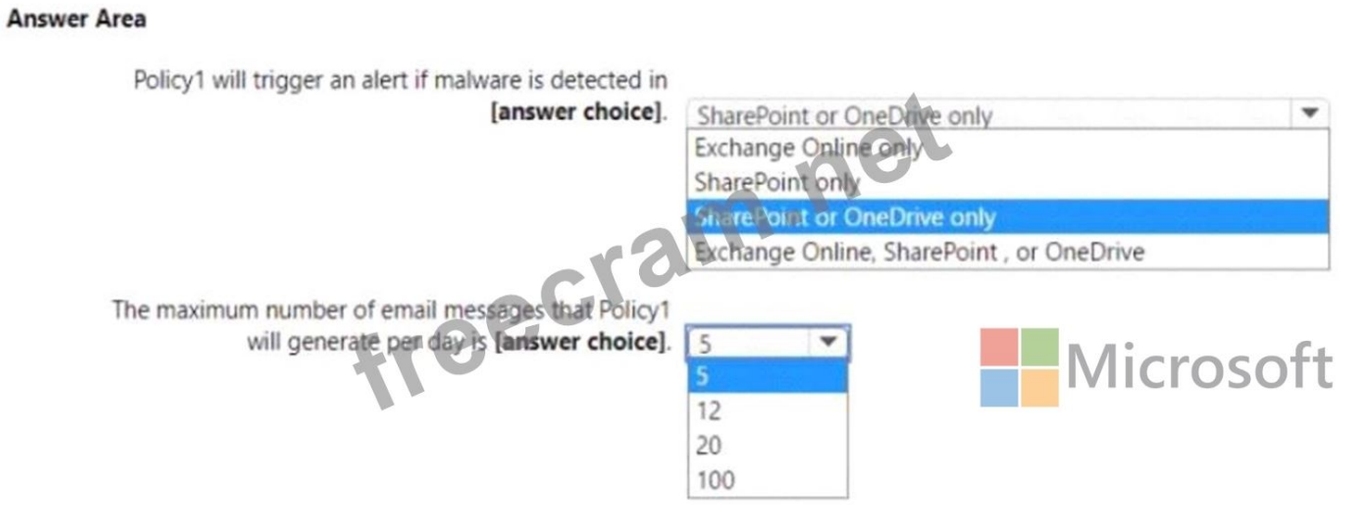
Explanation

NEW QUESTION: 42
You have Microsoft 365 subscription.
You create an alert policy as shown in the following exhibit.

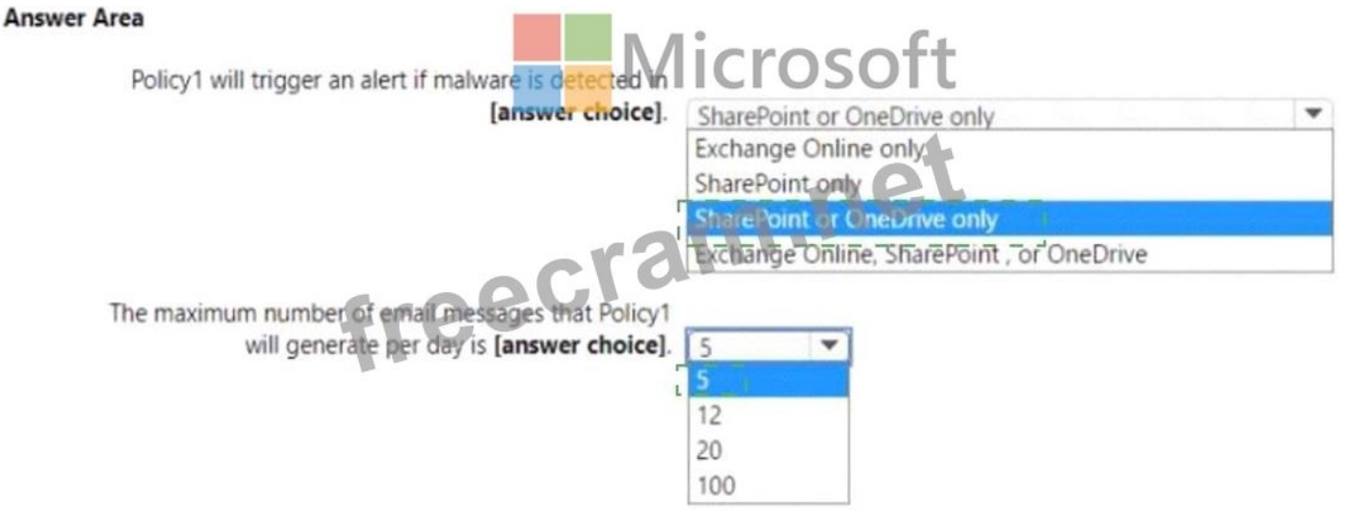




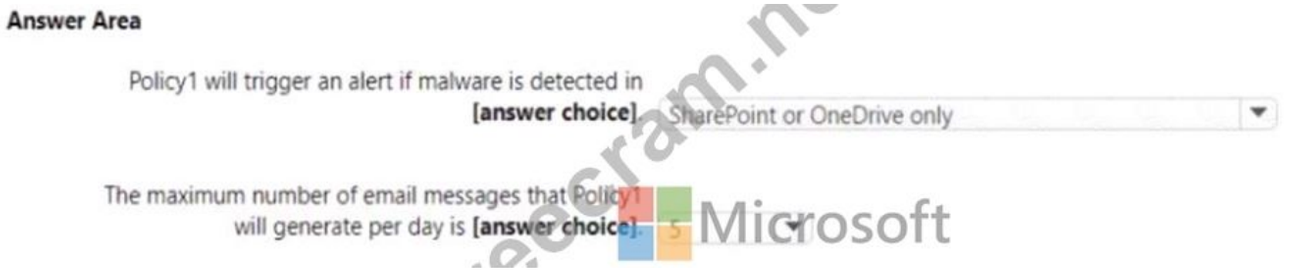
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic NOTE: Each correct selection is worth one point.



Answer:



Explanation



NEW QUESTION: 43

You have a Microsoft 365 E5 subscription.

Al users have Mac computers. ATI the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender for Endpoint.

You need to configure Microsoft Defender for Endpoint on the computers.

What should you create from the Endpoint Management admin center?

A. a mobile device management (MDM) security baseline profile

B. a Microsoft Defender for Endpoint baseline profile

C. an update policy for iOS

D. a device configuration profile

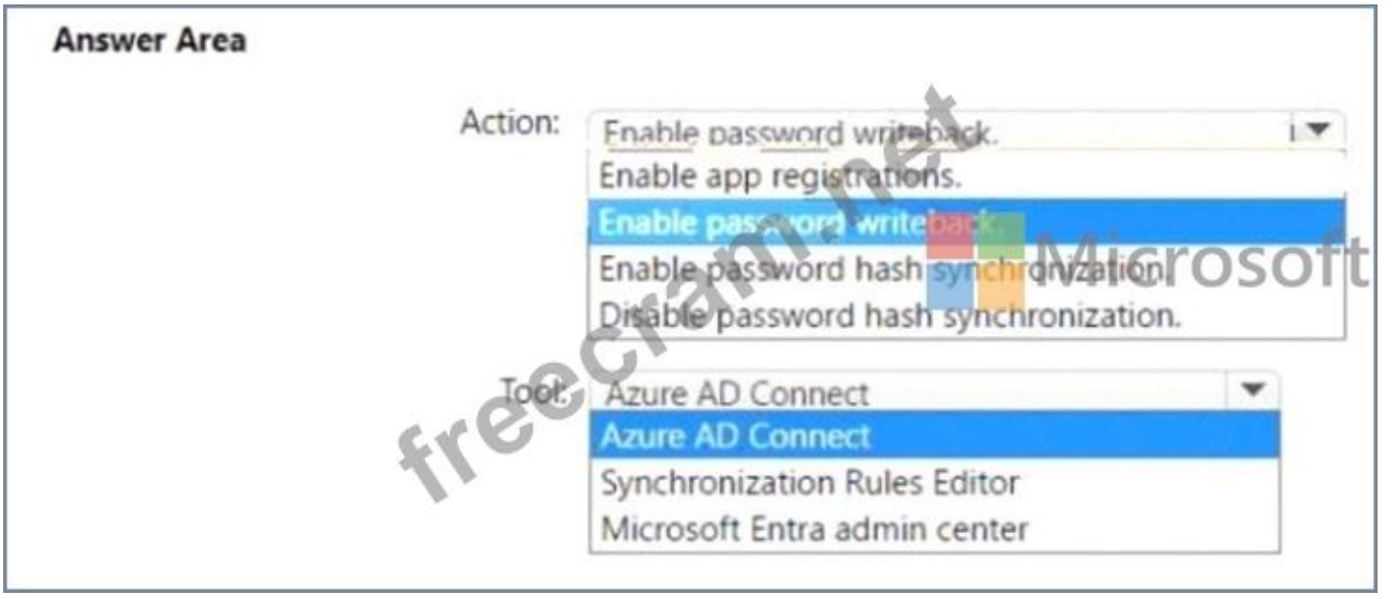
Answer: (SHOW ANSWER)

NEW QUESTION: 44

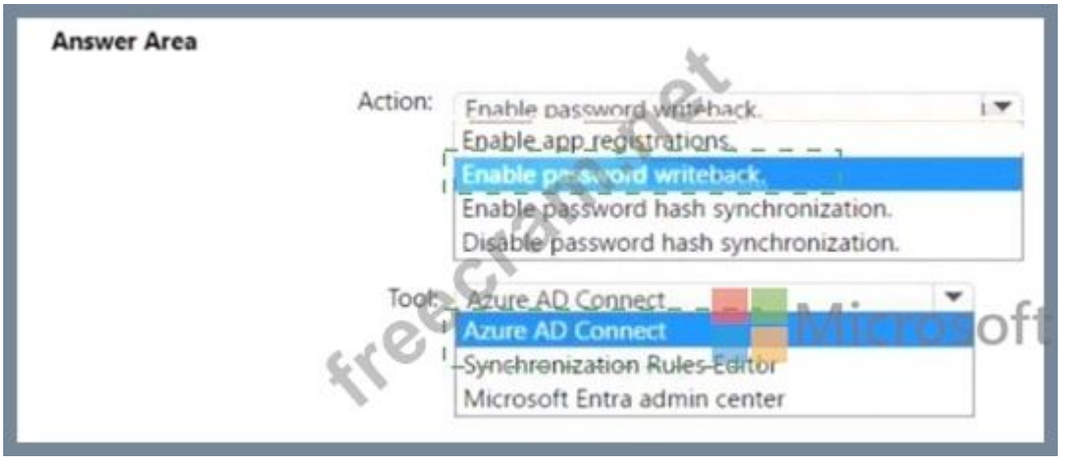
You need to ensure that Admin4 can use SSPR.

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:



Explanation

NEW QUESTION: 45

You have a Microsoft 365 E5 subscription.

You need to configure Microsoft Defender for Office 365 to meet the following requirements:

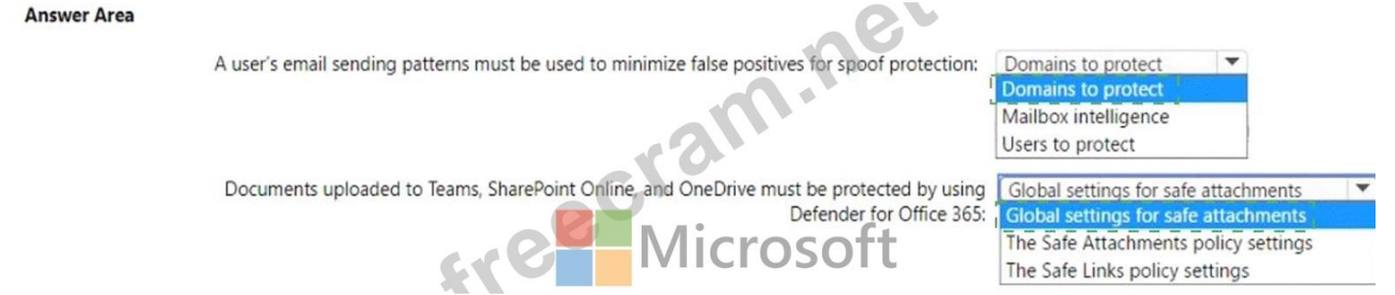
* A user's email sending patterns must be used to minimize false positives for spoof protection.

* Documents uploaded to Microsoft Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365.

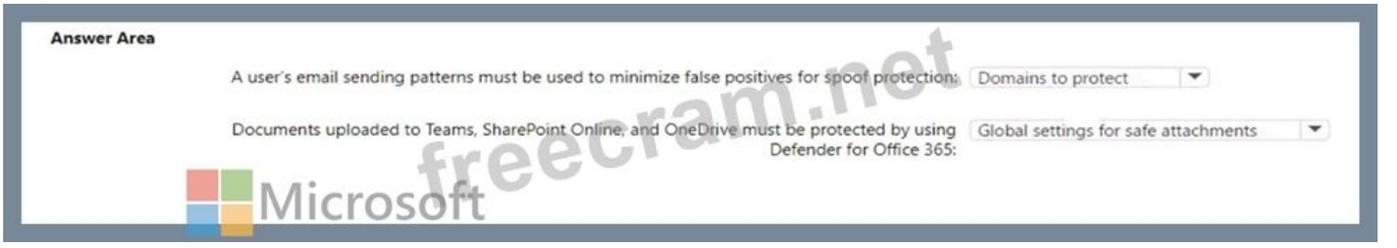
What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation



NEW QUESTION: 46

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 Area

Answer:

Answer Area

Explanation

NEW QUESTION: 47

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

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

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must minimize administrative effort.

What should you use to onboard each type of device? To answer, drag the appropriate onboarding methods to the correct device types. Each onboarding method 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

NEW QUESTION: 48

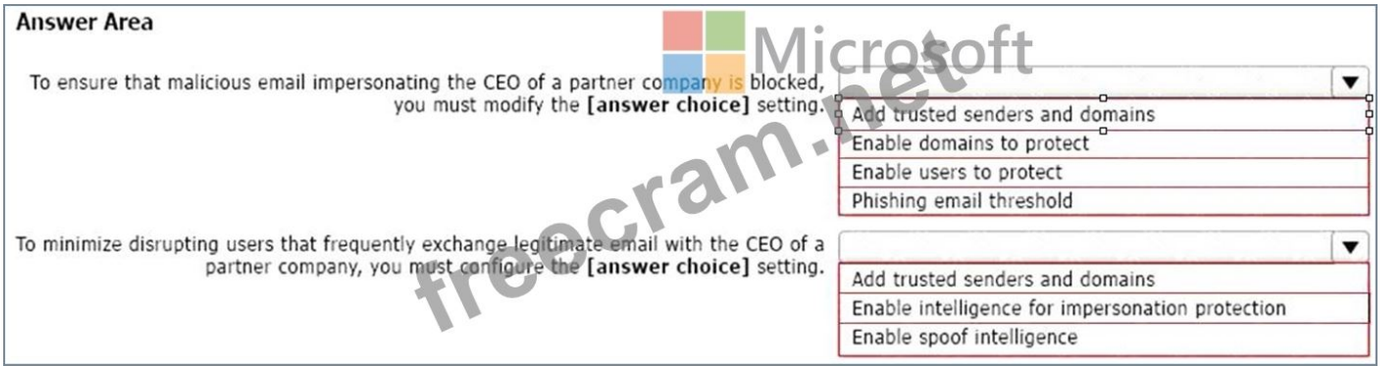
HOTSPOT

You have a Microsoft 365 subscription.

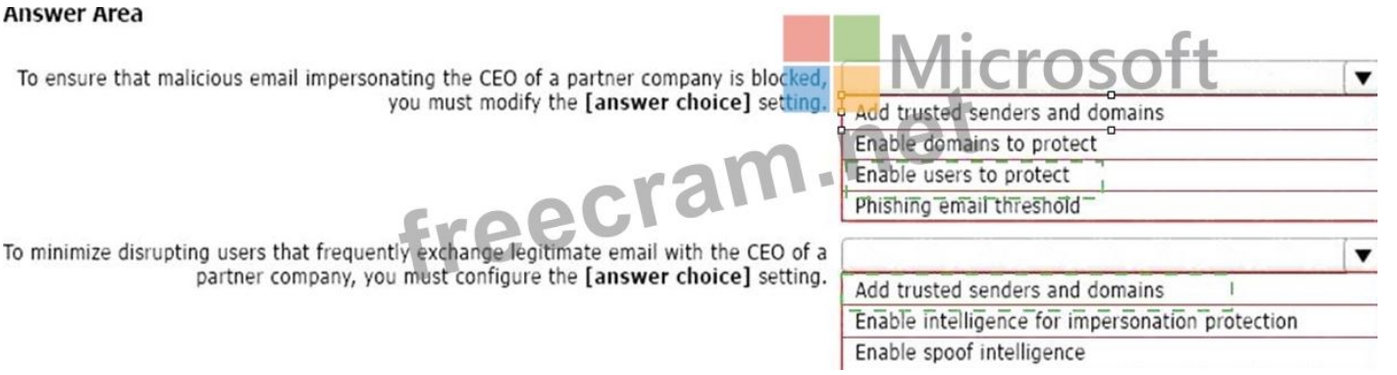
You deploy the anti-phishing policy shown in the following exhibit.

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

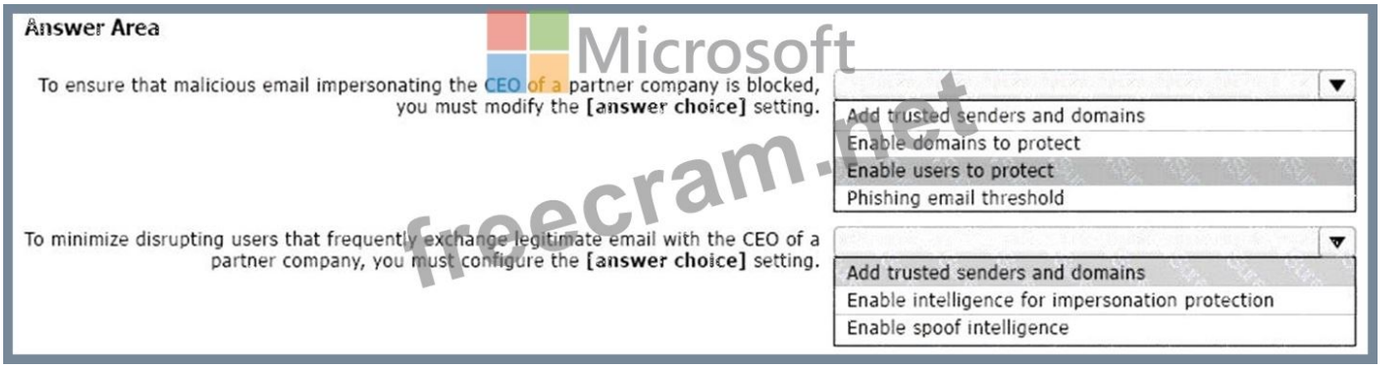
NOTE: Each correct selection is worth one point.



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: 49
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. a suppression rule
B. an indicator
C. a device configuration profile
Answer: (SHOW ANSWER)

NEW QUESTION: 50
You have a Microsoft 365 F5 subscription.
You plan to deploy 100 new Windows 10 devices.
You need to order the appropriate version of Windows 10 for the new devices. The version must Meet the following requirements.
Be serviced for a minimum of 24 moths.
Support Microsoft Application Virtualization (App-V)
Which version should you identify?

A. Window 10 Pro, version 1909
B. Window 10 Pro, version 2004
C. Window 10 Pro, version 1909

D. Window 10 Enterprise, version 2004

Answer: (SHOW ANSWER)

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

NEW QUESTION: 51

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. Windows 10, and Windows8.1 only

B. Windows 11, Windows 10-Windows8.1.andmacOS

C. Windows 11 only

D. Windows 11 and macOS only

E. Windows 11 and Windows 10 only

Answer: (SHOW ANSWER)

NEW QUESTION: 52

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

A. 1

B. 4

C. 7

D. 31

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 53

DRAG DROP

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

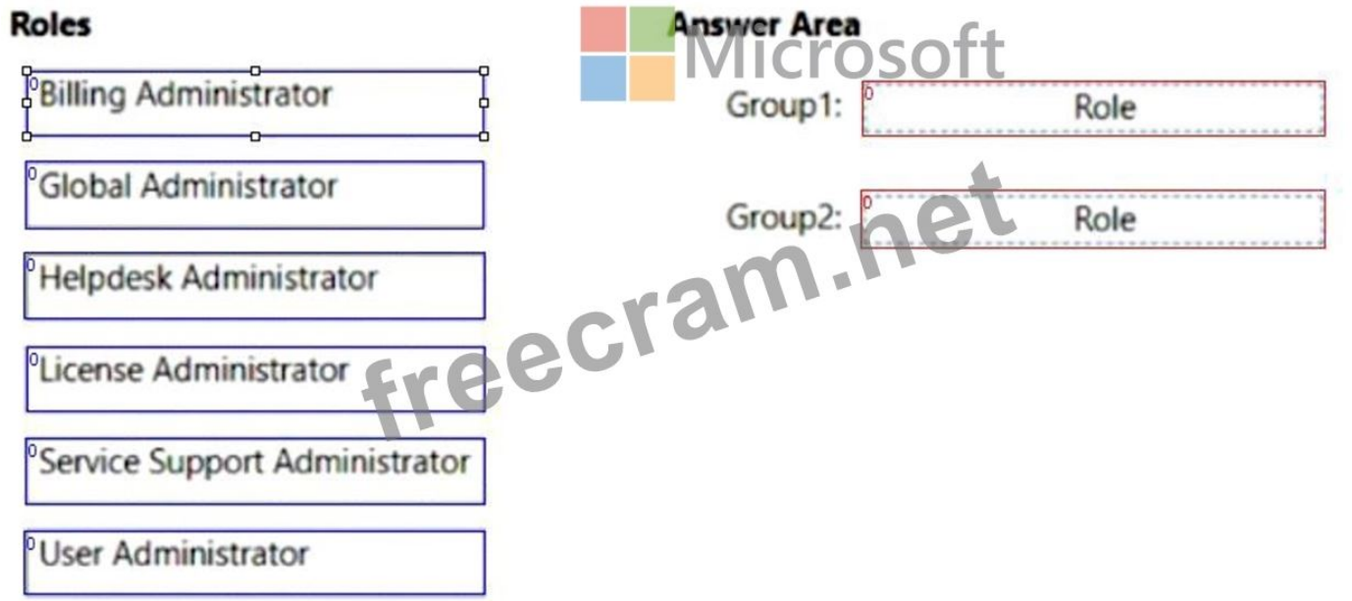
You need to ensure that each group can perform the tasks shown in the following table.

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.

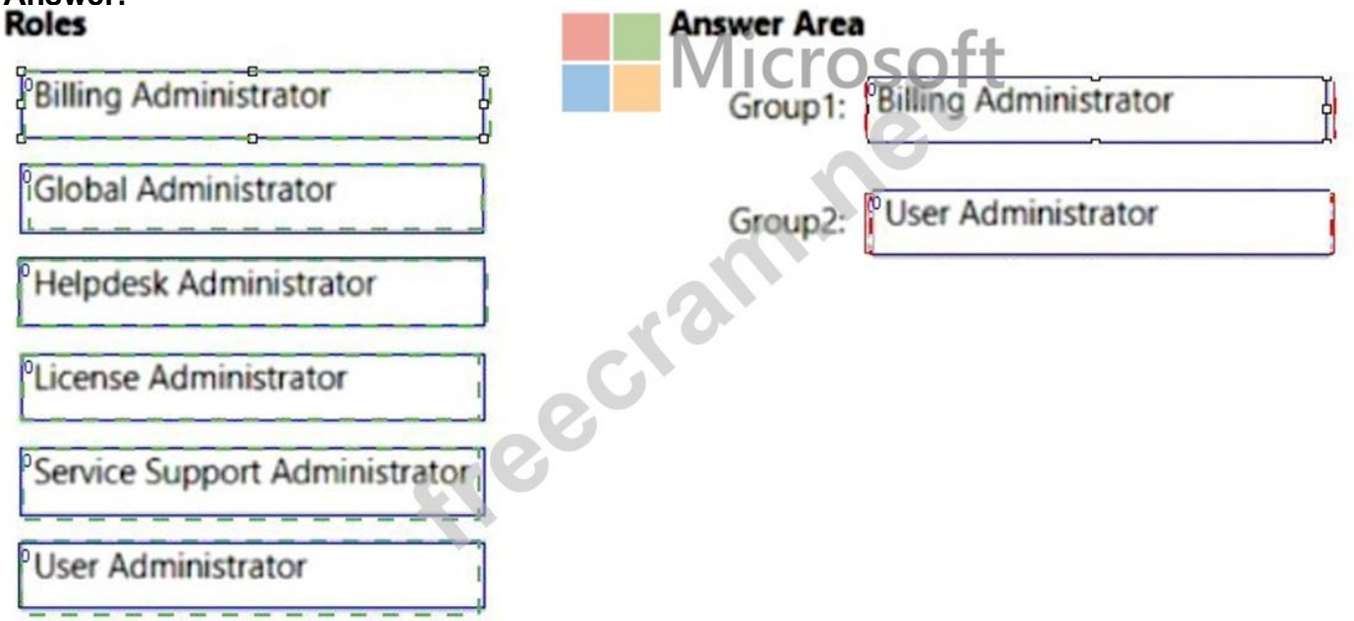
The solution must use the principle of least privilege.

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.

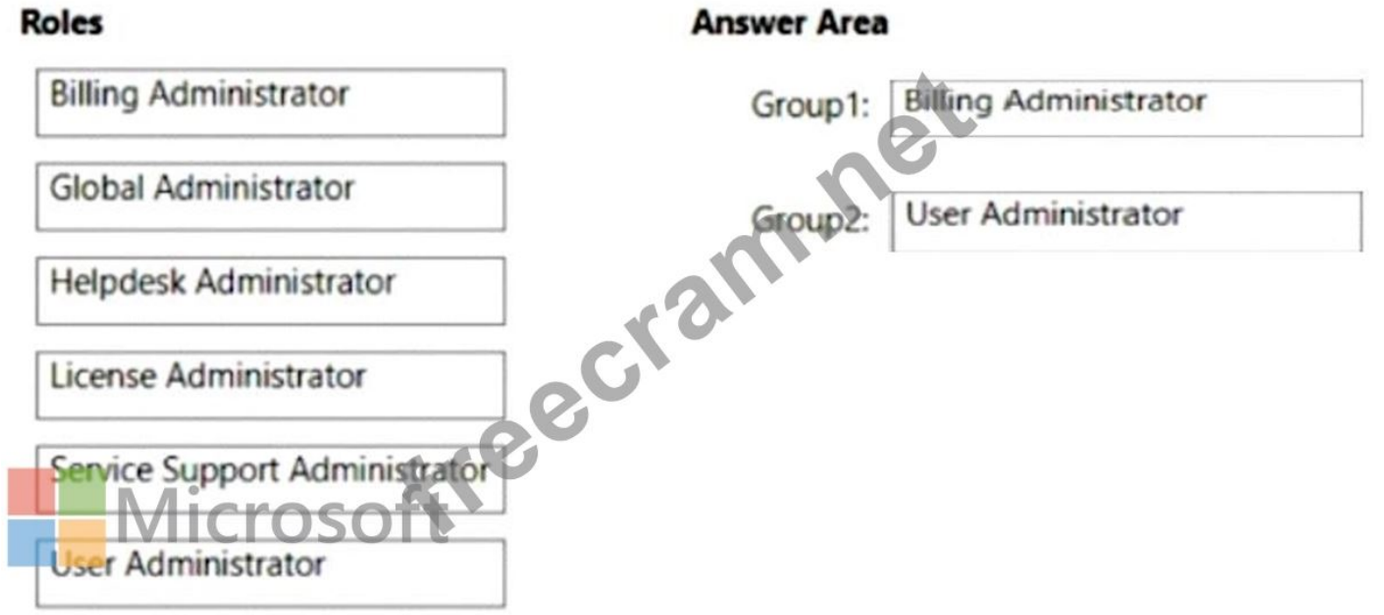
NOTE: Each correct selection is worth one point.



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: 54

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

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

You plan to join the devices to Azure Active Directory (Azure AD)

What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, of 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

NEW QUESTION: 55

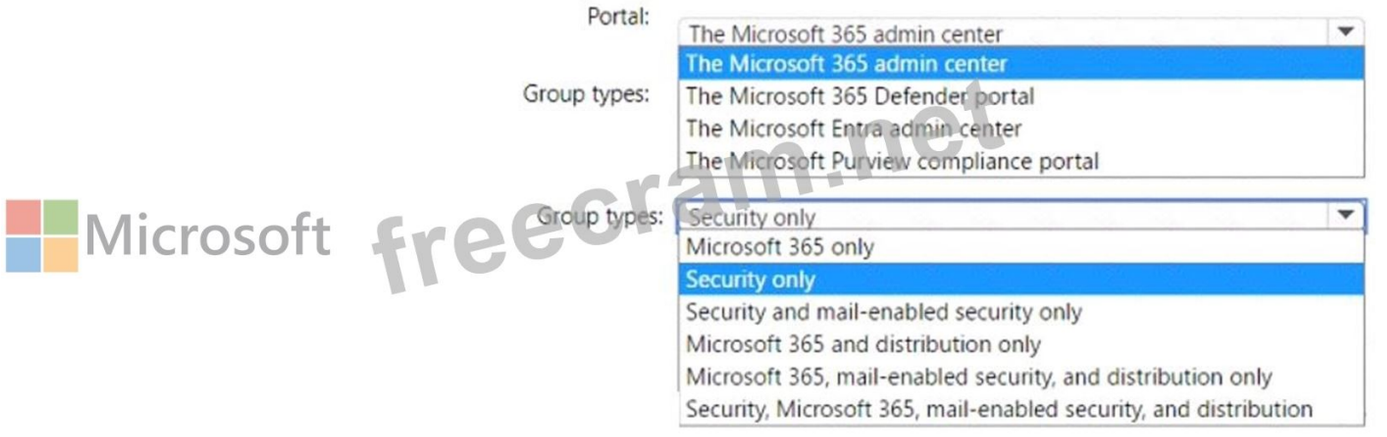
You have a Microsoft 365 E5 subscription.

You need to configure a group naming policy.

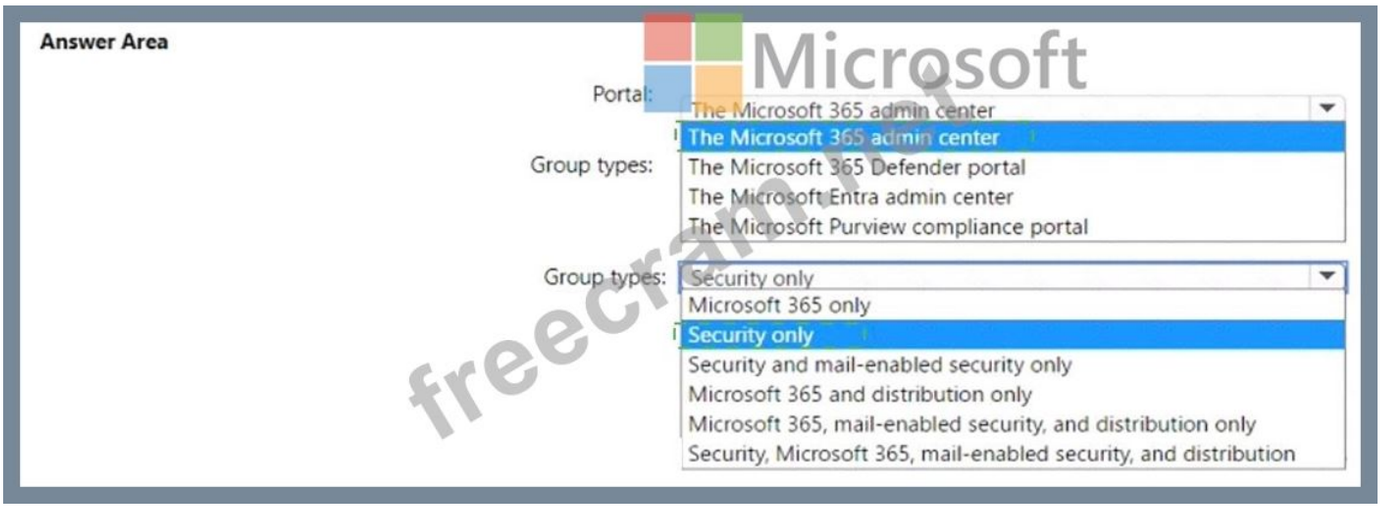
Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Explanation

NEW QUESTION: 56

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.

The tenant includes a user named User1.

You enable Azure AD Identity Protection.

You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk.

The solution must use the principle of least privilege.

To which role should you add User1?

A. Owner

B. User Administrator

C. Security Reader

D. Global Administrator

Answer: (SHOW ANSWER)

NEW QUESTION: 57

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. Android

B. CentOS Linux

C. iOS

D. Window 10

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 58

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 Purview compliance portal

C. the Microsoft Entra admin center

D. the Microsoft 365 admin center

Answer: (SHOW ANSWER)

NEW QUESTION: 59

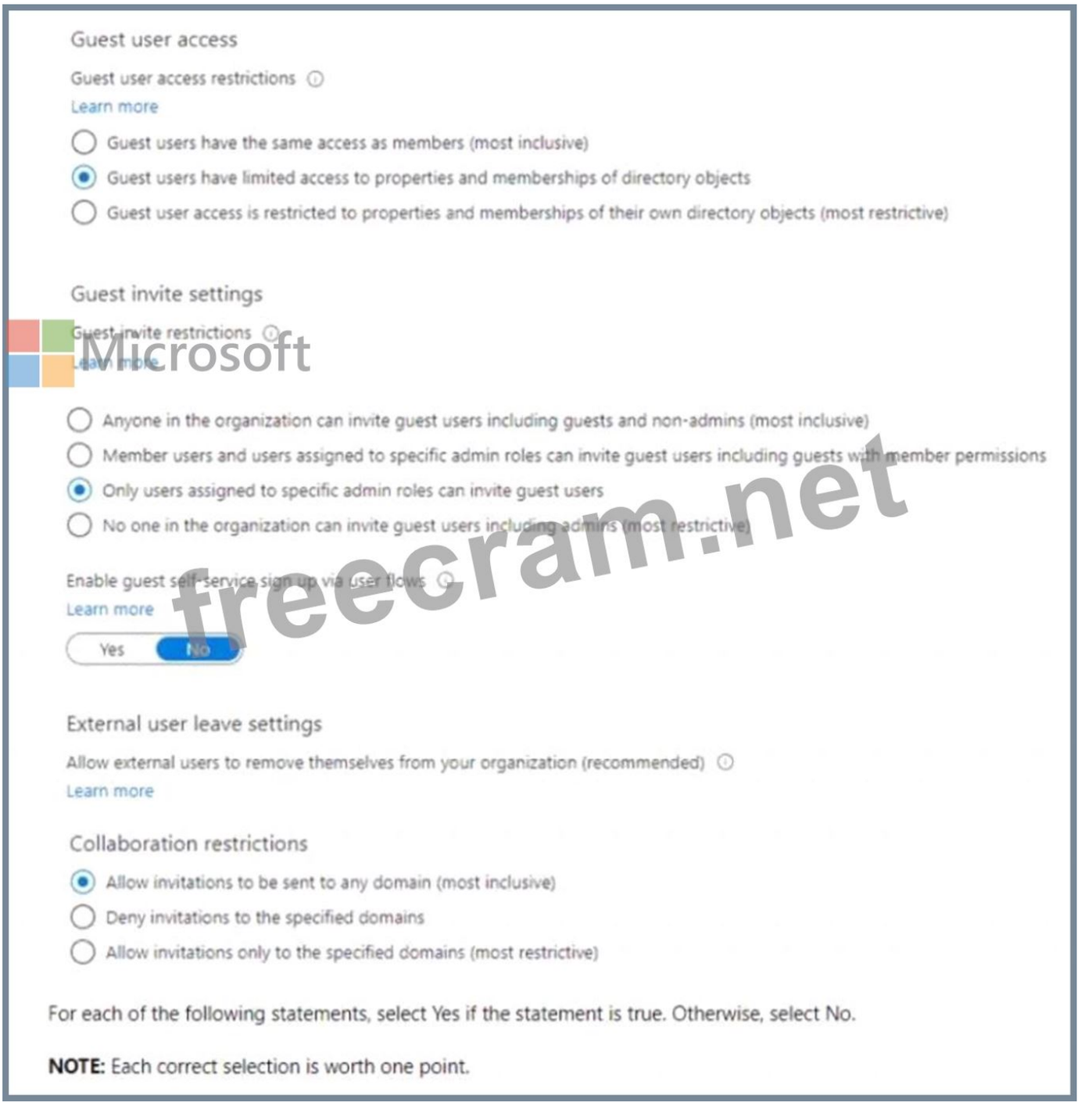
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type	Role
Group1	Security	Helpdesk Administrator
Group2	Security	*None*
Group3	Microsoft 365	User Administrator

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

In Azure AD, you configure the External collaboration settings as shown in the following 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 Area

Statements	Yes	No
User1 can invite guest users.	○	○
User2 can invite guest users.	○	○
User3 can invite guest users.	○	○

Answer:

Explanation

NEW QUESTION: 60

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named site1. You need to ensure that site1 meets the following requirements:

* Retains all data for 10 years
* Prevents the sharing of data outside the organization

Which two items should you create and apply to site1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a retention label

B. a retention label policy

C. a sensitivity label

D. a data loss prevention (DLP) policy

E. a retention policy

F. a sensitive info type

Answer: (SHOW ANSWER)

NEW QUESTION: 61

HOTSPOT

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

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

All the groups are deleted.

Which groups can be restored, and what is the retention period? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Groups that can be restored:

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

Retention period:

- 24 hours
- 7 days
- 14 days
- 30 days
- 90 days

Answer:

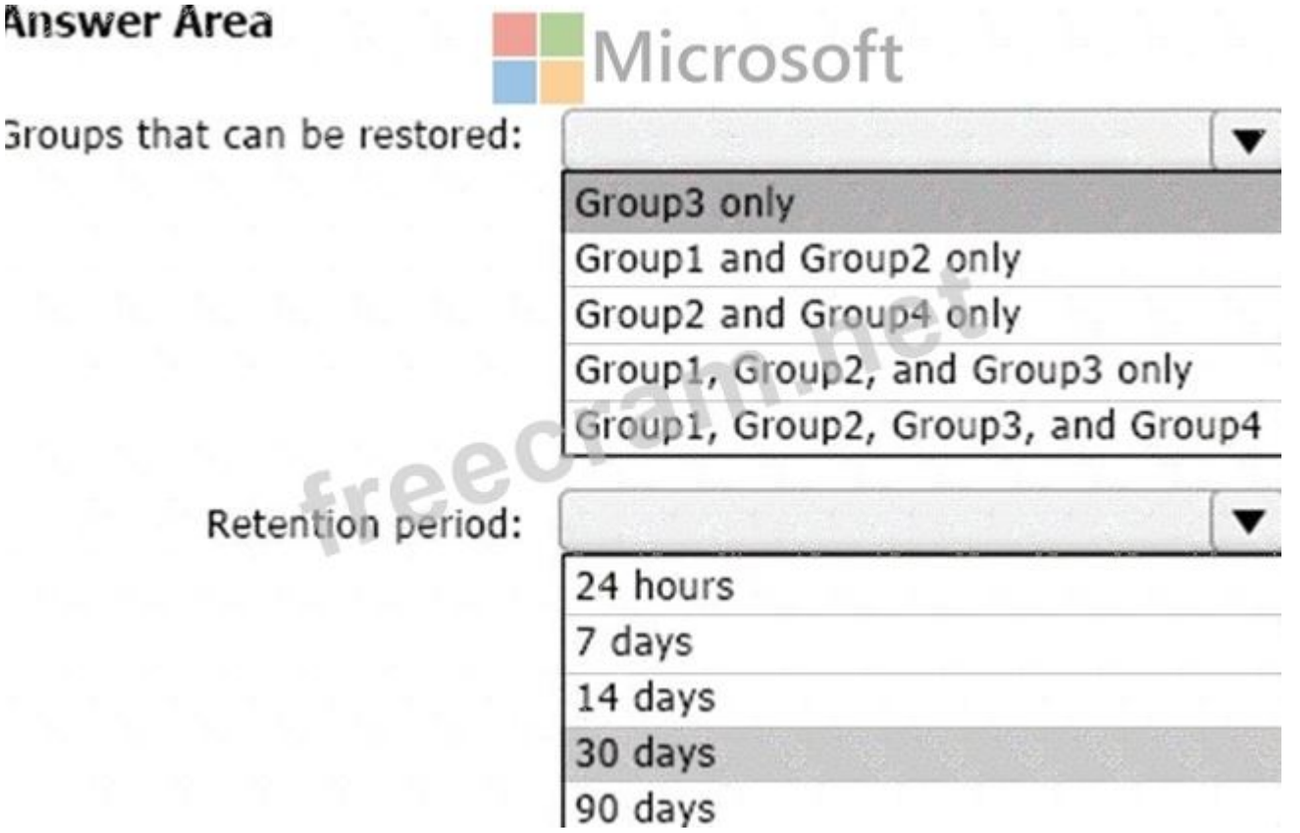
Groups that can be restored:

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

Retention period:

- 24 hours
- 7 days
- 14 days
- 30 days
- 90 days

Explanation



Box 1: Group3 only

Box 2: 30 days

If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a

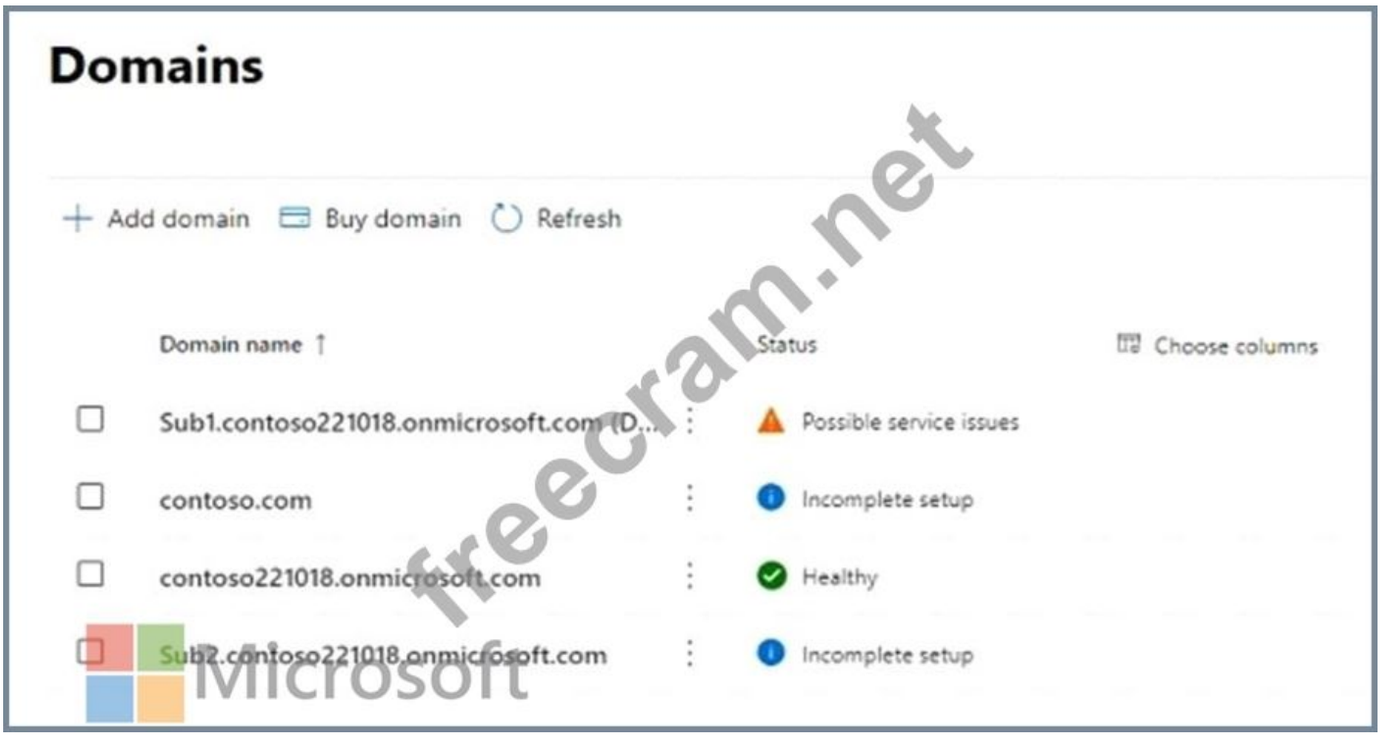
"soft-delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/restore-deleted-group

NEW QUESTION: 62

You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.



Which domain name suffixes can you use when you create users?

A. only Sub1.contoso221018.onmicrosoft.com

B. onlvcontoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com

C. all the domains in the subscription

D. onlycontoso.com and Sub2.contoso221018.onmicrosoft.com

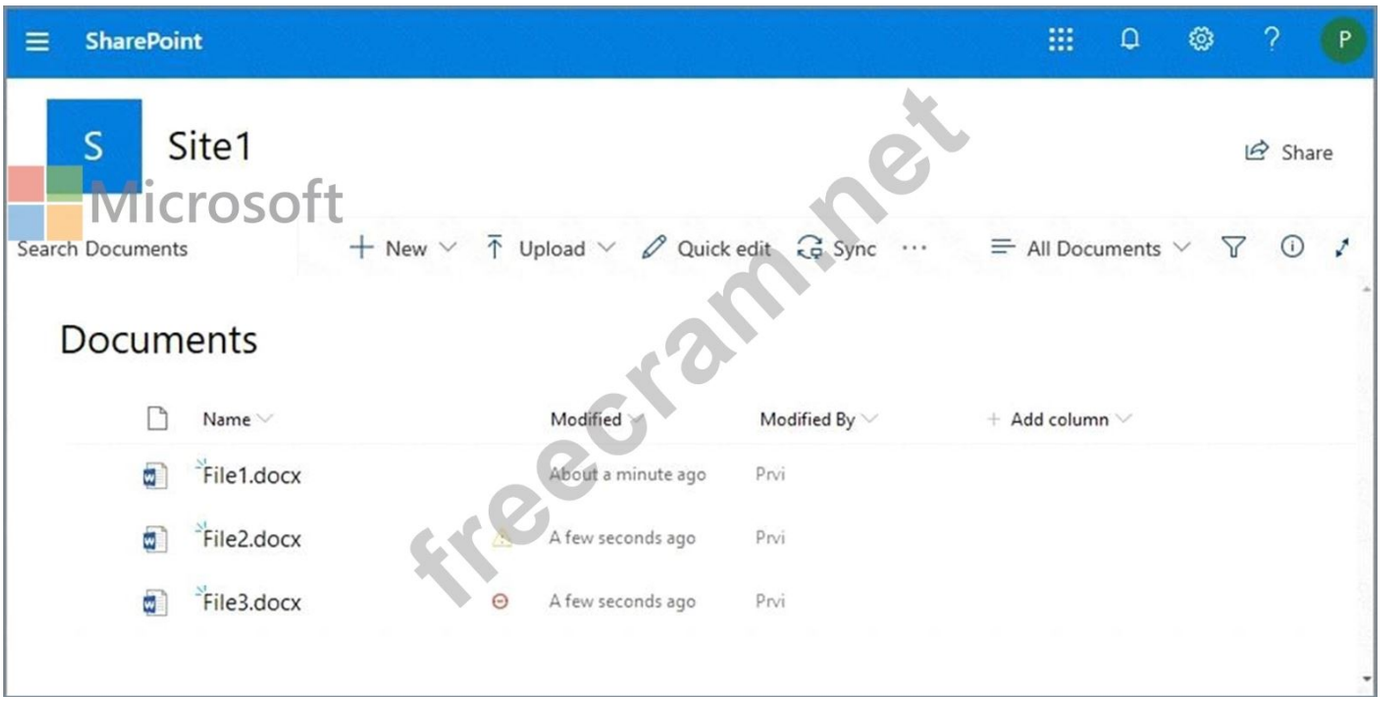
Answer: (SHOW ANSWER)

NEW QUESTION: 63

From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

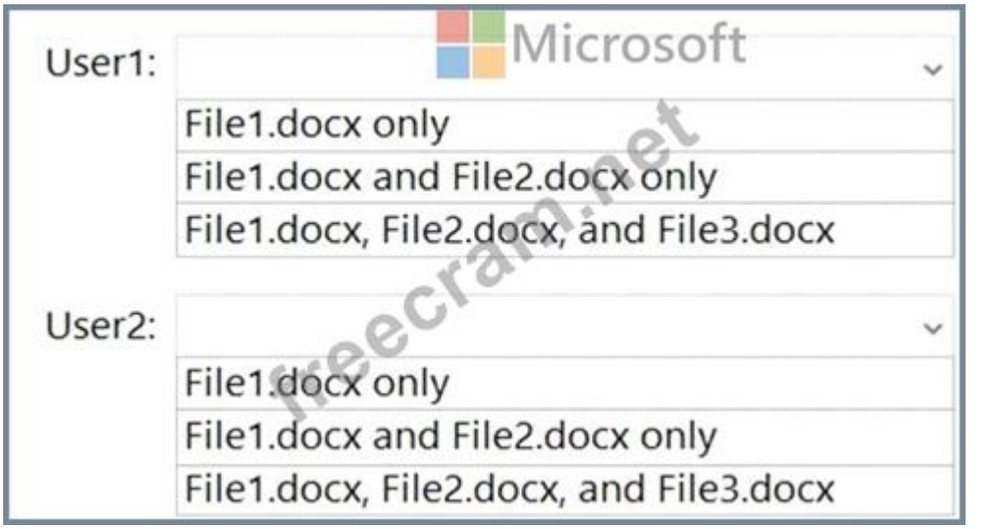
Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)



Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.

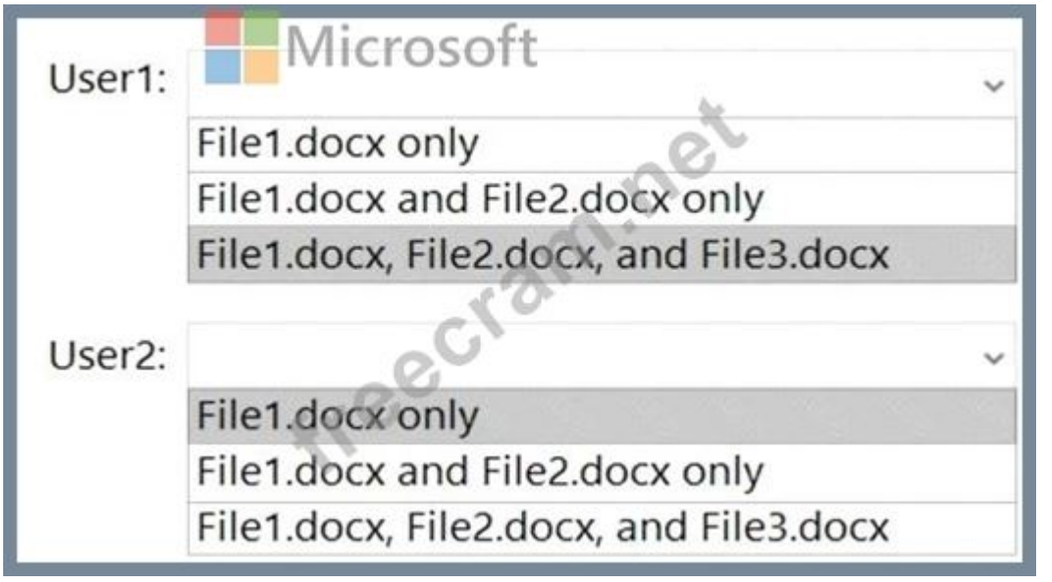
NOTE: Each correct selection is worth one point.



Answer:

Explanation

Graphical user interface, text, application, email Description automatically generated



Reference:

https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/

https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/

NEW QUESTION: 64

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

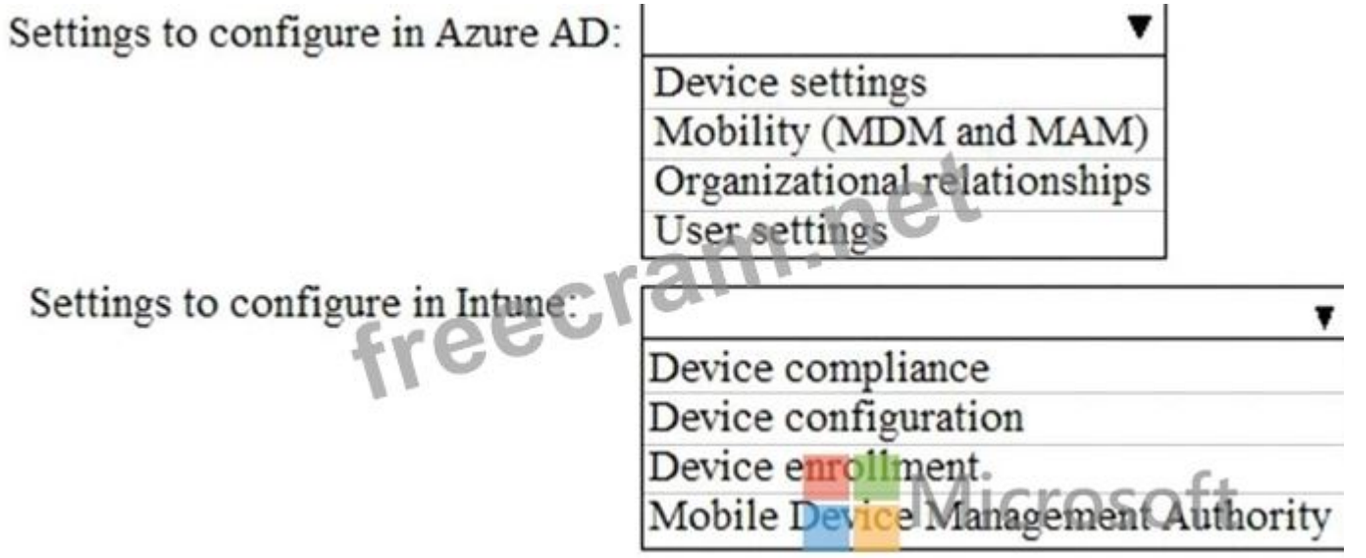
Answer: (SHOW ANSWER)

NEW QUESTION: 65

You need to meet the Intune requirements for the Windows 10 devices.

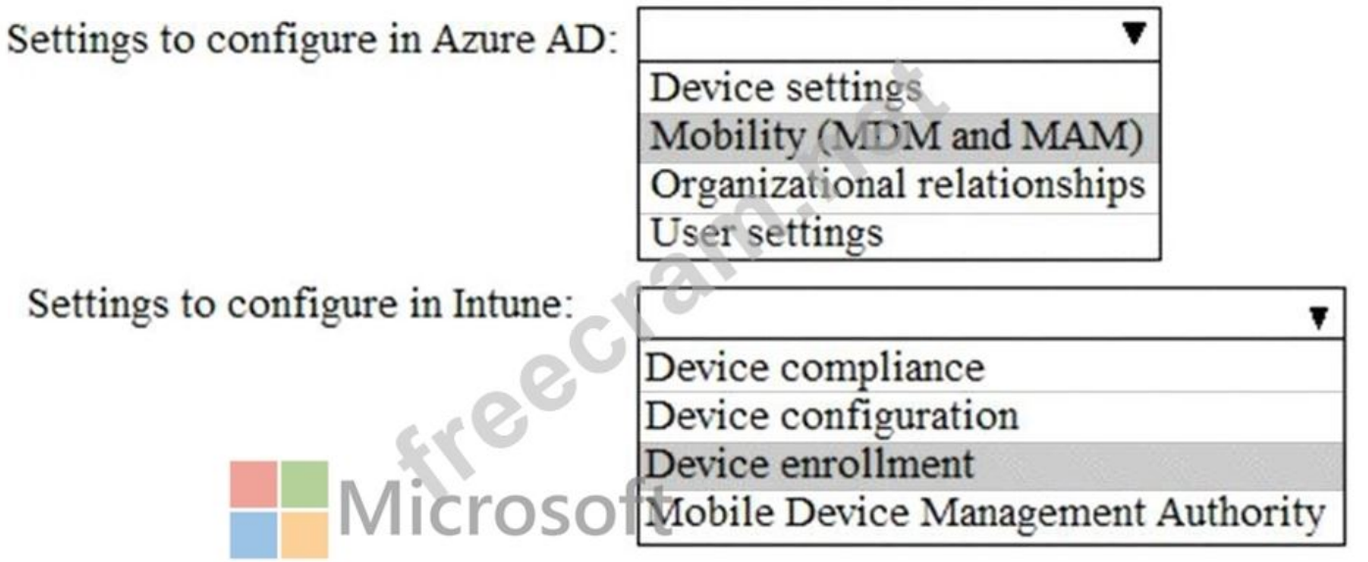
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation

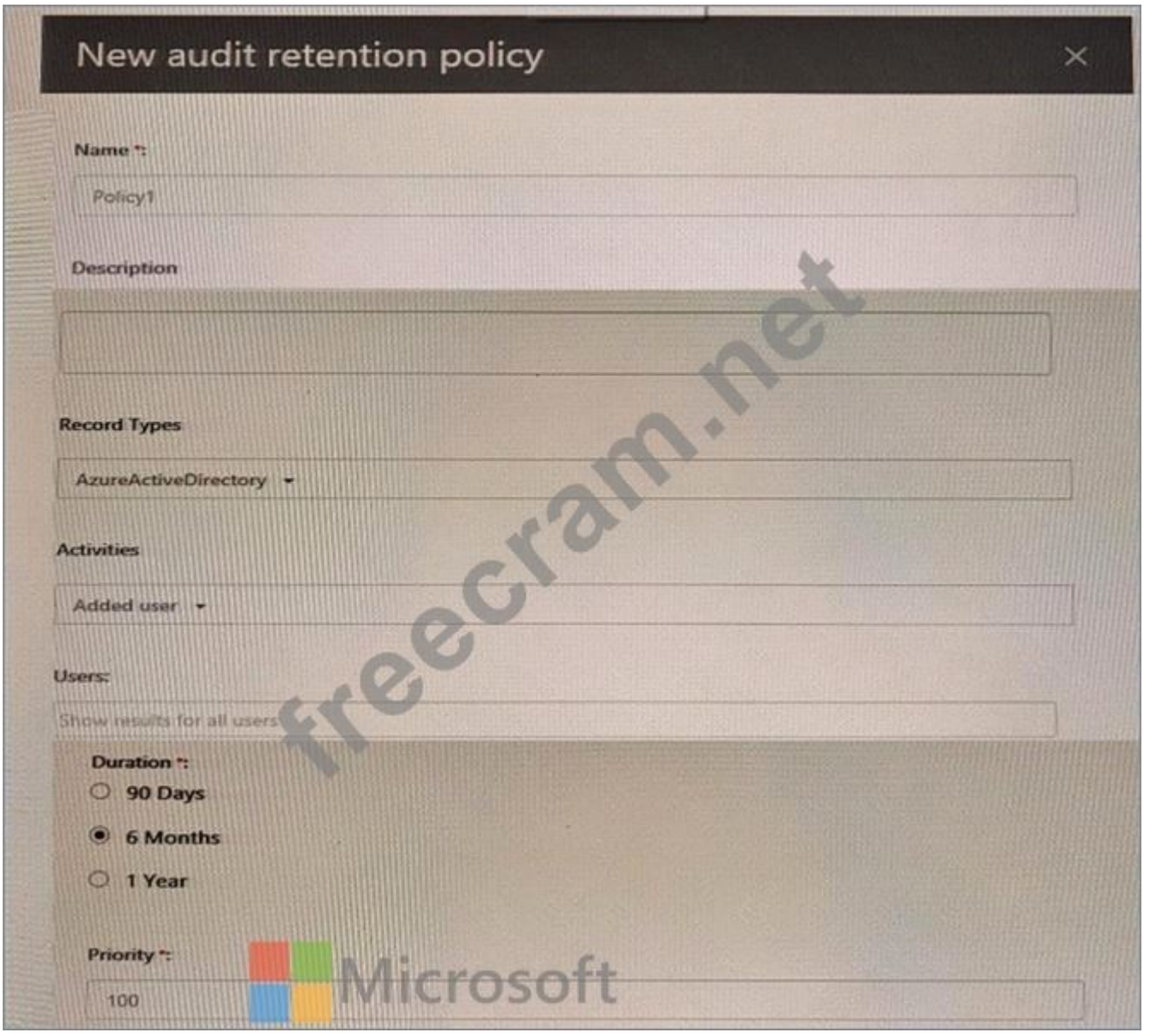


References:
https://docs.microsoft.com/en-us/intune/windows-enroll

NEW QUESTION: 66
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: 67
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*

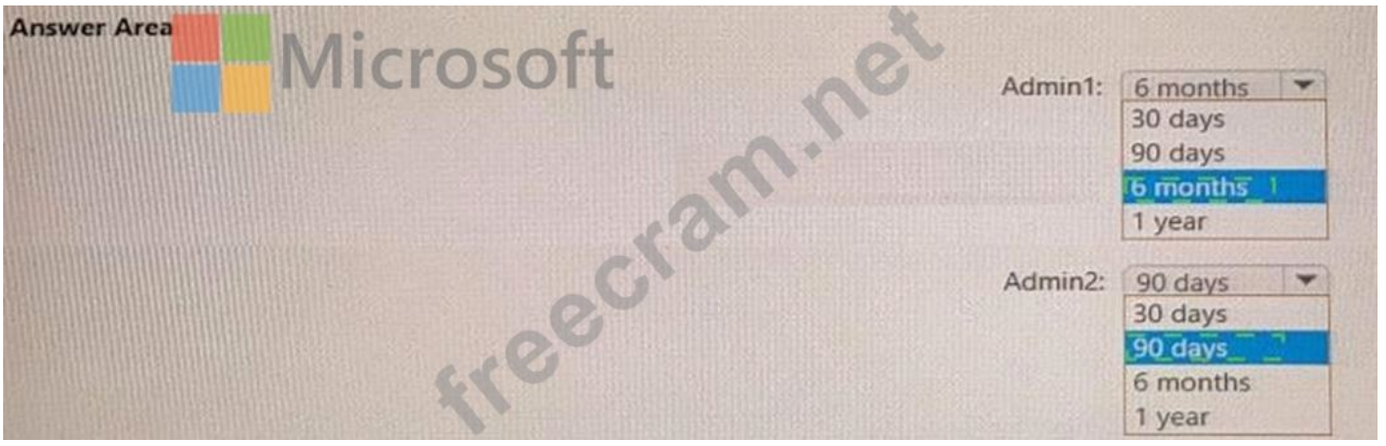


You plan to create a new user named User1.

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: 68

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 start-ADSyncSyncCycle cmdlet.

B. From PowerShell, run the Add-ADSyncConnectorAttnbuteinclusion cmdlet.

C. From the Microsoft Azure AD Connect wizard, select Manage federation.

D. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.

Answer: (SHOW ANSWER)

NEW QUESTION: 69

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

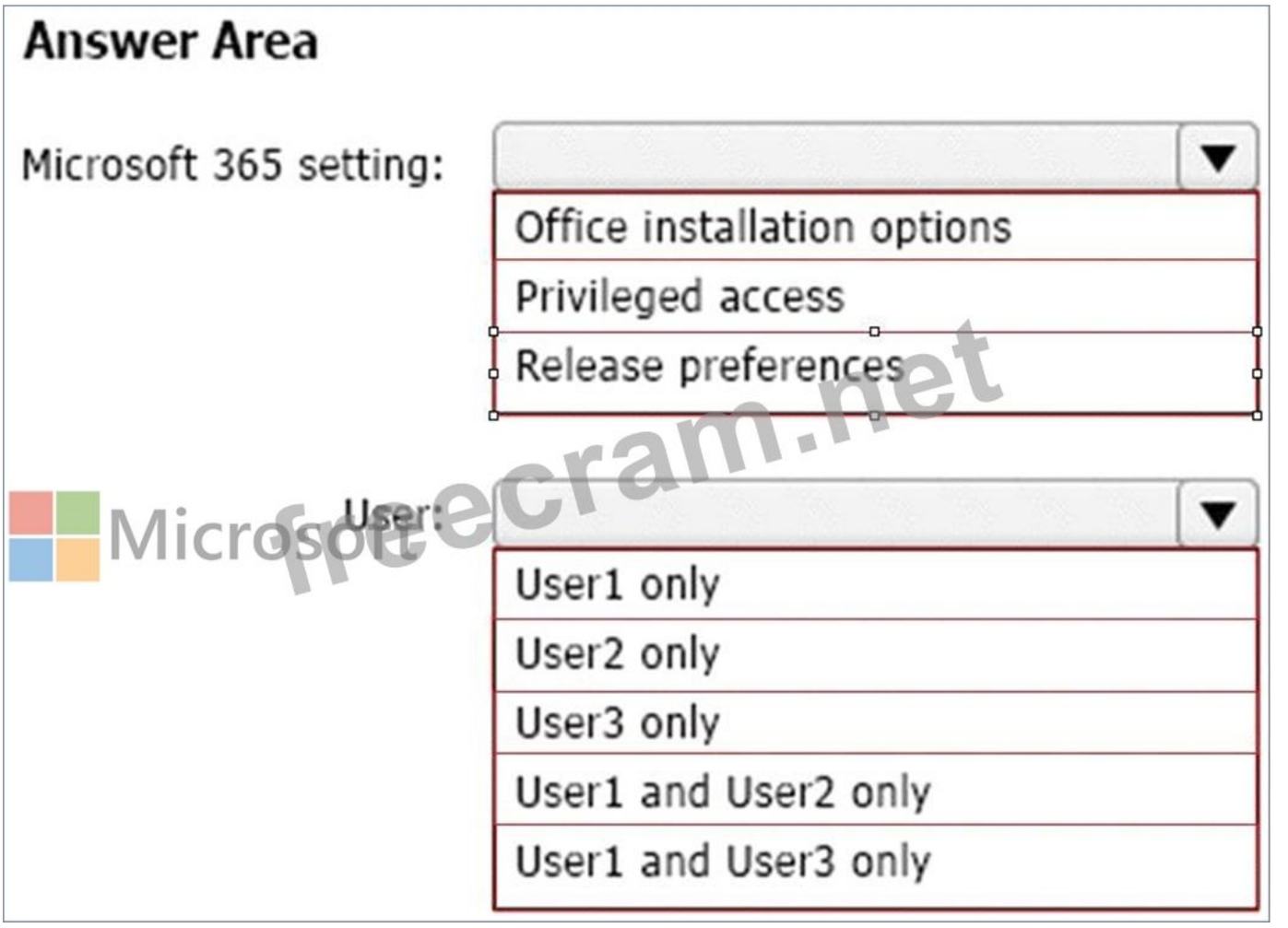
You plan to provide User4 with early access to Microsoft 365 feature and service updates.

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

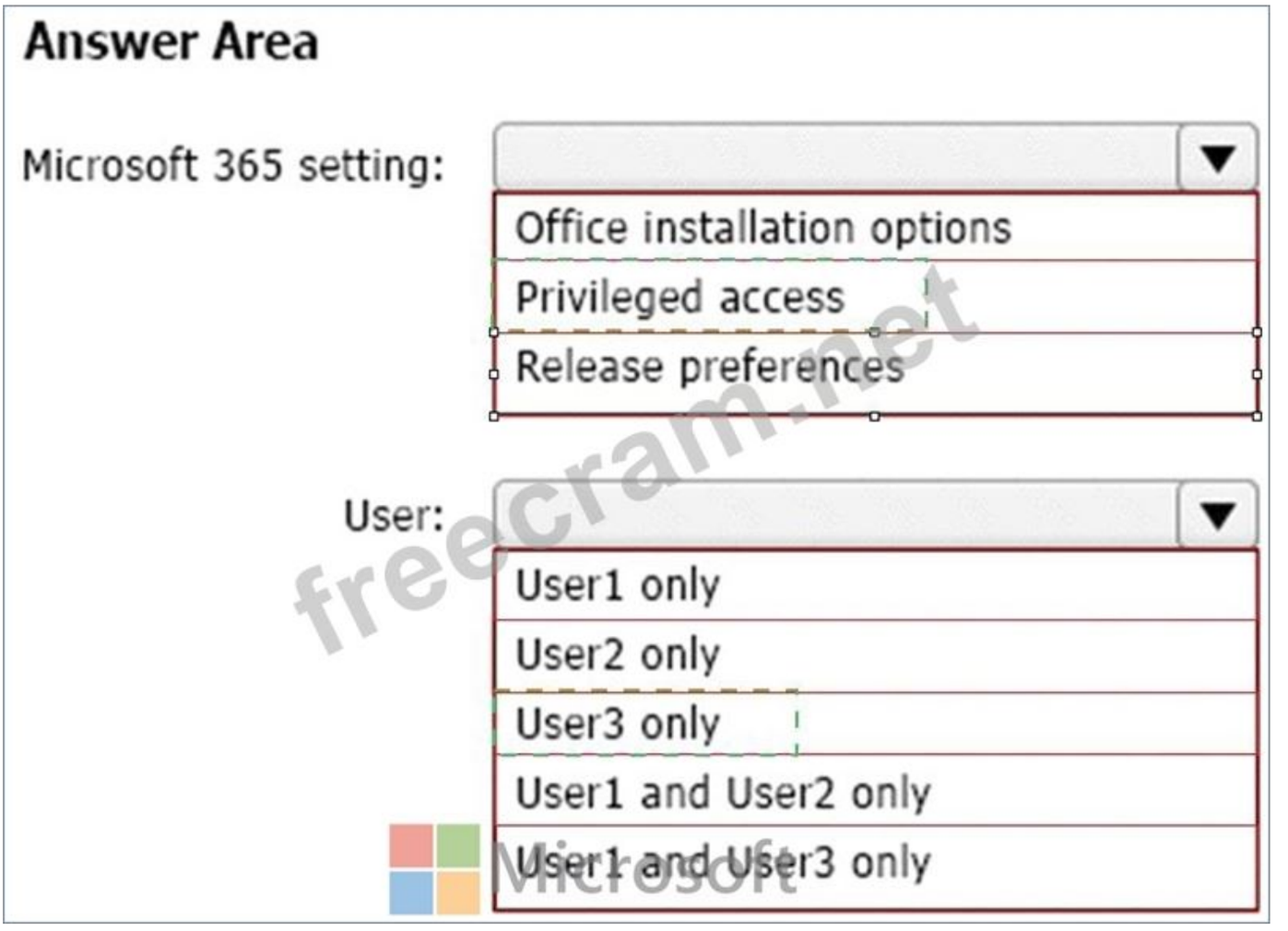
The solution must use the principle of least privilege.

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

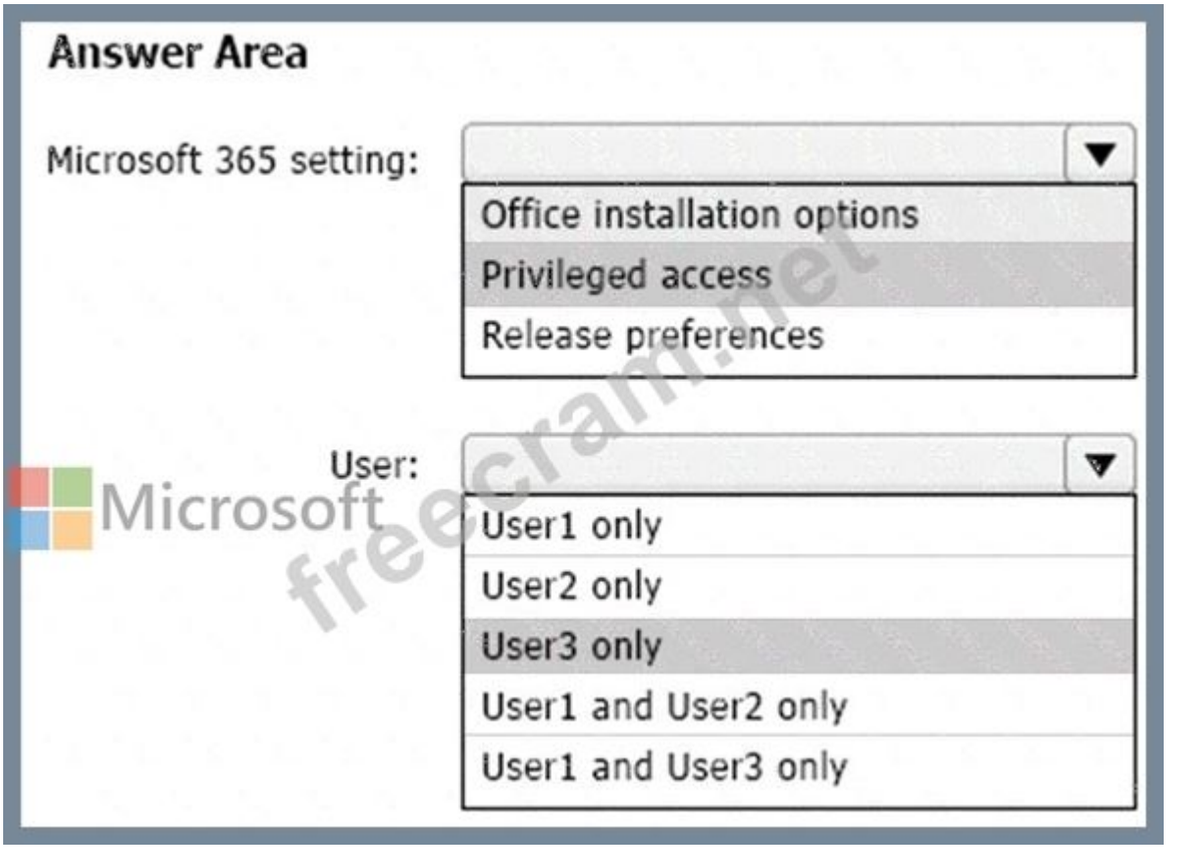
NOTE: Each correct selection is worth one point.


Answer Area
Microsoft 365 setting:
Office installation options
Privileged access
Release preferences
User:
User1 only
User2 only
User3 only
User1 and User2 only
User1 and User3 only

Answer:



Explanation



NEW QUESTION: 70

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)

Explanation

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-

NEW QUESTION: 71

HOTSPOT

Your company uses a legacy on-premises LDAP directory that contains 100 users.

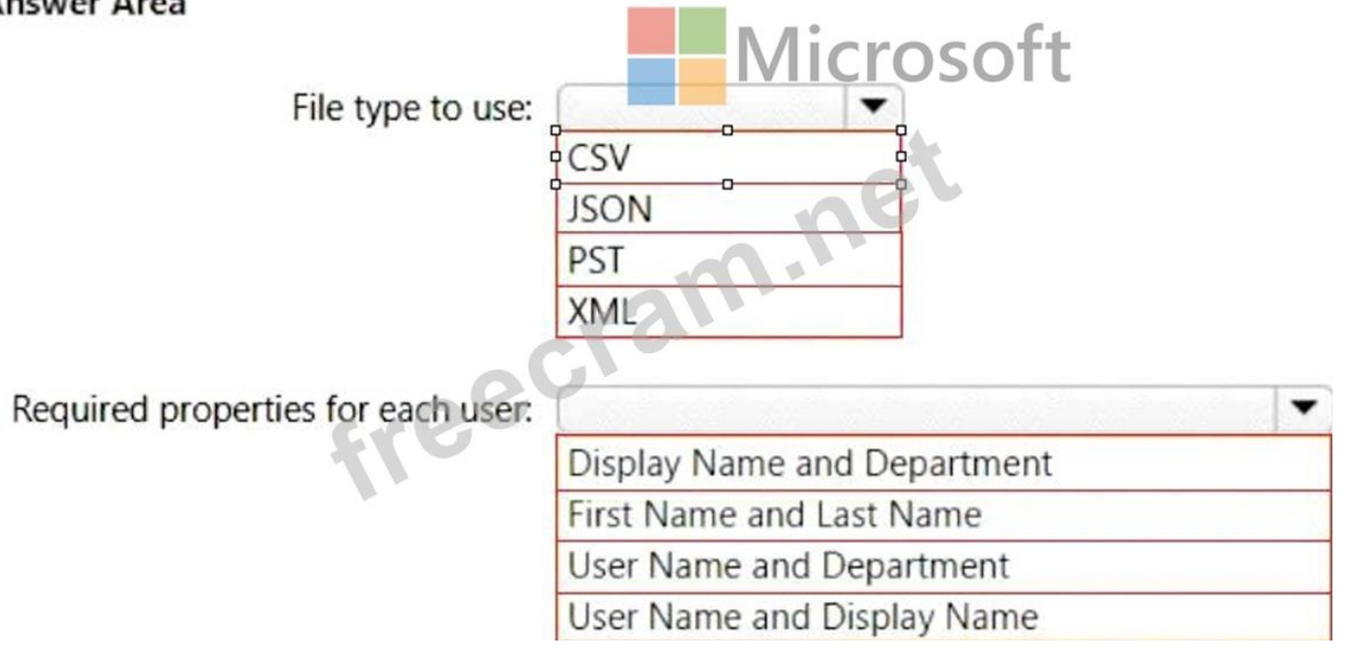
The company purchases a Microsoft 365 subscription.

You need to import the 100 users into Microsoft 365 by using the Microsoft 365 admin center.

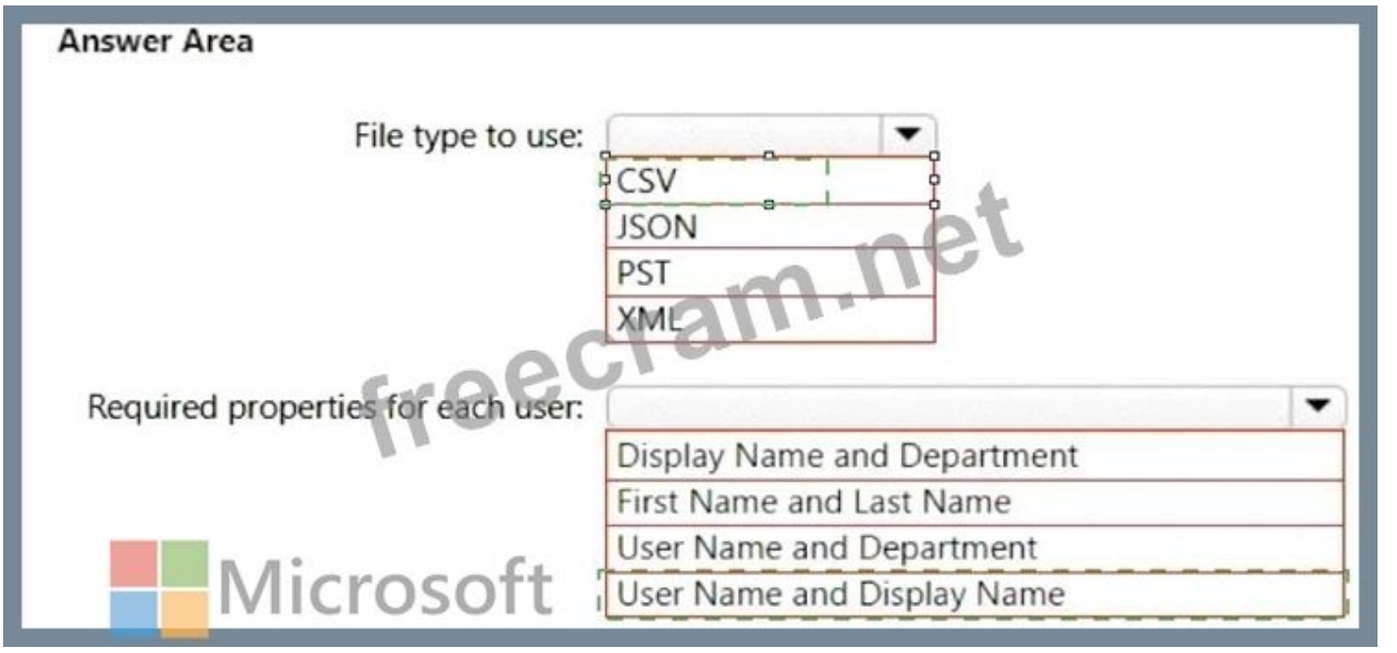
Which type of file should you use and which properties are required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

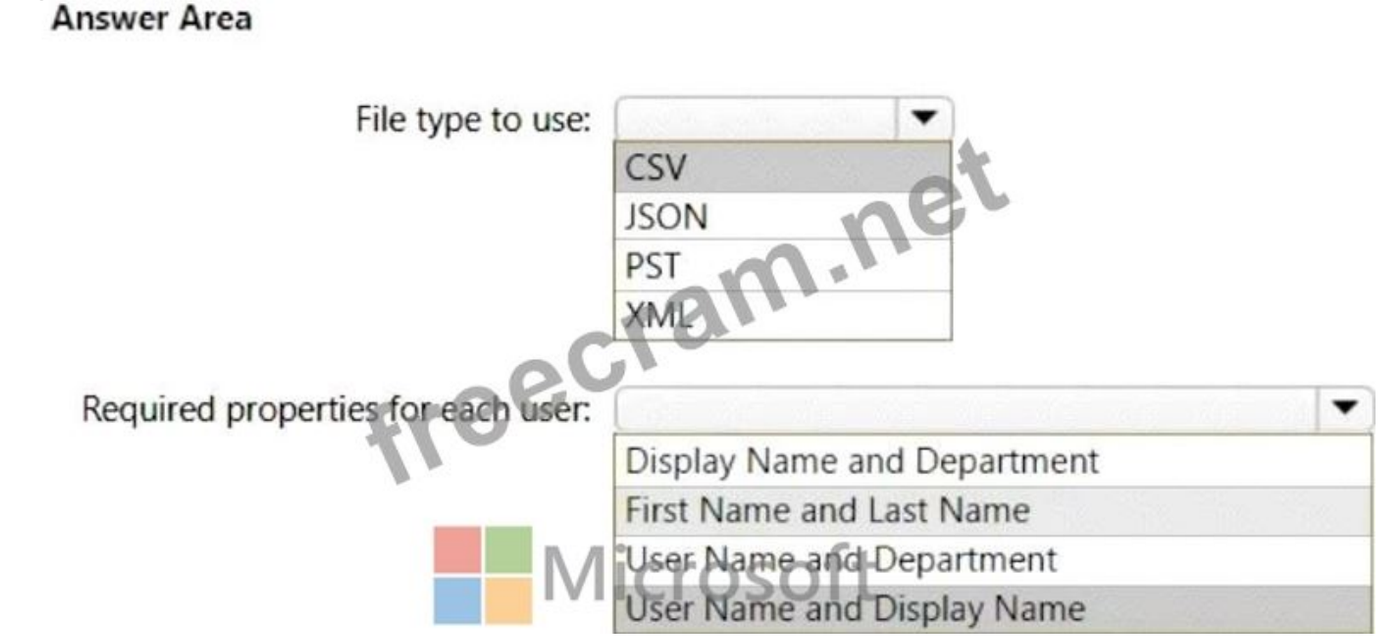
Answer Area



Answer:



Explanation



Box 1: CSV

Add multiple users in the Microsoft 365 admin center

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

In the admin center, choose Users > Active users.

Select Add multiple users.

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

Etc.

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

Not sure what CSV format is?

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

Box 2: User Name and Display Name

What if I don't have all the information required for each user? The user name and display name are required, and you cannot add a new user without this information. If you don't have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/enterprise/add-several-users-at-the-same-time

NEW QUESTION: 72
You have a Microsoft 365 subscription.
You have the retention policies shown in the following table.

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

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx.
File1.docx was created on January 1, 2022 and last modified on January 31,2022. The file was NOT modified again.
When will File1.docx be deleted automatically?
A. January 1,2023
B. January 1,2024
C. January 31, 2023
D. January 31, 2024
E. never
Answer: (SHOW ANSWER)
Explanation
Retention wins over deletion.
Note:
Explanation for the four different principles:
1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system-initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.
2. Etc.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

NEW QUESTION: 73
You have a Microsoft 365 subscription that contains the devices shown in the following table.

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

You install Microsoft Word on all the devices.

You plan to configure policies to meet the following requirements:

* Word files created by using Windows devices must be encrypted automatically.
* If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
* For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.

Which type of polio/ should you configure for each device? To answer, drag the appropriate policy types to the correct devices. 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

NEW QUESTION: 74

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

NEW QUESTION: 75
You have a Microsoft 365 E5 subscription.
Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.
You need to implement passwordless authentication. The solution must support all the devices.
Which authentication method should you use?
A. FID02 compliant security keys
B. Microsoft Authenticator app
C. Windows Hello
Answer: (SHOW ANSWER)

NEW QUESTION: 76
You have a Microsoft 365 E5 tenant.
You plan to deploy a monitoring solution that meets the following requirements:
* Captures Microsoft Teams channel messages that contain threatening or violent language.
* Alerts a reviewer when a threatening or violent message is identified.
What should you include in the solution?
A. Audit log retention policies
B. Insider risk management policies
C. Data Subject Requests (DSRs)
D. Communication compliance policies
Answer: (SHOW ANSWER)

NEW QUESTION: 77
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.
Corporate policy states that user passwords must not include the word Contoso.

What should you do to implement the corporate policy?

A. From Azure AD Identity Protection, configure a sign-in risk policy.

B. From the Microsoft Entra admin center, configure the Password protection settings.

C. From the Microsoft Entra admin center, create a conditional access policy.

D. From the Microsoft 365 admin center, configure the Password policy settings.

Answer: (SHOW ANSWER)

NEW QUESTION: 78

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 that contains a user named User1.

You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.

Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

Reference:

https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/pe

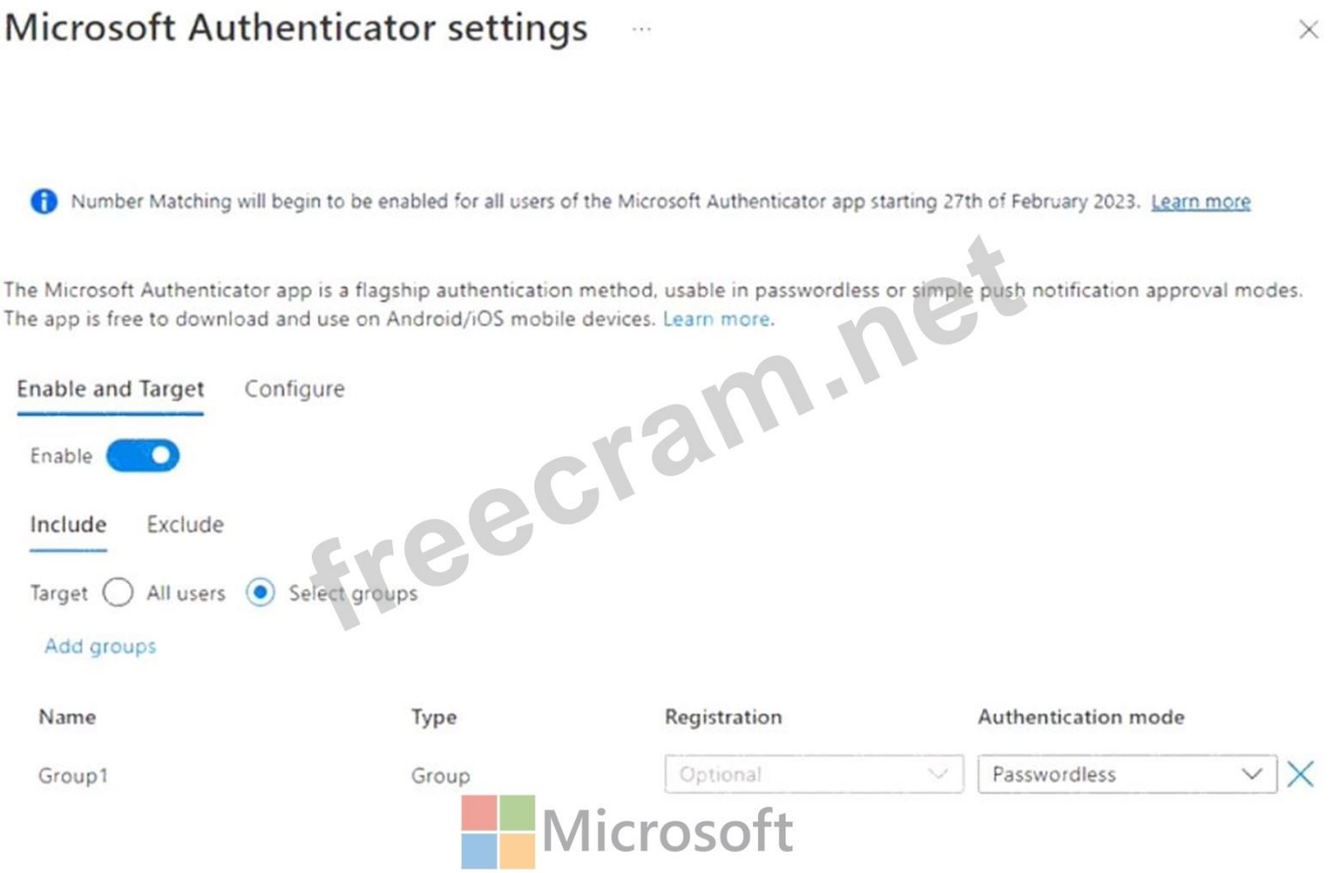
NEW QUESTION: 79

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

Name	Member of	Passwordless capable	Multi-factor authentication (MFA) method registered
User1	Group1	Capable	Microsoft Authenticator app (push notification)
User2	Group2	Capable	Microsoft Authenticator app (push notification)
User3	Group1, Group2	Capable	Mobile phone, Windows Hello for Business

Each user has a device with the Microsoft Authenticator app installed.

From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit 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 Area

Statements	Yes	No
User1 can use number matching during sign-in.	○	○
User2 can use number matching during sign-in.	○	○
User3 can use number matching during sign-in.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can use number matching during sign-in.	○	○
User2 can use number matching during sign-in.	○	○
User3 can use number matching during sign-in.	○	○

Explanation

Answer Area

Statements	Yes	No
User1 can use number matching during sign-in.	○	◉
User2 can use number matching during sign-in.	○	◉
User3 can use number matching during sign-in.	○	◉

NEW QUESTION: 80

You have a Microsoft 365 E5 subscription.

You plan to implement identity protection by configuring a sign-in risk policy and a user risk policy.

Which type of risk is detected by each policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation

Answer Area

NEW QUESTION: 81

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. 4

B. 1

C. 3

D. 2

Answer: (SHOW ANSWER)

NEW QUESTION: 82

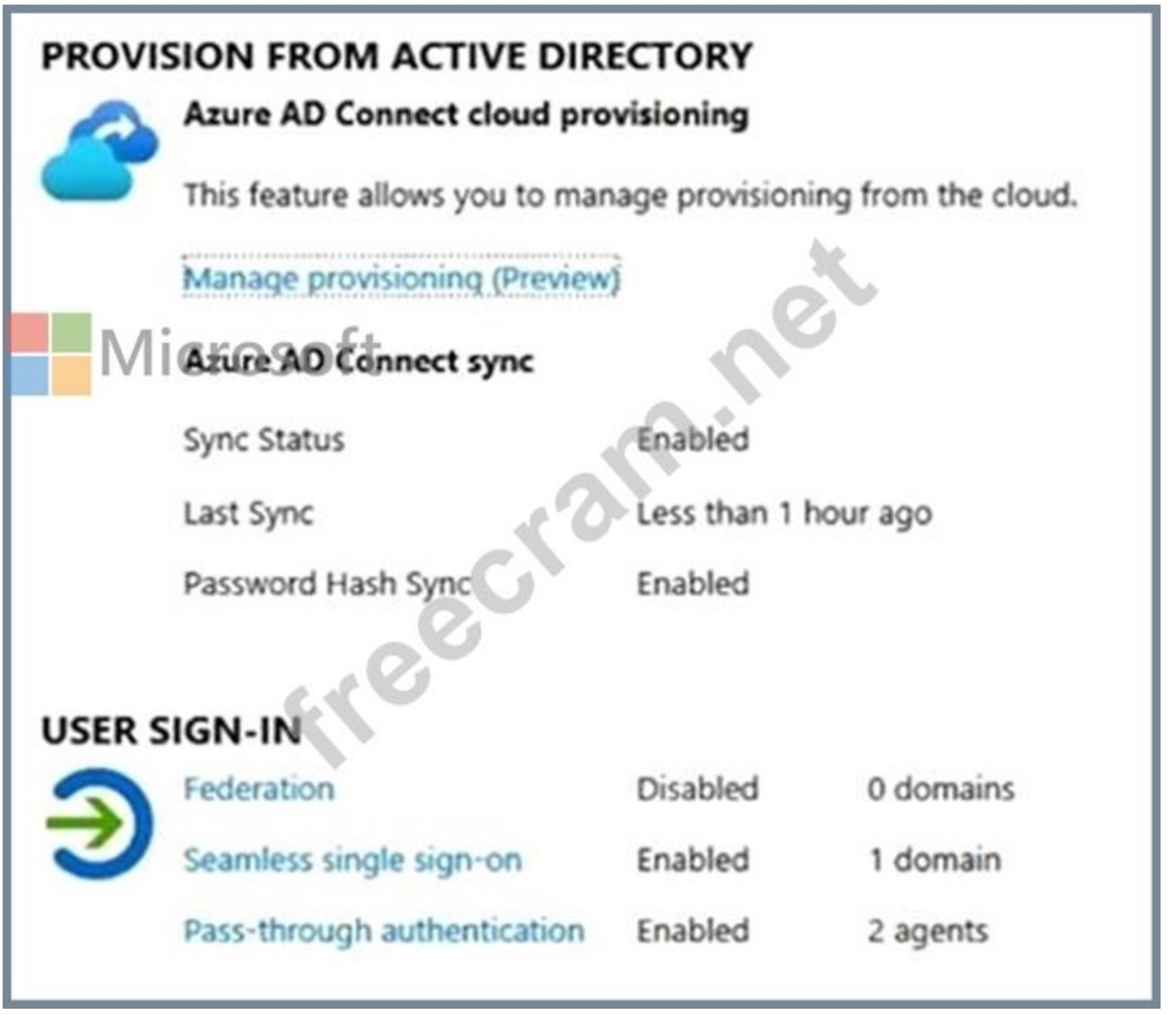
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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)
Explanation
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: 83

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 Alerts queue, create a suppression rule and assign an alert.
B. From Advanced hunting, create a query and a detection rule.
C. From the Microsoft Purview compliance portal, create an audit log search.
D. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 84
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: 85

You have a Microsoft 365 E5 tenant.

You need to evaluate compliance with European Union privacy regulations for customer data.

What should you do in the Microsoft 365 compliance center?

A. Create a Data Subject Request (DSR)

B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data

C. Create an assessment based on the EU GDPR assessment template

D. Create an assessment based on the Data Protection Baseline assessment template

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 86

HOTSPOT

You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

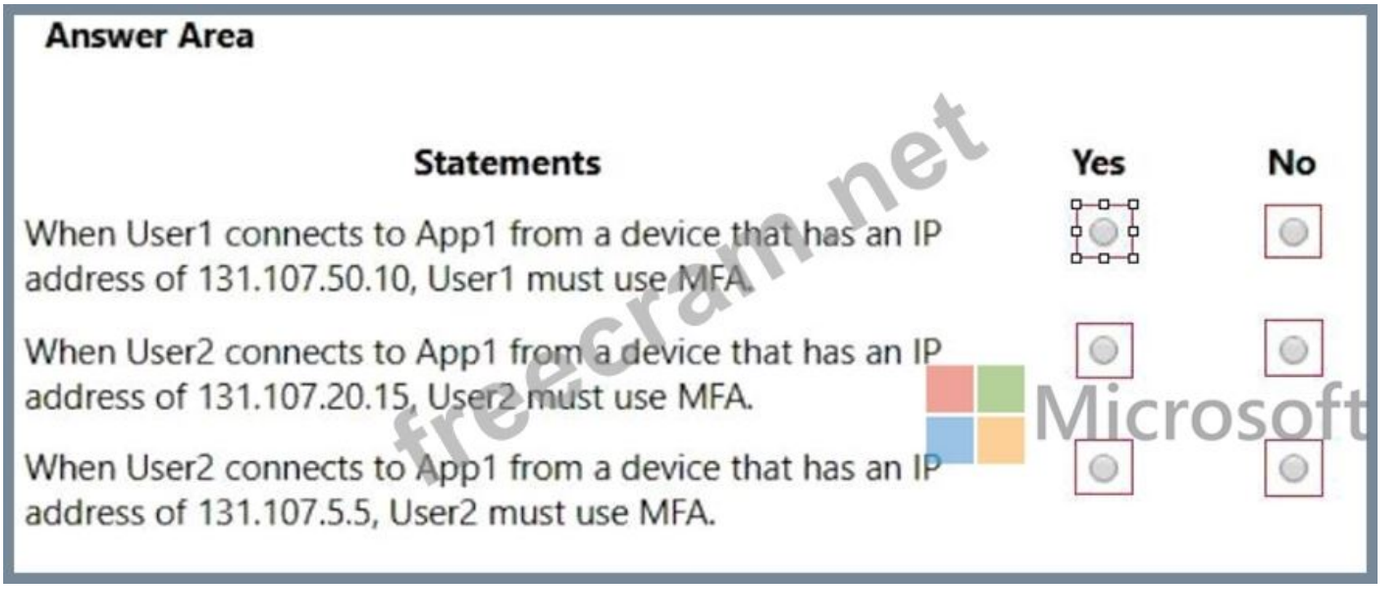
Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1	Enforced

Multi-factor authentication (MFA) 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

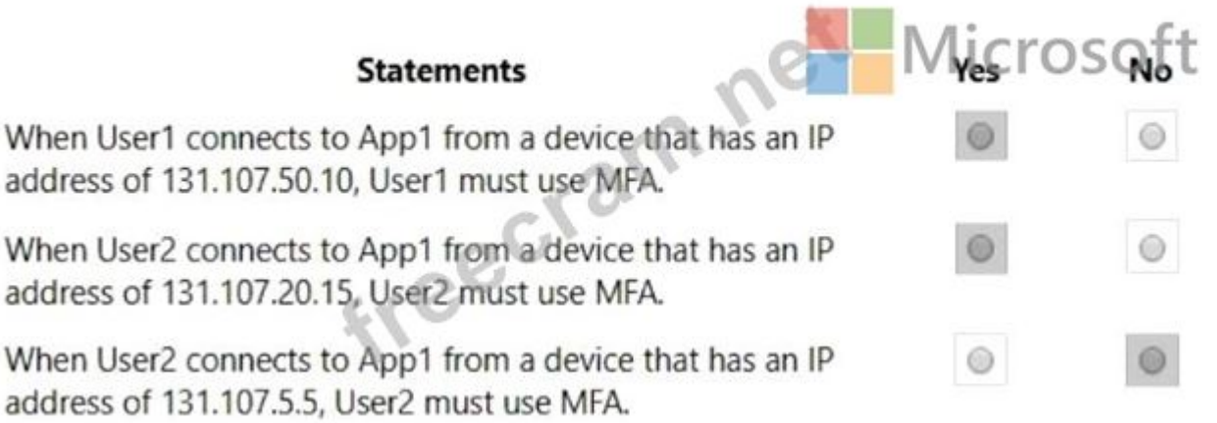
You create a conditional access policy that has the following configurations:
Users or workload identities assignments: All users
Cloud apps or actions assignment: App1
Conditions: Include all trusted locations
Grant access: Require multi-factor authentication
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer:

Explanation

Answer Area



Box 1: Yes
131.107.50.10 is in a Trusted Location so the conditional access policy applies. The policy requires MFA.
However, User1's MFA status is disabled. The MFA requirement in the conditional access policy will override the user's MFA status of disabled. Therefore, User1 must use MFA.
Box 2: Yes.
131.107.20.15 is in a Trusted Location so the conditional access policy applies. The policy requires MFA so User2 must use MFA.
Box 3: No.
IP not from Trusted Location so Policy does not apply, Subnet 131.107.5.5 is not in the range of 131.107.50.0/24
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

NEW QUESTION: 87
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)
Explanation
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-worldwi

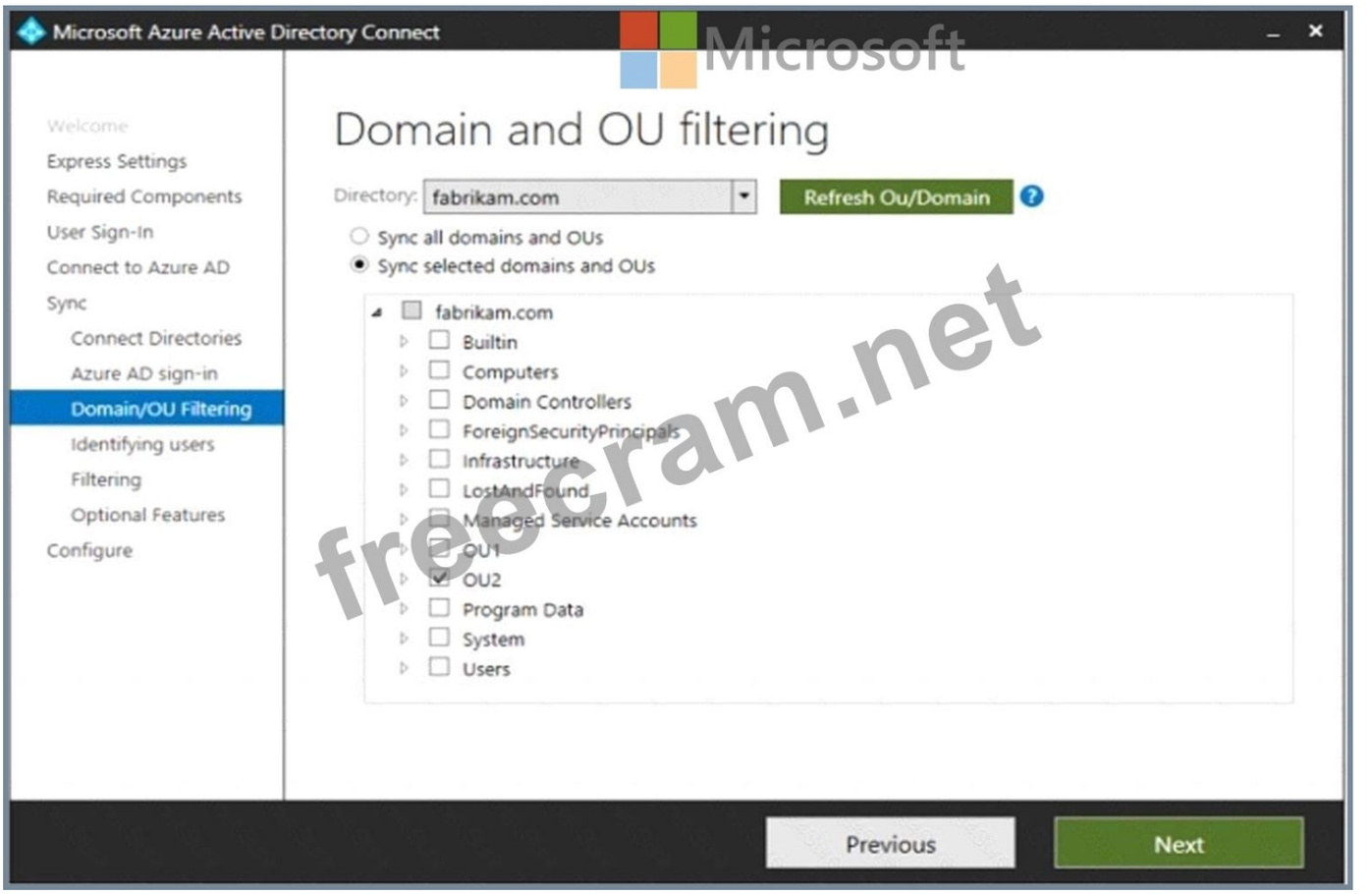
NEW QUESTION: 88
HOTSPOT
Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

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

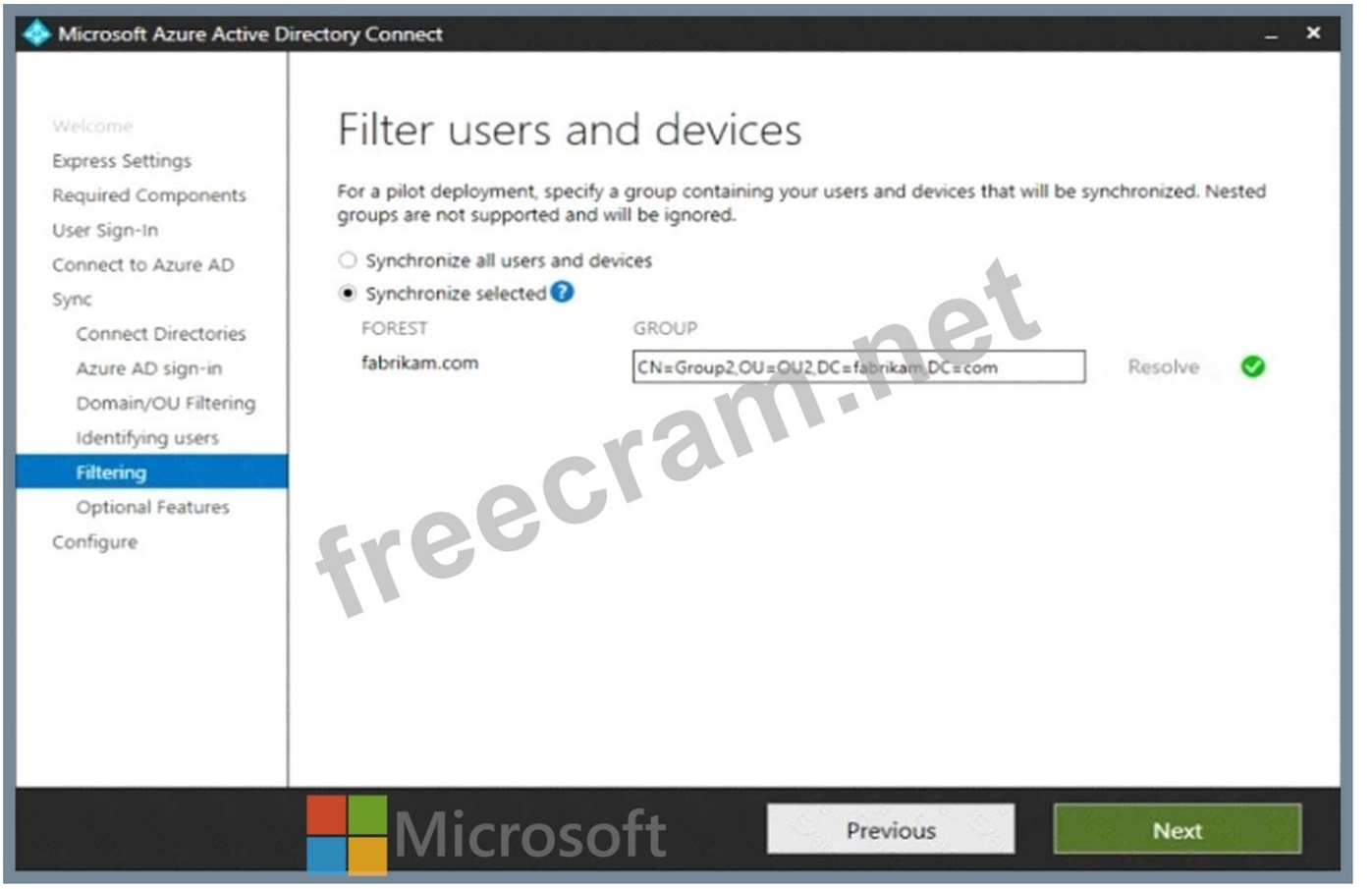
The groups have the members shown in the following table.

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.)



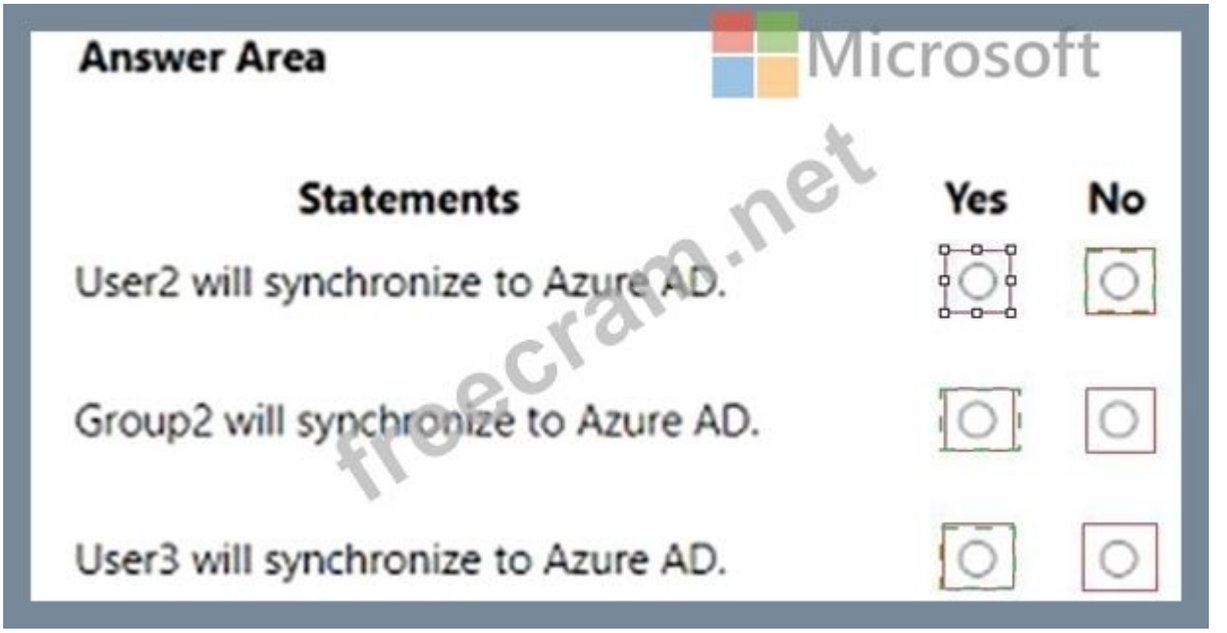
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:



Explanation

Box 1: No

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

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

Box 2: Yes

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

Box 3: Yes

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

Reference:

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

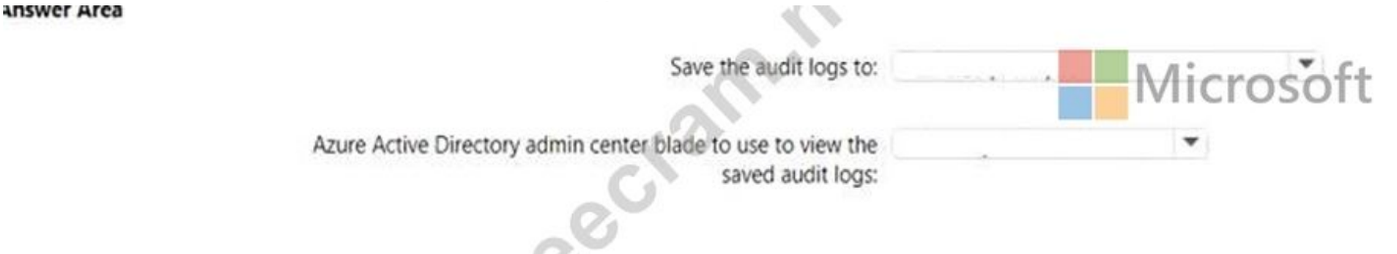
NEW QUESTION: 89

You have a Microsoft 365 tenant.

You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.

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

NOTE: Each correct selection is worth one point.



Answer:

See the answer below

Explanation

answer

NEW QUESTION: 90

You need to meet the compliance requirements for the Windows 10 devices.
What should you create from the Intune admin center?

A. an application policy

B. a device configuration profile

C. a device compliance policy

D. an app configuration policy

Answer: A (LEAVE A REPLY)

NEW QUESTION: 91

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)

Explanation

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.

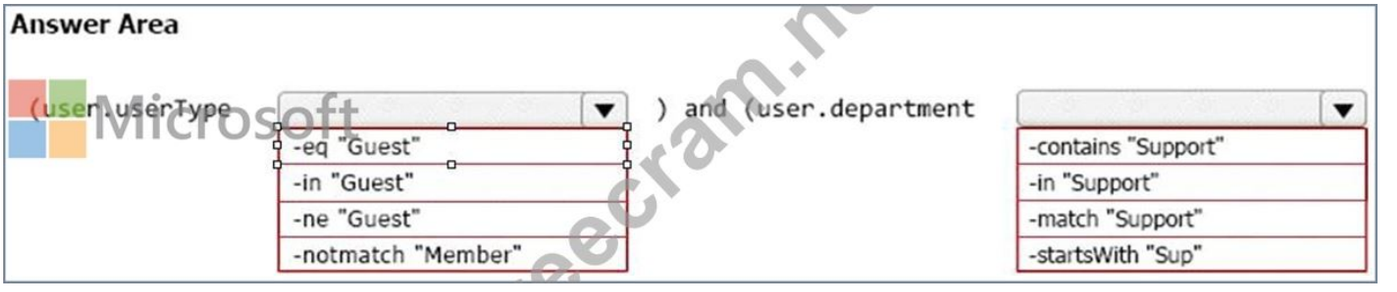
Configure the Azure AD multifactor authentication registration policy

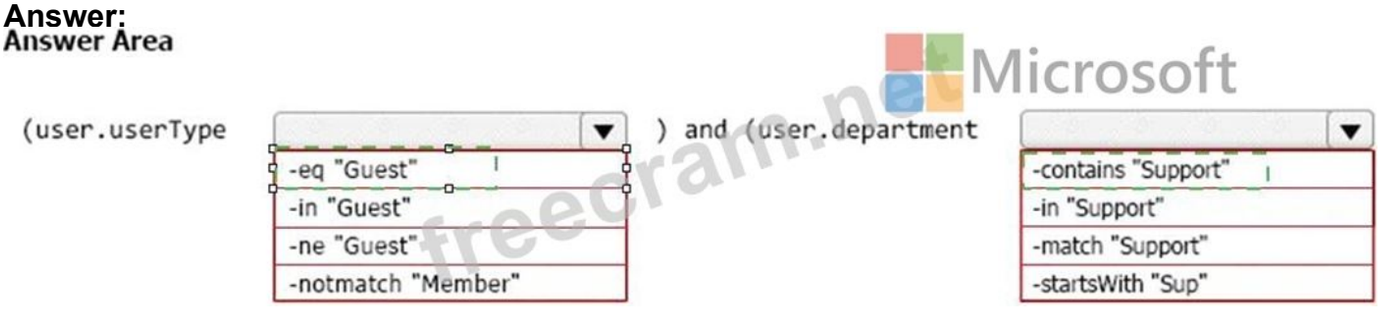
Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.
Reference:
https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname

NEW QUESTION: 92
HOTSPOT
You have a Microsoft 365 subscription that contains the users shown in the following table.

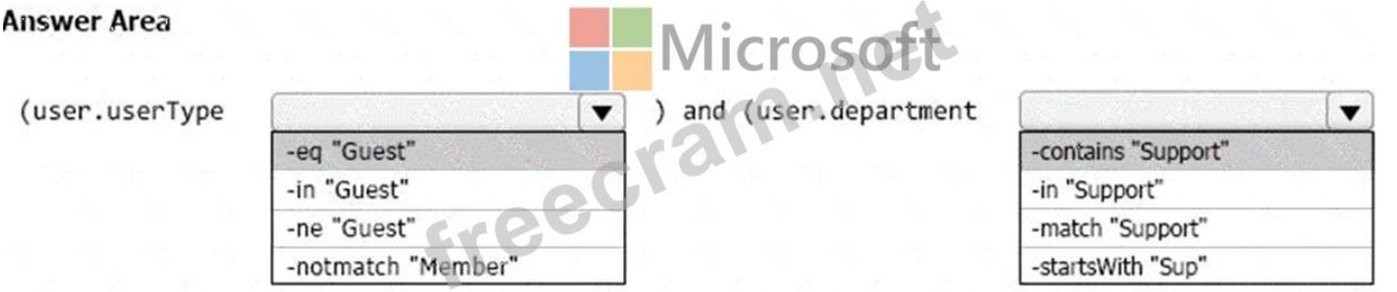
Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.
How should you complete the membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:


Explanation



Box 1: -eq "Guest"

Dynamic membership rules for groups in Azure Active Directory

Supported expression operators

The following table lists all the supported operators and their syntax for a single expression.

Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.

* Equals

-eq

* Contains

-contains

* Etc.

Box 2: -contains "Support"

Incorrect:

* -in

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

Reference:

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

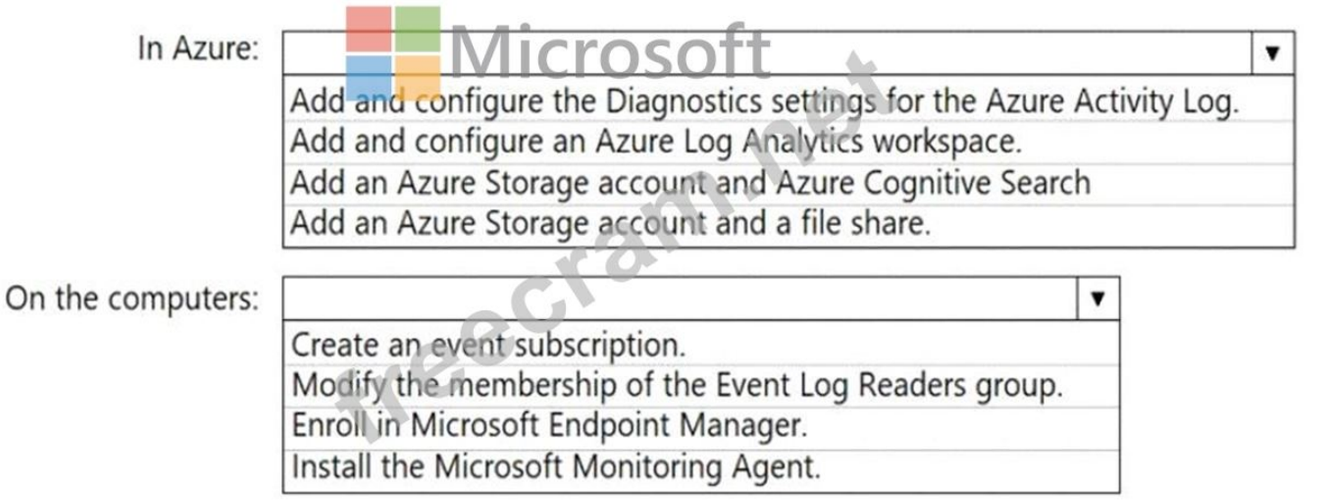
NEW QUESTION: 93

You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.

You need to centrally monitor System log events from the computers.

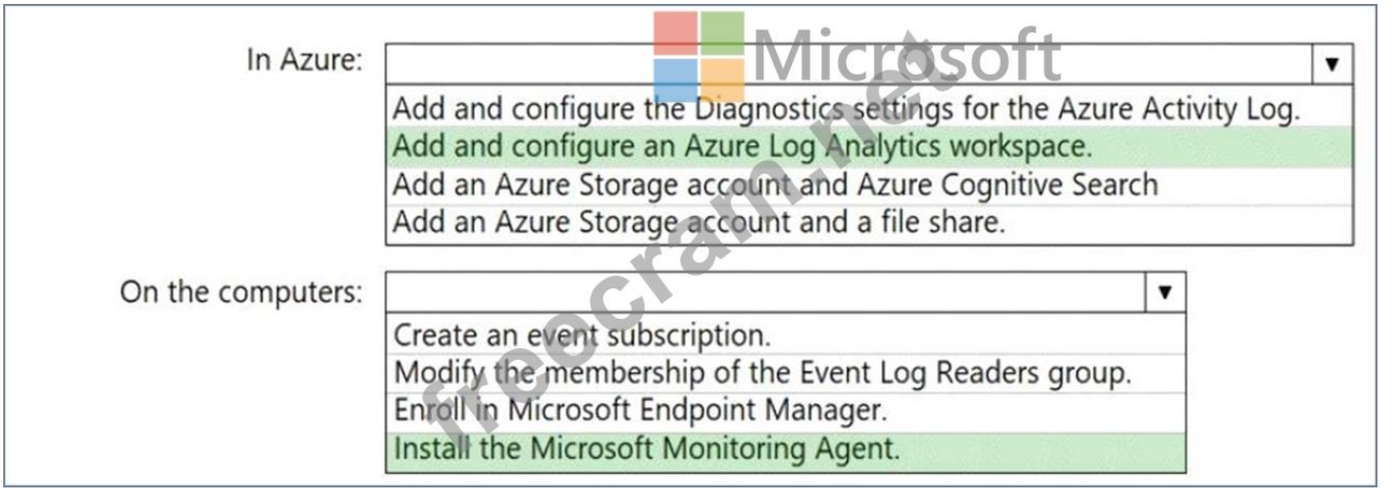
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation



Reference:

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

NEW QUESTION: 94

You have a Microsoft 365 E5 subscription.

You onboard all devices to Microsoft Defender for Endpoint

You need to use Defender for Endpoint to block access to a malicious website at

www.contoso.com.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct answer is worth one point.
A. Enable Custom network indicators.
B. Create a web content filtering policy.
C. Configure an enforcement scope.
D. Enable automated investigation.
E. Create an indicator.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 95
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 Area

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

Answer:

Explanation

NEW QUESTION: 96

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

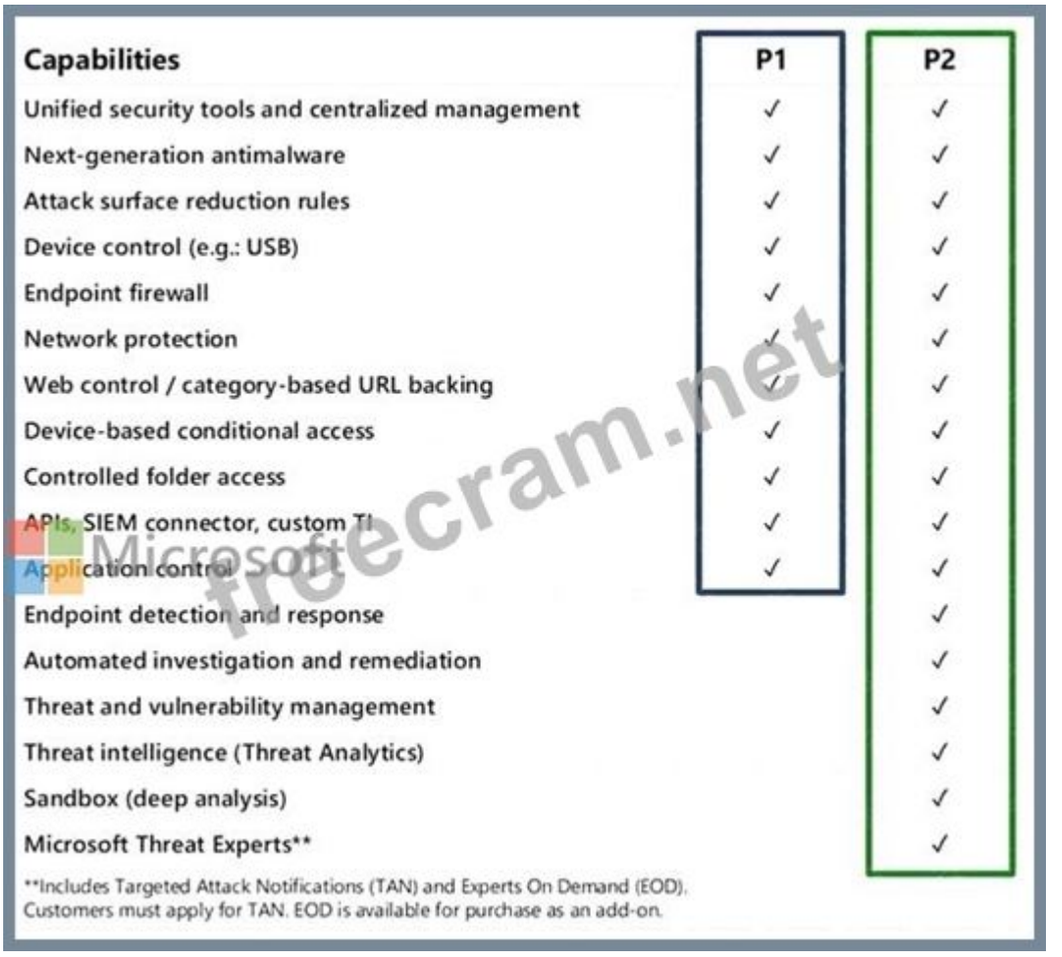
E. 5

Answer: (SHOW ANSWER)

Explanation
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-mo

NEW QUESTION: 97
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)
Explanation
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-

NEW QUESTION: 98

You need to meet the technical requirement for large-volume document retrieval. What should you create?

A. a data loss prevention (DLP) policy from the Security & Compliance admin center

B. an alert policy from the Security & Compliance admin center

C. a file policy from Microsoft Cloud App Security

D. an activity policy from Microsoft Cloud App Security

Answer: D (LEAVE A REPLY)

Explanation

References:

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

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 conditional access

B. a Microsoft Intune device compliance policy

C. Azure AD password protection

D. a Microsoft Intune device configuration profile

Answer: (SHOW ANSWER)

NEW QUESTION: 100

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

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

You ate implementing Microsoft Defender for Endpoint

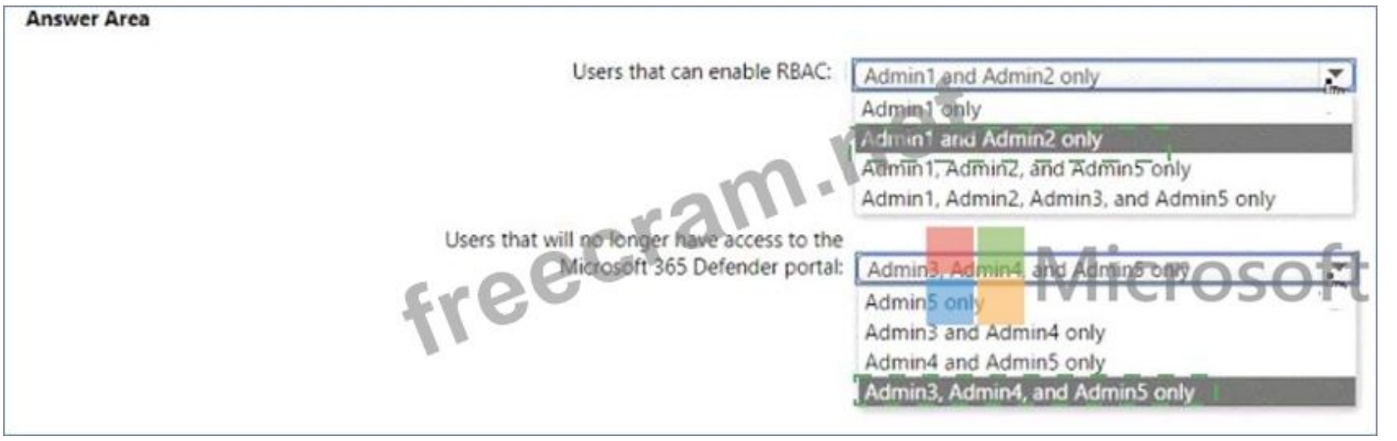
You need to enable role-based access control (RBAQ to restrict access to the Microsoft 365 Defender portal.

Which users can enable RBAC, and winch users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Answer Area

Answer:



Explanation

NEW QUESTION: 101

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

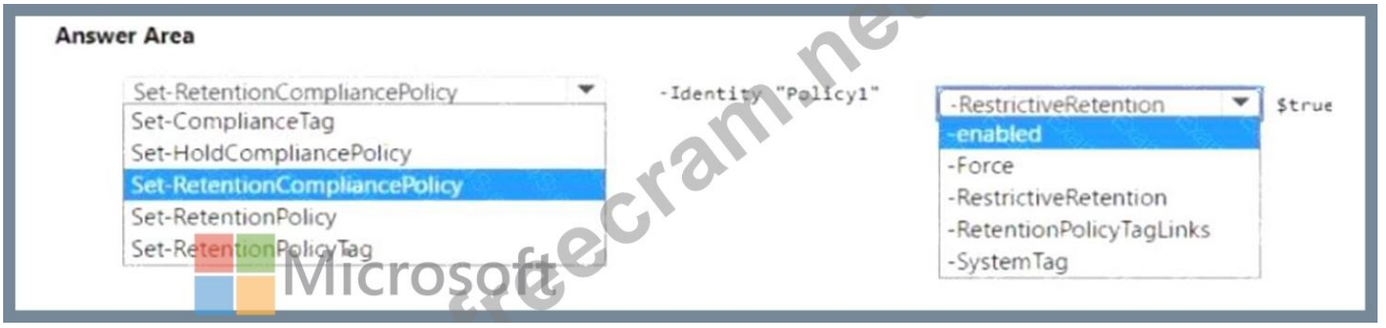
NEW QUESTION: 102

From the Microsoft Purview compliance portal, you create a retention policy named Policy 1.

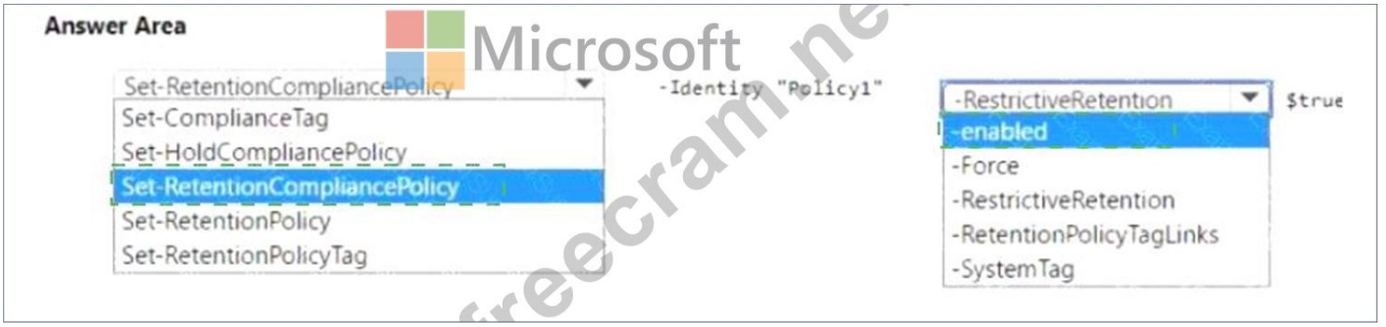
You need to prevent all users from disabling the policy or reducing the retention period.

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: 103

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

You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps.

Which policy type should you configure?

A. conditional access

B. account protection

C. attack surface reduction (ASR)

D. Endpoint detection and response

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 104

HOTSPOT

Your network contains an on-premises Active Directory domain.

You have a Microsoft 365 E5 subscription.

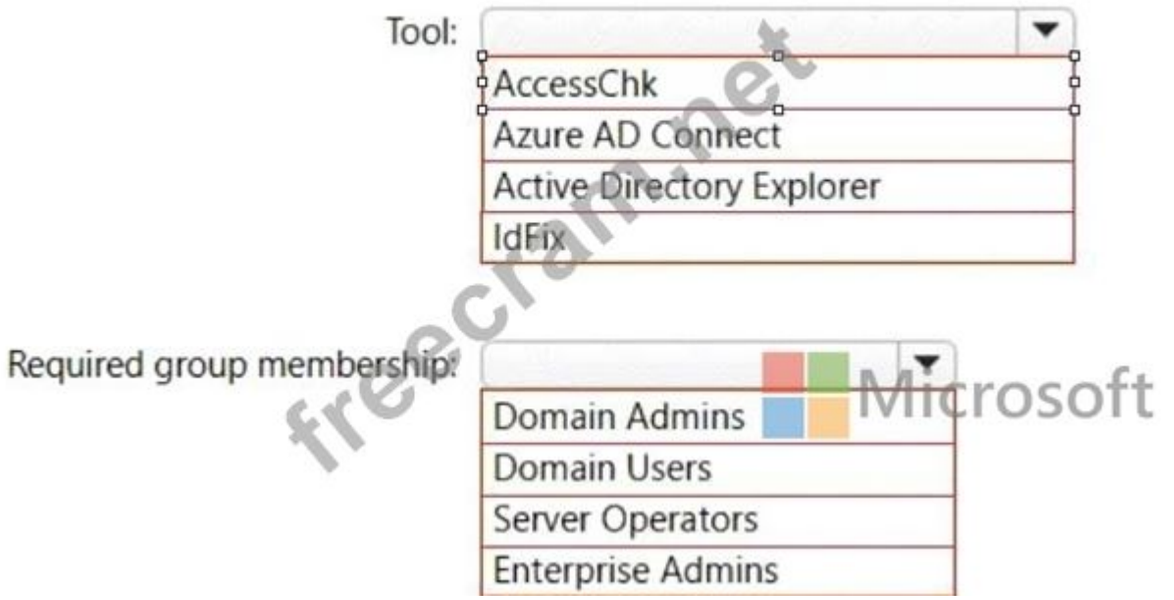
You plan to implement directory synchronization.

You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.

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

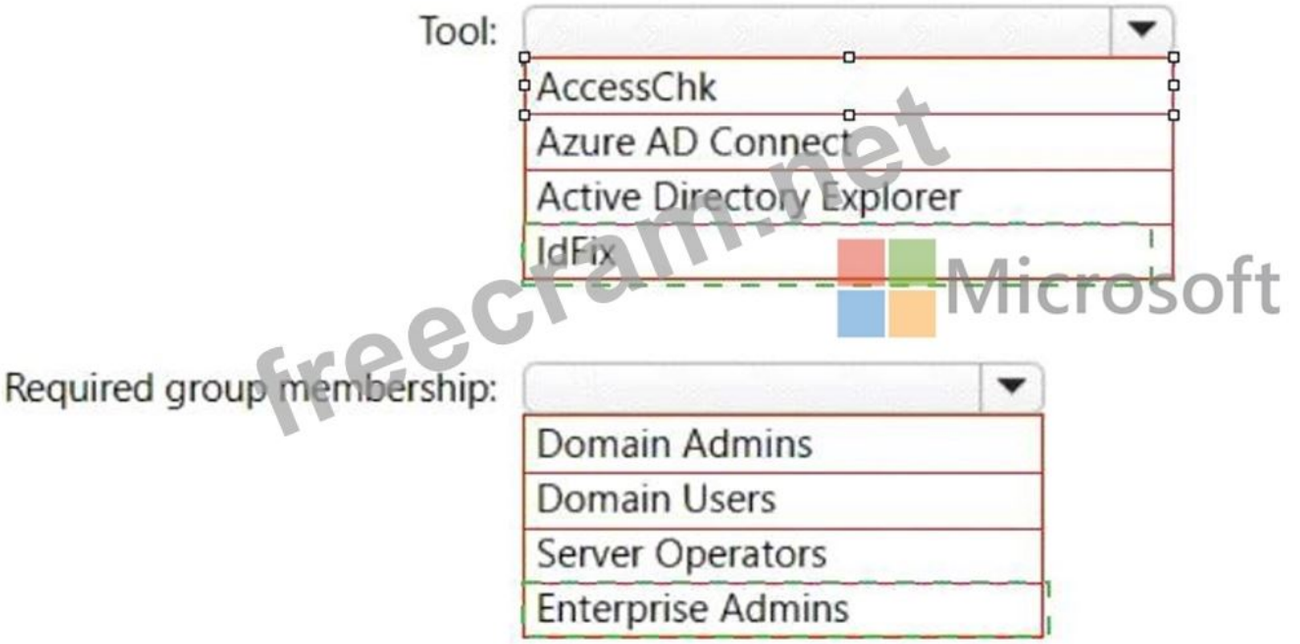
NOTE: Each correct selection is worth one point.

Answer Area



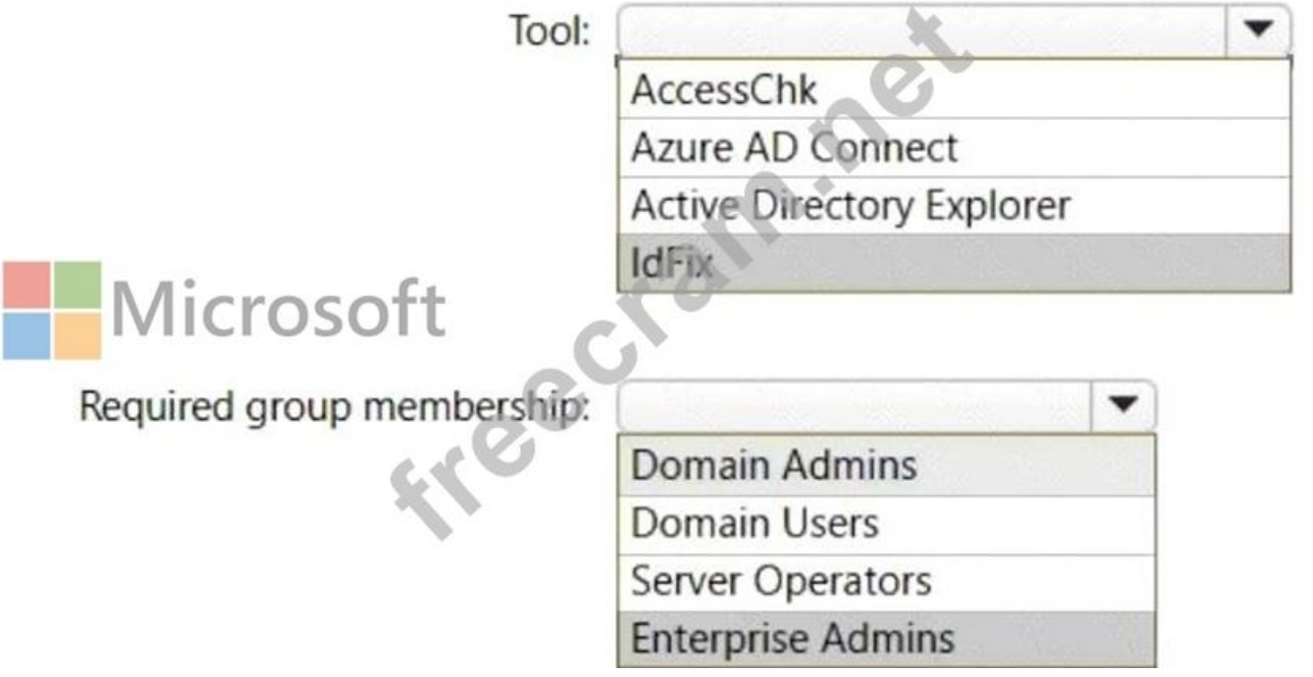
Answer:

Answer Area



Explanation

Answer Area



Box 1: IdFix

Query and fix invalid object attributes with the IdFix tool

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

365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization tools such as Azure AD Connect and Azure AD Connect cloud sync. The focus of IdFix is to

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

groups

NEW QUESTION: 105

You have a Microsoft 365 E5 subscription.

You configure a new alert policy as shown in the following exhibit.

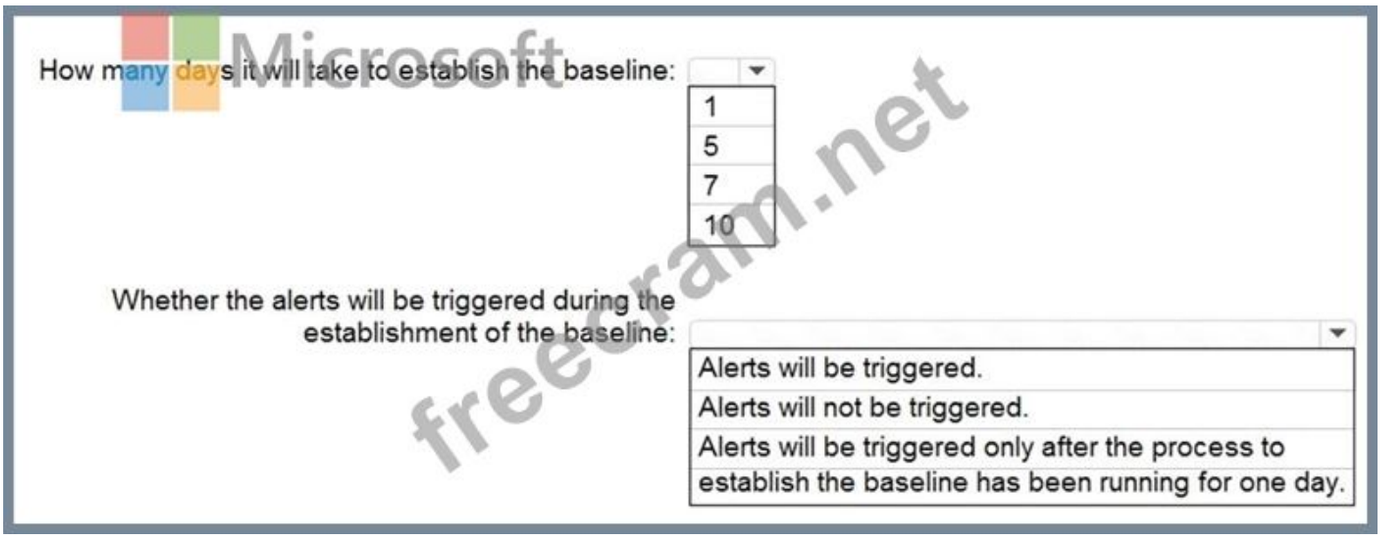
You need to identify the following:

How many days it will take to establish a baseline for unusual activity.

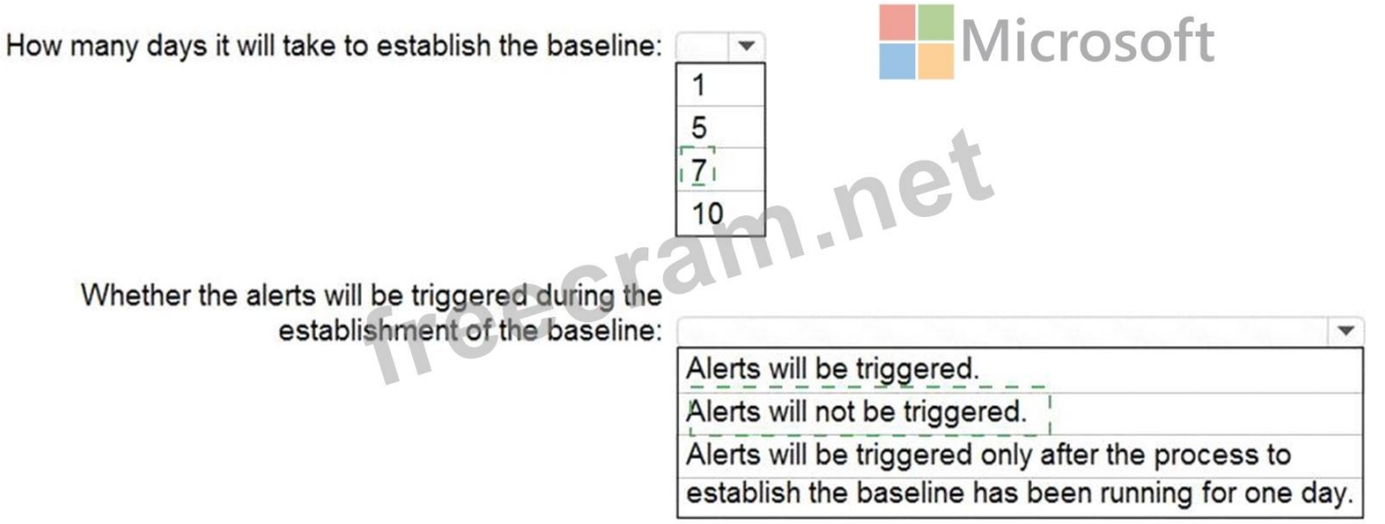
Whether alerts will be triggered during the establishment of the baseline.

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

NOTE: Each correct selection is worth one point.

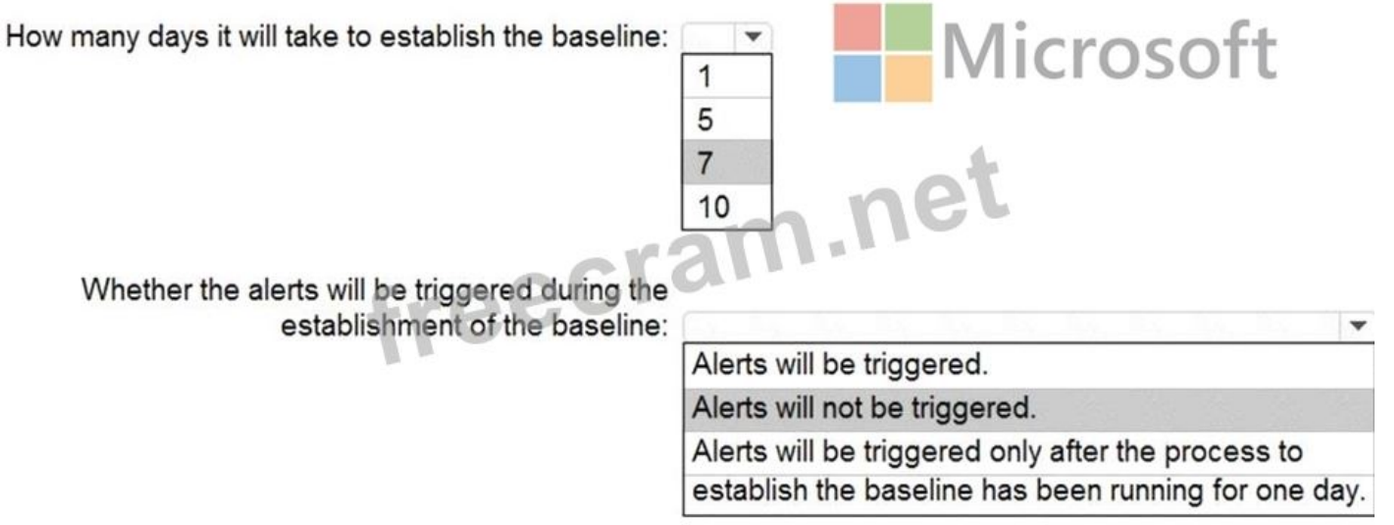


Answer:



Explanation

Graphical user interface, text, application Description automatically generated



Reference:

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

NEW QUESTION: 106

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 Update & Security to view the update history.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 107
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: 108

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)

Explanation

References:

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

Topic 2, A Datum

Case Study:

Overview

Existing Environment

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

If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
A security administrator requires a report that shows which Microsoft 36S users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive US.
PII data to other New York office users. Email messages must be monitored to ensure compliance.
Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

NEW QUESTION: 109
You have a Microsoft 365 subscription. You have a user named User1.
You need to ensure that Used can place a hold on all mailbox content.
What permission should you assign to User1?
A. the Compliance Management role from the Exchange admin center.
B. the User management administrator role from the Microsoft 365 admin center.
C. the Information Protection administrator ide from the Azure Active Directory admin center.
D. the eDiscovery Manager tote from the Microsoft 365 compliance center.
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which role should you assign to User1?
Available Choices (select all choices that are correct)

A. Hygiene Management
B. Security Reader
C. Security Administrator
D. Records Management
Answer: (SHOW ANSWER)
Explanation
A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office
365 Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles
Topic 5, Litware, Irk
Litware, Irk. is a consulting company that has a main office in Montreal and a branch office in

Seattle?

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

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

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

* Password hash synchronization is enabled.
* Synchronization is enabled for the UtwareAdmins OU only.

Users are assigned the roles shown in the following table.

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

Self-service password reset (SSPR) is enabled.

The Azure AD tenant has Security defaults enabled.

Litware identifies the following issues:

* Admin1 cannot create conditional access policies.
* Admin4 receives an error when attempting to use SSPR.
* Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Litware plans to implement the following changes:

* Implement Microsoft Intune.
* Implement Microsoft Teams.

* Implement Microsoft Defender for Office 365.
* Ensure that users can install Office 365 apps on their device.
* Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
* Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Litware identifies the following technical requirements:

* Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
* Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
* Litware users must be able to invite A. Datum users to participate in the following activities:
o Join Microsoft Teams channels,
o Join Microsoft Teams chats,
o Access shared files.
* Just in time access to critical administrative roles must be required.
* Microsoft 365 incidents and advisories must be reviewed monthly.
* Office 365 service status notifications must be sent to Admin2.
* The principle of least privilege must be used.

NEW QUESTION: 111

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: (SHOW ANSWER)

Explanation

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#availab

NEW QUESTION: 112

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

You need to access service health alerts from a mobile phone.

What should you use?

A. the Microsoft 365 Admin mobile app

B. the Intune app

C. the Microsoft Authenticator app

D. Intune Company Portal

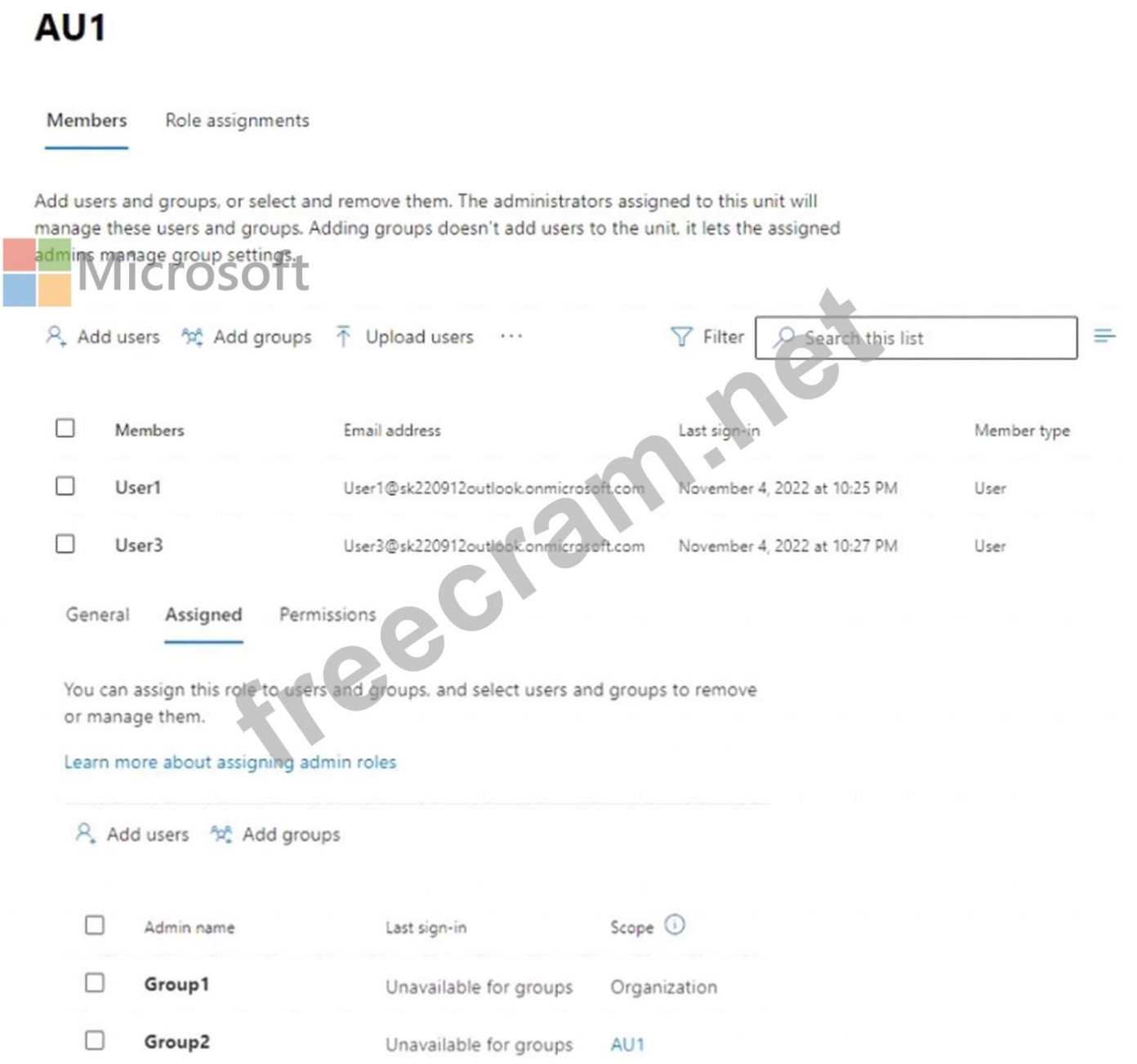
Answer: (SHOW ANSWER)

NEW QUESTION: 113

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

Name	Member of
User1	Group1
User2	Group2
User3	None

You create an administrative unit named AU1 that contains the members shown in the following exhibit.

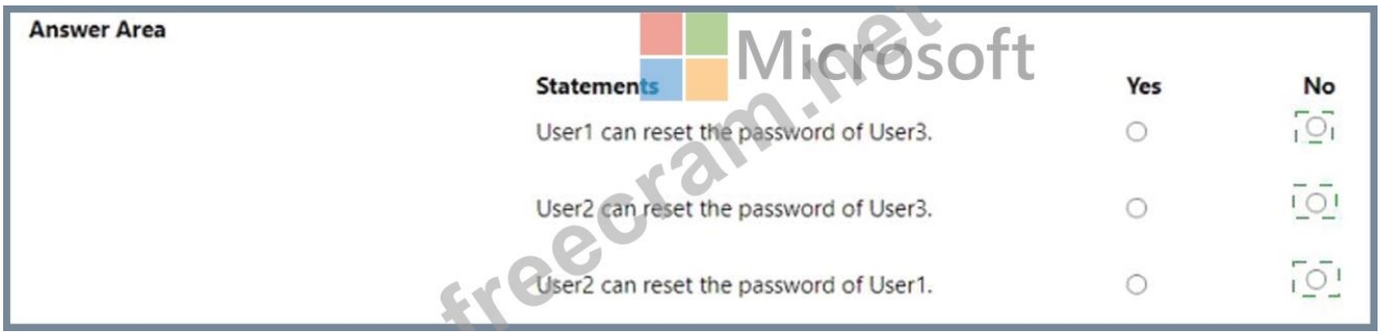


For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE; Each correct selection is worth one point.

Answer Area

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

Answer:



Explanation

NEW QUESTION: 114

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 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.

B. 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.

C. 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.

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: 115

You have a Microsoft 365 subscription.

You need to configure a compliance solution that meets the following requirements:

Defines sensitive data based on existing data samples
Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages Which two components should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. a trainable classifier
B. a sensitive info type
C. an insider risk policy
D. an adaptive policy scope
E. a data loss prevention (DLP) policy
Answer: (SHOW ANSWER)
Explanation
A: Classifiers
This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.
Where you can use classifiers
Classifiers are available to use as a condition for:
Office auto-labeling with sensitivity labels
Auto-apply retention label policy based on a condition
Communication compliance
Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.
Data loss prevention
E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp

NEW QUESTION: 116
You need to protect the U.S. PII data to meet the technical requirements.
What should you create?
A. a data loss prevention (DLP) policy that contains a domain exception
B. a Security & Compliance retention policy that detects content containing sensitive data
C. a Security & Compliance alert policy that contains an activity
D. a data loss prevention (DLP) policy that contains a user override

Answer: (SHOW ANSWER)

NEW QUESTION: 117

You need to meet the technical requirement for the EU PII data.

What should you create?

A. a retention policy from the Security & Compliance admin center.

B. a retention policy from the Exchange admin center

C. a data loss prevention (DLP) policy from the Exchange admin center

D. a data loss prevention (DLP) policy from the Security & Compliance admin center

Answer: A (LEAVE A REPLY)

Explanation

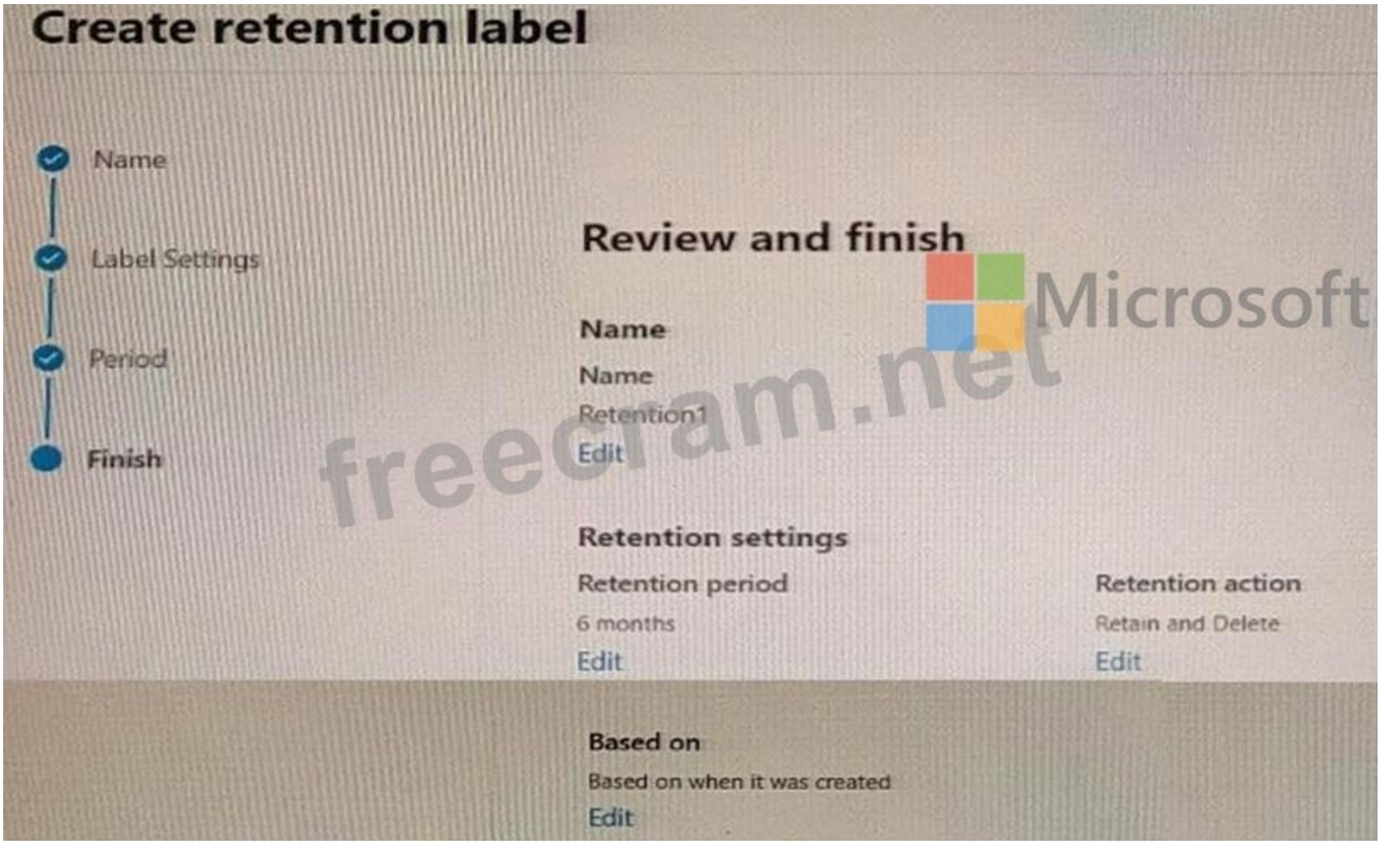
References:

https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

NEW QUESTION: 118

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. August 1, 2020

B. February 1, 2020

C. July 10, 2020

D. July 1.2020

Answer: (SHOW ANSWER)

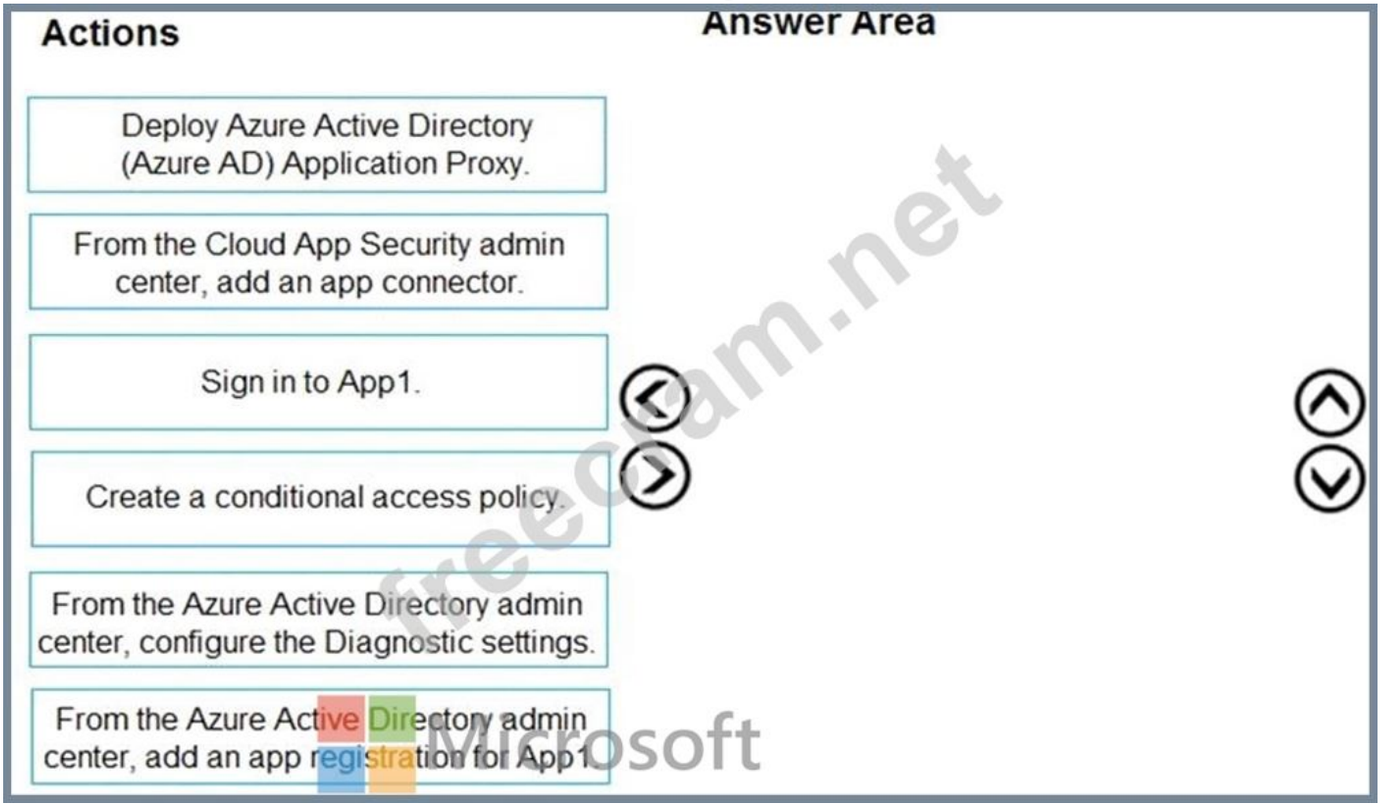
NEW QUESTION: 119

Your company purchases a cloud app named App1.

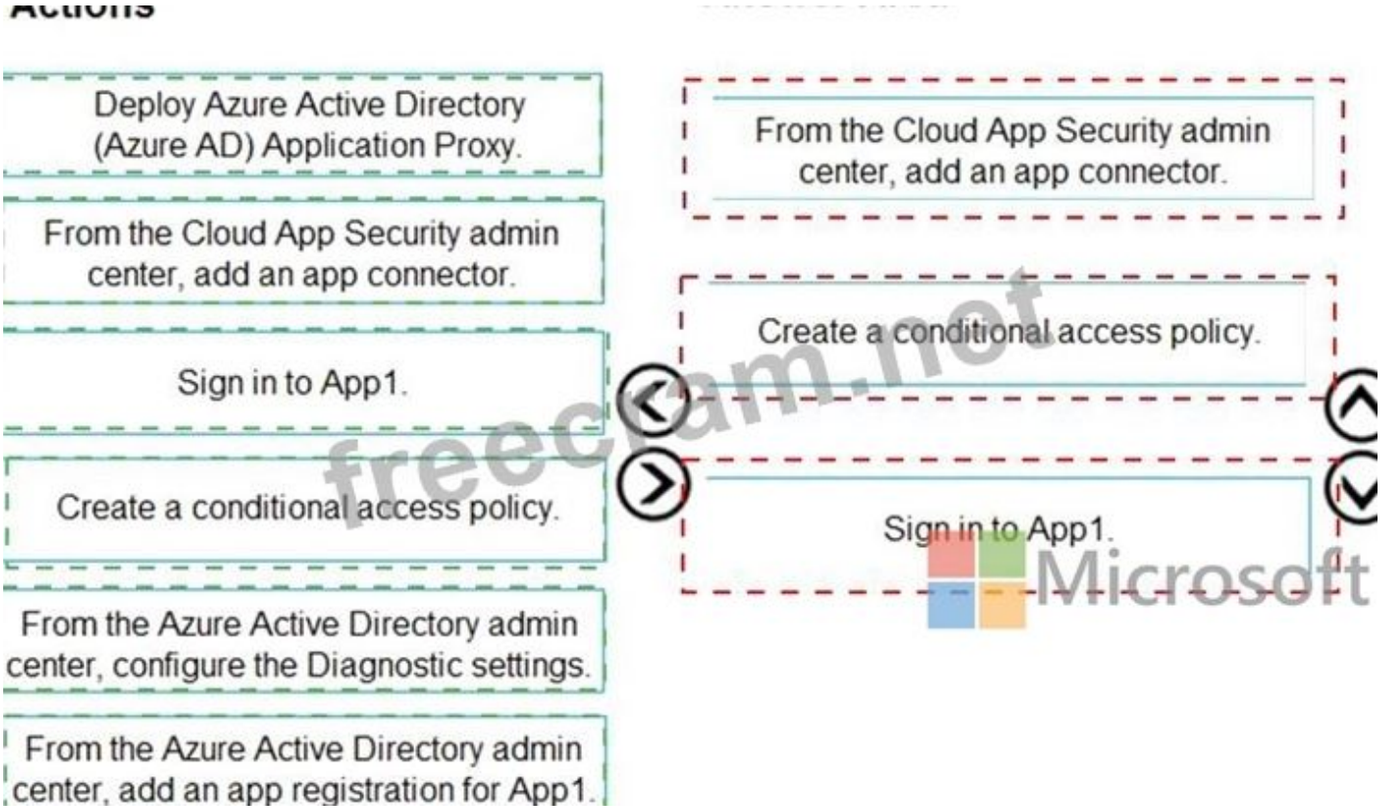
You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1.

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

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION: 120

HOTSPOT

Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.

The domain contains the users shown in the following table.

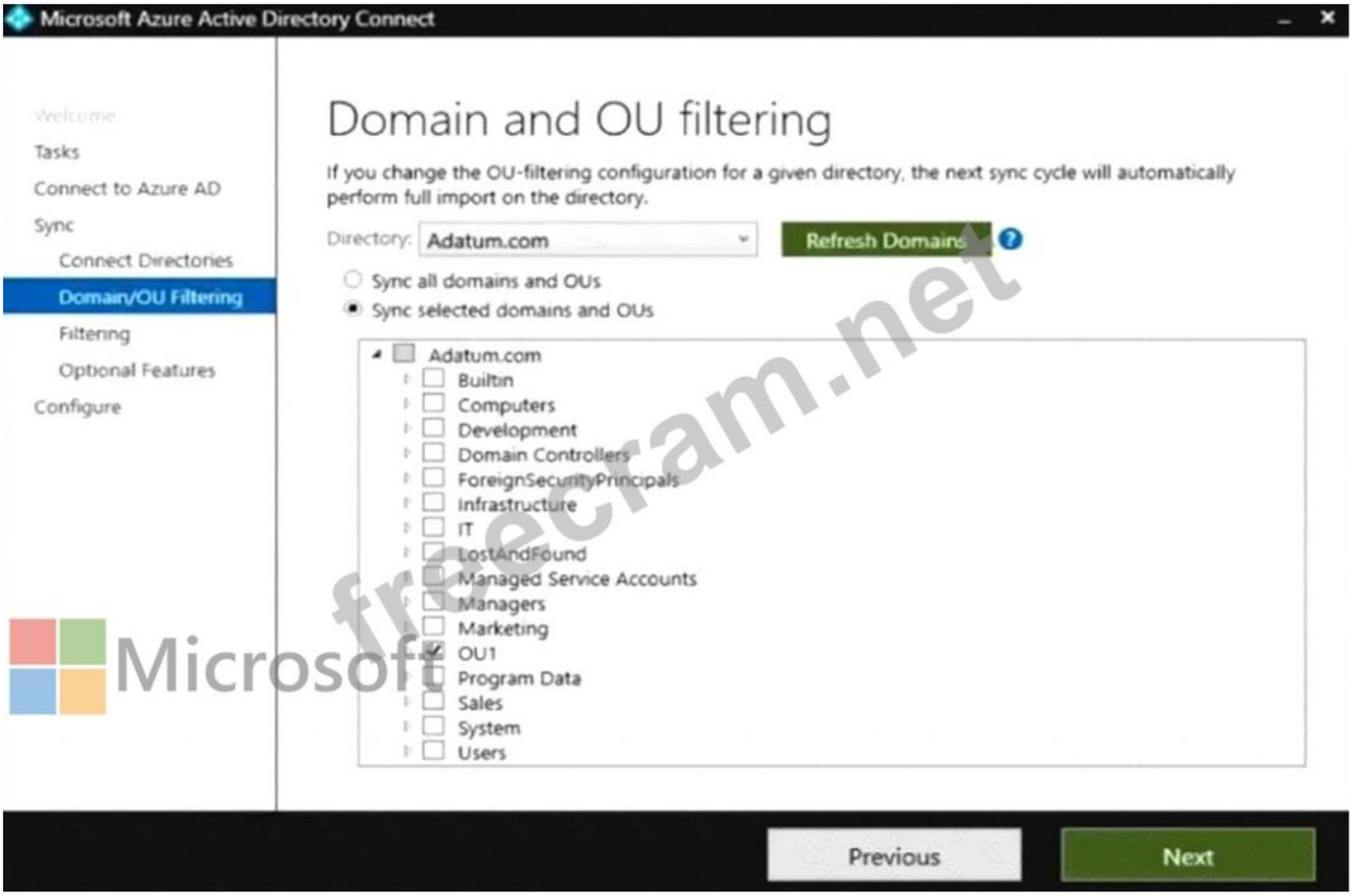
Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

The domain contains the groups shown in the following table.

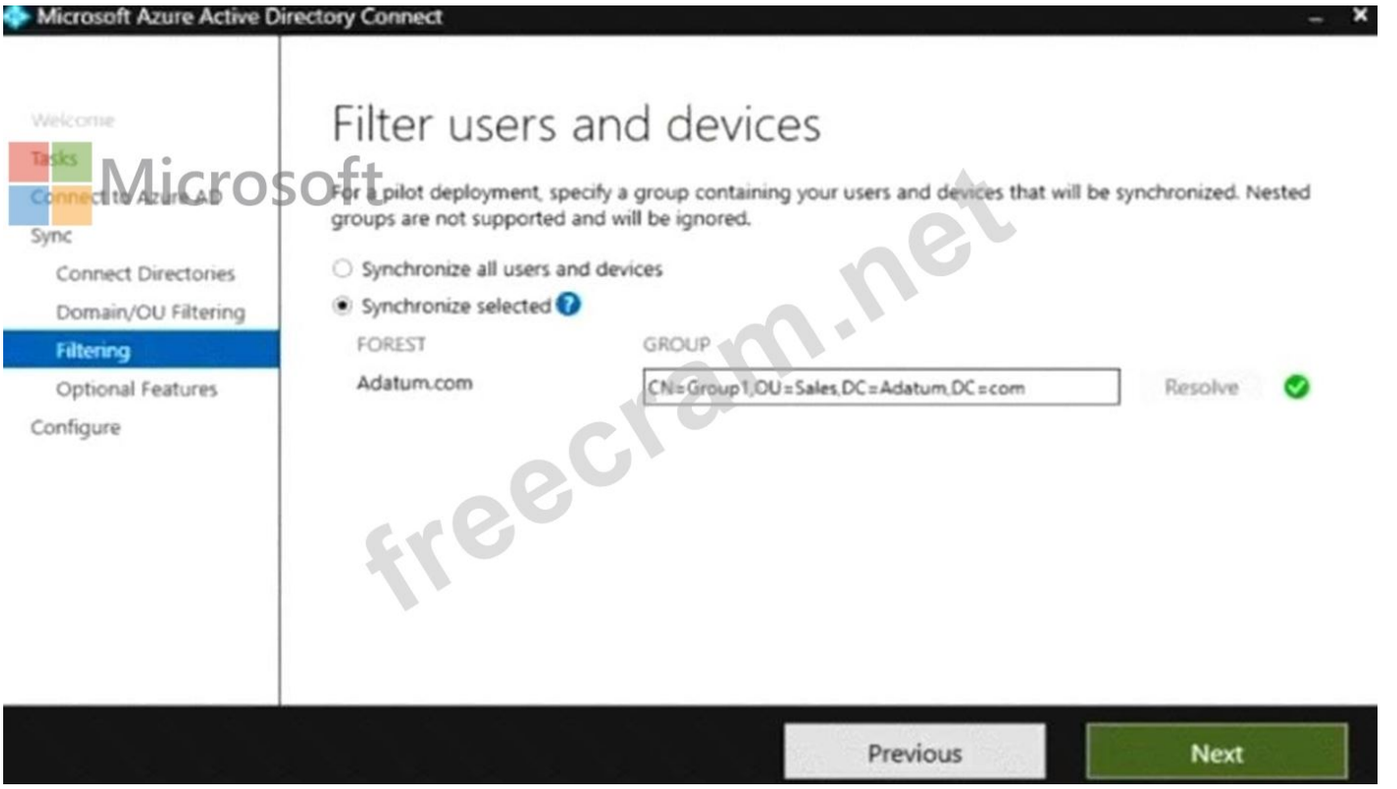
Name	Member of	In OU
Group1	*None*	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect.

You configure Domain and OU filtering as shown in the following exhibit.



You configure Filter users and devices as shown in the following exhibit.



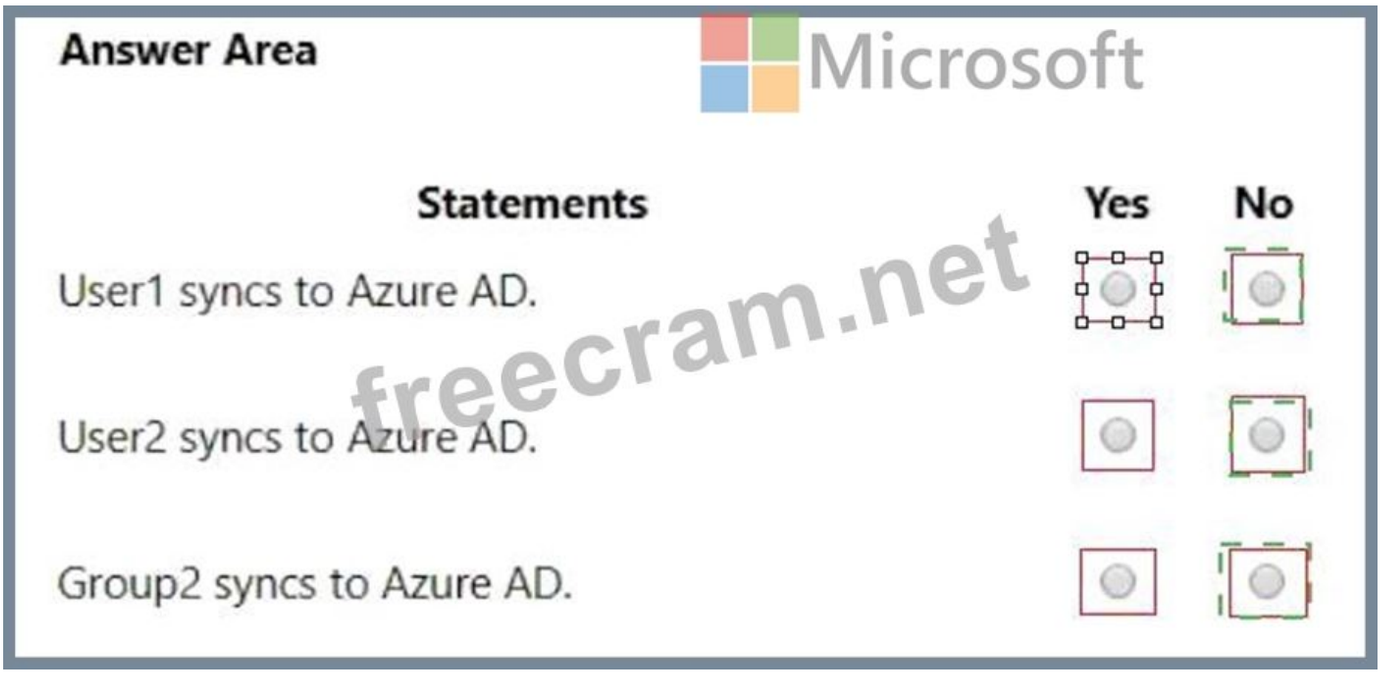
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

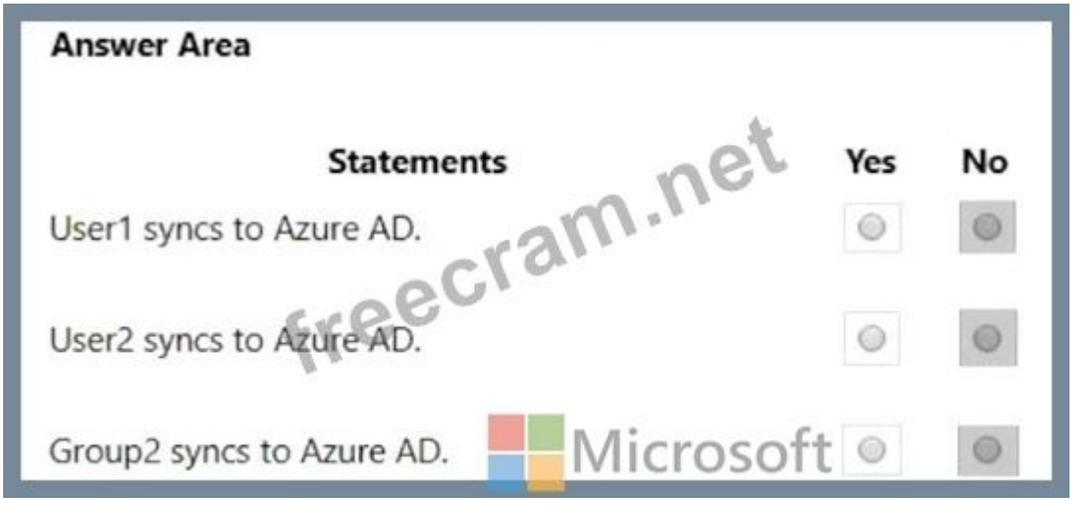
Answer Area

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

Answer:



Explanation



NEW QUESTION: 121

Your network contains an Active Directory domain and an Azure AD tenant.

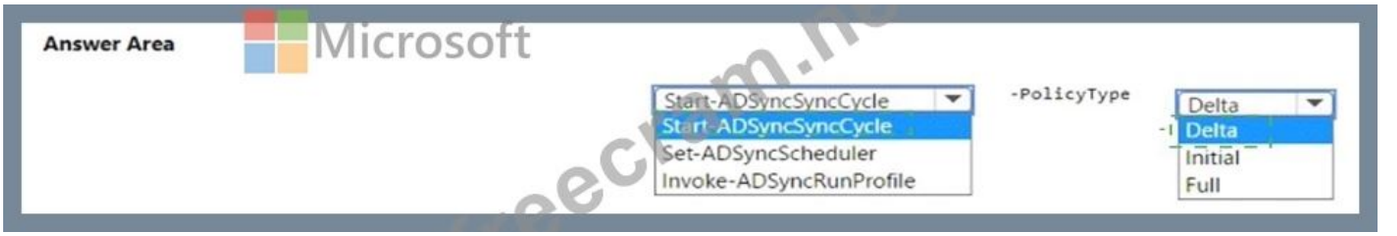
You implement directory synchronization for all 10.000 users in the organization.

You automate the creation of 100 new user accounts.

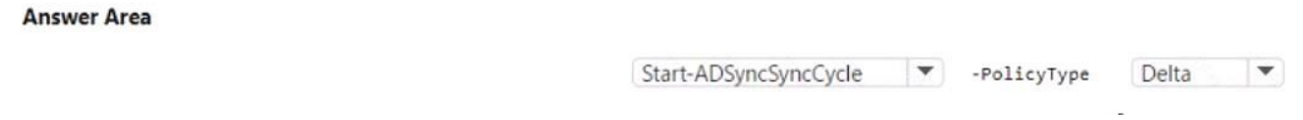
You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.

Which command should you run? To answer, select the appropriate options in the answer area.

Answer:



Explanation



NEW QUESTION: 122

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

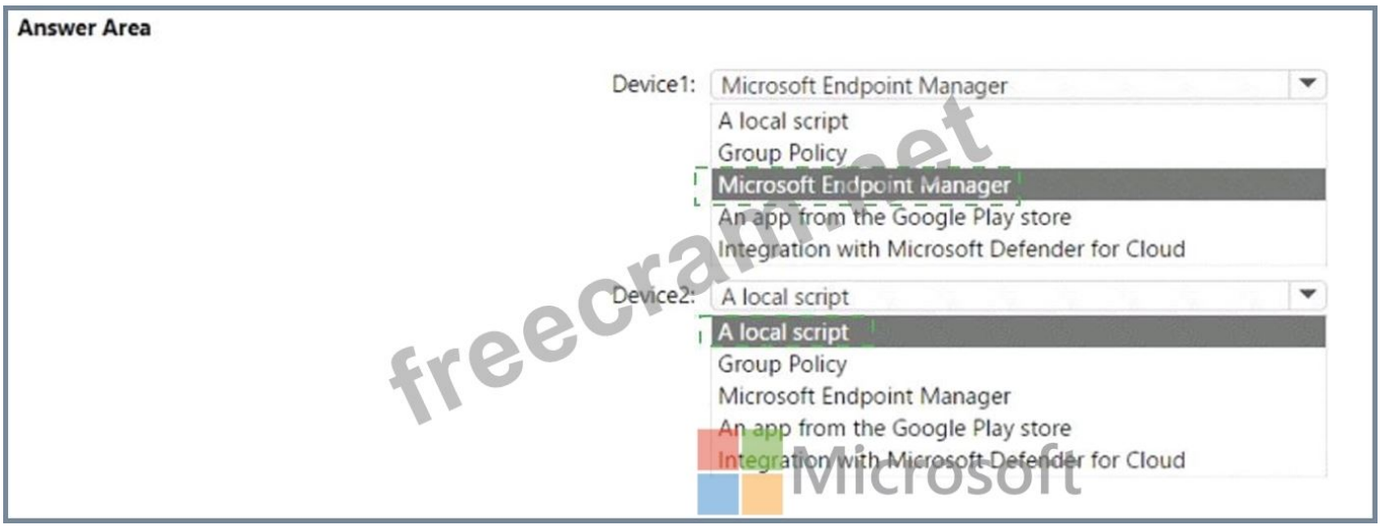
You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.

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 Area

Answer:



Explanation

NEW QUESTION: 123

You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:

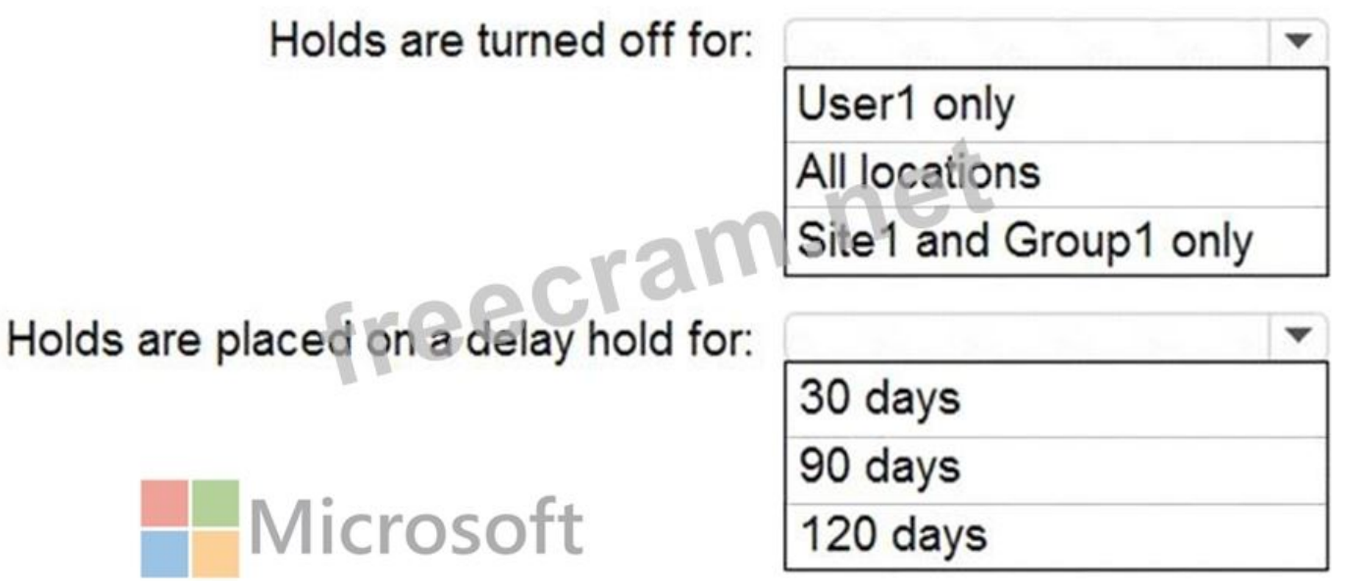
Name: Case1

Included content: Group1, User1, Site1

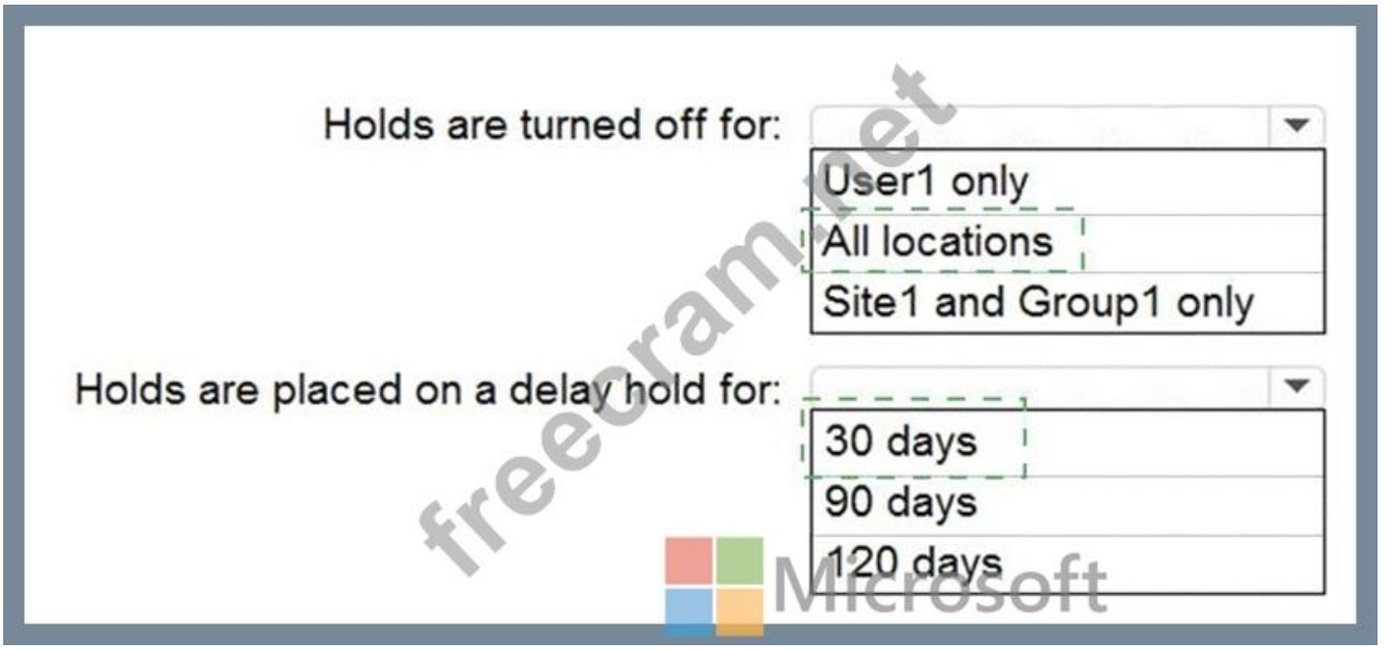
Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders The investigation for Case1 completes, and you close the case.

What occurs after you close Case1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

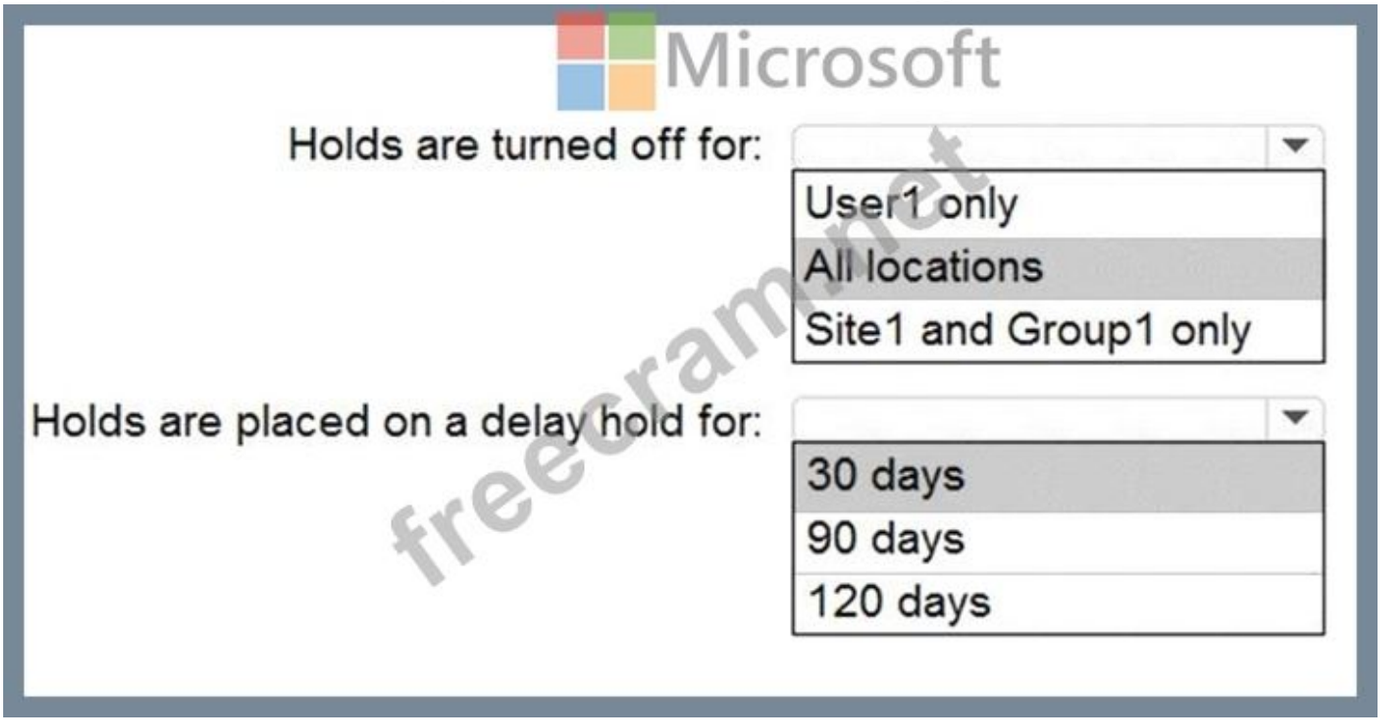


Answer:



Explanation

Graphical user interface, text, application Description automatically generated



Reference:

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

NEW QUESTION: 124

HOTSPOT

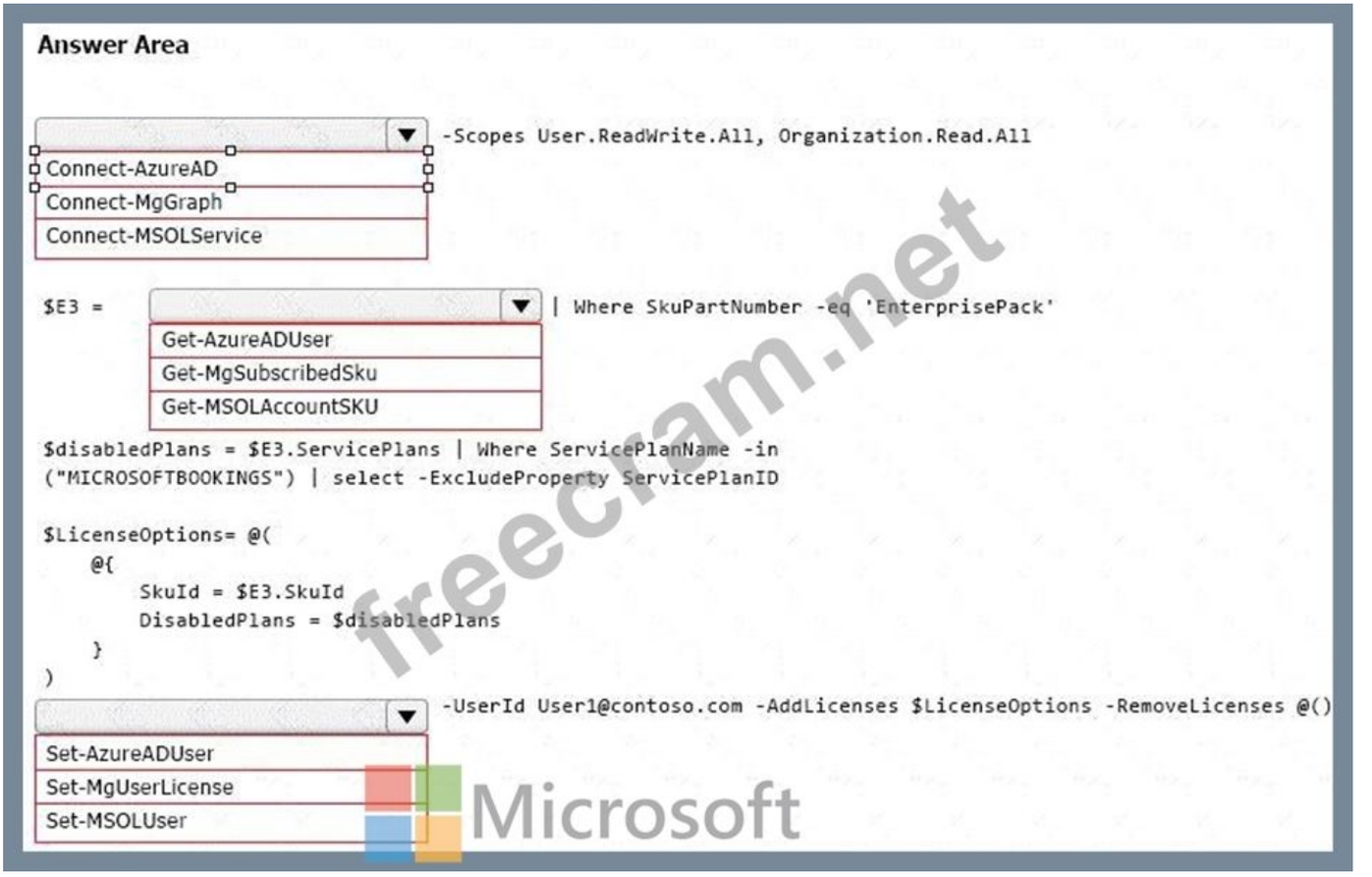
You have a Microsoft 365 subscription.

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.

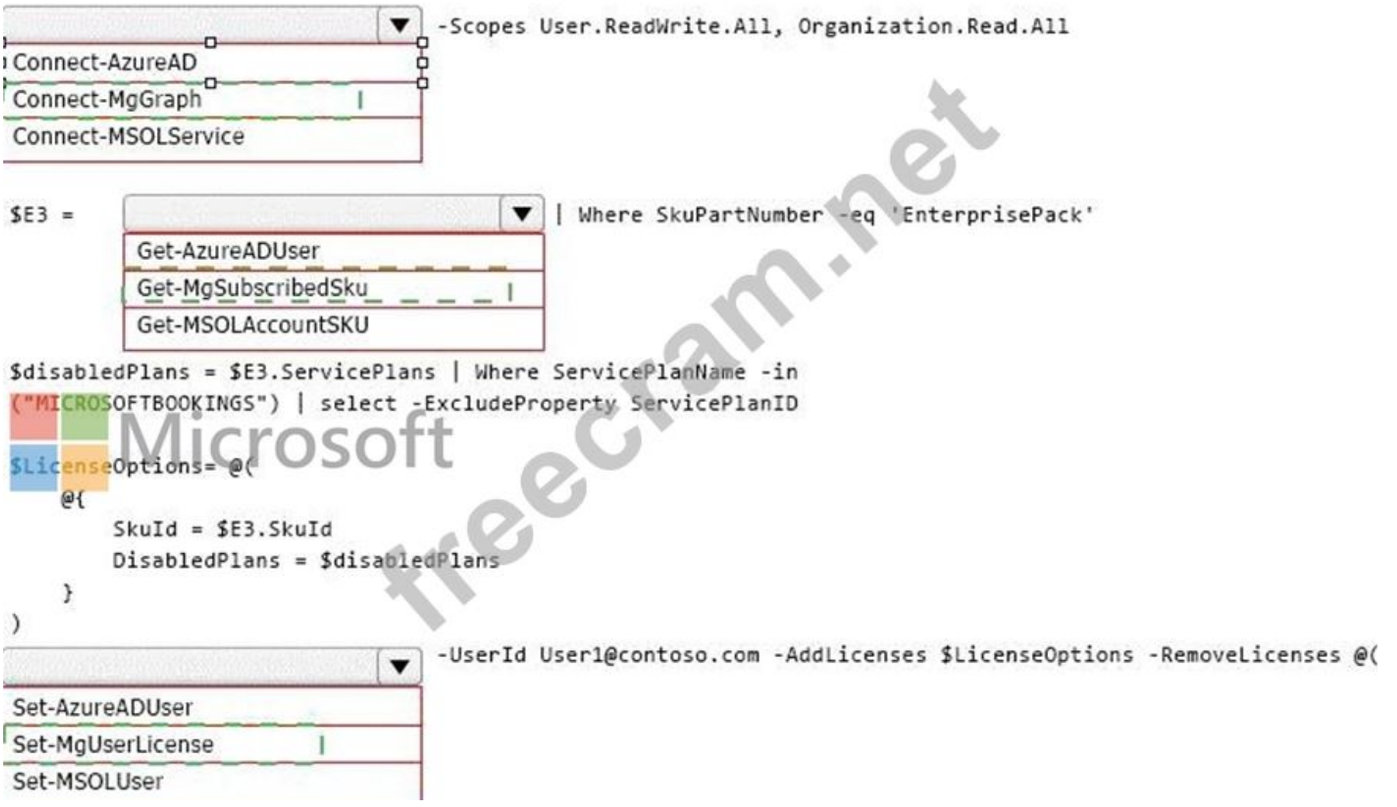
How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

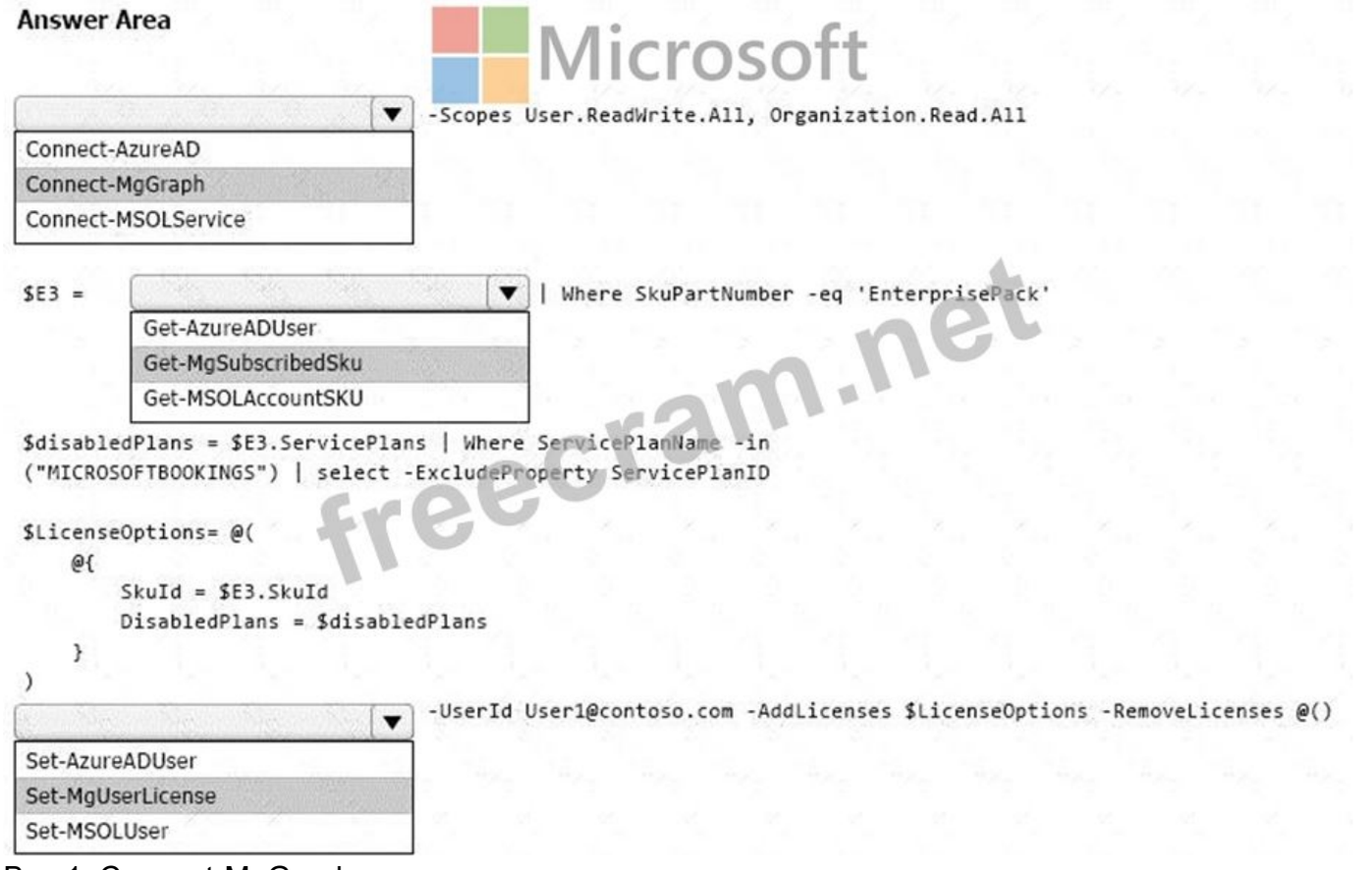


Answer:

Answer Area



Explanation



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-

NEW QUESTION: 125
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:

Answer Area

Explanation

Answer Area

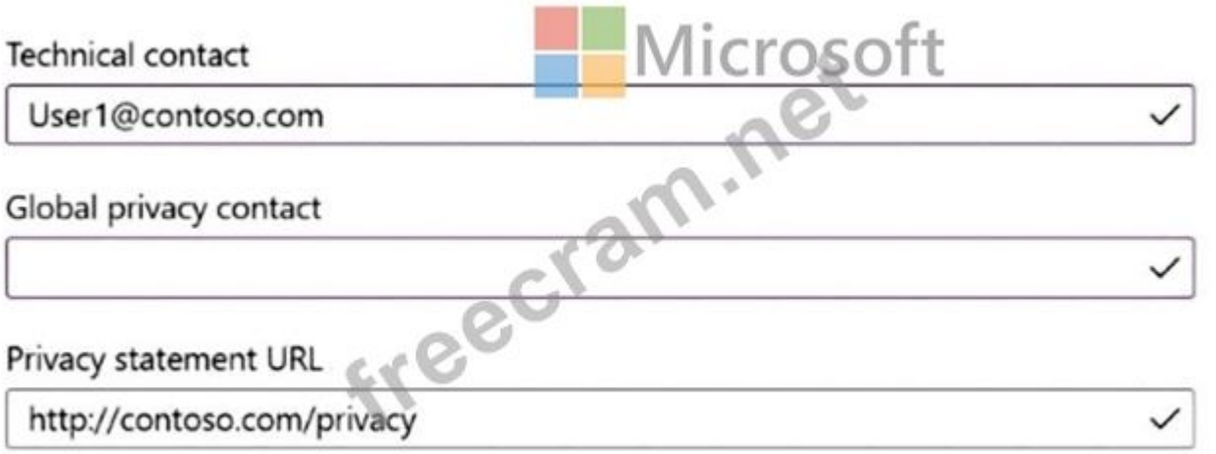
NEW QUESTION: 126

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)

Explanation

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: 127

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

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

You plan to create a new Windows 10 Security Baseline profile.

To which groups can you assign to the profile?

A. Group3 only

B. Group1 and Group3 only

C. Group2 and Group3 only

D. Group1. Group2. and Group3

Answer: (SHOW ANSWER)

Reference:

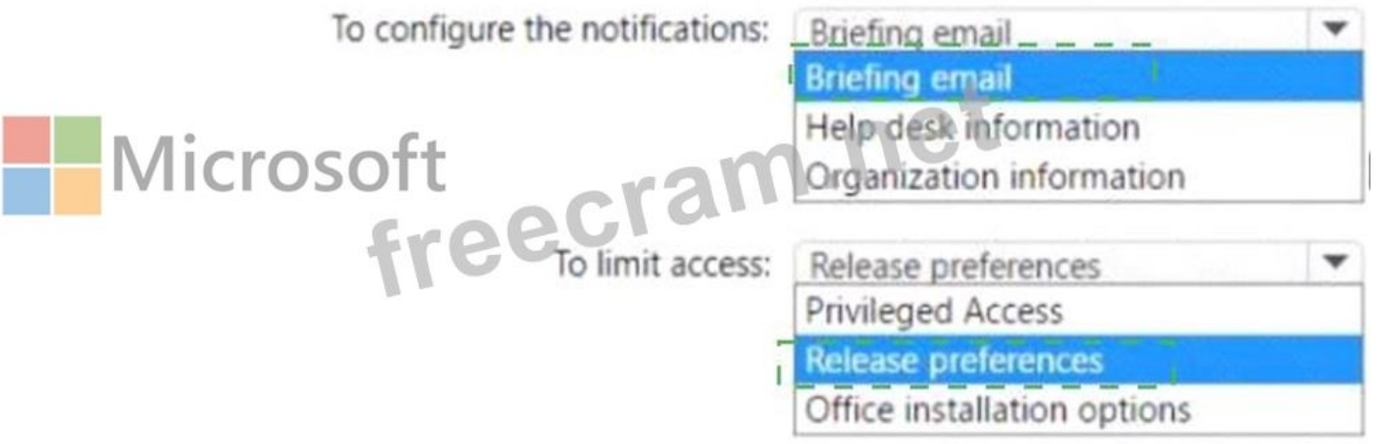
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile

https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

NEW QUESTION: 128
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft 365 compliance policies to meet the following requirements:
* Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
* Report on shared documents that contain PII.
What should you create?
A. an alert policy
B. a data loss prevention (DLP) policy
C. a retention policy
D. a Microsoft Cloud App Security policy
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

NEW QUESTION: 129
You need to configure the Office 365 service status notifications and limit access to the service and feature updates. The solution must meet the technical requirements.
What should you configure in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Explanation

NEW QUESTION: 130

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. Yes

B. no

Answer: B (LEAVE A REPLY)

NEW QUESTION: 131

You have a hybrid deployment of Azure AD that contains the users shown in the following table.

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

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

* View sync errors in Azure AD Connect Health.

* Configure Azure AD Connect Health settings.

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

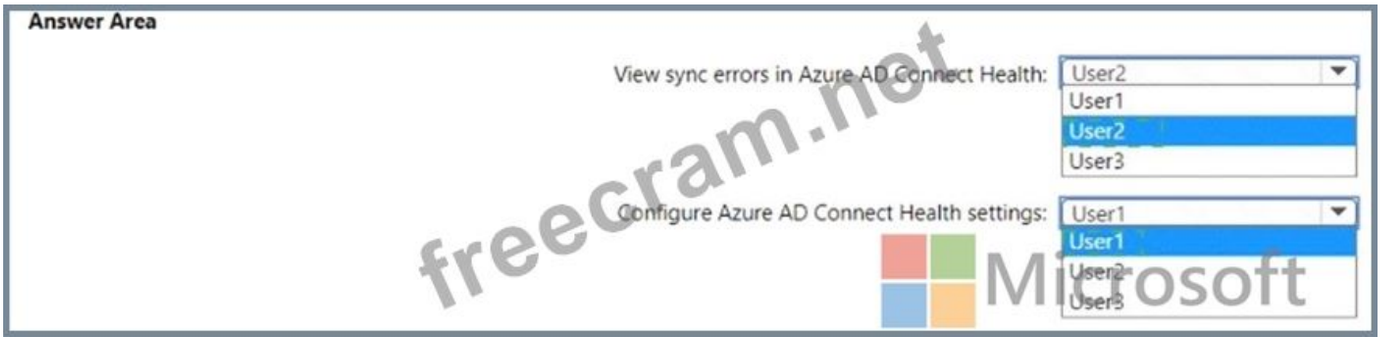
NOTE: Each correct selection is worth one point.

Answer Area

View sync errors in Azure AD Connect Health: User2 (User1, User2, User3)

Configure Azure AD Connect Health settings: User1 (User1, User2, User3)

Answer:



Explanation

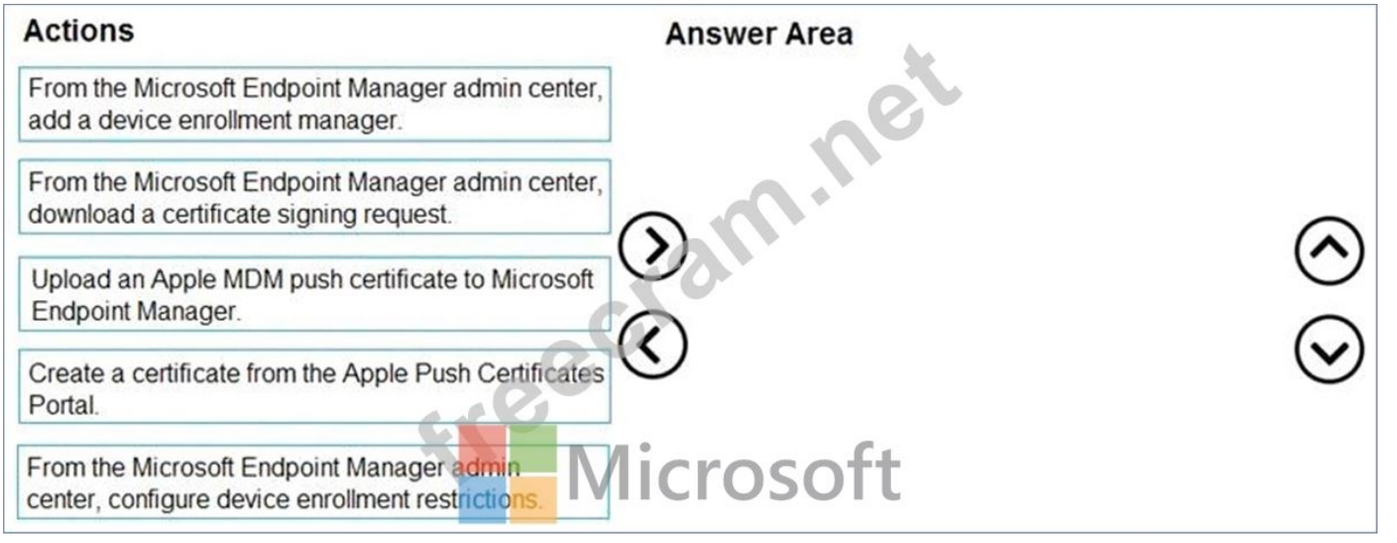
NEW QUESTION: 132

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.

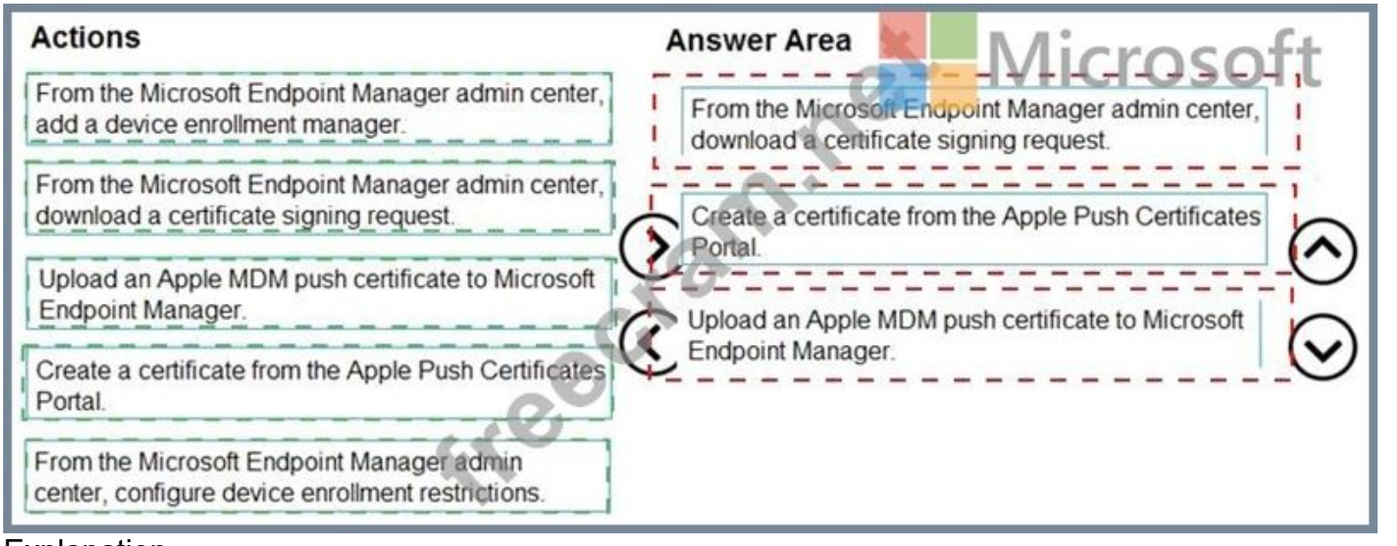
You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in

memory.
What should you configure in the profile?
A. Microsoft Defender Exploit Guard
B. Microsoft Defender Credential Guard
C. Microsoft Defender
D. BitLocker Drive Encryption (BitLocker)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 133
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: 134
You purchase a new computer that has Windows 10, version 21H1 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 21H1.
B. Install all the feature updates released since version 21H1 and all the quality updates released since version 21H1 only.
C. Install all the feature updates released since version 21H1 and the latest quality update only.
D. Install the latest feature update and the latest quality update only.
Answer: (SHOW ANSWER)

NEW QUESTION: 135
You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.
You have the devices shown in the following table.

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

You plan to enable co-management.
You need to identify which devices support co-management without requiring the installation of additional software.
Which devices should you identify?
A. Device1, Device2, and Device3
B. Device2 only
C. Device3 only

D. Device1 only
E. Device2 and Device3 only
Answer: (SHOW ANSWER)

NEW QUESTION: 136
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

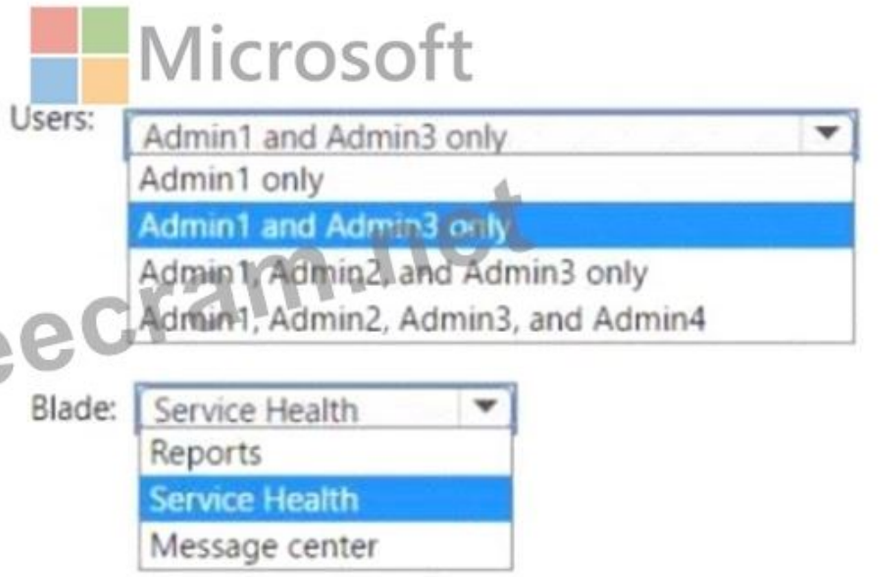
NEW QUESTION: 137

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.

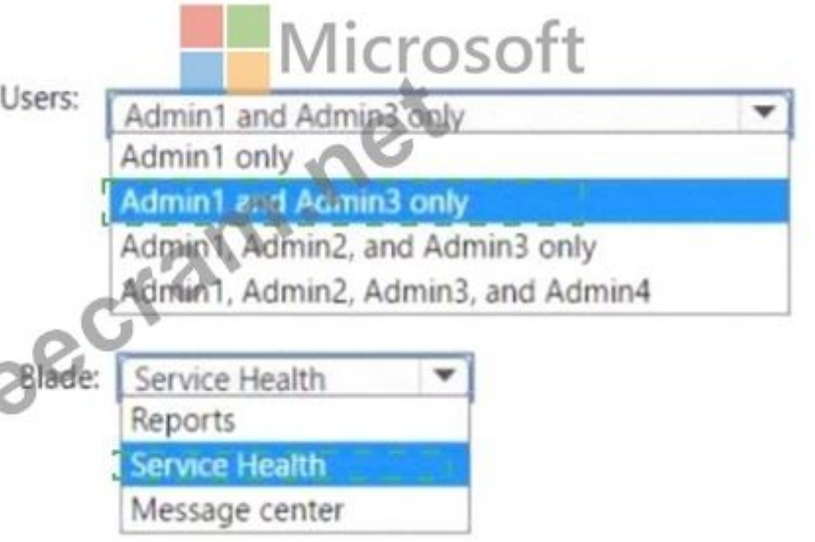
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation

NEW QUESTION: 138

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project.

Which DNS record should you recommend?

A. host (A)

B. host information

C. text (TXT)

D. alias (CNAME)

Answer: D (LEAVE A REPLY)

Explanation

When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.

Note:

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

Text (TXT)

Mail exchanger (MX)

incorrect answer options you may see on the exam include the following:

alias (CNAME)

Host (A)

host (AAA)

Pointer (PTR)

Name Server (NS)

host information (HINFO)

pointer (PTR)

Reference:

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

NEW QUESTION: 139

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=o3

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-po

NEW QUESTION: 140

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: 141
You have a Microsoft 365 subscription.
You configure a data loss prevention (DLP) policy.
You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.
You need to prevent the users from bypassing the DLP policy.
What should you configure?
A. actions
B. incident reports
C. exceptions
D. user overrides
Answer: (SHOW ANSWER)
Explanation
A DLP policy can be configured to allow users to override a policy tip and report a false positive. You can educate your users about DLP policies and help them remain compliant without blocking their work.
For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word.
If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

NEW QUESTION: 142
You have a Microsoft 365 E5 subscription that.

You need to identify whenever a sensitivity label is applied, changed, or removed within the subscription.
Which feature should you use, and how many days will the data be retained? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point.

Answer:

Explanation

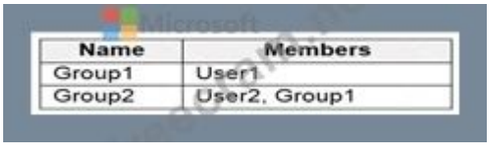
NEW QUESTION: 143
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune.
You plan to use Endpoint analytics to identify hardware issues.
You need to enable Window health monitoring on the devices to support Endpoint analytics What should you do?

A. Create a Windows 10 Security Baseline profile
B. Create a compliance policy.
C. Create a configuration profile.
D. Configure the Endpoint analytics baseline regression threshold.

Answer: (SHOW ANSWER)

NEW QUESTION: 144

You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.



Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:

MDM user scope: Some

Groups: Group1

MAM user scope: Some

Groups: Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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
User1 can enroll Device1 in Intune by using automatic enrollment	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

Answer:

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

Explanation

Graphical user interface, text, application, email Description automatically generated

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

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

NEW QUESTION: 145
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. No
B. yes
Answer: (SHOW ANSWER)

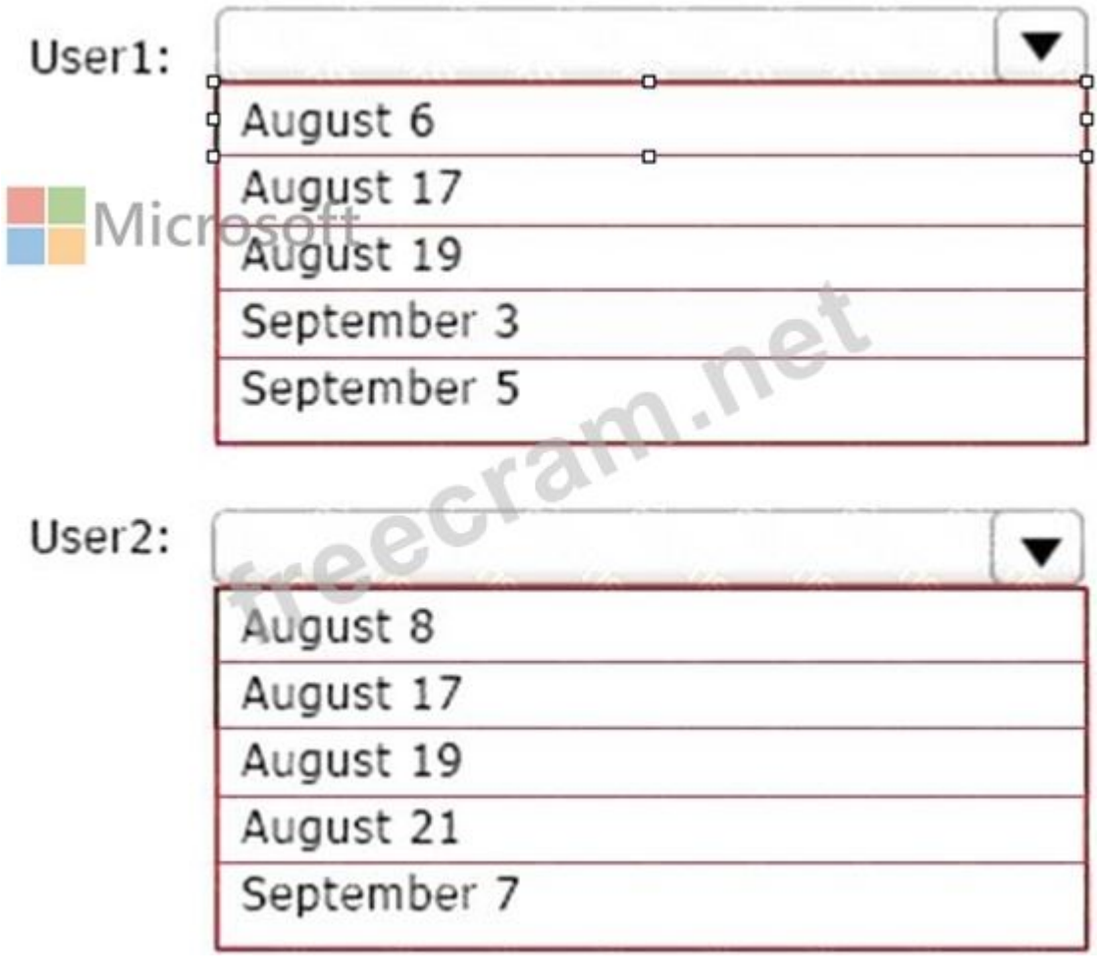
NEW QUESTION: 146
You plan to use Azure Sentinel and Microsoft Cloud App Security. You need to connect Cloud App Security to Azure Sentinel.
What should you do in the Cloud App Security admin center?
A. From Automatic log upload, add a data source.
B. From Automatic log upload, add a log collector.

C. From Security extension, add a SIEM agent.
D. From Connected apps, add an app connector.
Answer: C (LEAVE A REPLY)

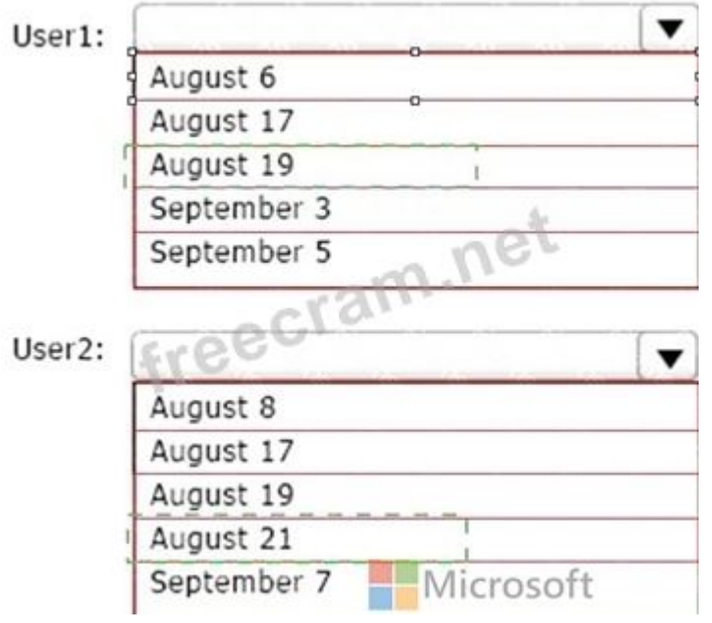
NEW QUESTION: 147
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:
Assignments: All users
Controls: Require Azure AD multifactor authentication registration
Enforce Policy: On
On August 3, you create two users named User1 and User2.
Users authenticate by using Azure Multi-Factor Authentication (MFA) for the first time on the dates shown in the following table.

User	Date
User1	August 5
User2	August 7

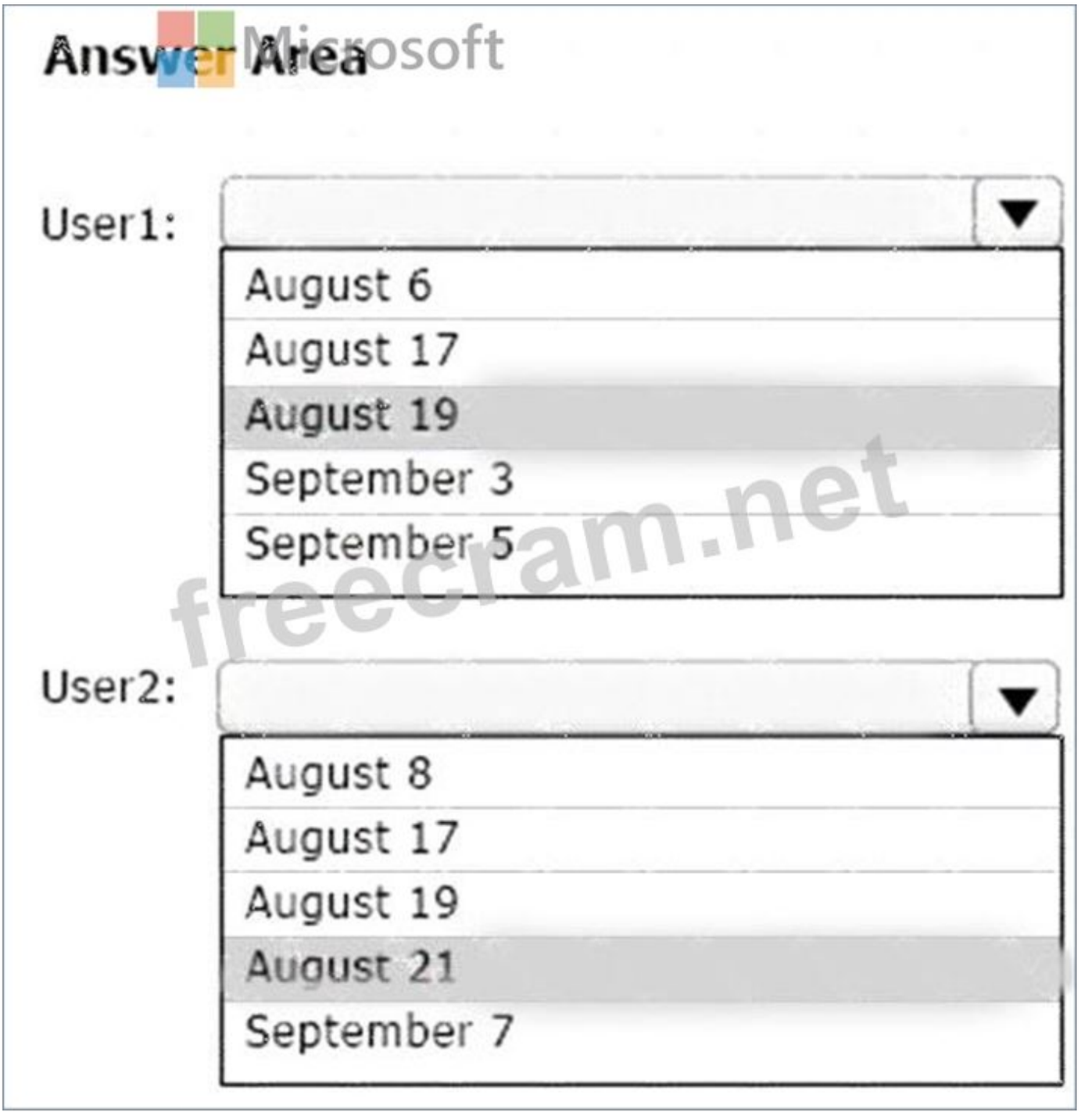
By which dates will User1 and User2 be forced to complete their Azure MFA registration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



Box 1: August 19

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

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

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

Box 2: August 21

Reference:

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

NEW QUESTION: 148

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

NEW QUESTION: 149

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)
Explanation
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: 150
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: 151

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: 152
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 Policy3
D. only the settings of Policy2
Answer: (SHOW ANSWER)

NEW QUESTION: 153
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

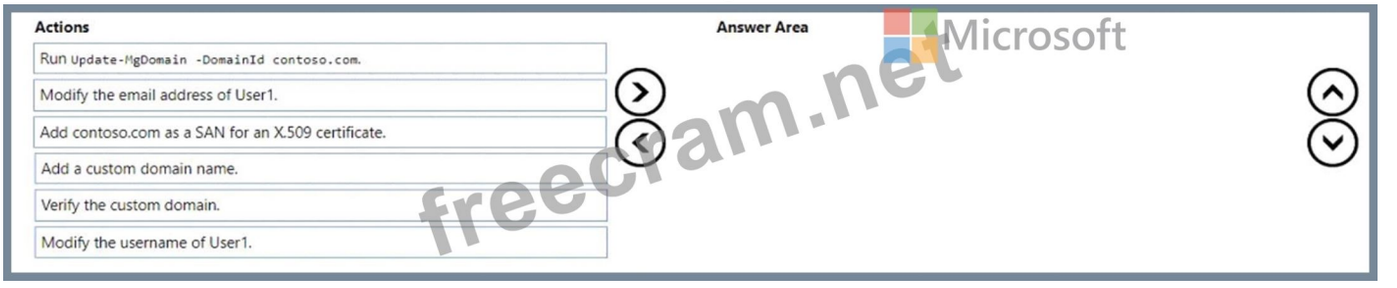
Exhibit tab.)

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: (SHOW ANSWER)
Explanation
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.

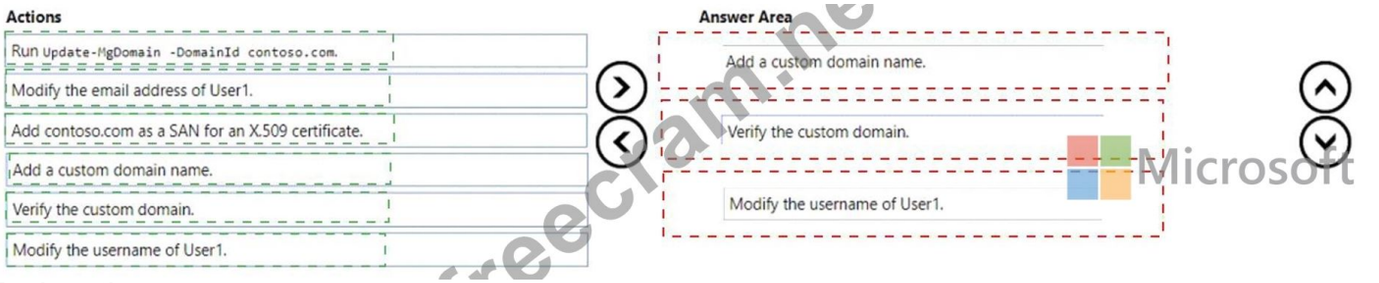
NEW QUESTION: 154
You have a Microsoft E5 subscription.
You need to ensure that administrators who need to manage Microsoft Exchange Online are

assigned the Exchange Administrator role for five hours at a time.
What should you implement?
A. Azure AD Privileged Identity Management (PIM)
B. a conditional access policy
C. a communication compliance policy)
D. Azure AD Identity Protection
E. groups that have dynamic membership
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-def

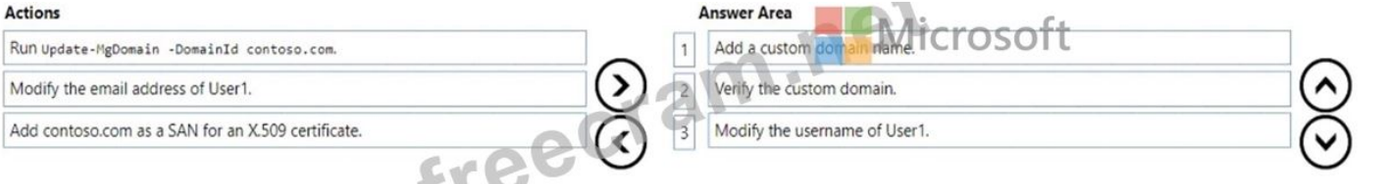
NEW QUESTION: 155
Your company has an Azure AD tenant named contoso.onmicrosoft.com.
You purchase a domain named contoso.com from a registrar and add all the required DNS records.
You create a user account named User1. User1 is configured to sign in as userl@contoso.onmicrosoft.com.
You need to configure User1 to sign in as user1@contoso.com.
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: 156

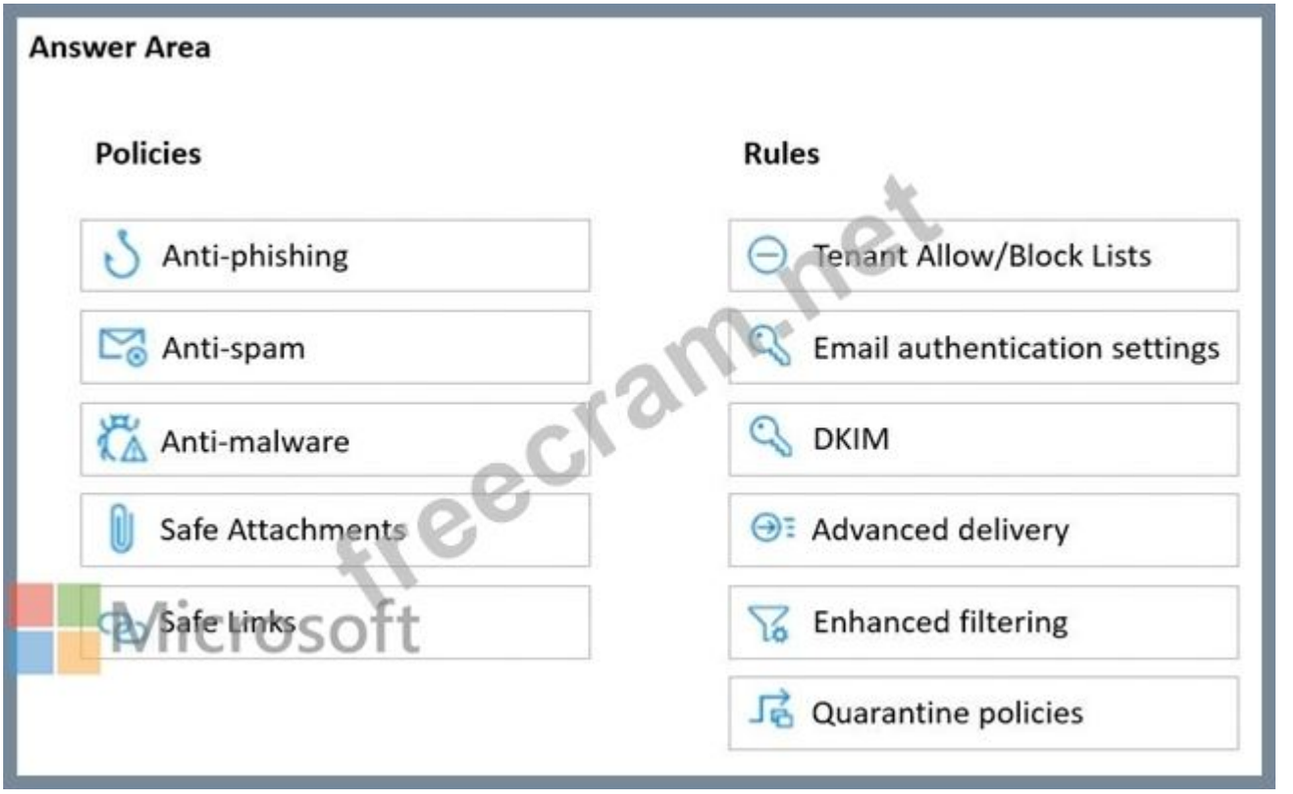
You have a Microsoft 365 E5 tenant.
industry regulations require that the tenant comply with the ISO 27001 standard.
You need to evaluate the tenant based on the standard
A. From Compliance Manager, create an assessment
B. From Policy in the Azure portal, select Compliance, and then assign a pokey
C. From the Microsoft 365 admin center enable the Productivity Score.
D. From the Microsoft J6i compliance center, create an audit retention policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 157
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

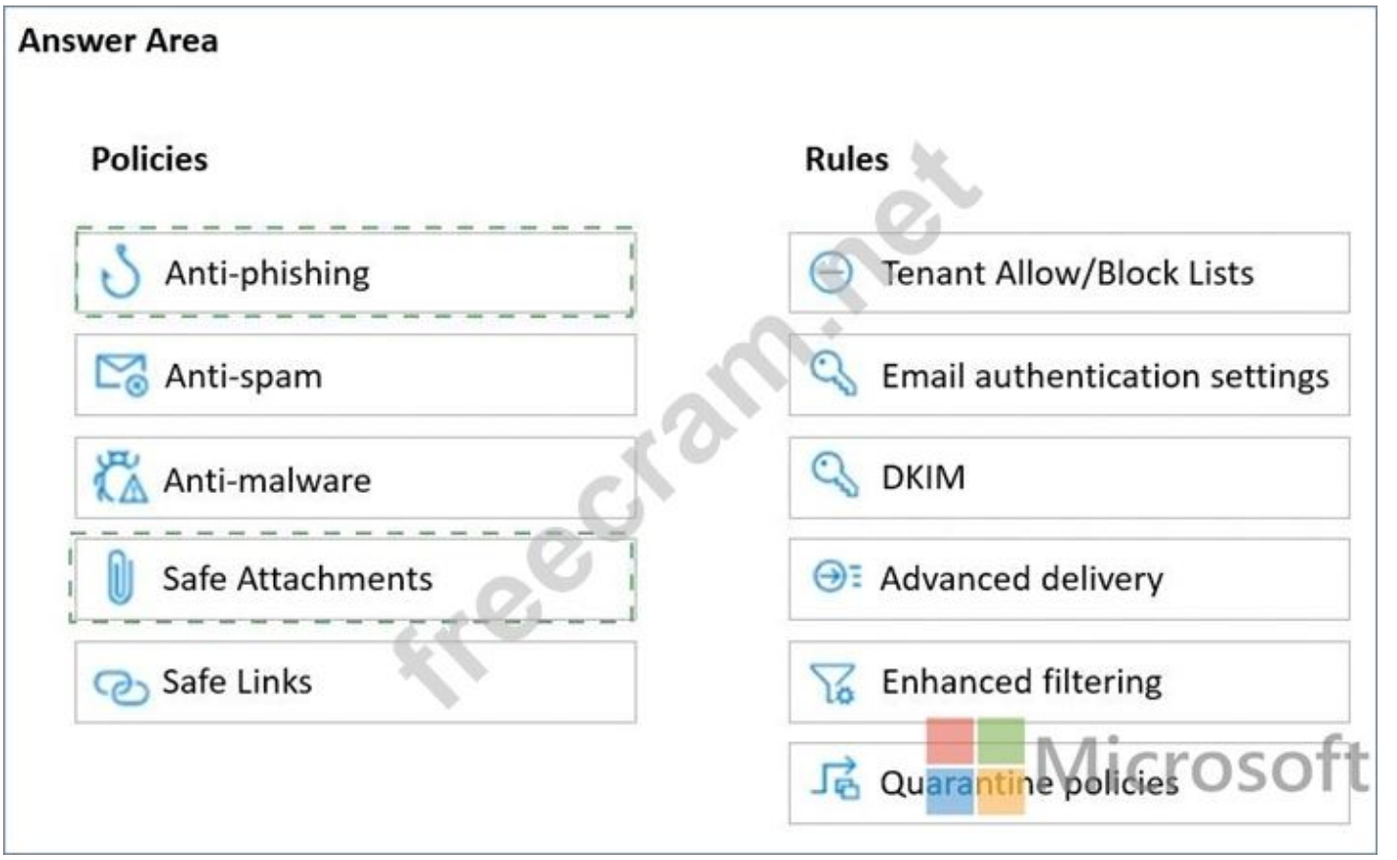
NEW QUESTION: 158
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profile?
A. Ubuntu Linux
B. macOS
C. iOS
D. Android
Answer: (SHOW ANSWER)
Explanation
Intune device configuration profiles can be applied 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: 159
You have a Microsoft 365 E5 subscription.
You plan to use a mailbox named Mailbox1 to analyze malicious email messages.
You need to configure Microsoft Defender for Office 365 to meet the following requirements:
* Ensure that incoming email is NOT filtered for Mailbox1.
* Detect impersonation and spoofing attacks on all other mailboxes in the subscription.
Which two settings should you configure? To answer, select the appropriate settings in the answer area.



Answer:



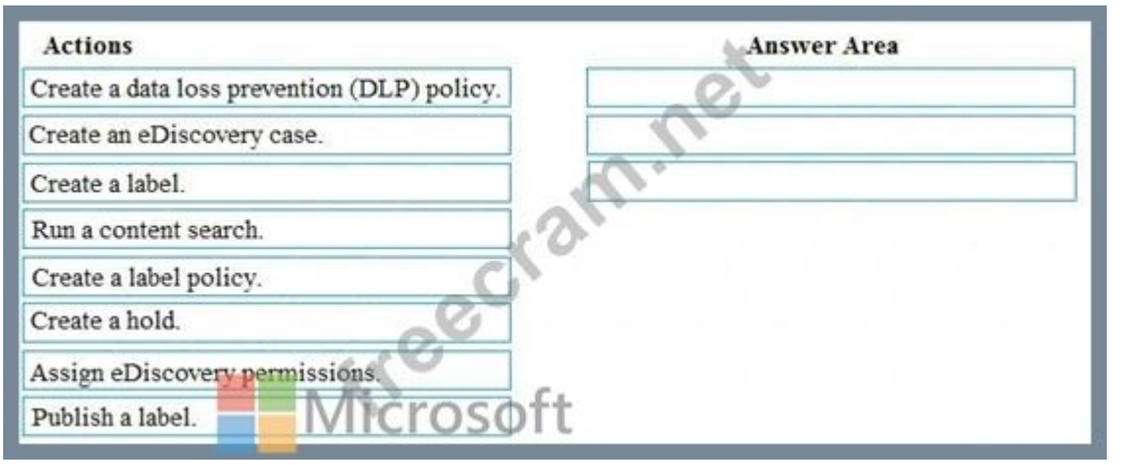
Safe Attachments policy: This policy allows you to specify how to handle email attachments that might contain malware. You can create a custom policy for Mailbox1 and set the action to Do not scan attachments. This will ensure that incoming email is not filtered for Mailbox1. You can also enable the Redirect attachment option to send a copy of the original attachment to another mailbox for analysis1.

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

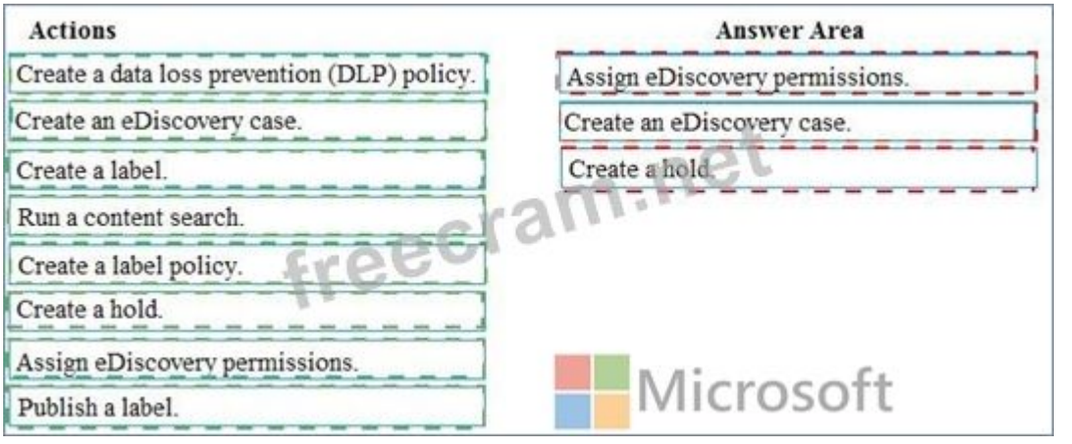
NEW QUESTION: 160

You need to meet the requirement for the legal department.

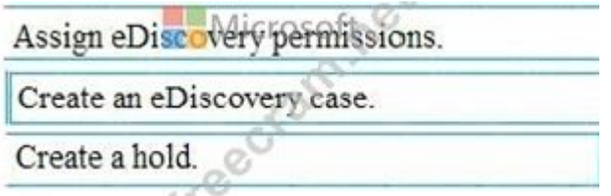
Which three actions should you perform in sequence from the Security & Compliance admin center? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

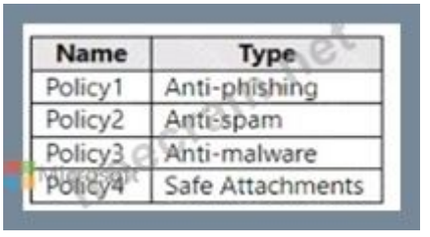


Explanation



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

NEW QUESTION: 161
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. Policy2 and Policy4 only
B. Policy1 and Policy2 only
C. Policy3 and Policy4 only

D. Policy1 and Policy3only

Answer: (SHOW ANSWER)

NEW QUESTION: 162

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: 163

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: 164

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 that contains a user named User1.
You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/pe

NEW QUESTION: 165
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.
The tenant contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
User5	User5@gmail.com	Guest

You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (PII) from being emailed to users outside your organization.
To which users can User! send documents that contain PII?
A. User2, User3, and User4 only
B. User2and User3only
C. User2only
D. User2, User3, User4, and User5
Answer: B (LEAVE A REPLY)

NEW QUESTION: 166
You have a Microsoft 365 E5 subscription.
All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).
You need to configure Microsoft Defender ATP on the computers.
What should you create from the Endpoint Management admin center?
A. a device configuration profile
B. an update policy for iOS
C. a Microsoft Defender ATP baseline profile

D. a mobile device management (MDM) security baseline profile

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 167

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

The policies are assigned to Device1.

Which policy settings will be applied to Device1?

A. only the settings of Policy1

B. only the settings of Policy3

C. no settings

D. only the settings of Policy2

Answer: (SHOW ANSWER)

NEW QUESTION: 168

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. a Conditional Access policy

B. an activity policy

C. a data loss prevention (DLP) policy
D. an access policy
Answer: (SHOW ANSWER)

NEW QUESTION: 169
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)
Explanation
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-team