Microsoft.MS-102.v2026-08-08.q241

Exam Code:	MS-102
Exam Name:	Microsoft 365 Administrator
Certification Provider:	Microsoft
Free Question Number:	241
Version:	v2026-08-08
# of views:	113
# of Questions views:	2747
https://www.freecram.net/torrent/Microsoft.MS-102.v2026-08-08.q241.html	

NEW QUESTION: 1
You implement Microsoft Azure Advanced Threat Protection (Azure ATP).
You have an Azure ATP sensor configured as shown in the following exhibit.

How long after the Azure ATP cloud service is updated will the sensor update?
A. 7 hours
B. 20 hours
C. 12 hours
D. 48 hours
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

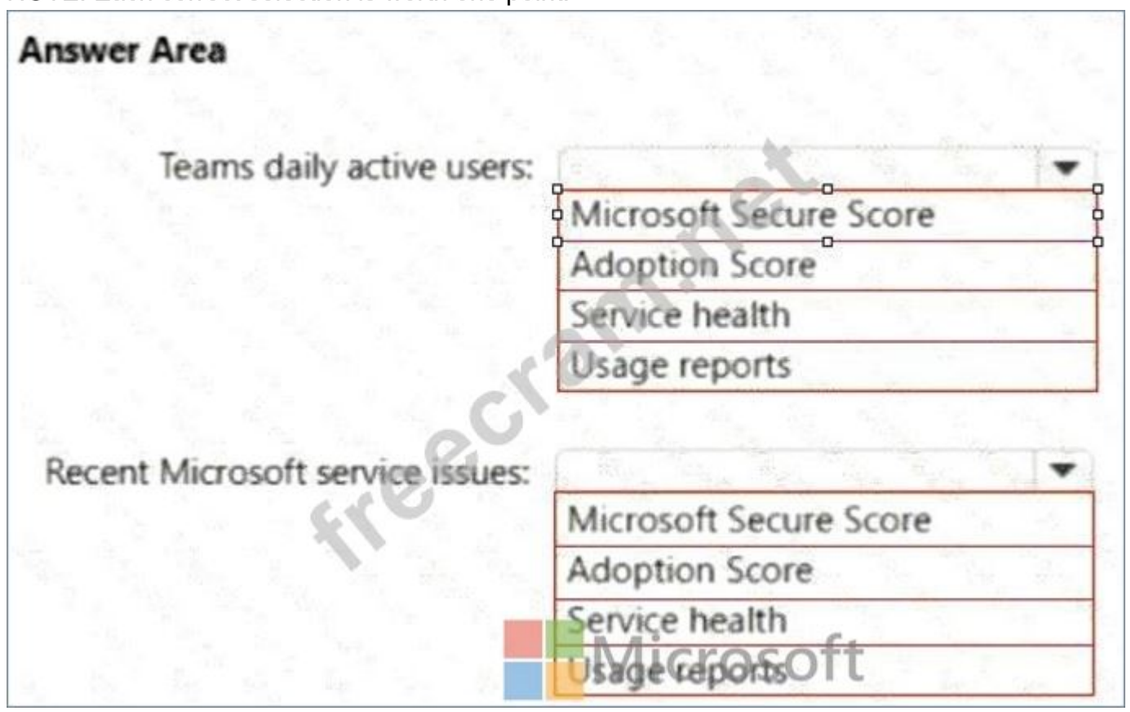
Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

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)
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: 3
HOTSPOT
You have a Microsoft 365 subscription.
You need to review metrics for the following:
The daily active users in Microsoft Teams
Recent Microsoft service issues

What should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Answer Area

Explanation:

Answer Area

Box 1: Usage reports

The daily active users in Microsoft Teams

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

Box 2: Service Health

Recent Microsoft service issues

You can view the health of your Microsoft services, including Office on the web, Yammer, Microsoft Dynamics CRM, and mobile device management cloud services, on the Service health page in the Microsoft

365 admin center. If you are experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

Reference:

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

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

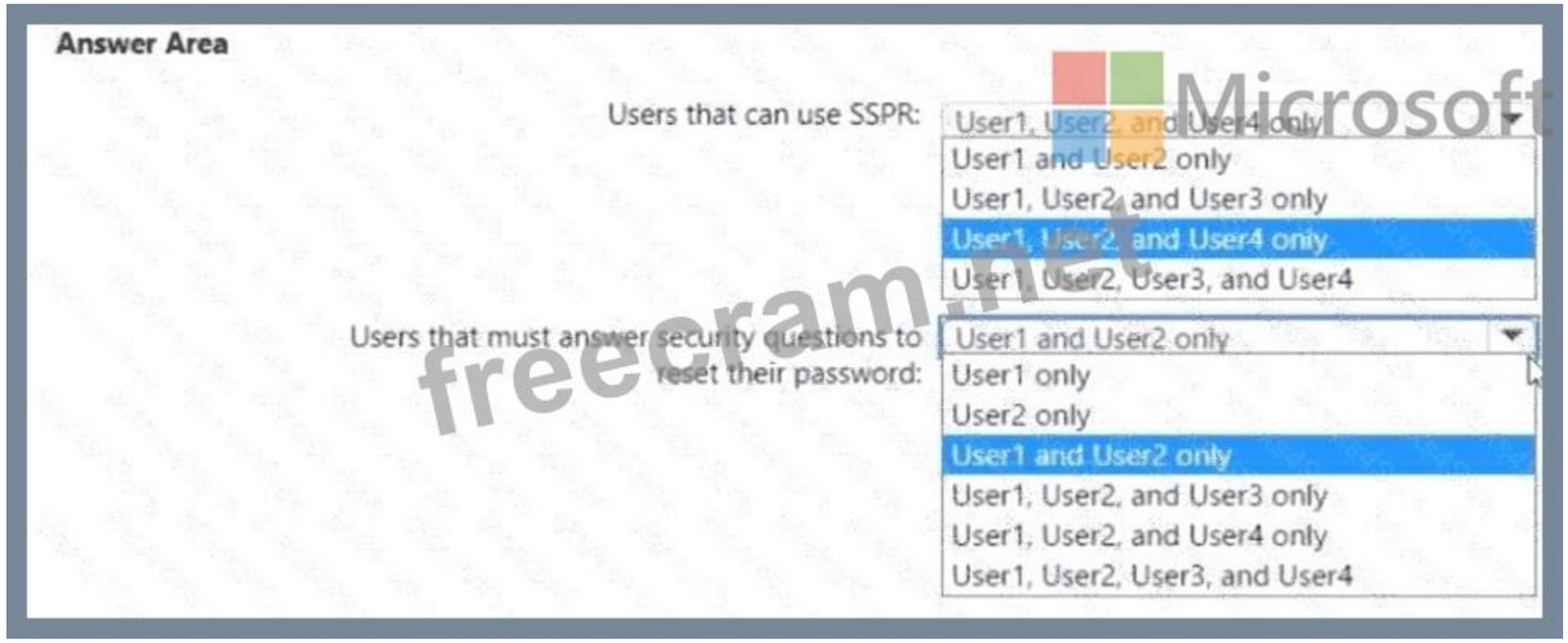
NEW QUESTION: 4

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

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

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

Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.
NOTE; Each correct selection is worth one point.



Answer:

Explanation:

NEW QUESTION: 5
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: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure- portal

NEW QUESTION: 6
You have a Microsoft 365 tenant that contains the groups shown in the following table.

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

You plan to create a compliance policy named Compliance1.
You need to identify the groups that meet the following requirements:
Can be added to Compliance1 as recipients of noncompliance notifications Can be assigned to Compliance1 To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

Answer:

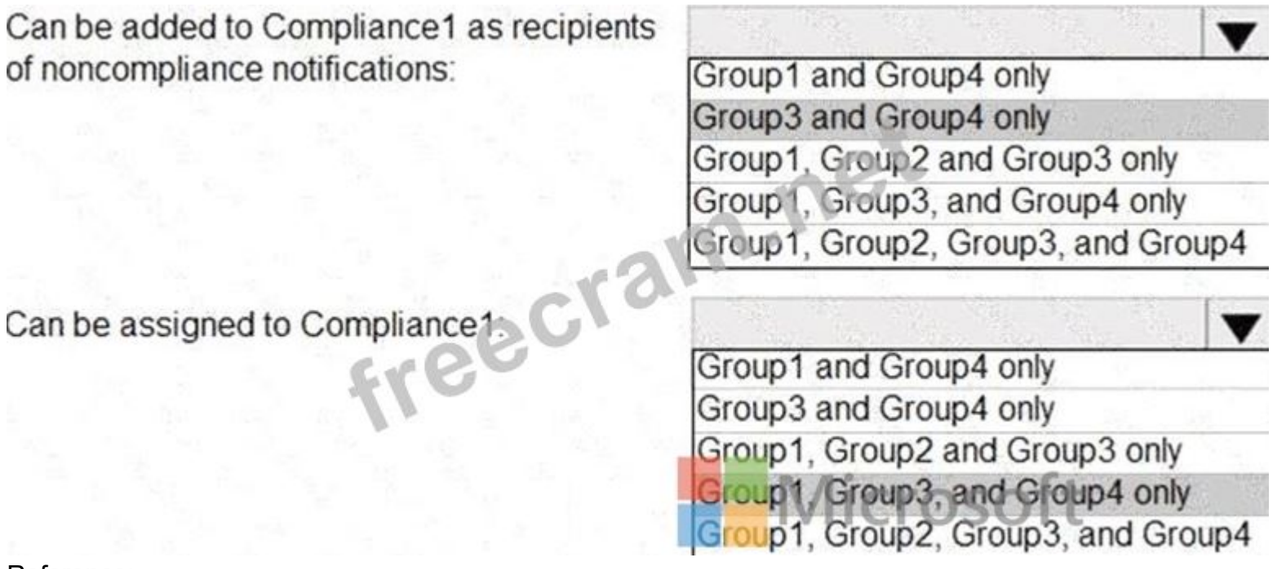
Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

Explanation:



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

NEW QUESTION: 7
HOTSPOT
Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:
Contoso.com
East.contoso.com
The forest contains the users shown in the following table.

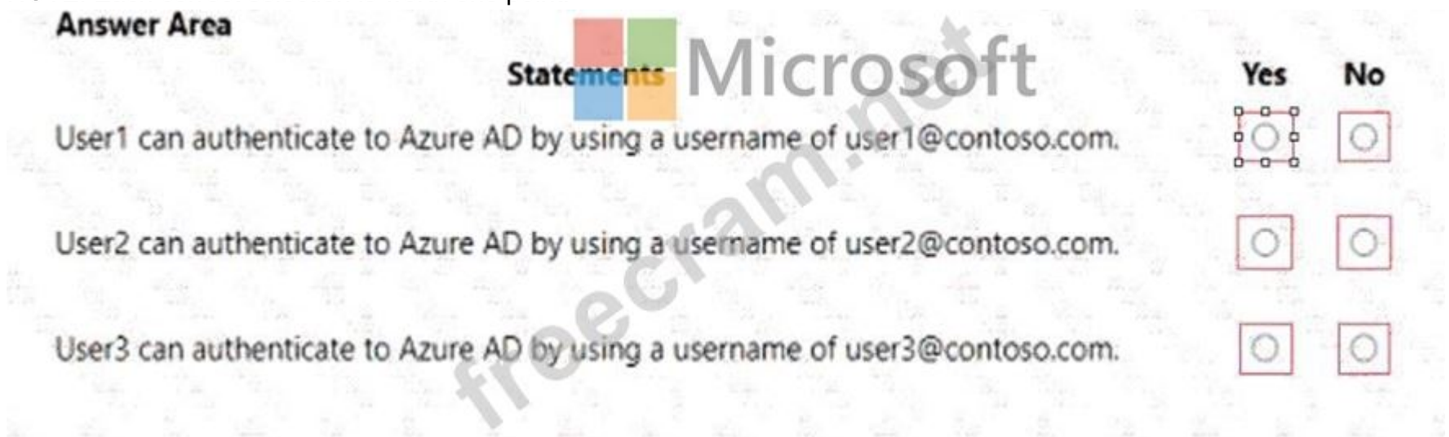
Name	UPN suffix
User1	Contoso.com
User2	East.contoso.com
User3	Fabrikam.com

The forest syncs to an Azure AD tenant named contoso.com 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



Answer:

Answer Area

Statements	Yes	No
User1 can authenticate to Azure AD by using a username of user1@contoso.com.	○	○
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	○	○
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	○	○

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

NEW QUESTION: 8
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

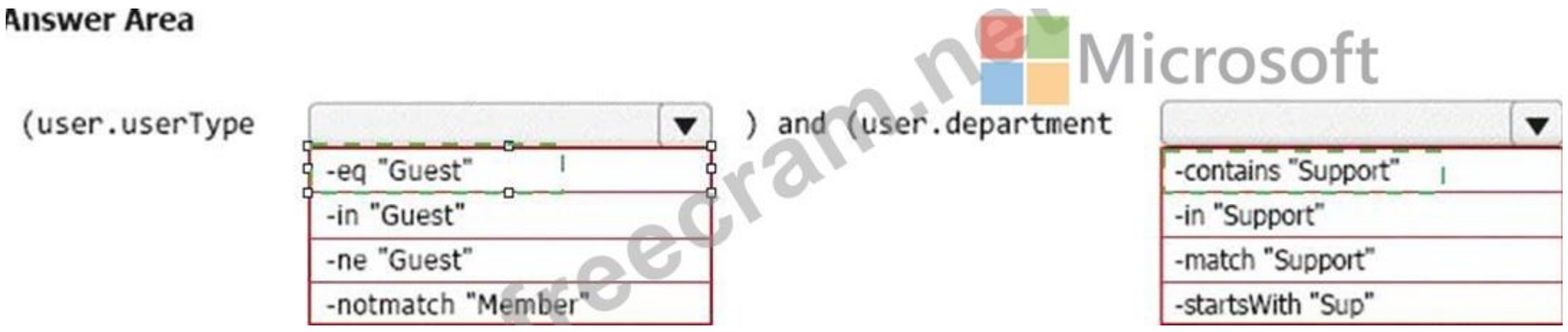
You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.
How should you complete the membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

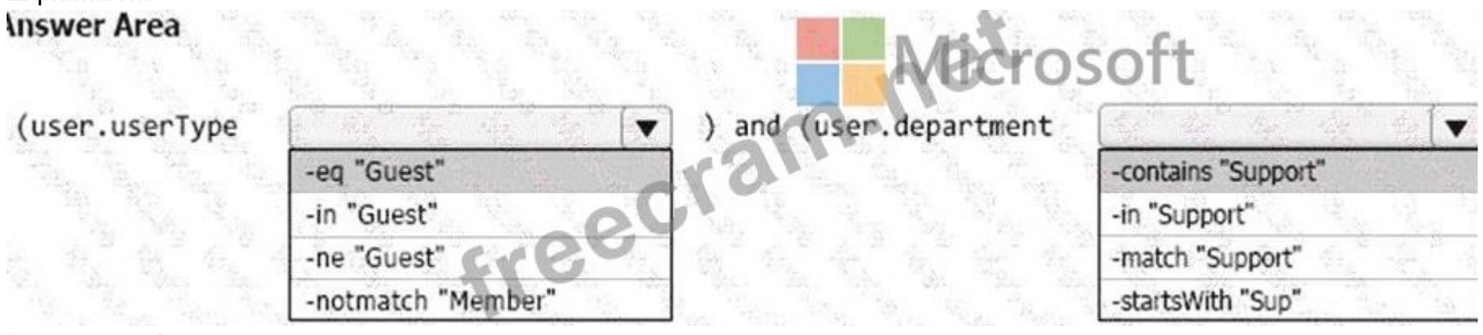
(user.userType ▼) and (user.department ▼

▼	▼
-eq "Guest"	-contains "Support"
-in "Guest"	-in "Support"
-ne "Guest"	-match "Support"
-notmatch "Member"	-startsWith "Sup"

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: 9

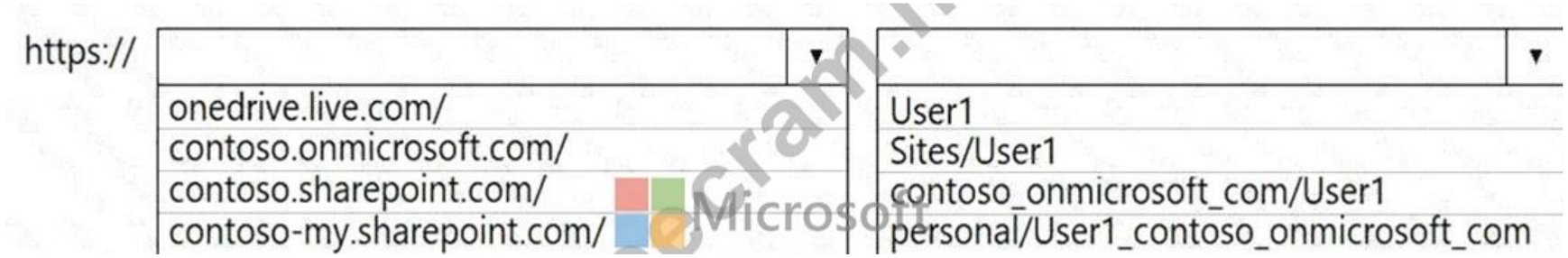
You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

A user named User1 stores documents in Microsoft OneDrive.

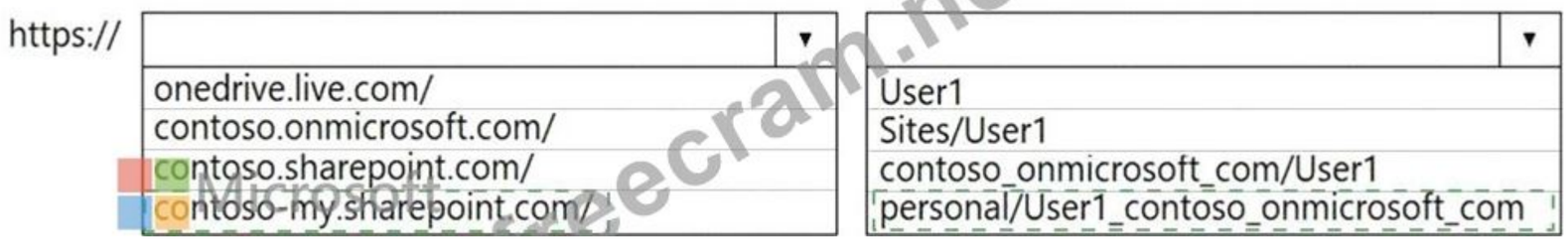
You need to place the contents of User1's OneDrive account on an eDiscovery hold.

Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.

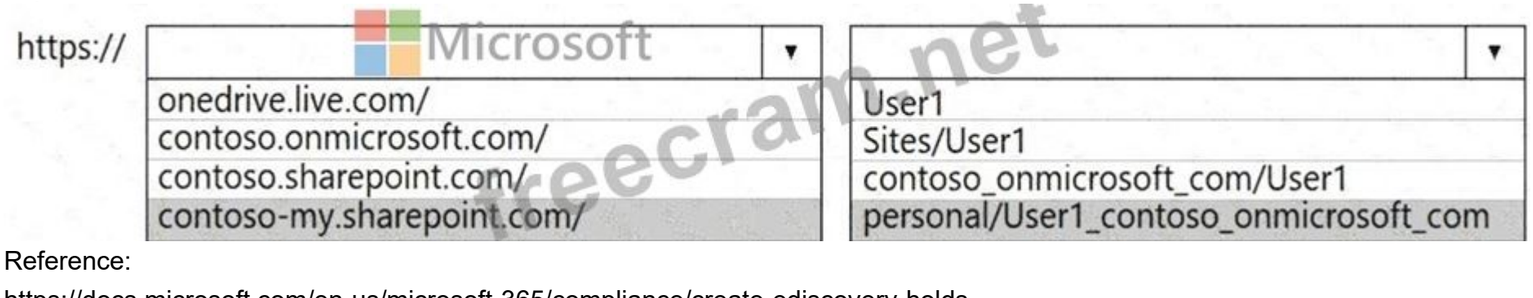
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds

NEW QUESTION: 10

You have a Microsoft 365 E5 tenant that uses Microsoft Intune.
You need to ensure that users can select a department when they enroll their device in Intune.
What should you create?

A. scope tags
B. device configuration profiles
C. device categories
D. device compliance policies
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

NEW QUESTION: 11

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. an anomaly detection policy

B. an activity policy
C. a file policy
D. a session policy
Answer: (SHOW ANSWER)

NEW QUESTION: 12
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: 13
You have a Microsoft 365 E5 subscription. You are implementing Microsoft Defender for Cloud Apps. You need to ensure that you can create OAuth app policies.
Solution: You connect Microsoft 365 to Defender for Cloud Apps.
Does this meet the goal?

A. No
B. Yes
Answer: B (LEAVE A REPLY)

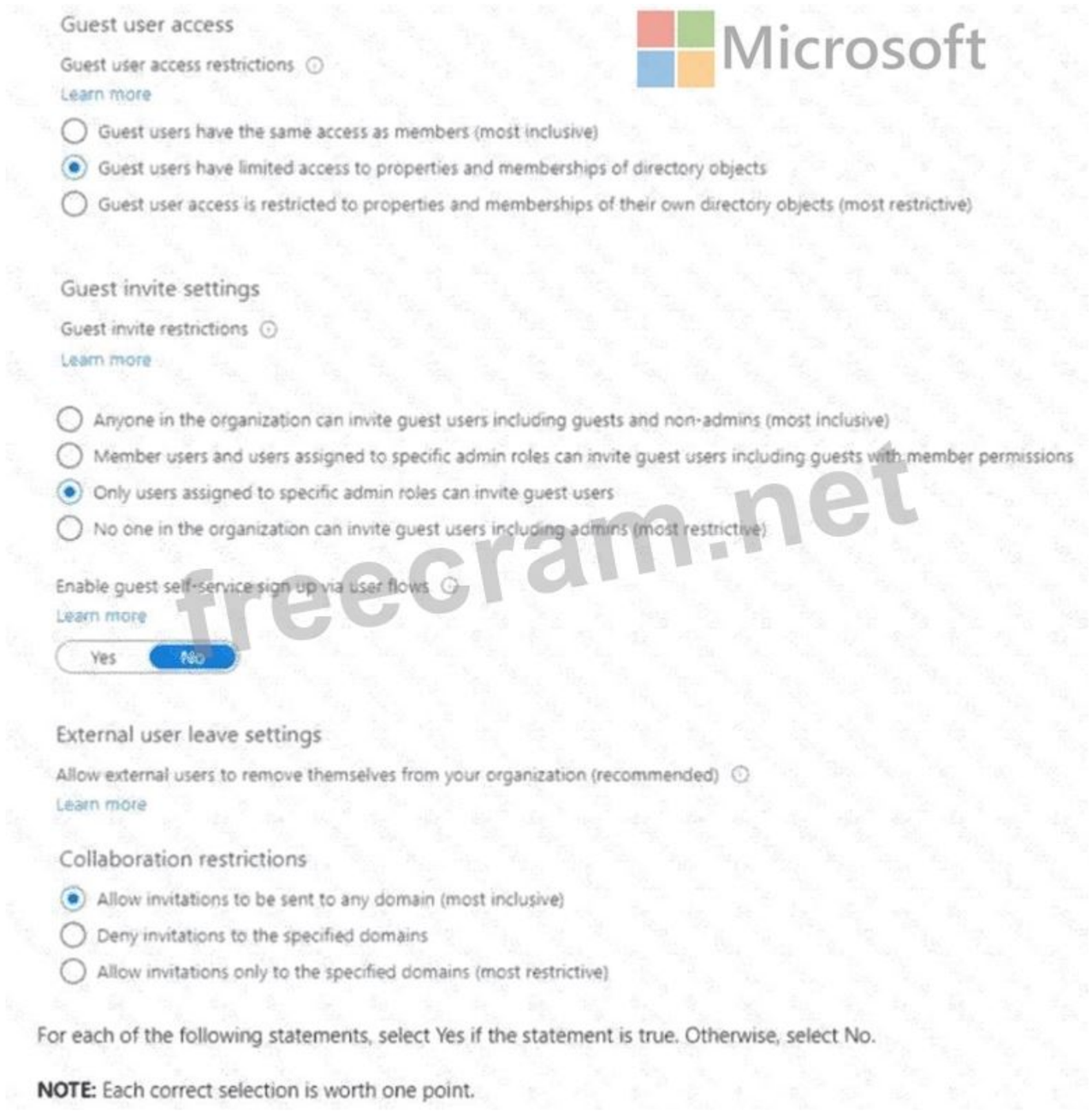
NEW QUESTION: 14
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

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:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 15

You have a Microsoft 365 E5 subscription. You plan to use Microsoft Entra ID Protection.

You need to ensure that account passwords must be changed if account credential. What should you configure?

A. a sign-in risk policy

B. Password protection

C. self-service password reset (SSPR)
D. a user risk policy
Answer: (SHOW ANSWER)

NEW QUESTION: 16
You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?
A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator rote.
B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
C. From the Intune admin center, add User1 as a device enrollment manager.
D. From the Intune admin center, configure the Enrollment restrictions.
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

NEW QUESTION: 17
You have a Microsoft 365 E5 subscription.
You create a user named Admin1.
You need to ensure that Admin1 can view Endpoint security policies from the Microsoft Defender portal. The solution must follow the principle of least privilege.
Which Microsoft Entra role should you assign to Admin1?
A. Security Administrator
B. Security Reader
C. Security Operator
D. Global Reader
E. Cloud Device Administrator
Answer: (SHOW ANSWER)

NEW QUESTION: 18
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune.
You plan to use Endpoint analytics to identify hardware issues.
You need to enable Window health monitoring on the devices to support Endpoint analytics What should you do?
A. Create a configuration profile.
B. Configure the Endpoint analytics baseline regression threshold.
C. Create a compliance policy.
D. Create a Windows 10 Security Baseline profile
Answer: (SHOW ANSWER)

NEW QUESTION: 19
You have a Microsoft 365 subscription.
You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.
What is the maximum number of onmicrosoft.com domains the subscription can contain?
A. 1
B. 2
C. 5
D. 10
Answer: (SHOW ANSWER)
You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to create a new one.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq

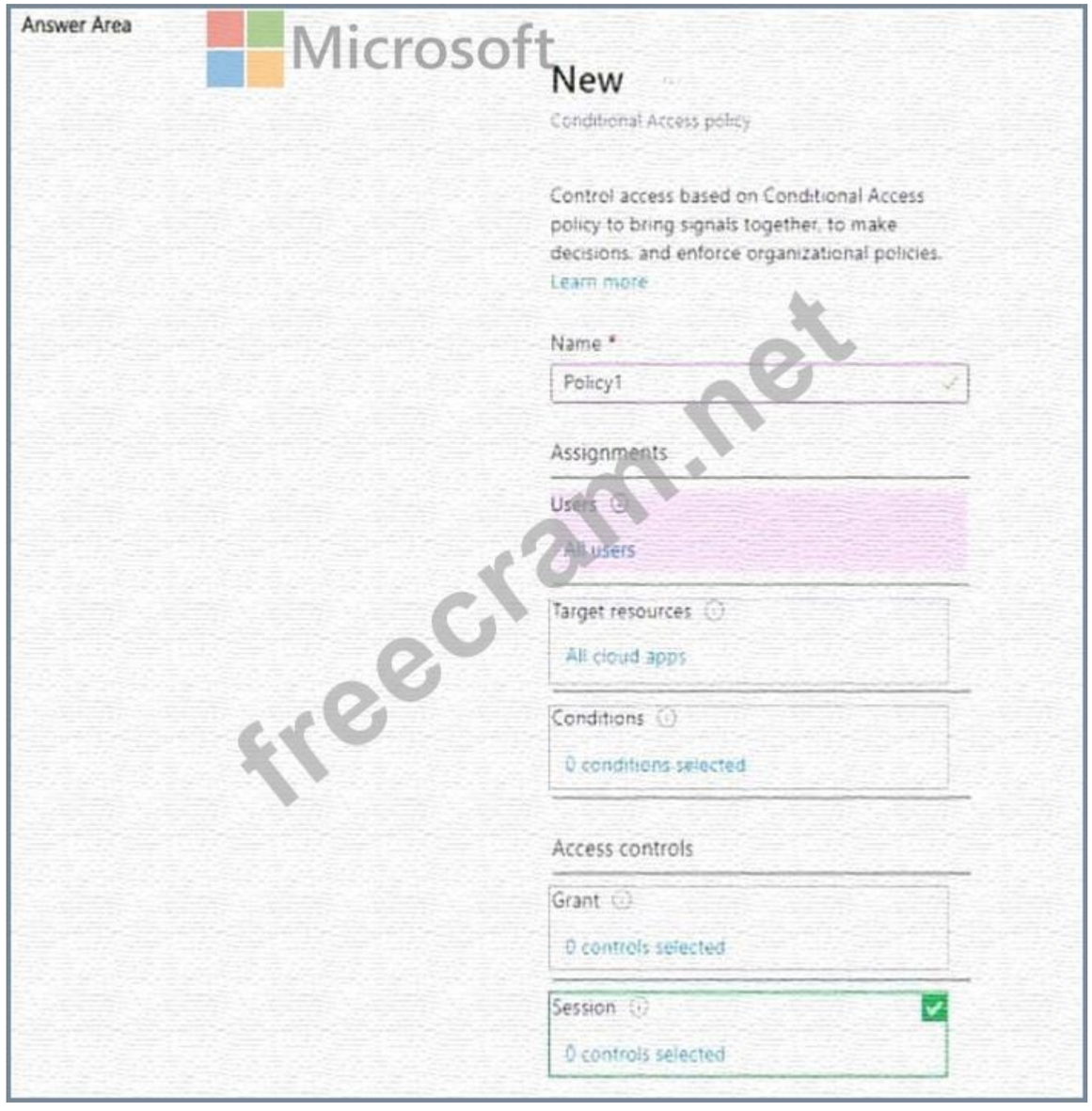
NEW QUESTION: 20
You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.
What should you do first?

A. From the Microsoft Purview compliance portal, create a label and a label policy.
B. From Microsoft Defender for Cloud Apps, create an activity policy.
C. From the Exchange admin center create a mail flow rule.
D. From Microsoft 365 Defender, start a message trace.
Answer: (SHOW ANSWER)

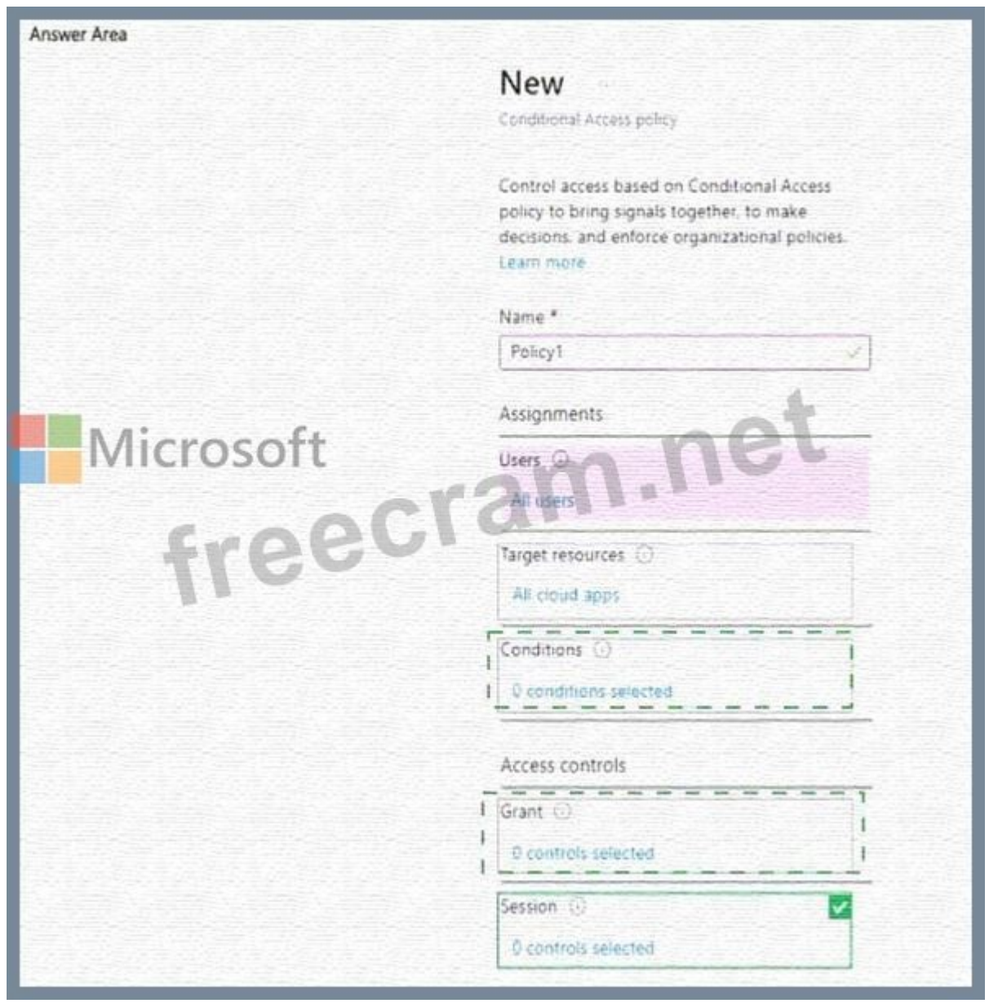
NEW QUESTION: 21
Your network contains an Active Directory domain.
You deploy a Microsoft Entra tenant.
Another administrator configures the domain to synchronize to the Microsoft Entra tenant You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.
You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.
Solution: From Microsoft Entra Connect you modify the Microsoft Entra credentials.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 22
You have a Microsoft 365 E5 subscription.
You create a Conditional Access policy named Policy1 and assign Policy1 to all users.

You need to configure Policy1 to enforce multi factor authentication (MFA) if the user risk level is high.
Which two settings should you configure in Policy1? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Conditions: Set " User risk " to " High "

To enforce MFA based on user risk, you need to configure the Conditional Access policy to trigger when the user risk level is high. This setting ensures that the policy is applied only to users who have a high-risk level.

Grant: Require multi-factor authentication

This setting enforces MFA for users who meet the condition set (high user risk). Requiring MFA ensures that users must provide additional verification, enhancing security for high-risk sign-ins.

NEW QUESTION: 23

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

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

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

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

D. From the Microsoft 365 admin center, modify Help desk information.

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 24
You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.
Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. advanced hunting
B. security reports
C. digital certificate assessment
D. device discovery
E. attack surface reduction (ASR)
Answer: (SHOW ANSWER)
B: Overview of Microsoft Defender for Endpoint Plan 1, Reporting
The Microsoft 365 Defender portal (https://security.microsoft.com) provides easy access to information about detected threats and actions to address those threats.
The Home page includes cards to show at a glance which users or devices are at risk, how many threats were detected, and what alerts/incidents were created.
The Incidents & alerts section lists any incidents that were created as a result of triggered alerts. Alerts and incidents are generated as threats are detected across devices.
The Action center lists remediation actions that were taken. For example, if a file is sent to quarantine, or a URL is blocked, each action is listed in the Action center on the History tab.
The Reports section includes reports that show threats detected and their status.
E: What can you expect from Microsoft Defender for Endpoint P1?
Microsoft Defender for Endpoint P1 is focused on prevention/EPP including:
Next-generation antimalware that is cloud-based with built-in AI that helps to stop ransomware, known and unknown malware, and other threats in their tracks.
(E) Attack surface reduction capabilities that harden the device, prevent zero days, and offer granular control over access and behaviors on the endpoint.
Device based conditional access that offers an additional layer of data protection and breach prevention and enables a Zero Trust approach.
The below table offers a comparison of capabilities are offered in Plan 1 versus Plan 2.

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

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

Incorrect:

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

Reference:

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

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

NEW QUESTION: 25

You have a Microsoft 365 E5 tenant.

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

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

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

What should you do?

A. Create a new label policy

B. Modify the Authority type setting for Retention!

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

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

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 26

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. You need to perform the following tasks:

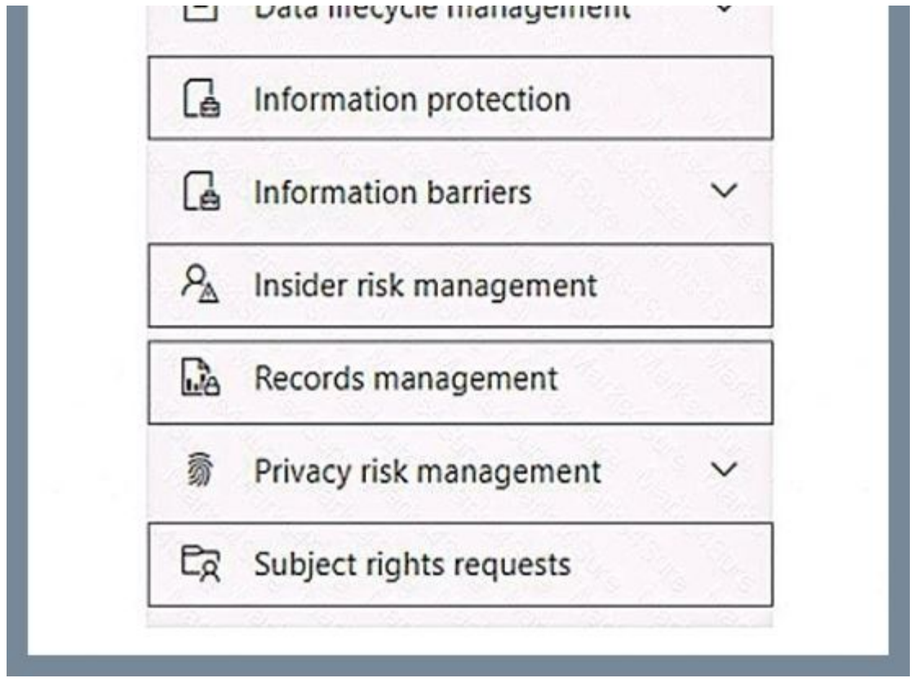
* Create a sensitive info type named SIT1 based on a regular expression.

* Add a watermark to all new documents that are matched by SIT1.

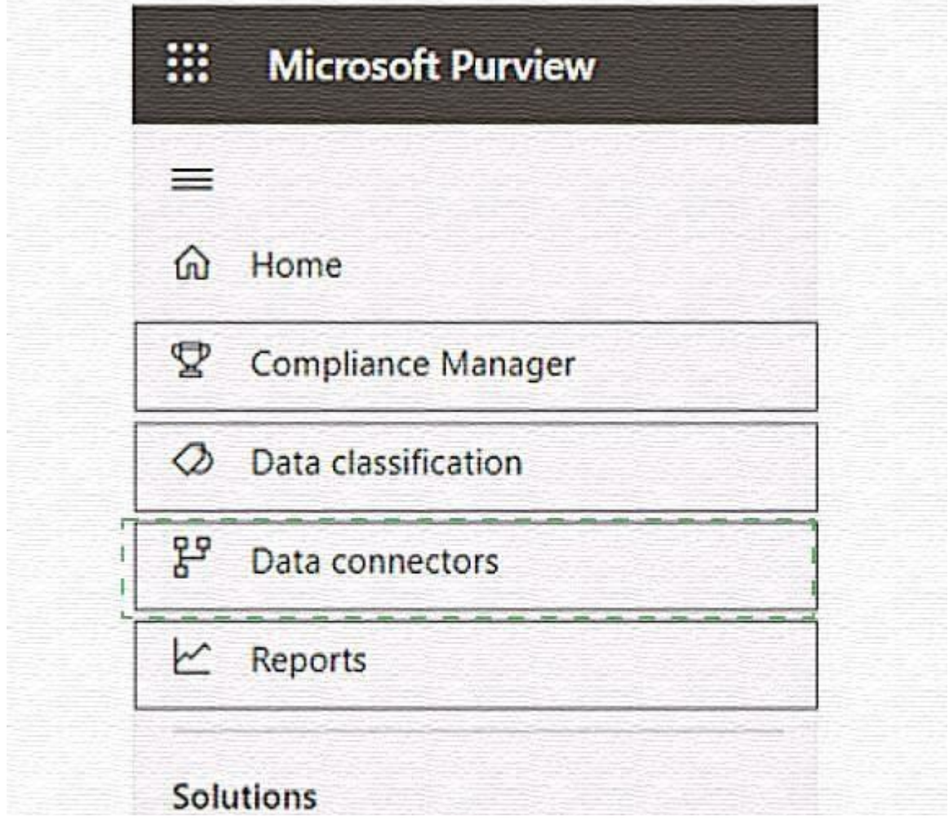
Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.

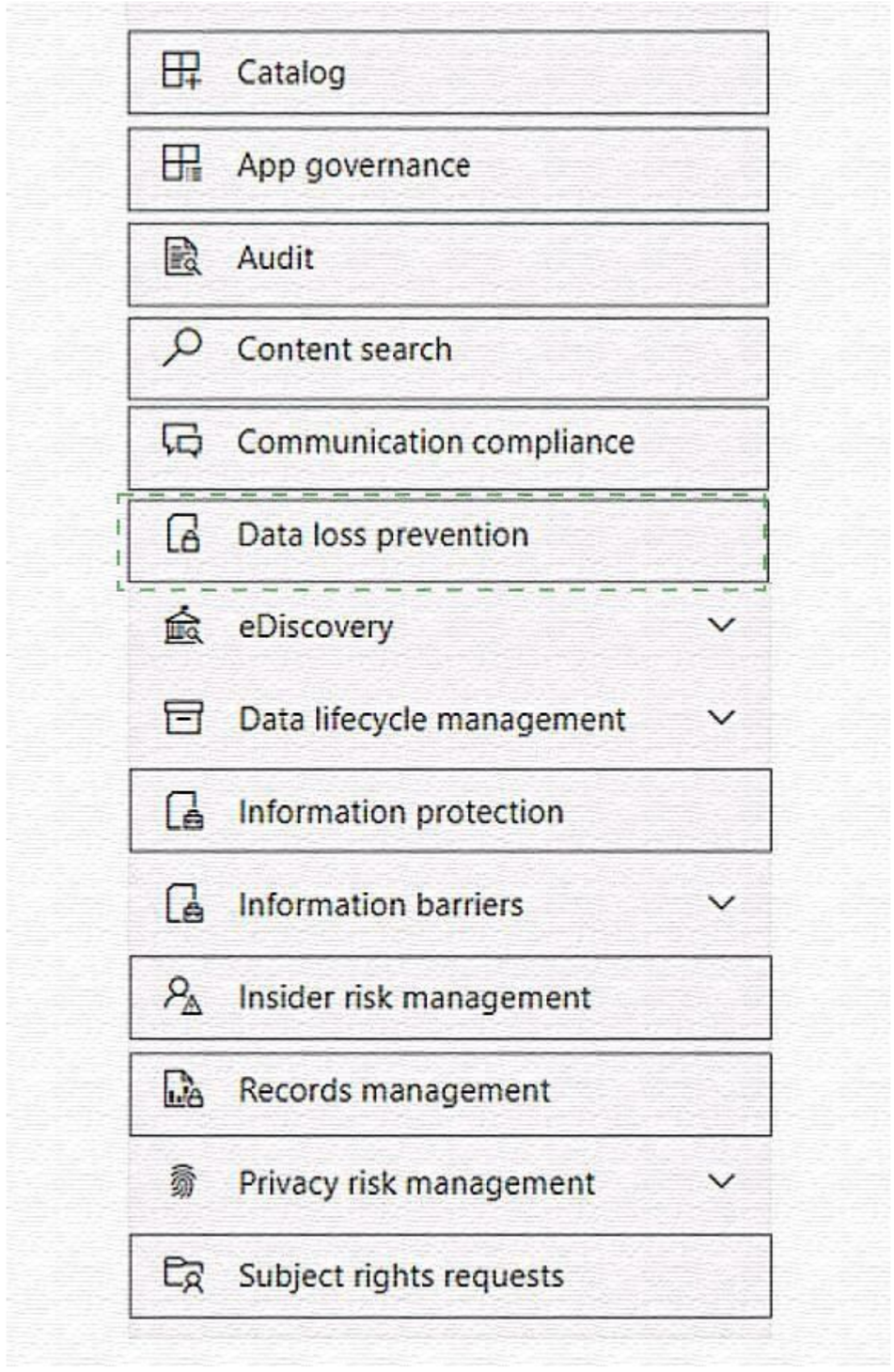
NOTE: Each correct selection is worth one point.

Answer Area


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
Reports
Solutions



Explanation:

Microsoft

NEW QUESTION: 27
You have a Microsoft 365 ES subscription that contains a domain named contoso.com You deploy a new Microsoft Defender (or Office 365 anti-phishing policy named Policy1 that has user impersonation protection enabled for a user named user1@contoso.com.
You discover that Policy1 blocks email messages from a regular contact named usei1@fabnkam.com.
You need to ensure that the messages are delivered successfully
What should you do for Policy1?
A. Configure the Phishing email threshold setting.
B. Configure which users to protect.
C. Select Enable domains to protect.
D. Select Enable mailbox intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it As a result these questions will not appear in the review screen.
Your network contains an Active Directory forest.
You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
* Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
* User passwords must be 10 characters or more.
Solution: implement password hash synchronization and configure password protection in the Azure AD tenant.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 29
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.

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

Answer:

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

Explanation:

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

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: 30
Your company has a Microsoft E5 tenant.
The company must meet the requirements of the ISO/IEC 27001:2013 standard.
You need to assess the company's current state of compliance.
What should you use?
A. eDiscovery
B. Information governance
C. Compliance Manager
D. Data Subject Requests (DSRs)
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

NEW QUESTION: 31
You have a Microsoft 365 subscription.
Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.
You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.
D18912E1457D5D1DDCBD40AB3BF70D5D
What should you create to ensure that the DLP policy can detect the customer IDs?
A. a sensitive information type
B. a sensitivity label
C. a supervision policy
D. a retention label
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide

NEW QUESTION: 32
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: 33
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 automated investigation.
B. Create a web content filtering policy.
C. Enable Custom network indicators.
D. Configure an enforcement scope.
E. Create an indicator.
Answer: (SHOW ANSWER)

NEW QUESTION: 34

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

...e following table.

You configure Tenant properties as shown in the following exhibit.

Which users will be contacted by Microsoft if the tenant experiences a data breach?

A. Used only

B. User2 only

C. User3 only

D. Used and User2 only

E. User2 and User3 only

Answer: (SHOW ANSWER)

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

Reference:

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

NEW QUESTION: 35

You have a Microsoft 365 E5 subscription.

You integrate Microsoft Defender for Endpoint with Microsoft Intune.

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

Solution: You create a compliance policy.

Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

NEW QUESTION: 36

You have a Microsoft 365 E5 subscription.

You plan to create an anti-malware policy named Policy1.

You need to ensure that Policy1 can detect malicious email messages that were already delivered to a user's mailbox.

What should you do in the Microsoft Defender portal?

A. Enable enhanced filtering.

B. Enable zero-hour auto purge (ZAP).

C. Modify the common attachments filter.

D. Configure a quarantine policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
You have a Microsoft J65 E5 subscription.
You integrate Microsoft Defender for Endpoint with Microsoft Intune.
You need to ensure that devices automatically onboard to Defender for Endpoint when they are enrolled in Intune.
Solution: You enable co-management.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 38
You have a Microsoft 365 E5 subscription.
You have an Azure AD tenant named contoso.com that contains the following users:
* Admin1
* Admin2
* User1
Contoso.com contains an administrative unit named AIM that has no role assignments. User1 is a member of AU1. You create an administrative unit named AU2 that does NOT have any members or role assignments.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer:

Answer Area

Statements	Yes	No
You can add Admin1 as a member of AU1.	○	○
You can add User1 as a member of AU2.	○	○
You can assign Admin2 the User administrator role for AU1.	○	○

Explanation:

Answer Area

Statements	Yes	No
You can add Admin1 as a member of AU1.	●	○
You can add User1 as a member of AU2.	●	○
You can assign Admin2 the User administrator role for AU1.	○	●

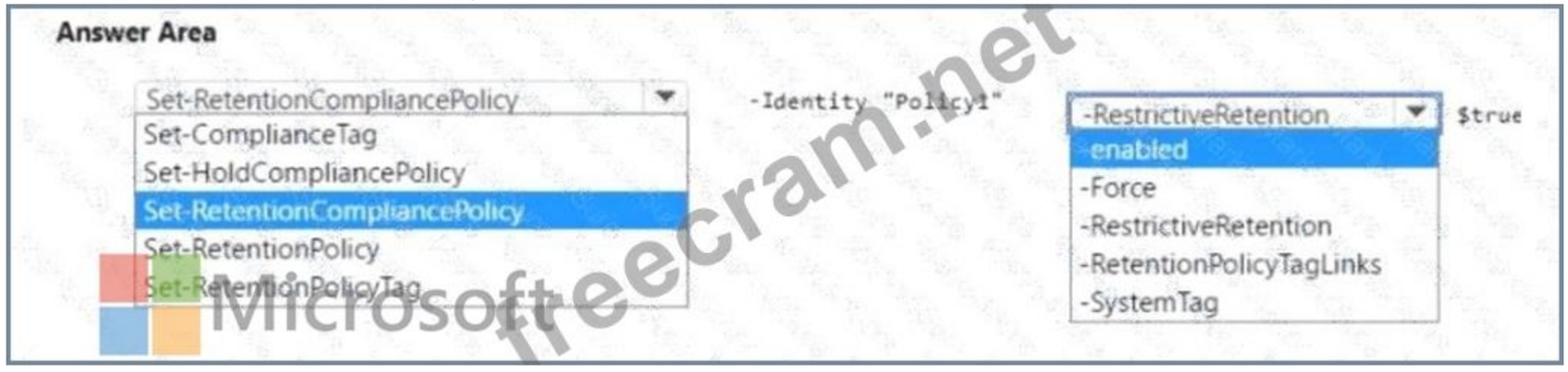
NEW QUESTION: 39

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

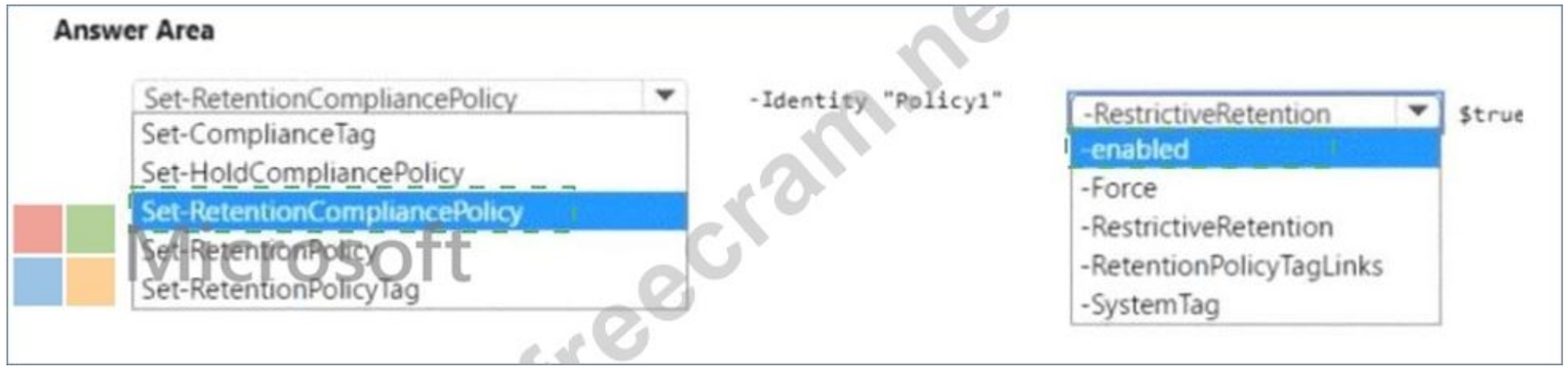
You need to prevent all users from disabling the policy or reducing the retention period.

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: 40

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

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager.

To which devices can you deploy Microsoft 365 Apps for enterprise?

A. Device1 only

B. Device1 and Device3 only

C. Device2 and Device4 only

D. Device1, Device2. and Device3 only

E. Device1, Device2, Device3, and Device4

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 41

You have a Microsoft 365 E5 tenant.

Users store data in the following locations:

Microsoft Teams

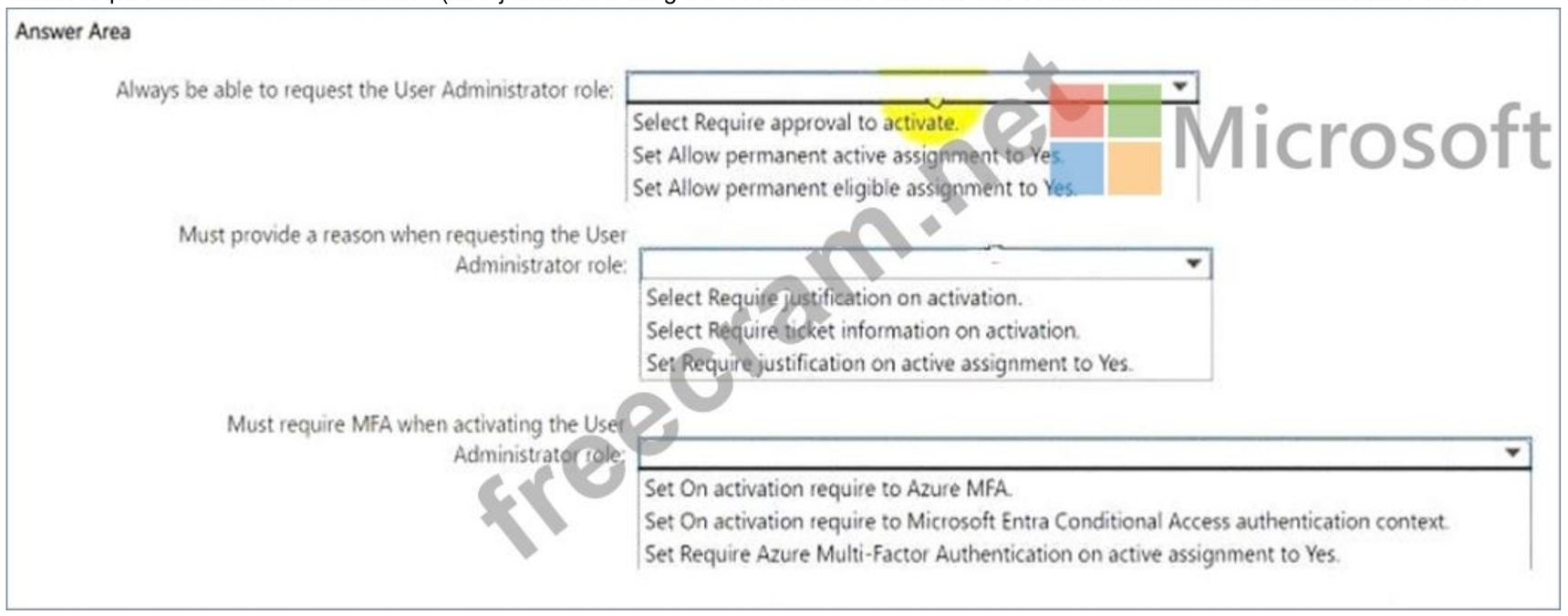
Microsoft OneDrive

Microsoft Exchange Online

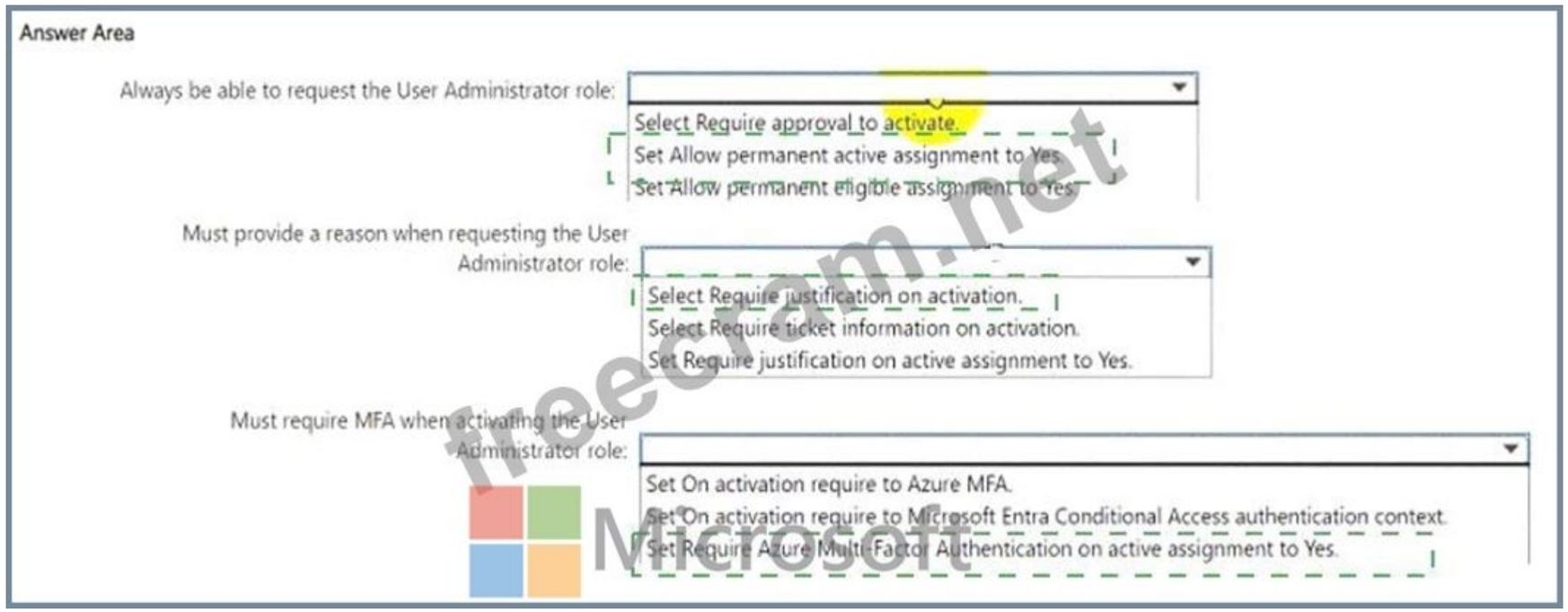
Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.
What is the minimum number of retention policies that you should create?
A. 1
B. 2
C. 3
D. 4
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide

NEW QUESTION: 42
You have a Microsoft 365 E5 subscription.
You need to configure Privileged Identity Management (PIM) for the User Administrator role in Microsoft Entra. Eligible users must meet the following requirements:
* Always be able to request the User Administrator role.
* Must provide a reason when requesting the User Administrator role
* Must require multi-factor authentication (MFA} when activating the User Administrator role The solution must minimize administrative effort.



Answer:



Explanation:

Always be able to request the User Administrator role: Setting " Allow permanent eligible assignment to Yes " ensures that users can always request the User Administrator role when needed.

Must provide a reason when requesting the User Administrator role: Selecting " Require justification on activation " ensures that users must provide a reason each time they activate the User Administrator role, which adds a layer of accountability and tracking.

Must require MFA when activating the User Administrator role: Setting " Require Azure Multi-Factor Authentication on active assignment to Yes " ensures that users must perform MFA to activate the User Administrator role, enhancing security.

NEW QUESTION: 43

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps. You need to create a file policy named Policy1 that meets the following requirements:

* Inspects files in connected software as a service (SaaS) apps
* Inspects protected files

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

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

- Admin quarantine
- Microsoft Information Protection ✓
- Azure security
- Files ✓

Conditional Access App Control

- General Settings
- User monitoring
- Device identification
- App onboarding/maintenance
- Edge for Business protection

App governance

- Service status

Explanation:

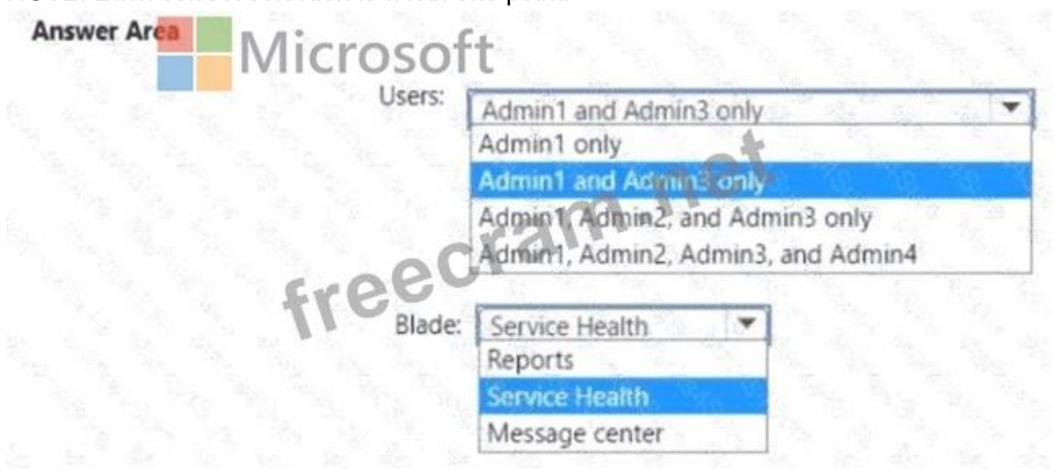
Answer Area

NEW QUESTION: 44
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft Defender XDR. Which Microsoft service source will appear on the Incidents page of the Microsoft Defender portal?
A. Microsoft Defender for Cloud
B. Azure Information Protection
C. Azure Arc
D. Microsoft Defender for Cloud Apps
Answer: (SHOW ANSWER)

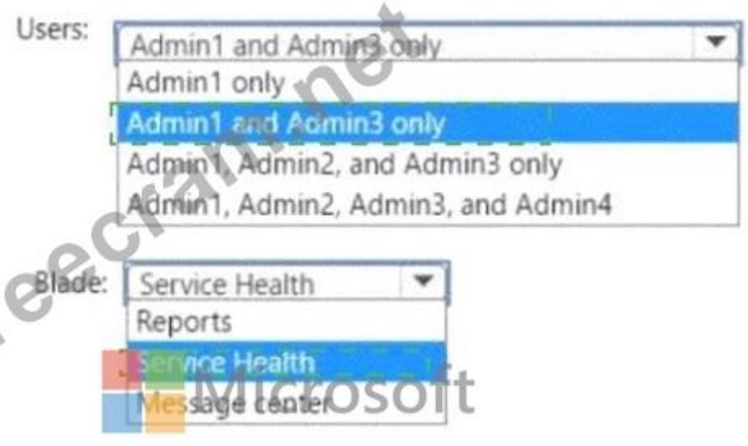
NEW QUESTION: 45
Your on-premises network contains an Active Directory domain.
You have a Microsoft 365 E5 subscription.
You plan to implement a hybrid configuration that has the following requirements:
* Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources
* Supports the use of Azure AD Identity Protection

You need to configure Azure AD Connect to support the planned implementation. Which two options should you select? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Password Hash Synchronization
B. Password writeback
C. Enable single sign-on
D. Directory extension attribute sync
E. Pass-through authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 46
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:
Answer Area



Explanation:

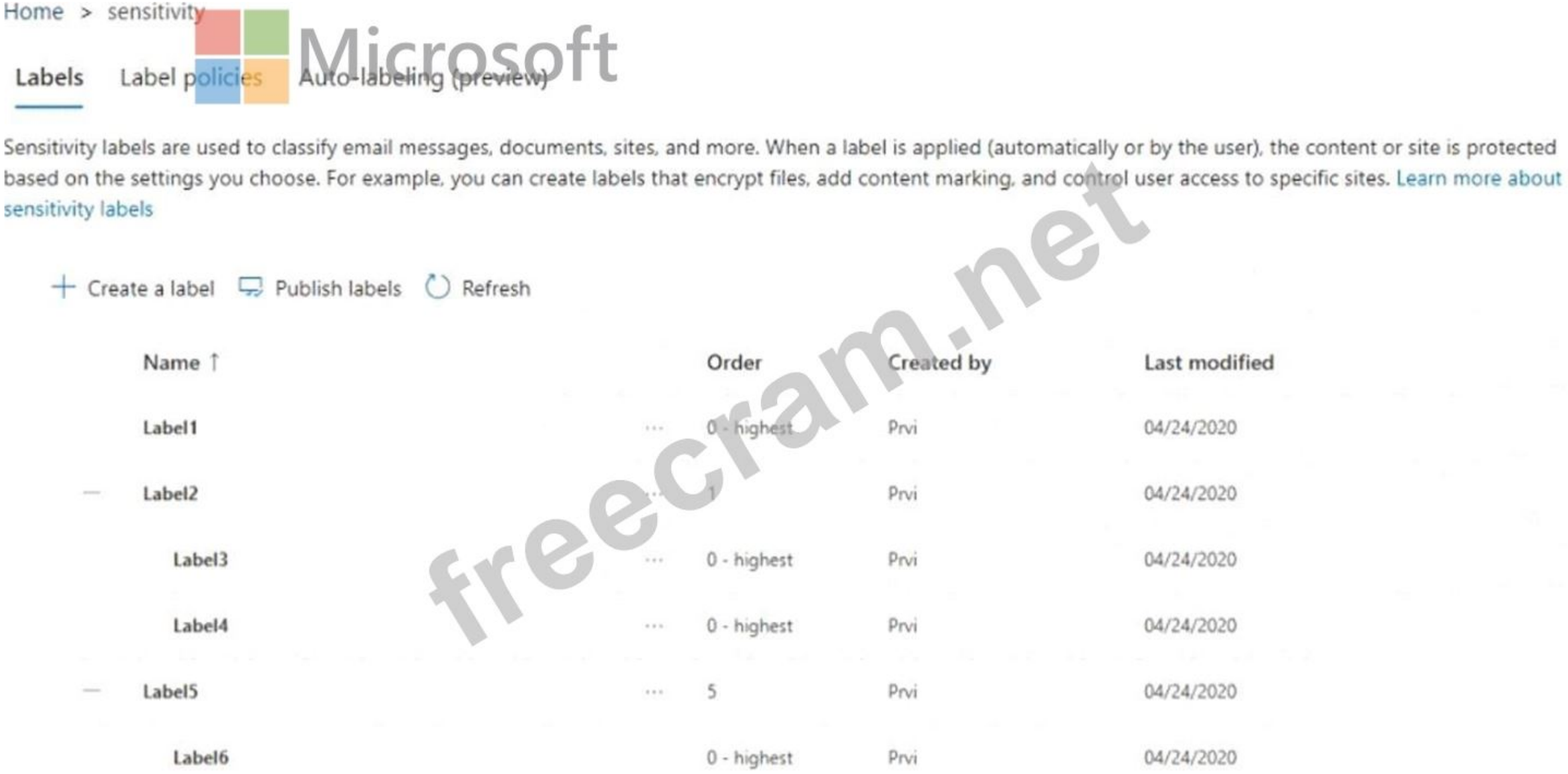
NEW QUESTION: 47
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals.
More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have a Microsoft 365 E5 subscription and use Microsoft Defender for Office 365.
You need to implement a threat policy that will apply a balanced baseline protection profile to protect against spam, phishing, and malware.
Solution: You create a Standard preset security policy.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 48
You have a Microsoft 365 E5 subscription that contains the identities shown in the following table:

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

You create a shared mailbox named Shared1.
Which identities can you add to Shared1 as a member?
A. User1, Group2, and Group3 only
B. User1 and Group1 only
C. User1 and Group2 only
D. User1 only
E. User1 and Group3 only
Answer: (SHOW ANSWER)
NEW QUESTION: 49

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.



Which labels can users apply to content?

A. Label1, Label3, Labe2, and Label6 only

B. Label1, Label2, and Label5 only

C. Label3. Label4, and Label6 only

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

Answer: (SHOW ANSWER)

NEW QUESTION: 50

You need to configure the compliance settings to meet the technical requirements.
What should you do in the Microsoft Endpoint Manager admin center?

A. From Compliance policies, modify the Notifications settings.
B. From Locations, create a new location for noncompliant devices.
C. From Retire Noncompliant Devices, select Clear All Devices Retire State.
D. Modify the Compliance policy settings.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION: 51
You have a Microsoft 365 E5 subscription.
You are evaluating Microsoft Defender for Cloud Apps.
Which two types of policy rely on Conditional Access App Control? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. file policy
B. access policy
C. app discovery policy
D. activity policy
E. session policy
F. OAuth app policy
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You create a device configuration profile from the Device Management admin center.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
It looks like the given answer is correct. There is an on-premises Active Directory synced to Azure Active Directory (Azure AD) So the co-management path1 - Auto-enroll existing clients 1. Hybrid Azure AD 2.
Client agent setting for hybrid Azure AD-join 3. Configure auto-enrollment of devices to Intune 4. Enable co- management in Configuration Manager https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial- co-manage-client

NEW QUESTION: 53

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:

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.	○	○

NEW QUESTION: 54

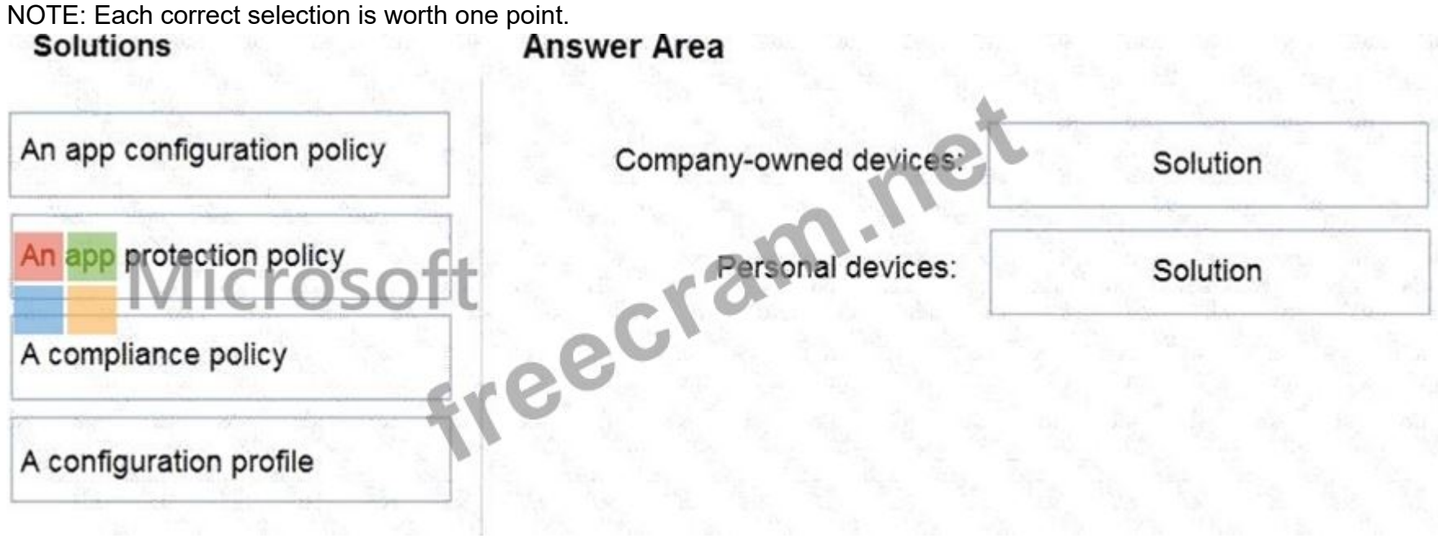
Your company has a Microsoft 365 E5 tenant.

Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.

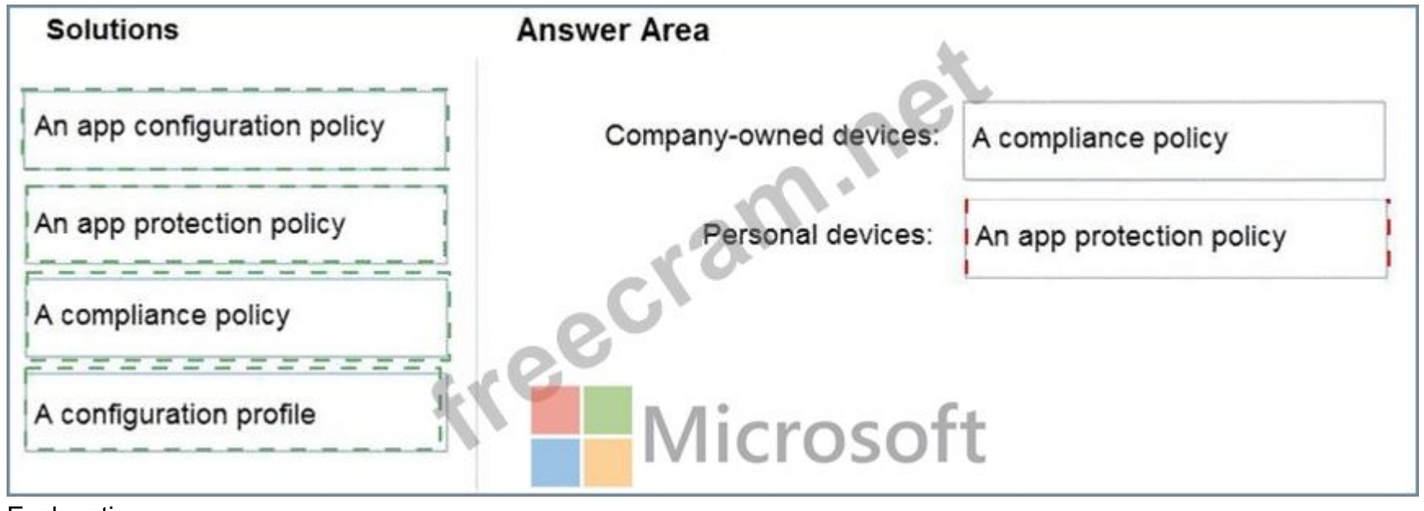
You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.

What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component 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.

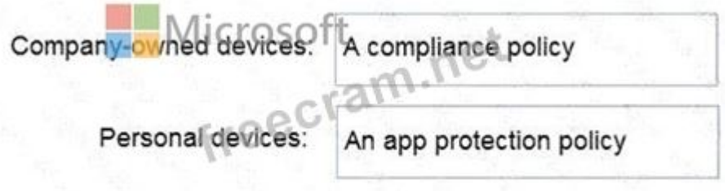
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 55

You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.

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

You plan to enable VPN access for the devices.

What is the minimum number of configuration policies required?

A. 3

B. 1

C. 4

D. 5

Answer: (SHOW ANSWER)

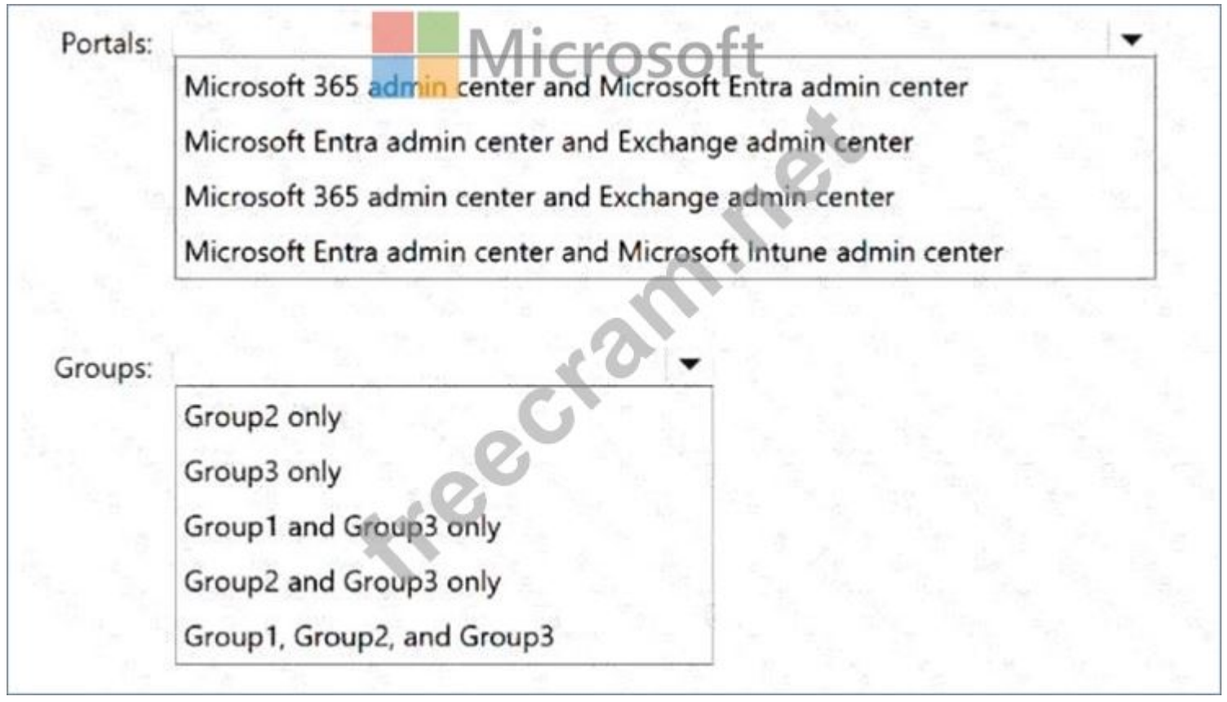
NEW QUESTION: 56

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

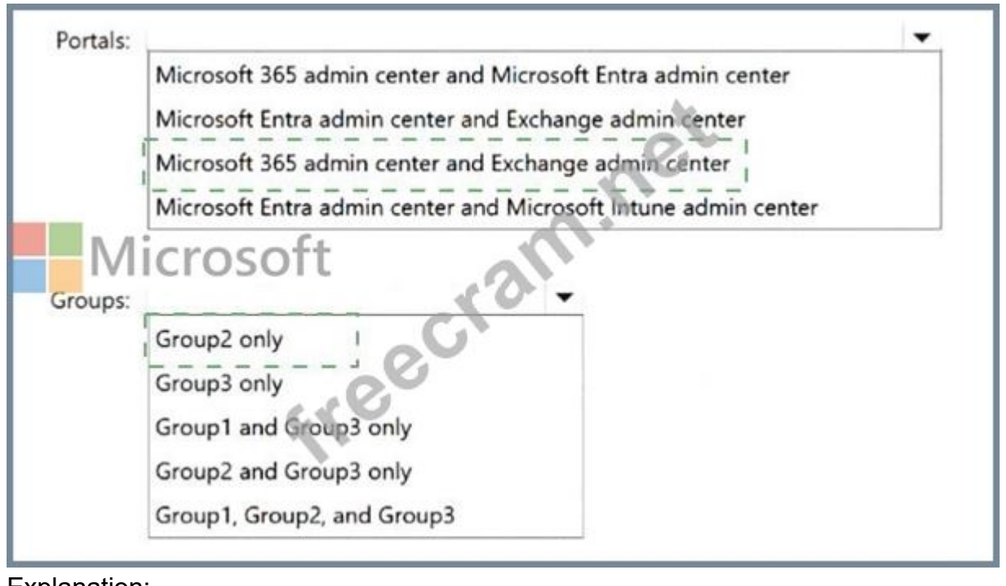
Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365

You need to create a contact named Contact1 and add Contact1 to a group.

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



Answer:



Explanation:
Portals: Microsoft 365 admin center and Exchange admin center
Groups: Group2 only
Creating a contact (mail contact)
A contact (also called a mail contact) is an Exchange object. Microsoft documentation states that mail contacts are created and managed using Exchange-related admin experiences.
* The Exchange admin center explicitly supports creating and managing mail contacts.

* The Microsoft 365 admin center provides a simplified interface that also allows admins to create contacts (which are stored in Exchange Online).
Therefore, the two correct portals that can be used to create Contact1 are:
* Microsoft 365 admin center
* Exchange admin center
Other portals are incorrect:
* Microsoft Entra admin center manages users, groups, and devices, but does not support creating mail contacts .
* Microsoft Intune admin center is for device and app management only.
Adding a contact to a group
Microsoft documentation clearly differentiates which group types can contain contacts:
* Distribution groups support adding mail-enabled objects , including:
* Mail users
* Mail contacts
* Security groups do not support mail contacts.
* Microsoft 365 groups only support user mailboxes and do not support contacts.

NEW QUESTION: 57
You have a Microsoft 365 tenant.
You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.
What should you use?
A. an attack surface reduction (ASR) policy
B. an app configuration policy
C. a device compliance policy
D. a device configuration profile
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

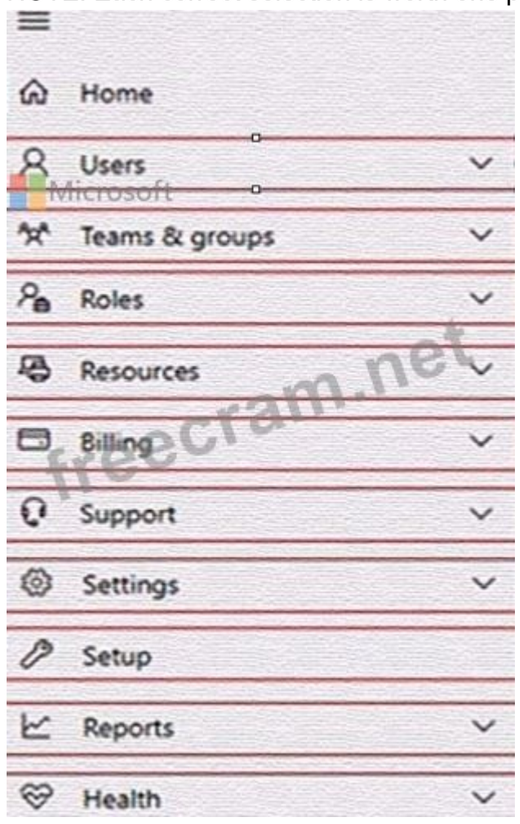
NEW QUESTION: 58
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

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

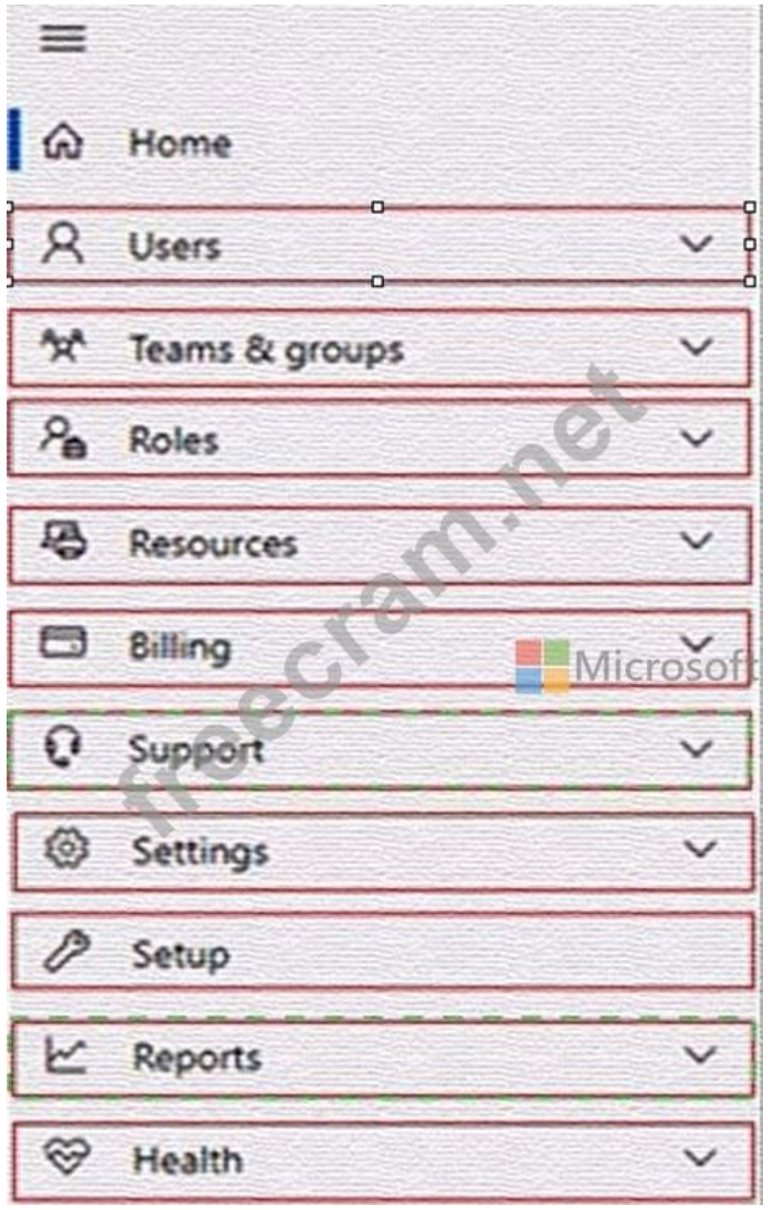
You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (PII) from being emailed to users outside your organization.
To which users can User! send documents that contain PII?
A. User2, User3,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

B. User2and User3only
C. User2only
D. User2, User3, and User4 only
Answer: (SHOW ANSWER)

NEW QUESTION: 59
HOTSPOT
Your company has a Microsoft 365 E5 subscription.
You need to perform the following tasks:
View the Adoption Score of the company.
Create a new service request to Microsoft.
Which two options should you use 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:



Explanation:

Box 1: Reports

View the Adoption Score of the company.

How to enable Adoption Score

To enable Adoption Score:

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

Box 2: Support

Create a new service request to Microsoft.

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

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

Reference:

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

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

NEW QUESTION: 60

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.
During testing, you discover that a user can share credit card information with external users by using email.
However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint.
You need to prevent the user from sharing the credit card information by using email and SharePoint.
What should you configure?

A. the status of the DLP policy
B. the locations of the DLP policy
C. the user overrides of the DLP policy rule
D. the conditions of the DLP policy rule
Answer: (SHOW ANSWER)

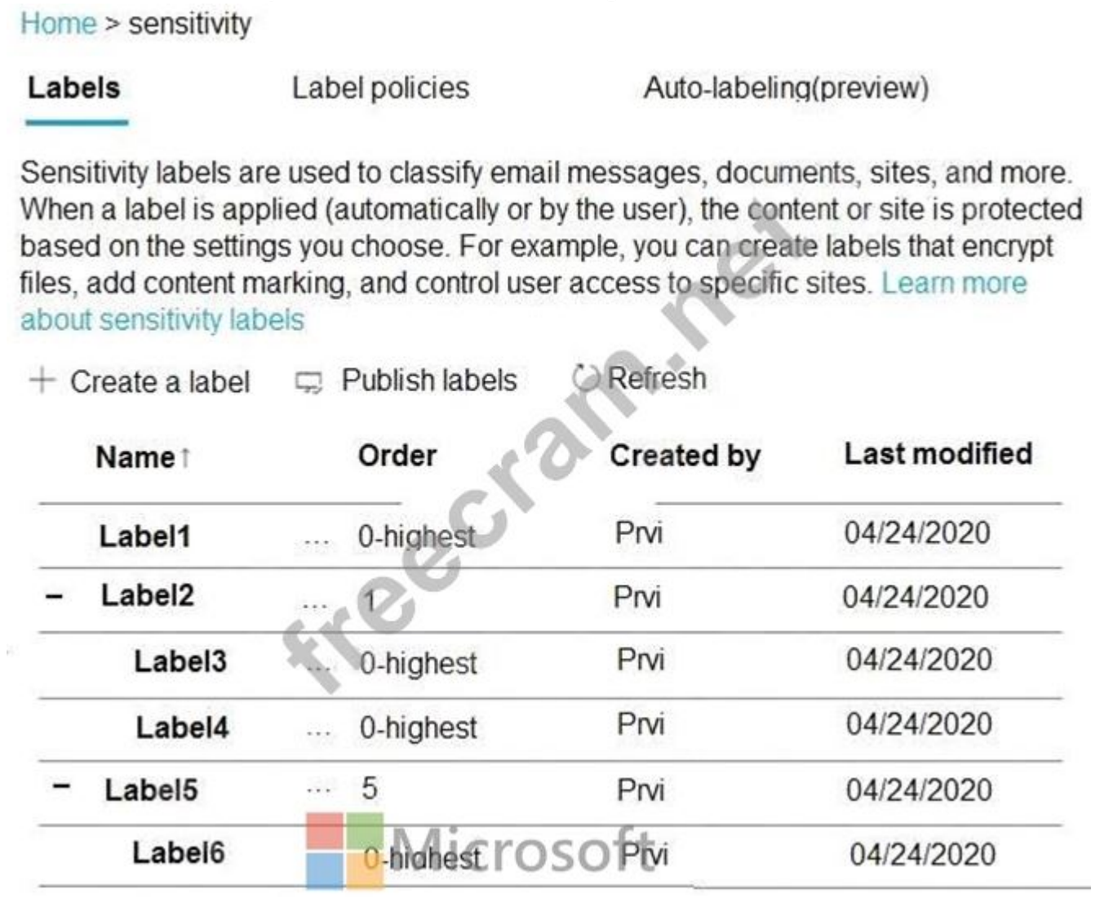
NEW QUESTION: 61

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)
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: 62

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

NEW QUESTION: 63
You have the sensitivity labels shown in the following exhibit.



Which labels can users apply to content?
A. Label3, Label4, and Label6 only
B. Label1, Label2. Label3. Label4. Label5. and Label6
C. Label1, Label2, and Label5 only
D. Label1, Label3, Label4, and Label6 only
Answer: (SHOW ANSWER)
Reference:

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

NEW QUESTION: 64

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

User2 runs a script that modifies a file in a Microsoft SharePoint Online library once every four minutes and runs for a period of two hours.

How many alerts will User1 receive?

A. 10

B. 5

C. 25

D. 2

Answer: (SHOW ANSWER)

NEW QUESTION: 65

HOTSPOT

You have a Microsoft 365 subscription.

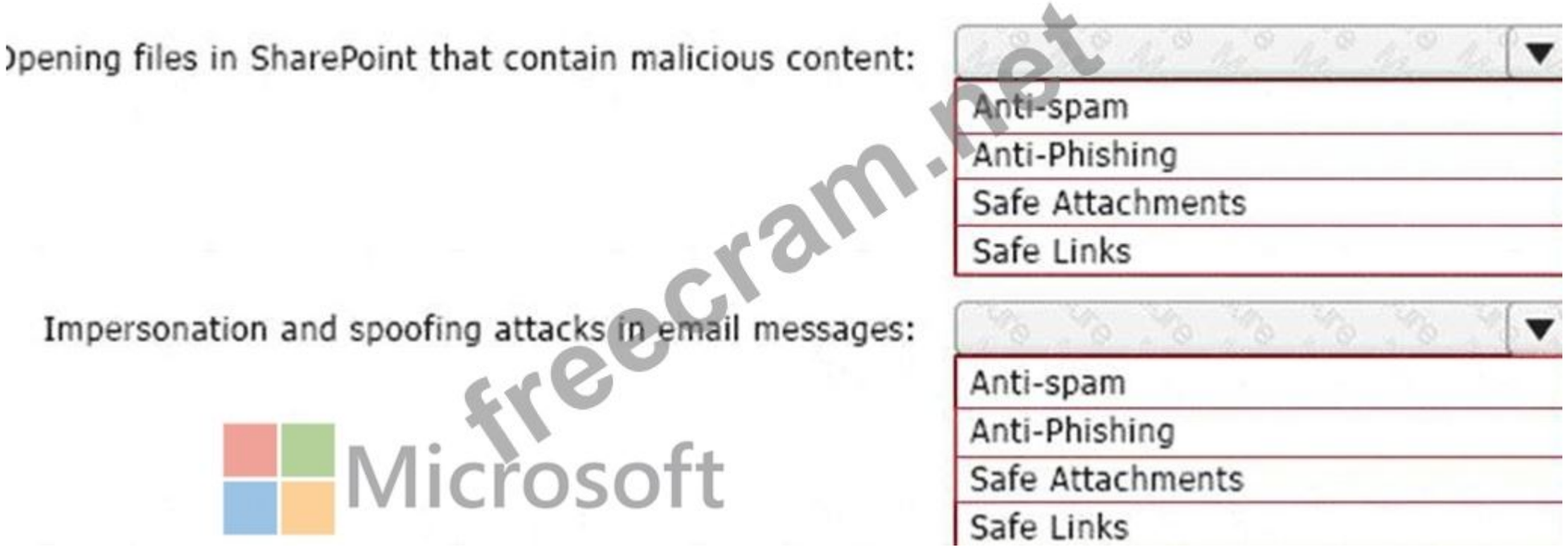
You are planning a threat management solution for your organization.

You need to minimize the likelihood that users will be affected by the following threats:
Opening files in Microsoft SharePoint that contain malicious content

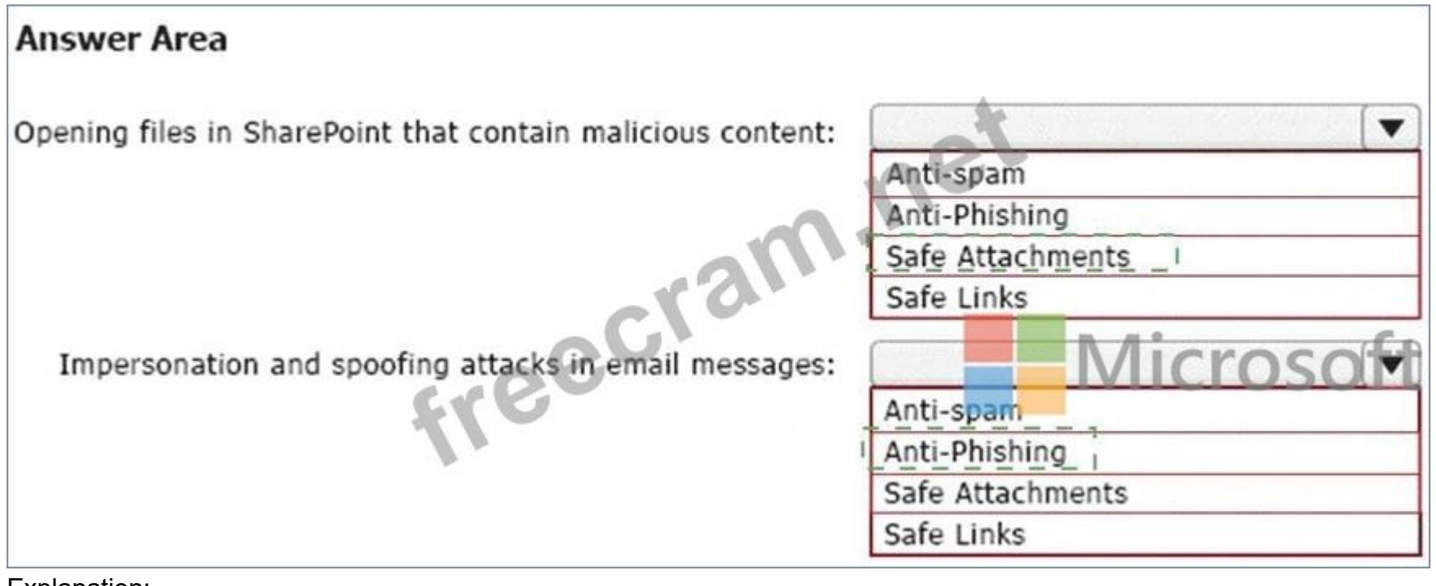
Impersonation and spoofing attacks in email messages

Which policies should you create in Microsoft 365 Defender? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Explanation:

NEW QUESTION: 66
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 the Microsoft 365 admin center, configure the Password policy settings.
B. From the Microsoft Entra admin center, configure the Password protection settings.
C. From Azure AD Identity Protection, configure a sign-in risk policy.
D. From the Microsoft Entra admin center, create a conditional access policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
HOTSPOT
You have a Microsoft 365 tenant.
You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)

The label policy is configured as shown in the following table.

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

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
Any sent email message that contains the word ProjectX will be deleted immediately.	○	○
Any sent email message that contains the word ProjectX will be retained for six months.	○	○
Users are required to manually apply a label to email messages that contain the word ProjectX.	○	○

Answer:

Answer Area

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

Explanation:

Answer Area

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

Box 1: No

Box 2: Yes

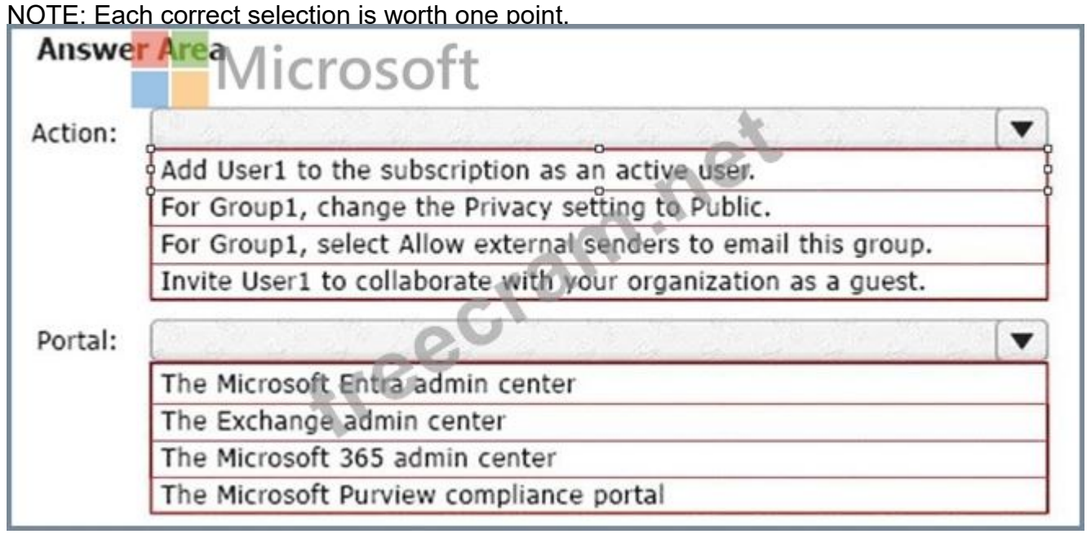
Box 3: No

Reference:

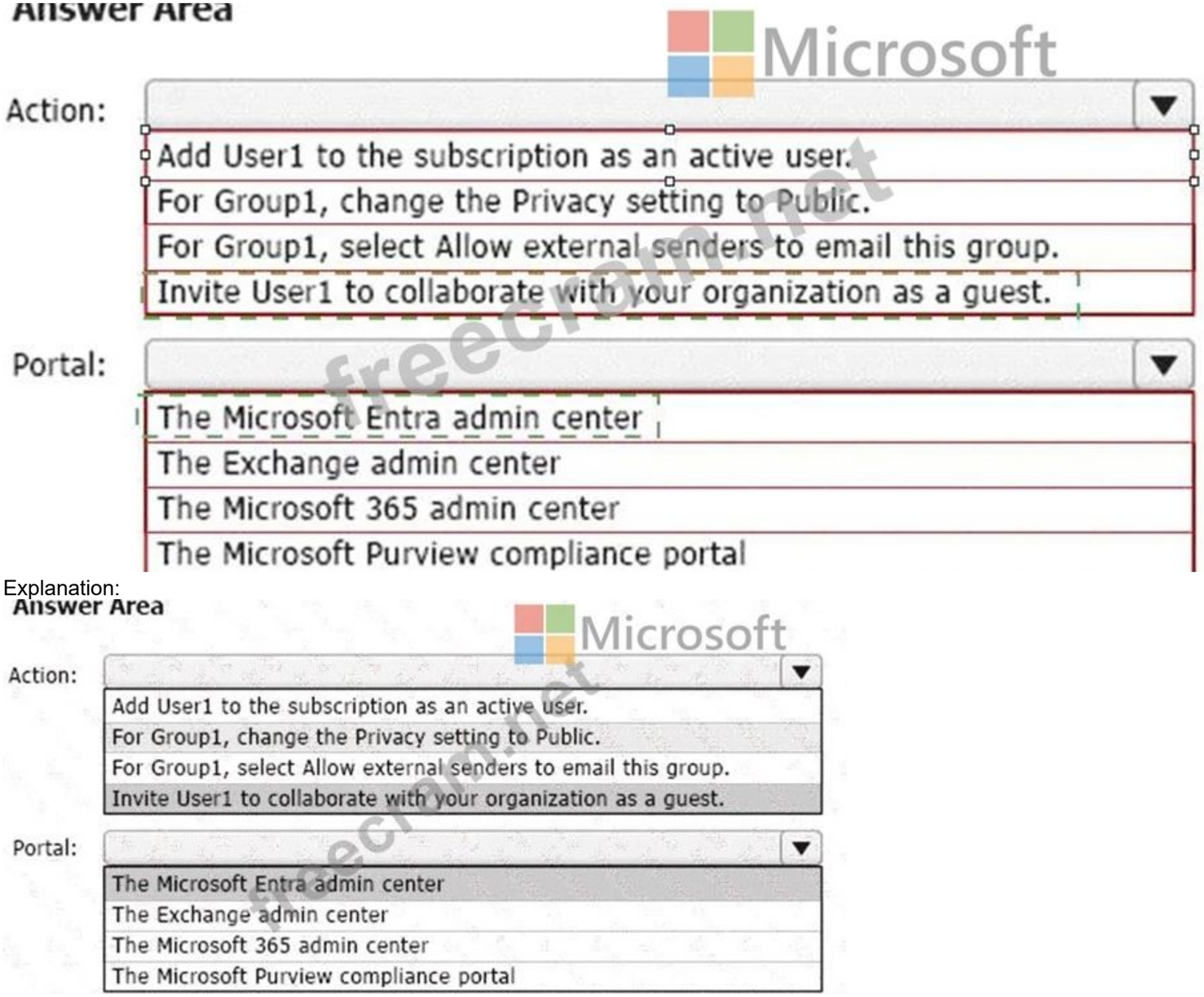
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

NEW QUESTION: 68
HOTSPOT
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.

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



Answer:



Explanation:

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

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

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

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

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

com.

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

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

NEW QUESTION: 69
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 Microsoft Defender for Endpoint baseline profile
B. a mobile device management (MDM) security baseline profile
C. a device configuration profile
D. an update policy for iOS
Answer: (SHOW ANSWER)

NEW QUESTION: 70
You have a Microsoft 365 E5 subscription that contains a user named User1.
You create an outbound anti-spam policy named Policy1 as shown in the following exhibit.

You assign Policy1 to User1.

What is the maximum number of email messages that User1 can send in a 24-hour period?

A. 720

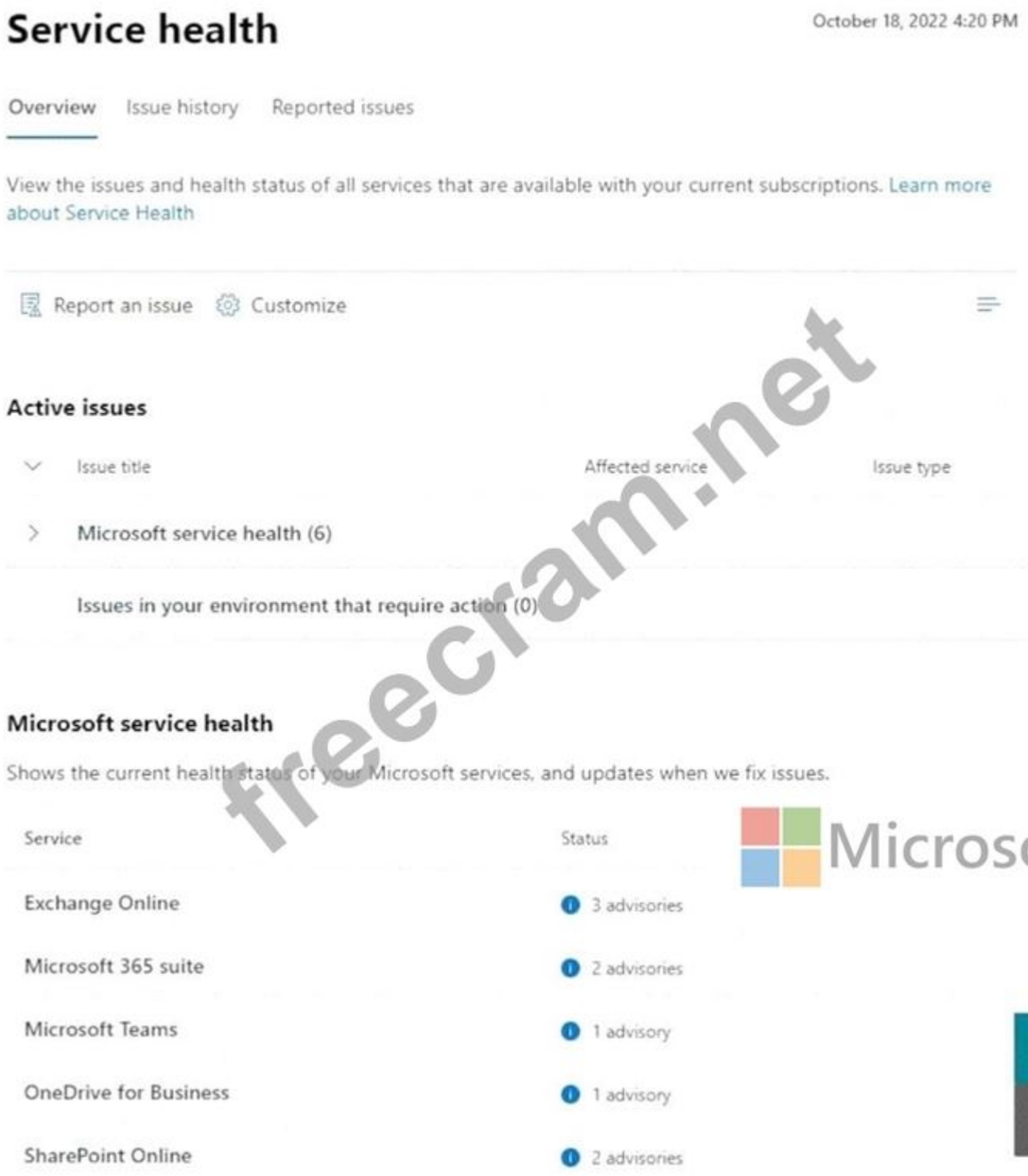
B. 1000

C. 30

D. 1030
Answer: (SHOW ANSWER)

NEW QUESTION: 71
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: 72
You have a Microsoft 365 subscription.
You view the Service health Overview as shown in the following exhibit.



You need to ensure that a user named User1 can view the advisories to investigate service health issues.
Which role should you assign to User1?

A. Message Center Reader
B. Reports Reader
C. Service Support Administrator
D. Compliance Administrator

Answer: (SHOW ANSWER)

Service Support admin

Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:
- Open and manage service requests
- View and share message center posts
- Monitor service health
Incorrect:
* Message center reader
Assign the Message center reader role to users who need to do the following:
- Monitor message center notifications
- Get weekly email digests of message center posts and updates
- Share message center posts
- Have read-only access to Azure AD services, such as users and groups
* Reports reader
Assign the Reports reader role to users who need to do the following:
- View usage data and the activity reports in the Microsoft 365 admin center
- Get access to the Power BI adoption content pack
- Get access to sign-in reports and activity in Azure AD
- View data returned by Microsoft Graph reporting API
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

NEW QUESTION: 73
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: 74

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. Device2 and Device3 only

B. Device1 only

C. Device2 only

D. Device3 only

E. Device1, Device2, and Device3

Answer: (SHOW ANSWER)

NEW QUESTION: 75

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:

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

Explanation:

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

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:
Conditional Access policies can be enabled in report-only mode.
During sign-in, policies in report-only mode are evaluated but not enforced.
Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.

Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report- only

NEW QUESTION: 76
Your company has offices in Seattle and Denver.
You have a Microsoft 365 subscription.
You plan to create a Conditional Access policy named Policy1 that will enforce multifactor authentication (MFA).
You need to ensure that users at the Seattle office are excluded from MFA. Users at the Denver office must always be prompted for MFA.
What should you configure for Policy1?
A. VPN connectivity from the Seattle office
B. a named location that has Countries location set to United States
C. a named location that has IP ranges location set to the Seattle office
D. Authentication strengths
Answer: (SHOW ANSWER)

NEW QUESTION: 77
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. Site!
contains the files shown in the following table.

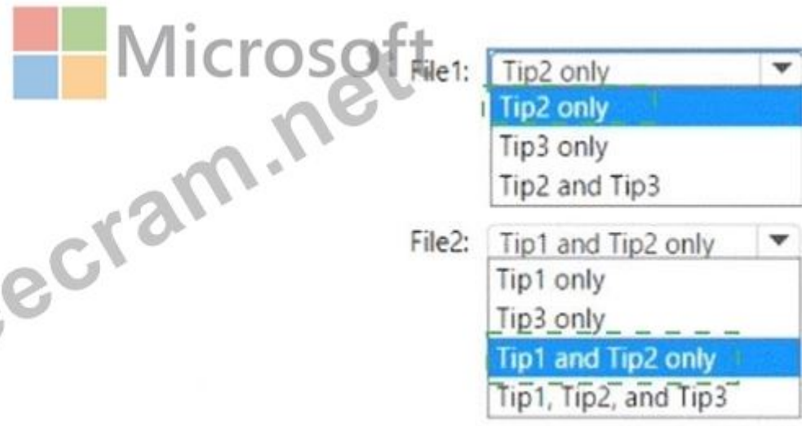
Name	Number of IP addresses in the file
File1	2
File2	3

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: 78

Your company has digitally signed applications.

You need to ensure that Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) considers the digitally signed applications safe and never analyzes them.

What should you create in the Microsoft Defender Security Center?

A. a custom detection rule

B. an allowed/blocked list rule

C. an alert suppression rule
D. an indicator
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators

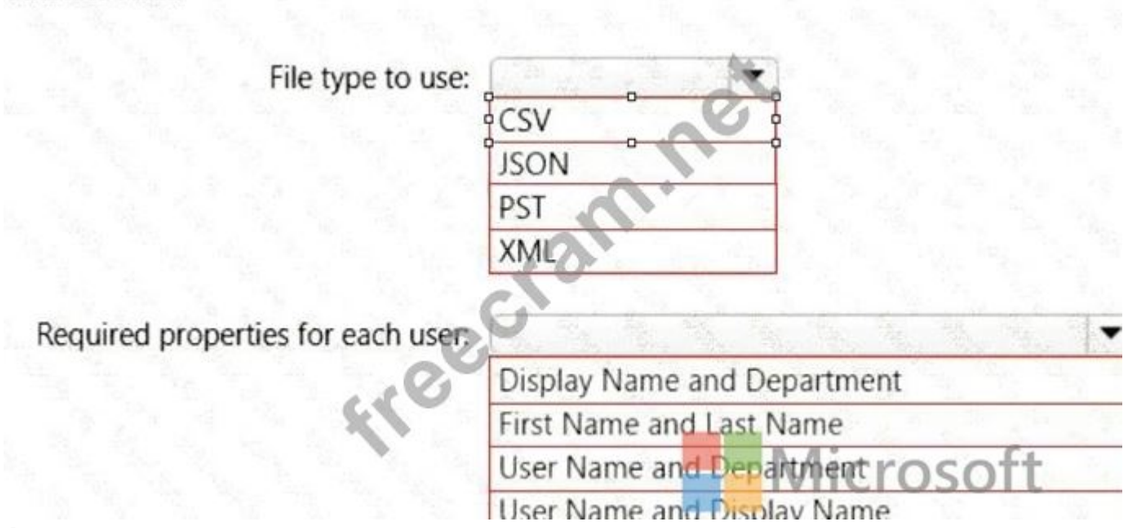
NEW QUESTION: 79
You have a Microsoft 365 E5 tenant.
industry regulations require that the tenant comply with the ISO 27001 standard.
You need to evaluate the tenant based on the standard
A. From the Microsoft J6i compliance center, create an audit retention policy.
B. From Policy in the Azure portal, select Compliance, and then assign a pokey
C. From Compliance Manager, create an assessment
D. From the Microsoft 365 admin center enable the Productivity Score.
Answer: (SHOW ANSWER)

NEW QUESTION: 80
You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1. You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:
* Assign licenses to users.
* Procure apps from Microsoft Store.
* Manage private store availability for all items.
The solution must use the principle of least privilege.
Which Microsoft Store for Business role should you assign to User1?

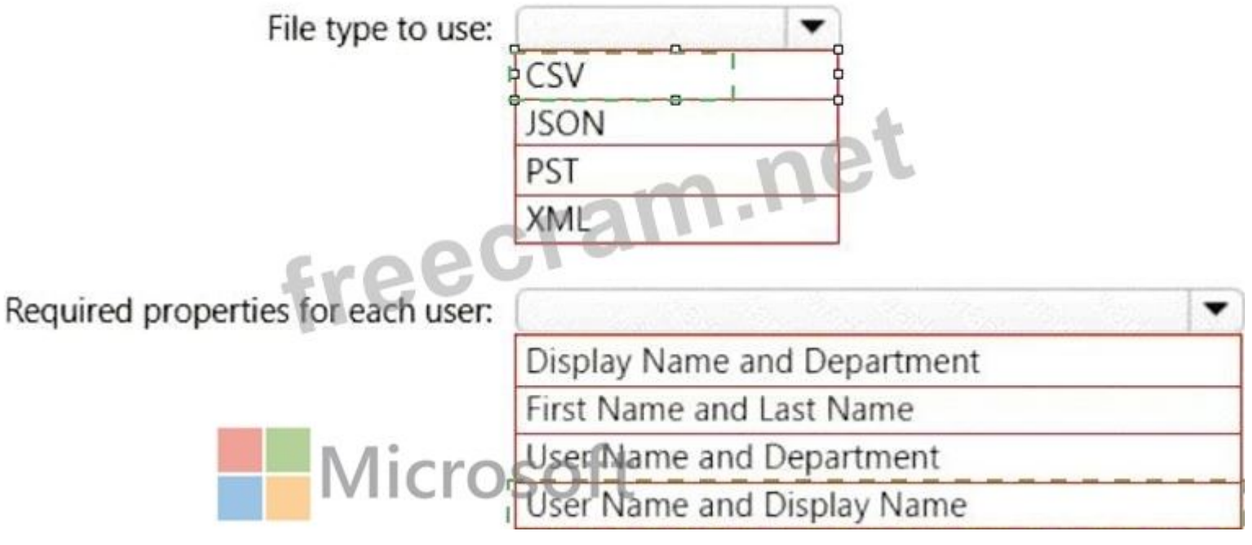
A. Basic Purchaser
B. Device Guard signer
C. Admin
D. Purchaser
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

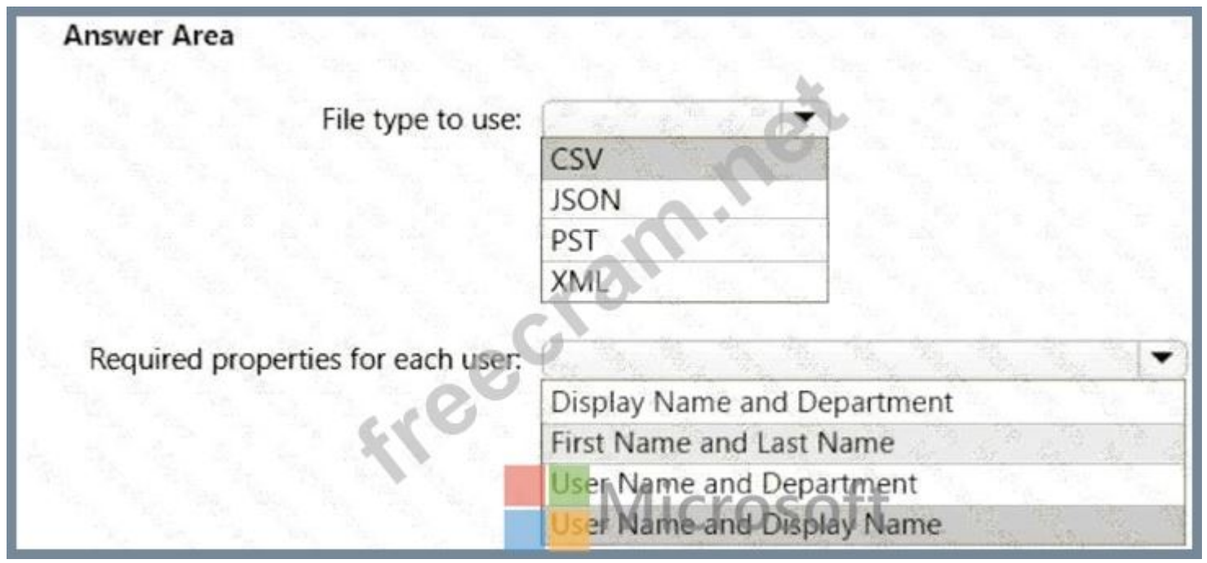
NEW QUESTION: 81
You have a Microsoft 365 E5 subscription.
Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.
You need to implement passwordless authentication. The solution must support all the devices.
Which authentication method should you use?
A. Microsoft Authenticator app
B. FID02 compliant security keys
C. Windows Hello
Answer: (SHOW ANSWER)

NEW QUESTION: 82
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:
Answer Area





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

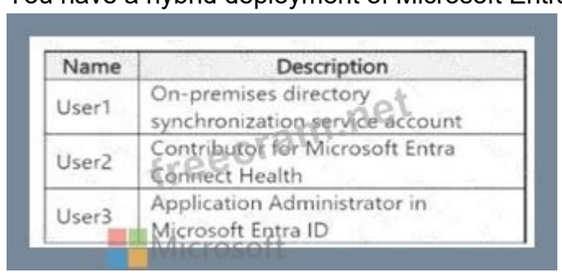
What if I don ' t have all the information required for each user? The user name and display name are required, and you cannot add a new user without this information. If you don ' t have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/enterprise/add-several-users-at-the-same-time

NEW QUESTION: 83

You have a hybrid deployment of Microsoft Entra that contains the users shown in the following table.



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

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

* View sync errors in Microsoft Entra Connect Health.

* Configure Microsoft Entra 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

Answer:

Answer Area

Explanation:

NEW QUESTION: 84

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. a Microsoft Intune device configuration profile

B. Azure AD conditional access

C. a Microsoft Intune device compliance policy

D. Azure AD password protection

Answer: (SHOW ANSWER)

NEW QUESTION: 85

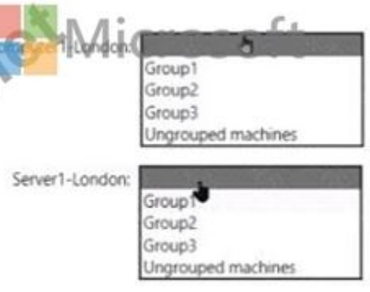
You use Microsoft Defender for Endpoint.

You have the Microsoft Defender for Endpoint device groups shown in the following table

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	*Not applicable*

You plan to onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Answer Area



Answer:

Explanation:

Answer Area

Computer1-London: Group1

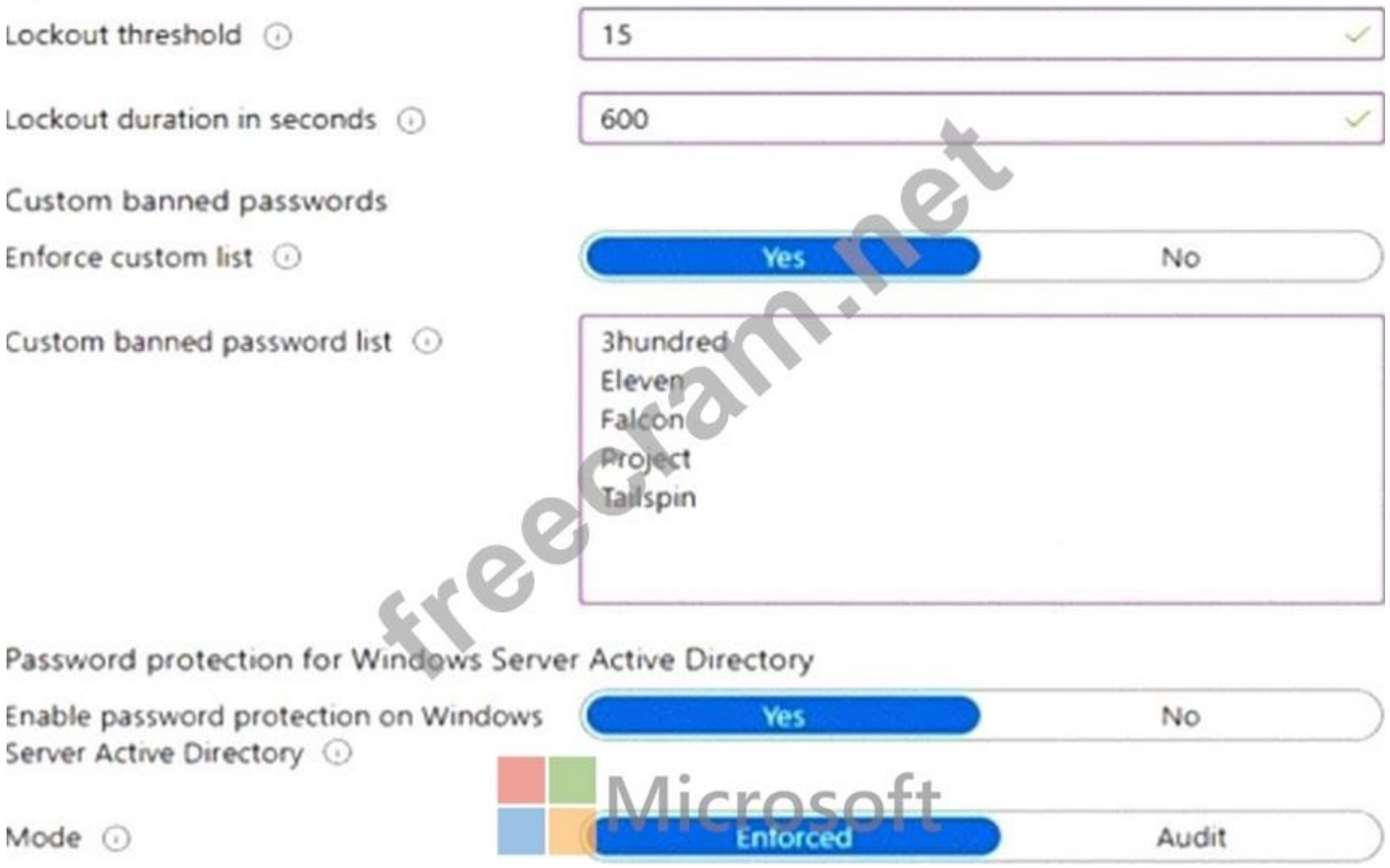
Server1-London: Group2

NEW QUESTION: 86

HOTSPOT

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

Azure AD Password Protection is configured as shown in the following exhibit.



User1 attempts to update their password to the following passwords:

F@lcon

Project22

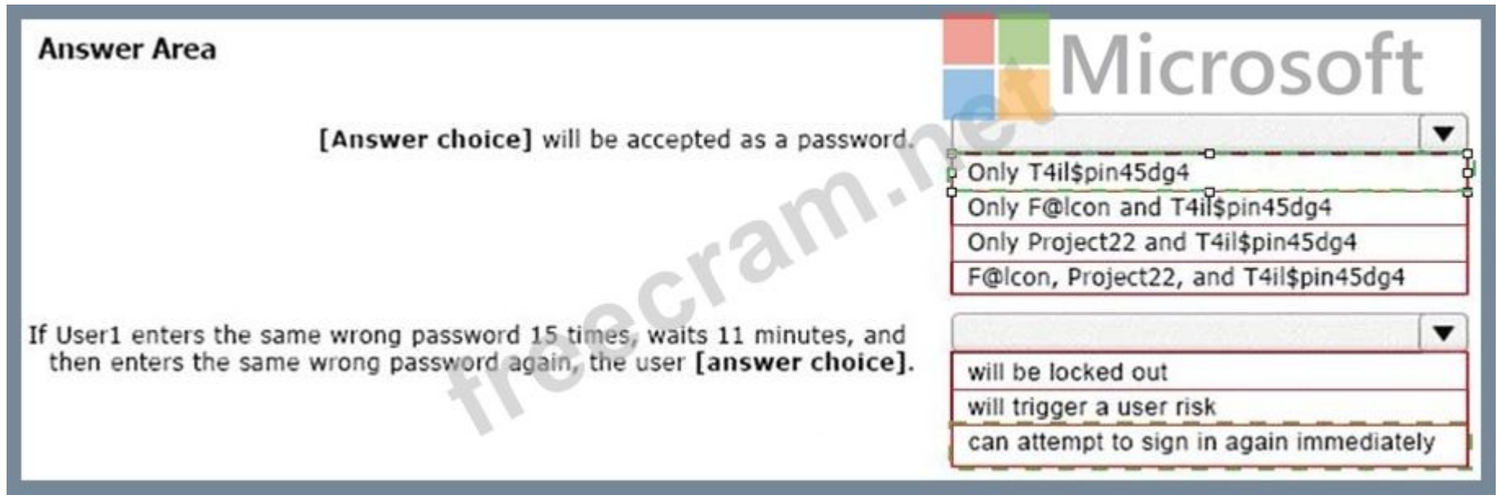
T4il$pin45dg4

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

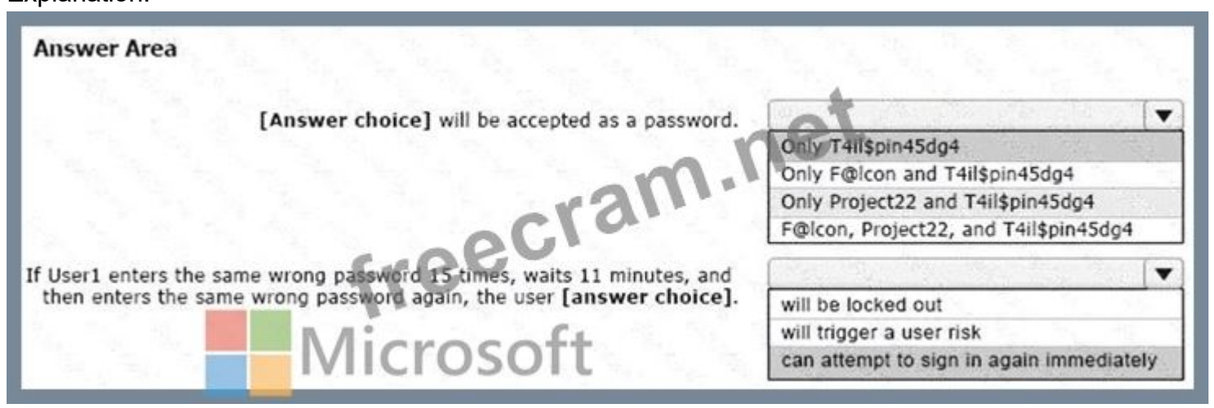
NOTE: Each correct selection is worth one point.

Answer Area

Answer:



Explanation:



Box 1: Only T4il$pin45dg4

Box 2: can attempt to sign in immediately

Note: Manage Azure AD smart lockout values

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

Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users. Customization of the smart lockout settings is not available for Azure China 21Vianet tenants.

To check or modify the smart lockout values for your organization, complete the following steps:

Sign in to the Entra portal.

Search for and select Azure Active Directory, then select Security > Authentication methods > Password protection.

Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.

The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.

Set the Lockout duration in seconds, to the length in seconds of each lockout.

The default is 60 seconds (one minute).

If the first sign-in after a lockout period has expired also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

NEW QUESTION: 87

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

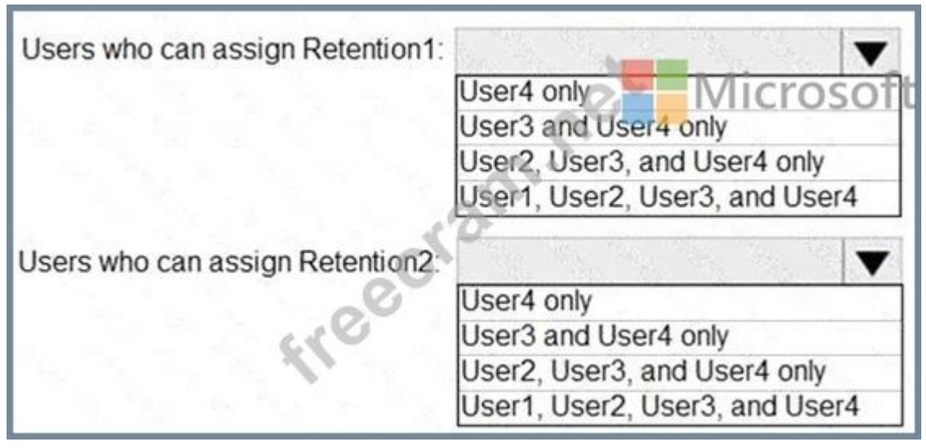
Name	Mailbox size
User1	5 MB
User2	15 MB
User3	25 MB
User4	55 MB

You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email.

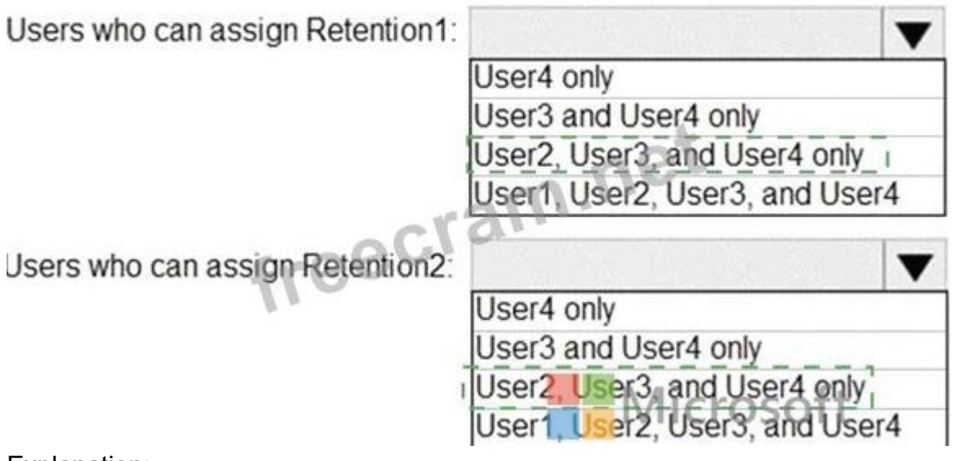
You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2.

Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.

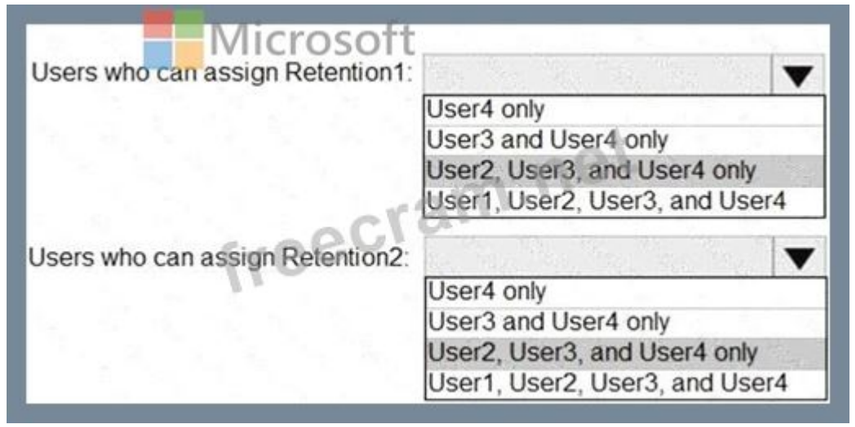
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

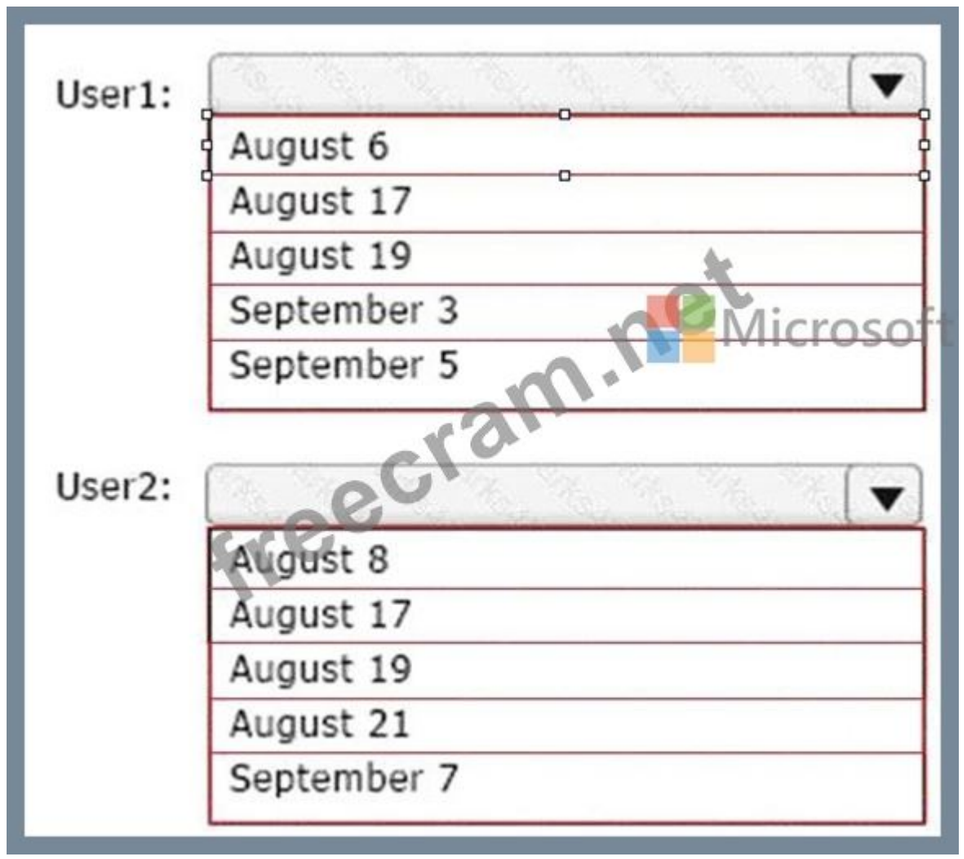


Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-exchange?view=o365- worldwide

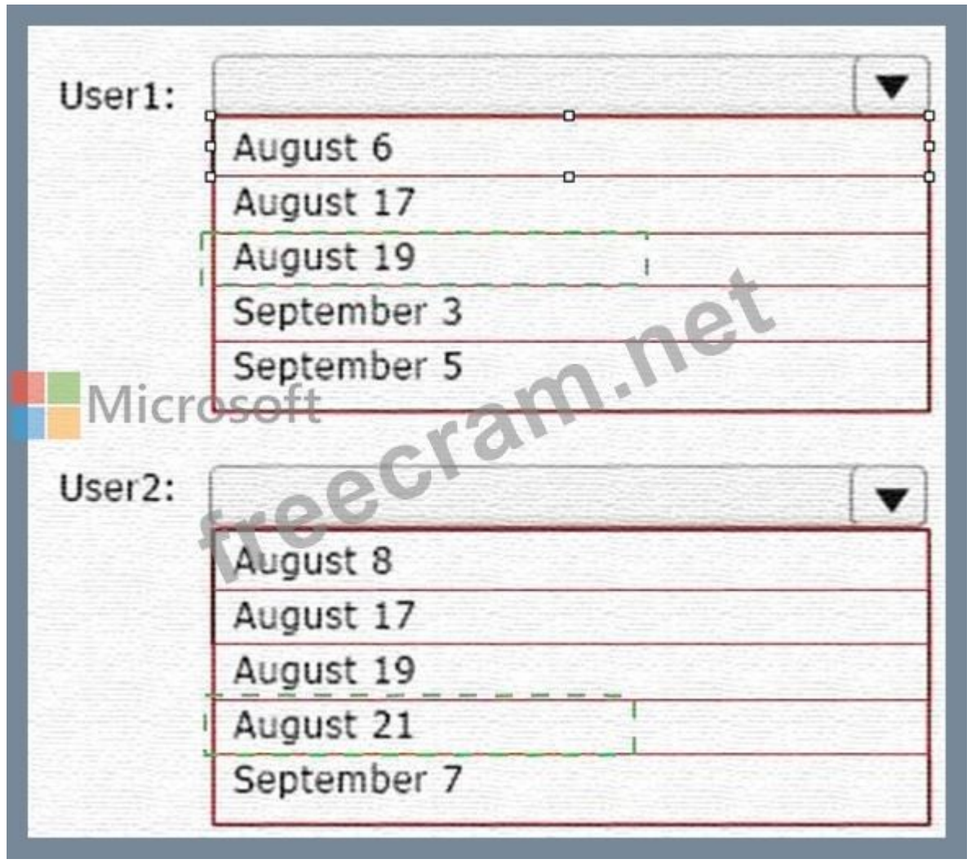
NEW QUESTION: 88
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:
Assignments: All users
Controls: Require Azure AD multifactor authentication registration
Enforce 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

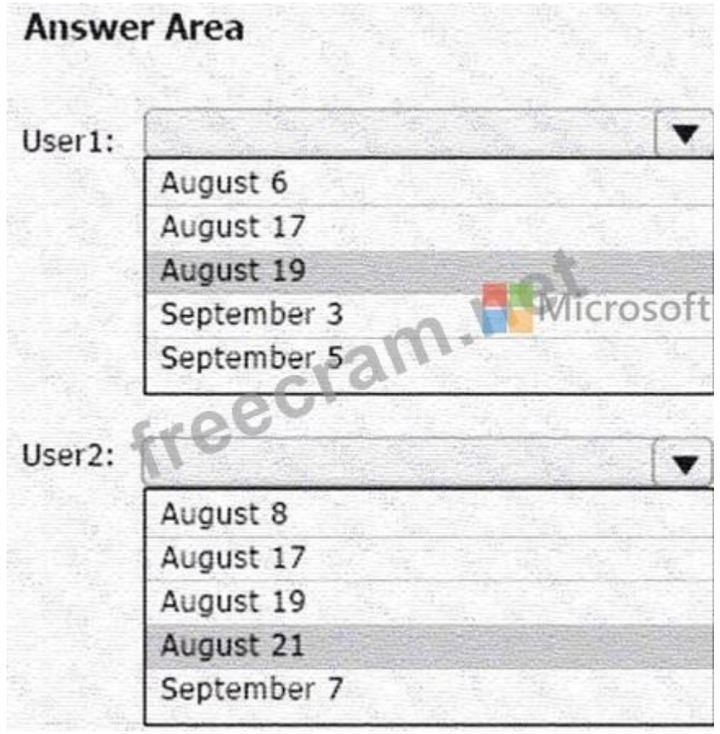
By which dates will User1 and User2 be forced to complete their Azure MFA registration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.


User1:
August 6
August 17
August 19
September 3
September 5
User2:
August 8
August 17
August 19
August 21
September 7

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: 89

You have a Microsoft 365 E5 subscription that uses Microsoft intune. The subscription contains the resources shown in the following table.

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.

You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table.

On Thursday, you review the results of the app deployments.

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

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: 90

Your network contains an Active Directory forest named contoso.local.
You purchase a Microsoft 365 subscription.
You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months.
You need to prepare for the planned move to Microsoft 365.
What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

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

NEW QUESTION: 91

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

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

Azure AD Connect has the following settings:
Password Hash Sync: Enabled
Pass-through authentication: Enabled
You need to identify which users will be able to authenticate by using Azure AD if connectivity between on- premises Active Directory and the internet is lost.
Which users should you identify?
A. none
B. Used only1
C. User1 and User2 only
D. User1. User2, and User3
Reference:
Answer: D (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn¨

NEW QUESTION: 92

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. only the settings of Policy!
B. only the settings of Policy3
C. only the settings of Policy2
D. no settings
Answer: (SHOW ANSWER)

NEW QUESTION: 93

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains a server named Server1 that runs Windows Server. The domain contains the users shown in the following table.

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

You have a Microsoft 365 subscription that contains the following user accounts:

Answer Area

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

Answer:

Explanation:

NEW QUESTION: 94

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

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

The tenant contains the devices shown in the following table.

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

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

Answer:

Explanation:

NEW QUESTION: 95

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:

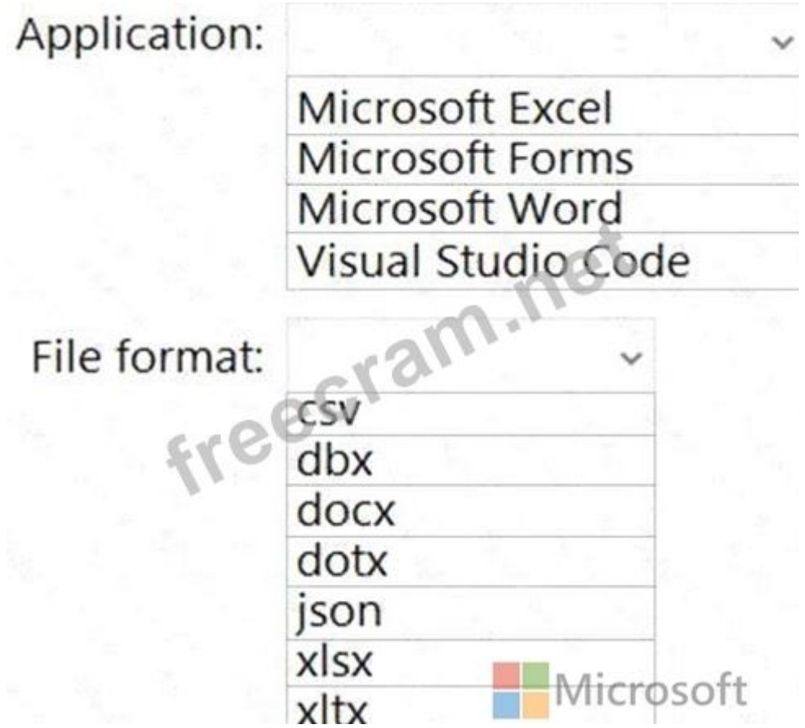
https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin-data?view=o365-worldwide

NEW QUESTION: 96
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. Yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 97
You have a Microsoft 365 tenant.
You need to create a custom Compliance Manager assessment template.
Which application should you use to create the template, and in which file format should the template be saved? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

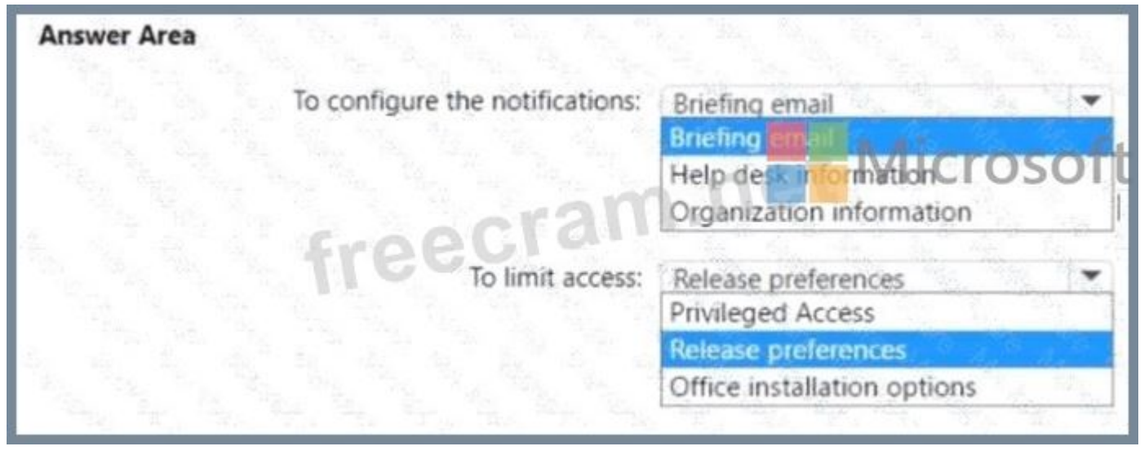


Answer:

Explanation:

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

NEW QUESTION: 98
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:

Explanation:

NEW QUESTION: 99

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 Policy3

B. only the settings of Policy2

C. no settings

D. only the settings of Policy1

Answer: (SHOW ANSWER)

NEW QUESTION: 100

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-628bec99-476a-2c13-5296-9dd081cdd808

NEW QUESTION: 101

(Your network contains two on-premises Active Directory Domain Services (AD DS) forests named contoso.

com and fabrikam.com that are connected by using a forest trust.

You have a Microsoft 365 E5 subscription.

You need to sync a subset of users from both forests to Microsoft Entra ID. The solution must support device objects and device writeback.

What should you use?)

A. Microsoft Entra Cloud Sync

B. Microsoft Entra Domain Services

C. Microsoft Entra Connect Sync
D. Active Directory Federation Services (AD FS)
Answer: (SHOW ANSWER)
The correct answer is Microsoft Entra Connect Sync because it is the only Microsoft-supported solution that meets all of the stated requirements.
1. Support for multiple on-premises AD DS forests
Microsoft Entra Connect Sync is designed to synchronize identities from multiple on-premises Active Directory forests into a single Microsoft Entra tenant. Microsoft documentation explicitly states that when multiple forests are present, they can all be synchronized as long as they are reachable by the same Entra Connect server. A forest trust between contoso.com and fabrikam.com is a supported and common configuration.
2. Ability to sync only a subset of users
Microsoft Entra Connect Sync supports filtering and scoping at multiple levels (domain-based, OU-based, or attribute-based). Microsoft documentation lists pilot deployments and limited user synchronization as a primary use case, allowing administrators to synchronize only selected users from each forest.
3. Support for device objects and hybrid device scenarios
Microsoft Entra Connect Sync supports hybrid device identity , including Microsoft Entra hybrid joined devices. These devices are registered both in on-premises Active Directory and in Microsoft Entra ID, which is required for many Microsoft 365 and Conditional Access scenarios.
4. Device writeback support
Device writeback is a feature that allows device objects from Microsoft Entra ID to be written back into on- premises Active Directory. Microsoft documentation clearly identifies device writeback as a feature of Microsoft Entra Connect Sync .
Important documented behavior:
* Device writeback is supported when device objects and users are correctly located and configured in the same forest.
* Device writeback is not a feature of Cloud Sync or federation services.
Why the other options are incorrect
A). Microsoft Entra Cloud Sync
Cloud Sync is a lightweight provisioning agent and does not provide the full hybrid identity feature set required for this scenario. Microsoft documentation associates advanced device features and device writeback with Microsoft Entra Connect Sync, not Cloud Sync.
B). Microsoft Entra Domain Services
Microsoft Entra Domain Services is a managed domain service used to run legacy, domain-joined workloads in Azure. It does not synchronize on-premises forests into Microsoft Entra ID and is not a replacement for Entra Connect in hybrid identity scenarios.
D). Active Directory Federation Services (AD FS)
AD FS is an authentication and federation service. It does not synchronize users or devices to Microsoft Entra ID and does not support device writeback. Microsoft documentation positions AD FS as an authentication method, not a directory synchronization solution.

NEW QUESTION: 102
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 Area

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

- Domains to protect
- Mailbox intelligence
- Users to protect

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

- Global settings for safe attachments
- The Safe Attachments policy settings
- The Safe Links policy settings

Answer:

Answer Area

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

- Domains to protect
- Mailbox intelligence
- Users to protect

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

- Global settings for safe attachments
- The Safe Attachments policy settings
- The Safe Links policy settings

Explanation:

Answer Area

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

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

NEW QUESTION: 103

You have a Microsoft 365 E5 tenant that has sensitivity label support enabled for Microsoft and SharePoint Online.

You need to enable unified labeling for Microsoft 365 groups.

Which cmdlet should you run?

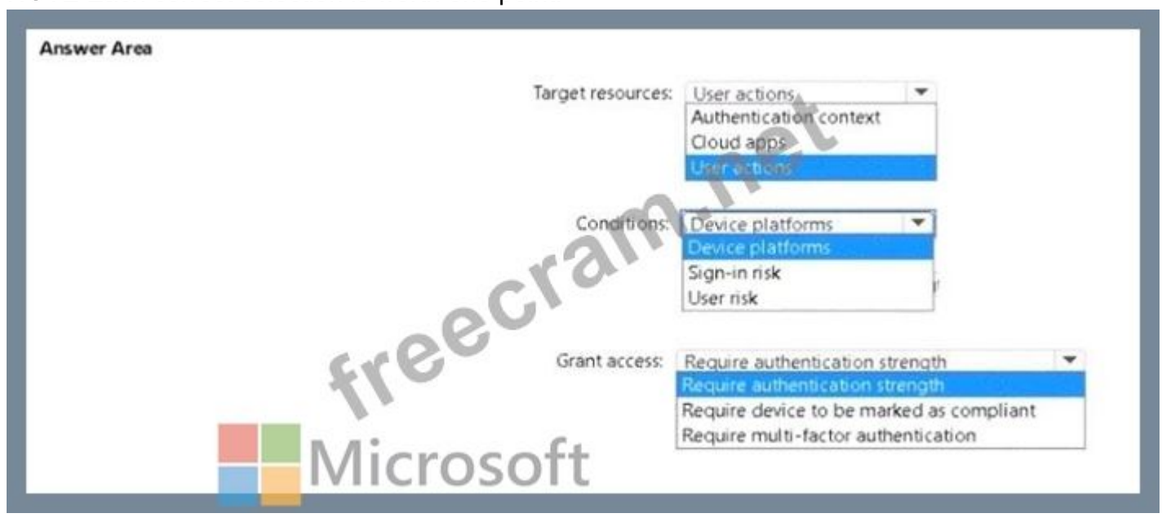
A. Add-UnifiedGroupLinks
B. Set-Labelpolicy
C. set-unifiedGroup
D. Execute-AzureAdLebelSync
Answer: (SHOW ANSWER)

NEW QUESTION: 104
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

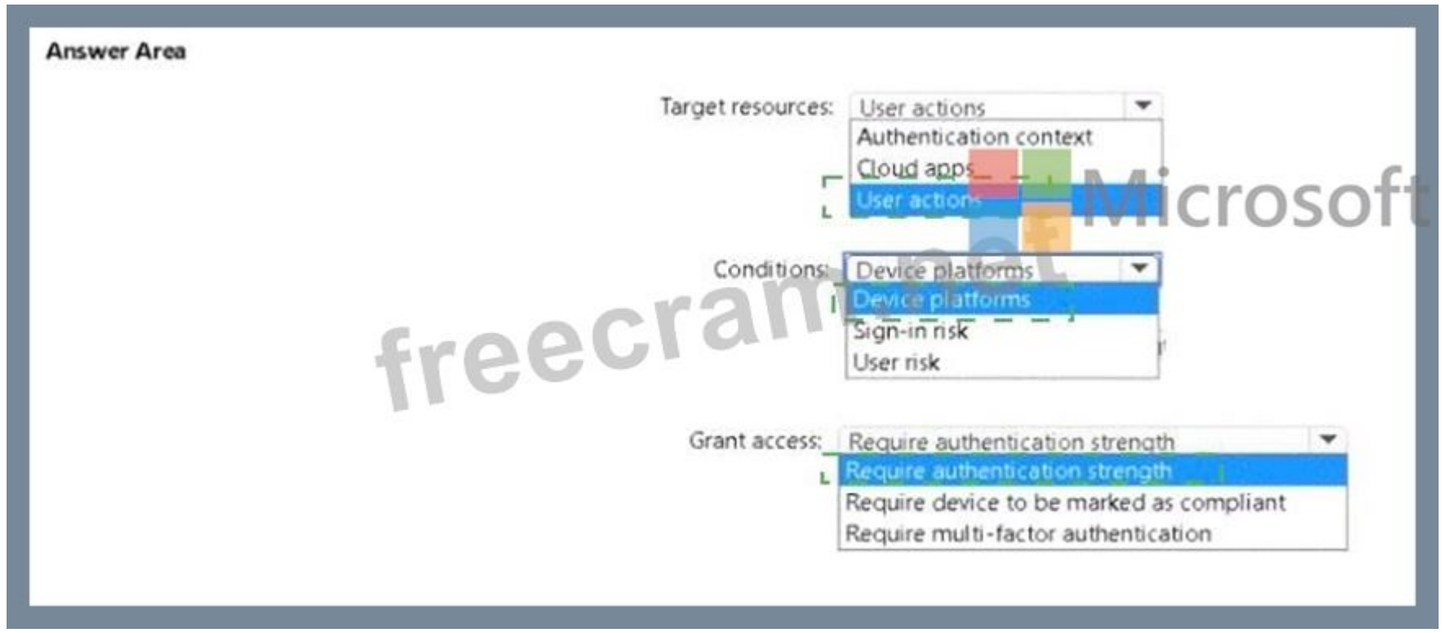
Name	Type
Policy1	Anti-phishing
Policy2	Anti-spam
Policy3	Anti-malware
Policy4	Safe Attachments

All the policies are configured to send malicious email messages to quarantine. Which policies support a customized quarantine retention period?
A. Policy3 and Policy4 only
B. Policy1 and Policy3only
C. Policy2 and Policy4 only
D. Policy1 and Policy2 only
Answer: D (LEAVE A REPLY)

NEW QUESTION: 105
You have a Microsoft 365 E5 subscription.
You need to create a Conditional Access policy that will require the use of FID02 security keys only when users join their Windows devices to Microsoft Entra ID.
How should you configure the policy? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point.



Answer:



Explanation:

Answer Area

NEW QUESTION: 106

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

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

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

* Reset the password of User4.

* Modify the value for the manager attribute of User4.

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

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

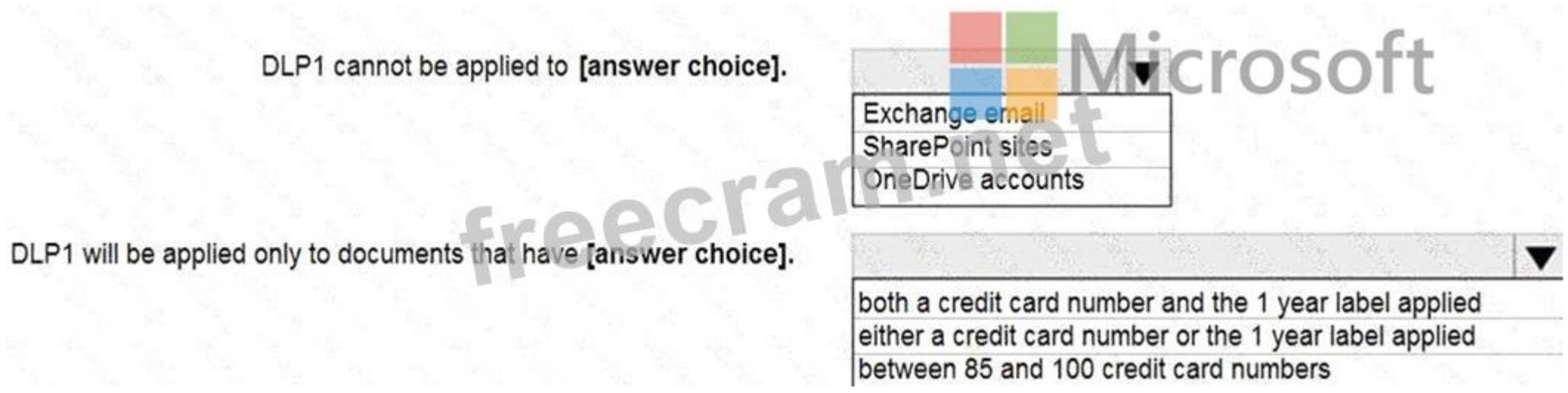
Explanation:

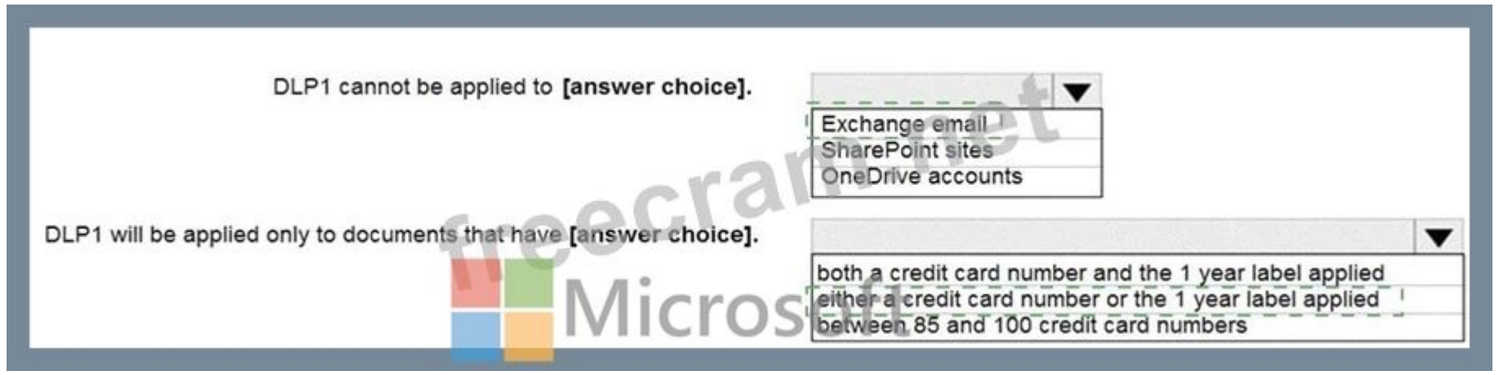
NEW QUESTION: 107

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

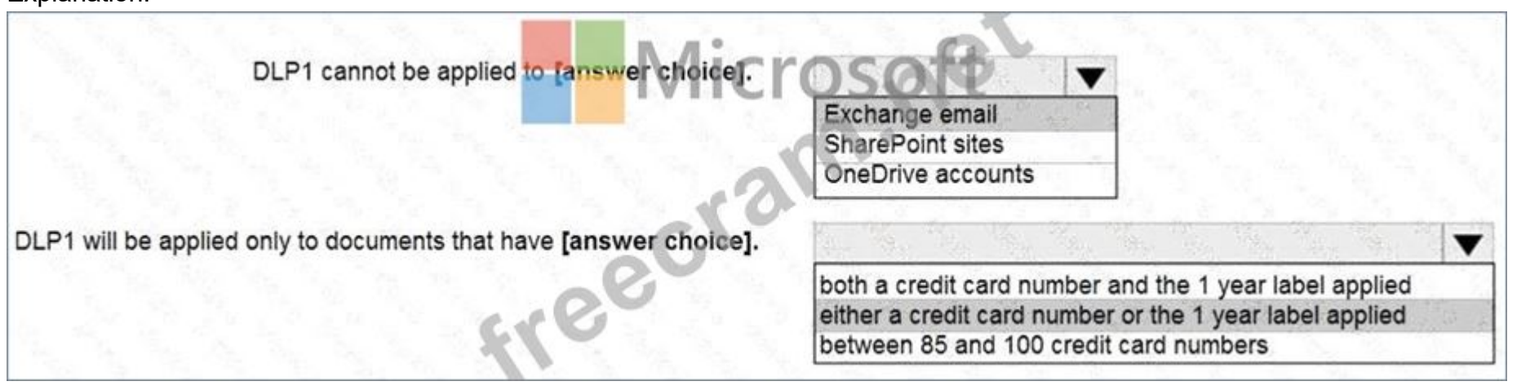
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.





Explanation:



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

nce:

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

NEW QUESTION: 108

You have a Microsoft 365 E5 subscription.

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

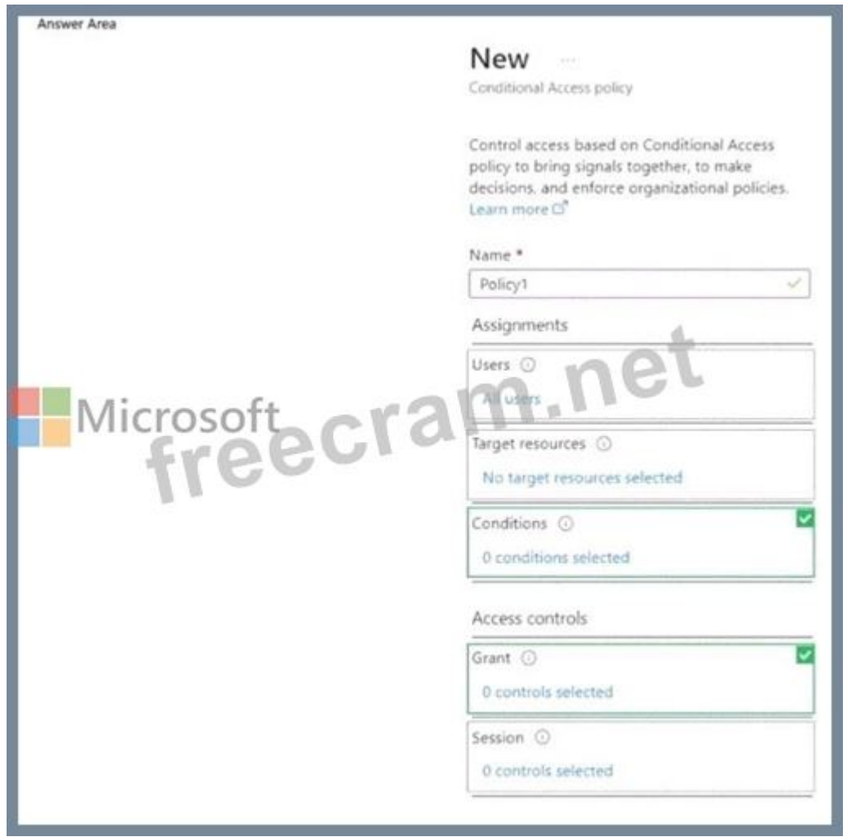
* Applies to high-risk users

* Requires multifactor authentication (MFA)

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

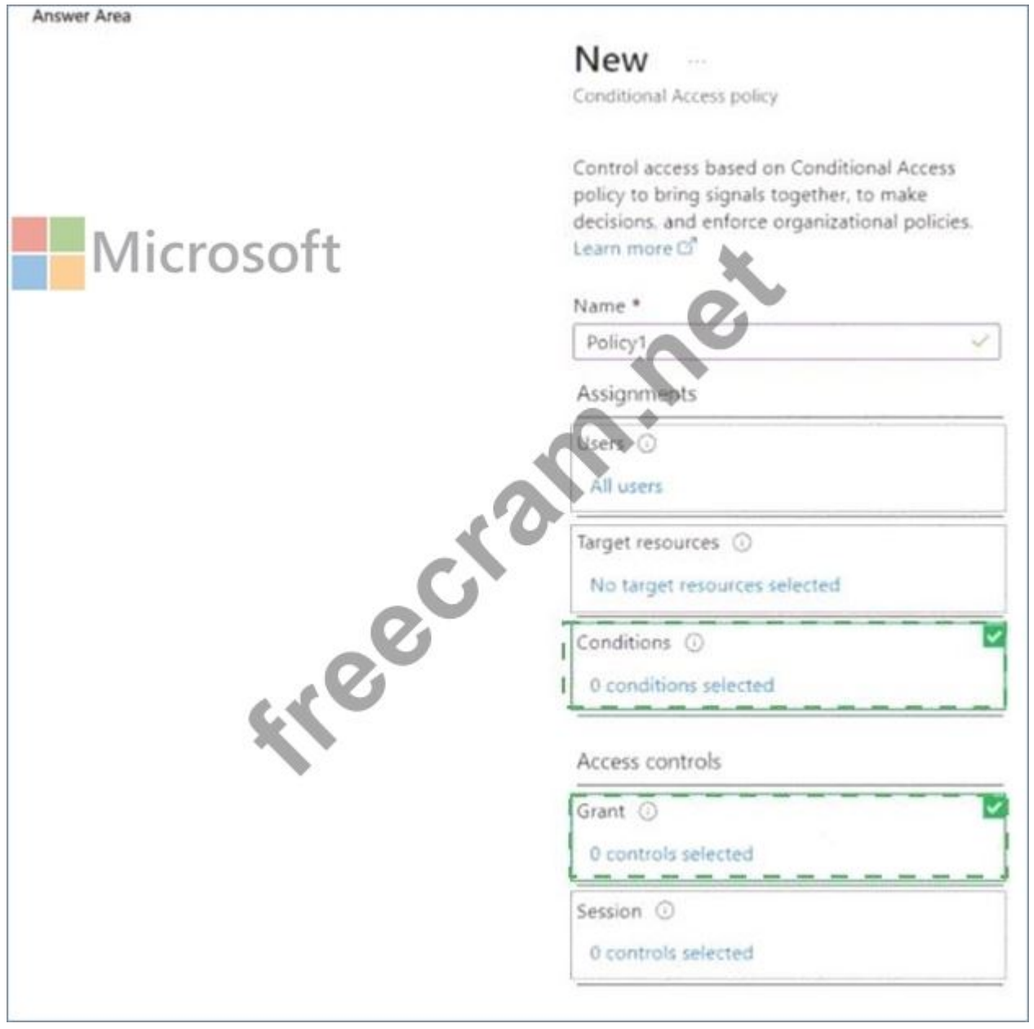
NOTE: Each correct selection is worth one point.

Answer Area

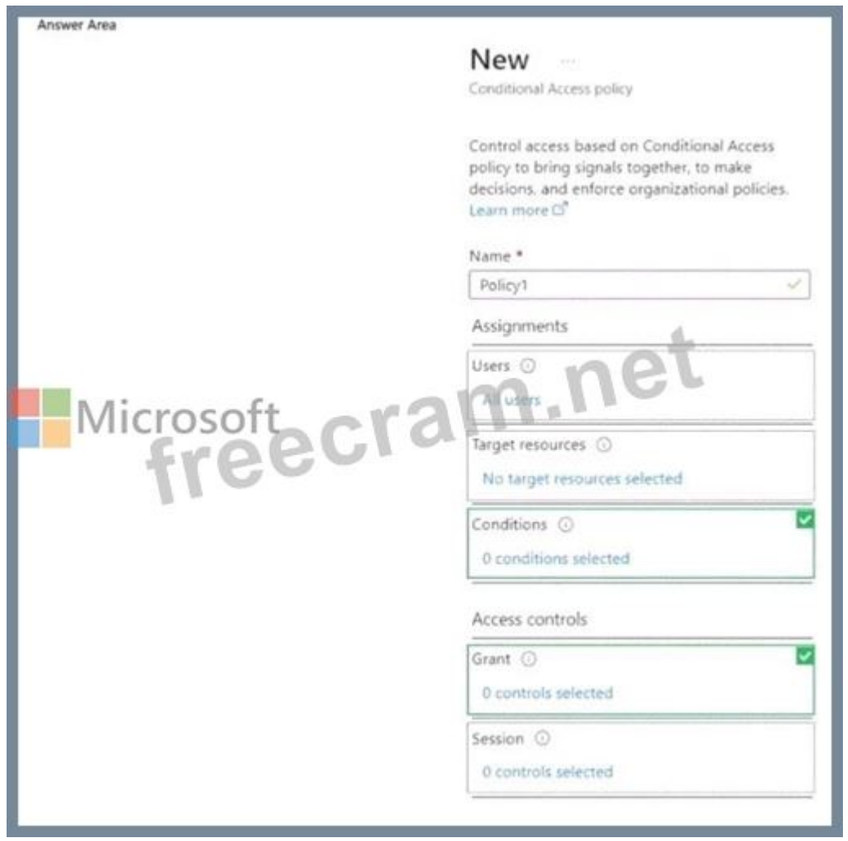


Answer:

Answer Area



Explanation:



NEW QUESTION: 109

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:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 110

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

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

You have the named locations shown in the following table.

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

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

* Users or workload identities:
o Include: Group1
o Exclude: Group2
* Cloud apps or actions: Include all cloud apps
* Conditions:
o Include: Any location
o Exclude: Montreal
* Access control: Grant access, Require multi-factor authentication

User1 is on the multi-factor authentication (MFA) blocked users list.

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 access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	○	○
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	○	○
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	○	○

Answer:

Answer Area

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

Explanation:

NEW QUESTION: 111
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

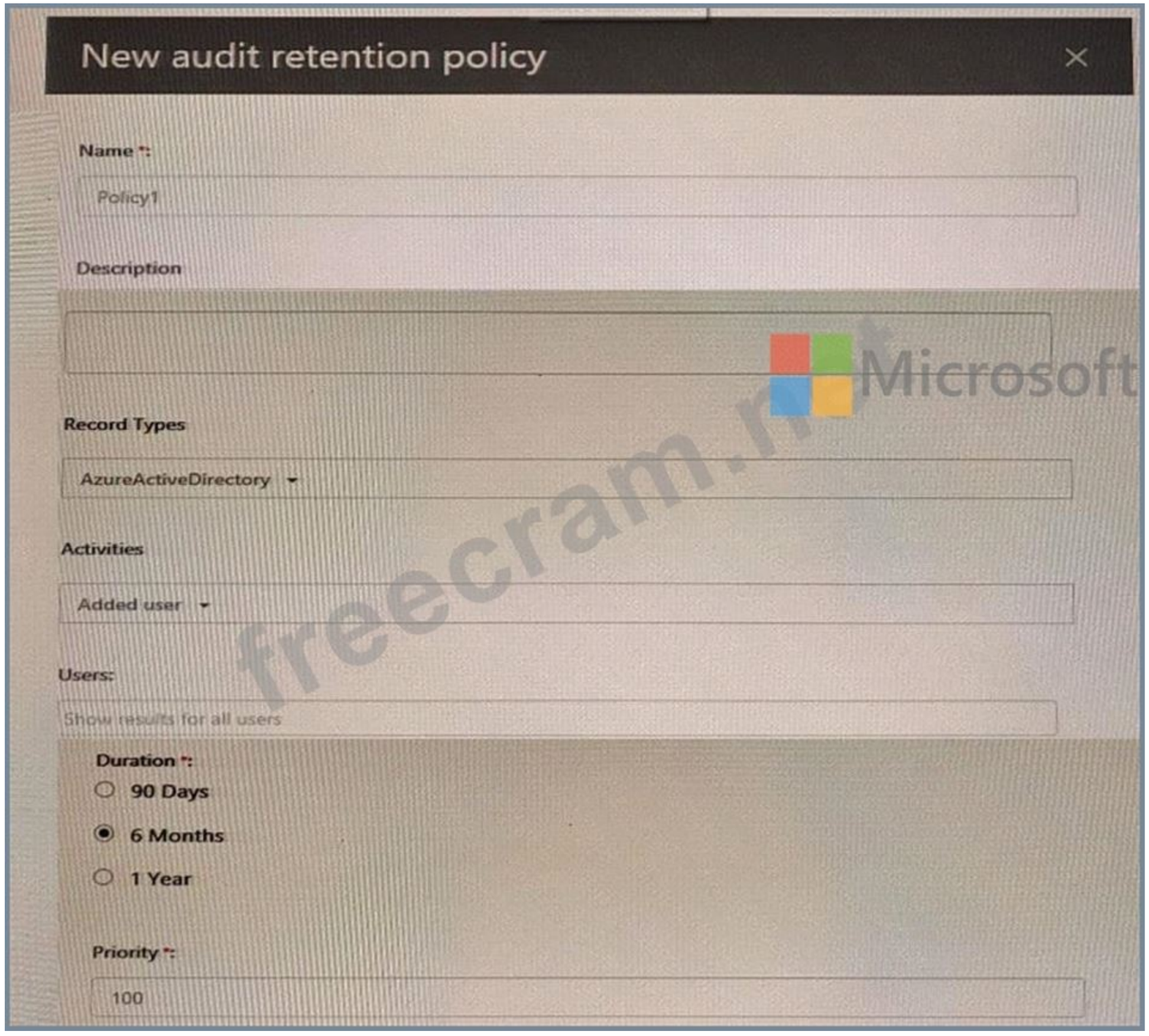
You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User3 to modify the Defender for identity sensor configuration.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 112
You have a Microsoft 365 subscription.

You plan to use Adoption Score and need to ensure that it can obtain device and software metrics.
What should you do?
A. Enable Endpoint analytics.
B. Enable privileged access.
C. Configure Support integration.
D. Run the Microsoft 365 network connectivity test on each device.
Answer: (SHOW ANSWER)

NEW QUESTION: 113
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

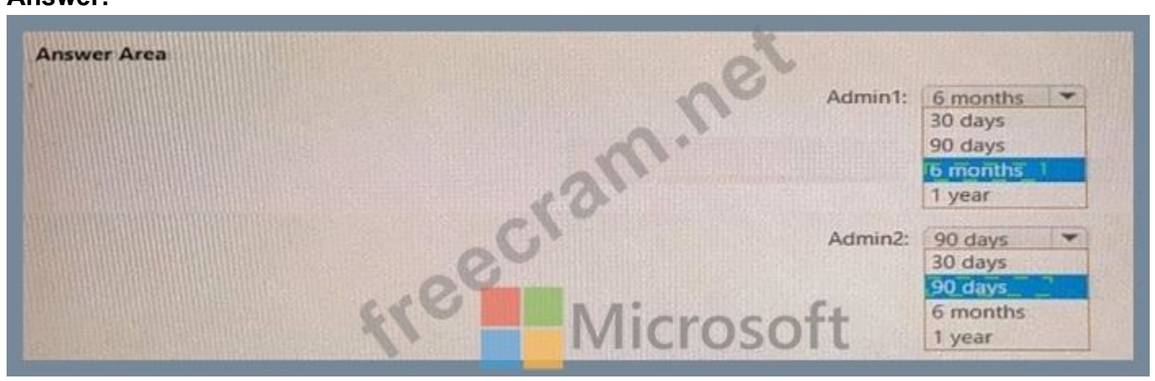


You plan to create a new user named User1.

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:

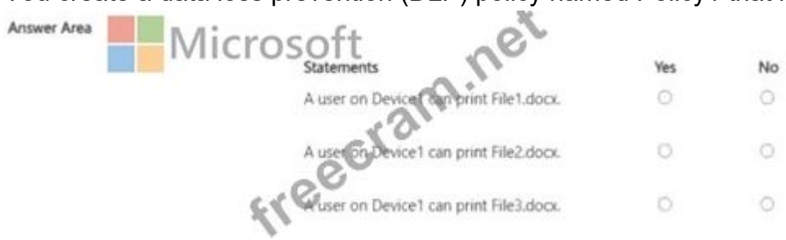


NEW QUESTION: 114

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

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

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



Answer:

Explanation:

NEW QUESTION: 115

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

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

You configure a Multifactor authentication registration policy that has the following settings:

* Assignments:
* Include: Group1
* Exclude: Group2
* Controls: Requite Microsoft Entra ID multifactor authentication registration
* Policy enforcement: Enabled

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

* Name: Policy1
* Assignments:
* Include: Group1
* Exclude; Group1
* Grant: Require multifactor authentication
* Enable policy. On

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

NOTE: Each coned selection is one point.

Answer:

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

NEW QUESTION: 116
You have a Microsoft 365 ES subscription.
From the Microsoft 365 Defender portal, you review your company's Microsoft Secure Score.
You discover a large number of recommended actions.
You need to ensure that the actions can be filtered based on specific department names.
What should you create first?
A. a dynamic security group
B. an administrative unit
C. a custom detection rule
D. a tag
Answer: (SHOW ANSWER)

NEW QUESTION: 117
You have a Microsoft 365 E5 subscription. The subscription contains users that have Windows 11 devices.
You plan to onboard the devices to Microsoft Defender for Endpoint. The devices will connect to Defender for Endpoint through a proxy service.
You need to ensure that the devices use consolidated URLs and static IP ranges when connecting to Defender for Endpoint. What should you do?
A. Configure a device group.
B. Use the standard connectivity type.
C. Enable device discovery.
D. Use the streamlined connectivity type.
Answer: (SHOW ANSWER)

NEW QUESTION: 118
HOTSPOT

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

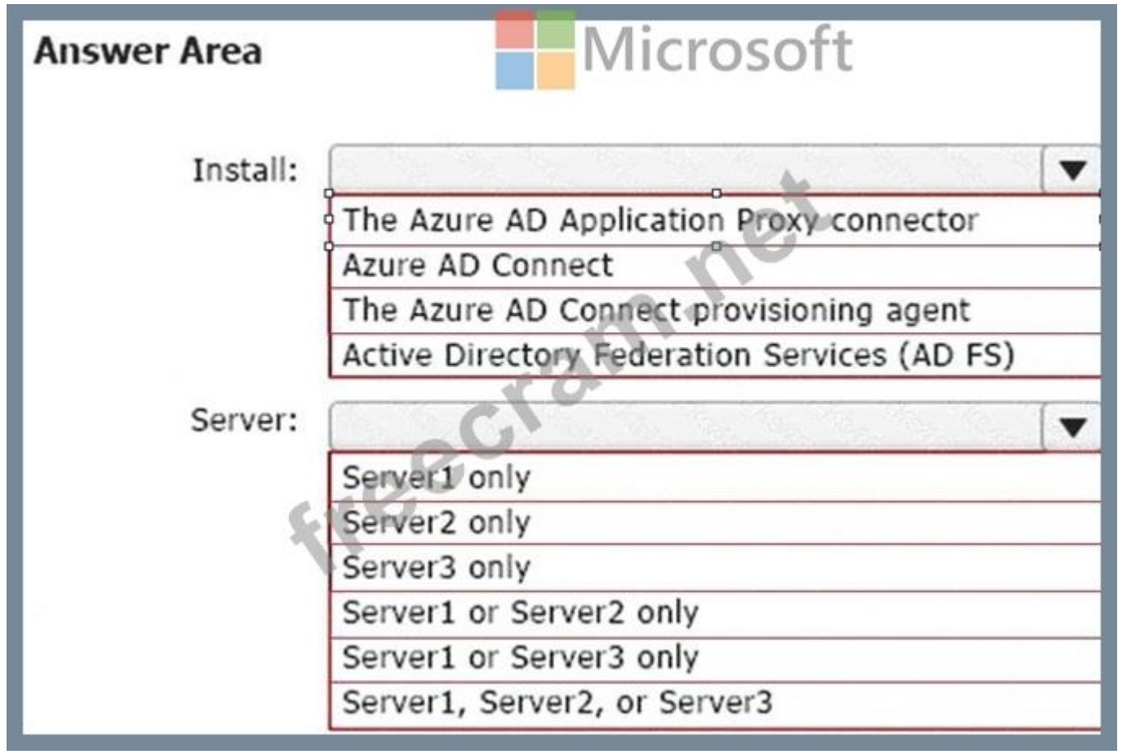
Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.

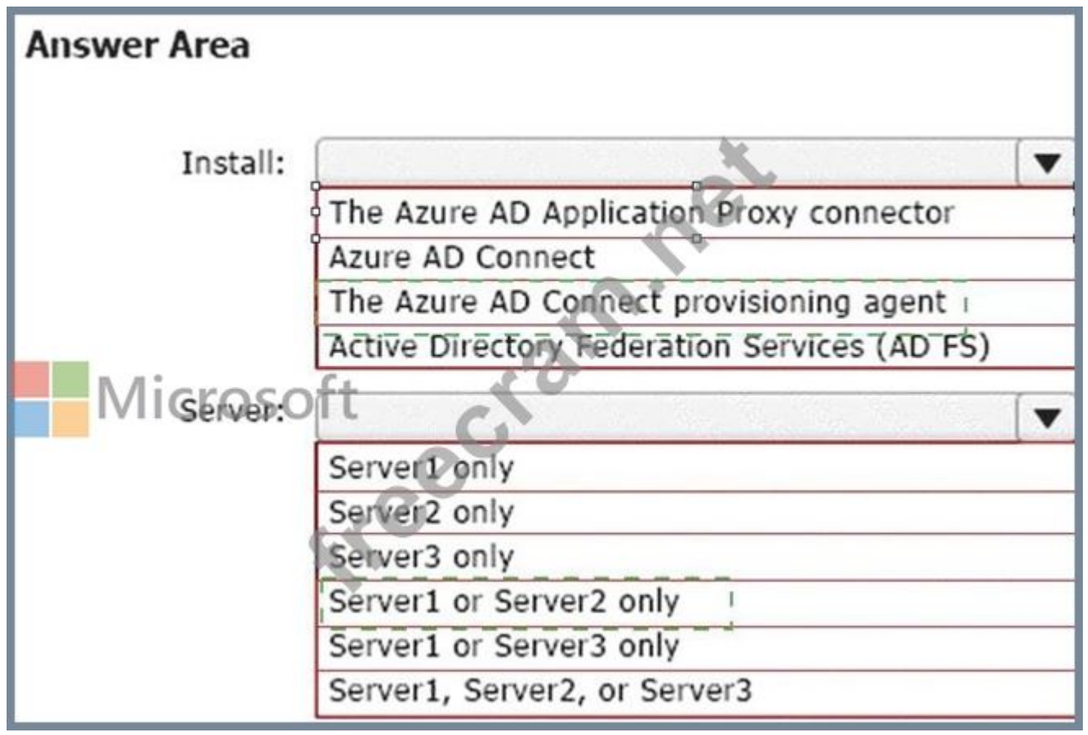
You need to implement Azure AD Connect cloud sync.

What should you install first and on which server? To answer, select the appropriate options in the answer area.

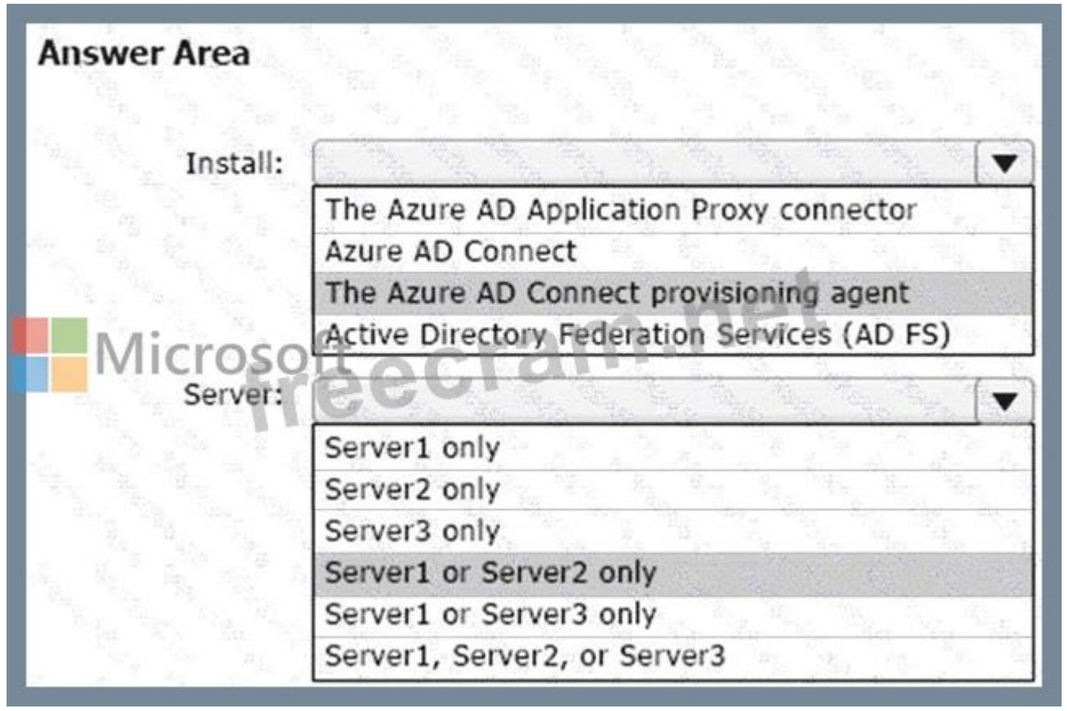
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Box 1: The Azure AD Connect provisioning agent

Install the Azure AD Connect provisioning agent

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

With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted

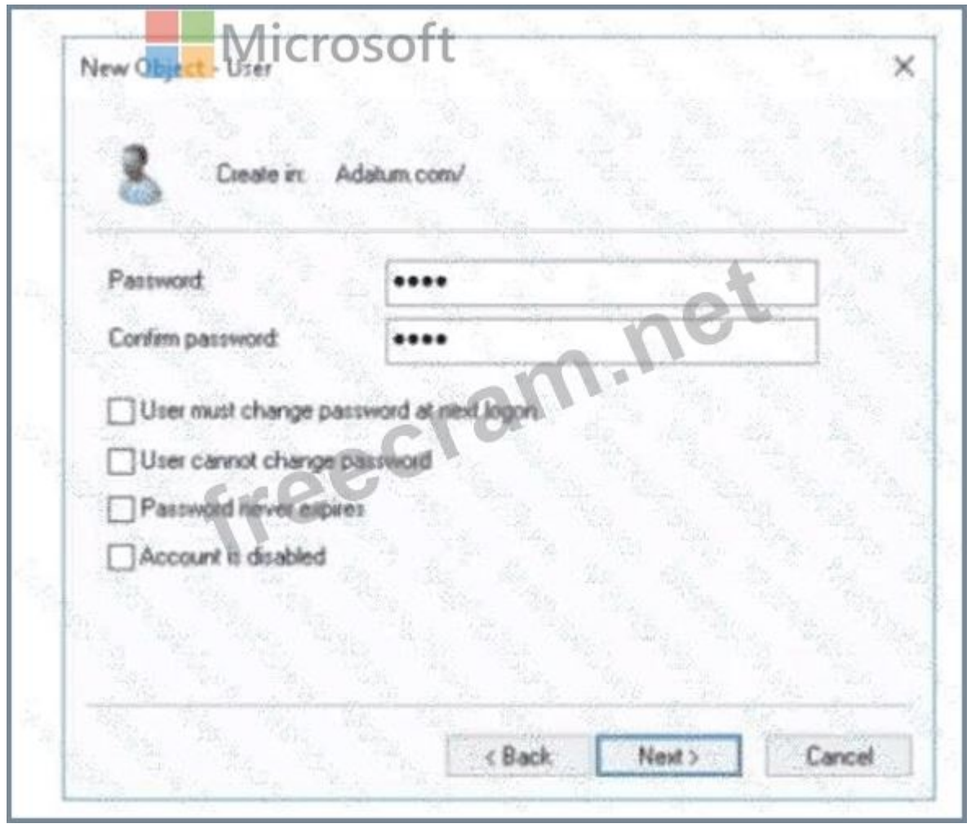
environment, a light- weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.
Box 2: Server1 or Server2 only.
Cloud provisioning agent requirements include:
* An on-premises server for the provisioning agent with Windows 2016 or later.
This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.
Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-install
https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites

NEW QUESTION: 119
You have a Microsoft 365 subscription that contains the alerts shown in the following table.

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

Which properties of the alerts can you modify?
A. Status only
B. Status and Comment only
C. Status and Severity only
D. Status, Severity, and Comment only
E. Status, Severity, Comment and Category
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365- worldwide#limitations

NEW QUESTION: 120
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 Area

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

Answer:

Answer Area

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

Explanation:

NEW QUESTION: 121

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

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

Block a vulnerable app until the app is updated.

Block an application executable based on a file hash.

The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

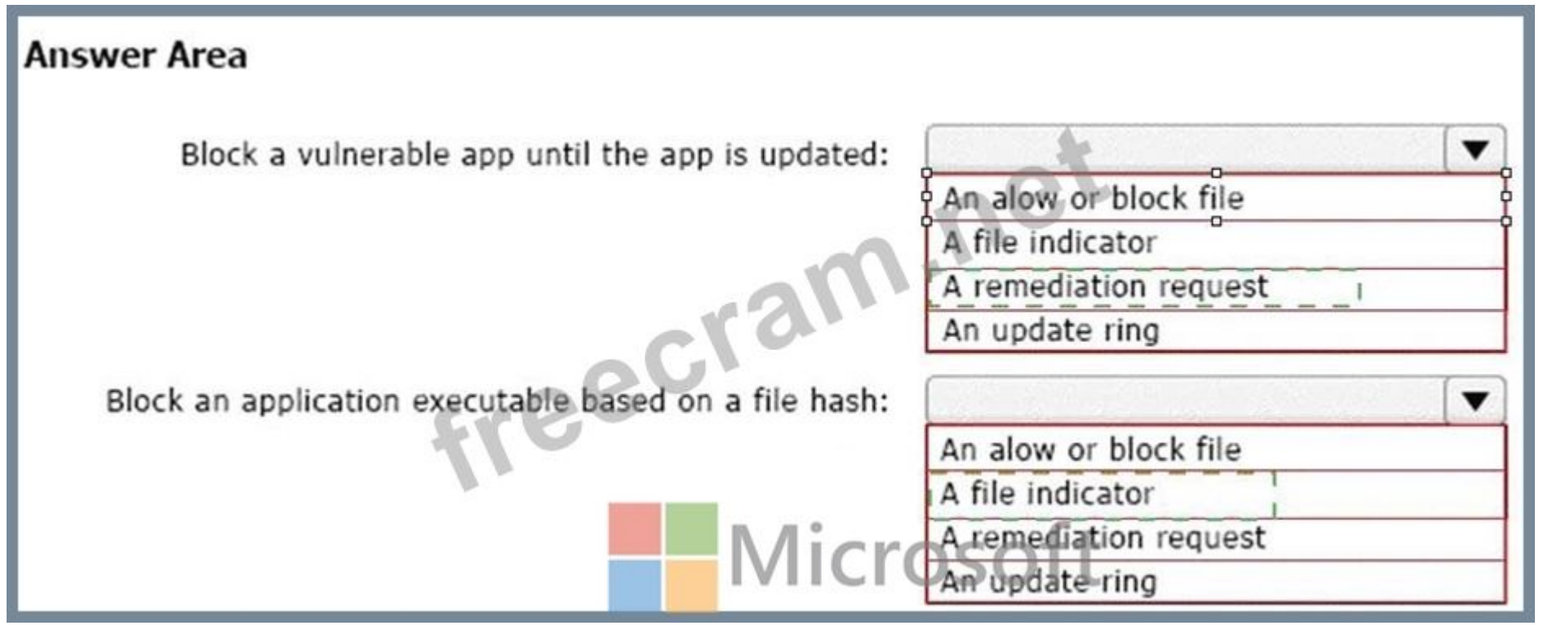
Block a vulnerable app until the app is updated:

- An alow or block file
- A file indicator
- A remediation request
- An update ring

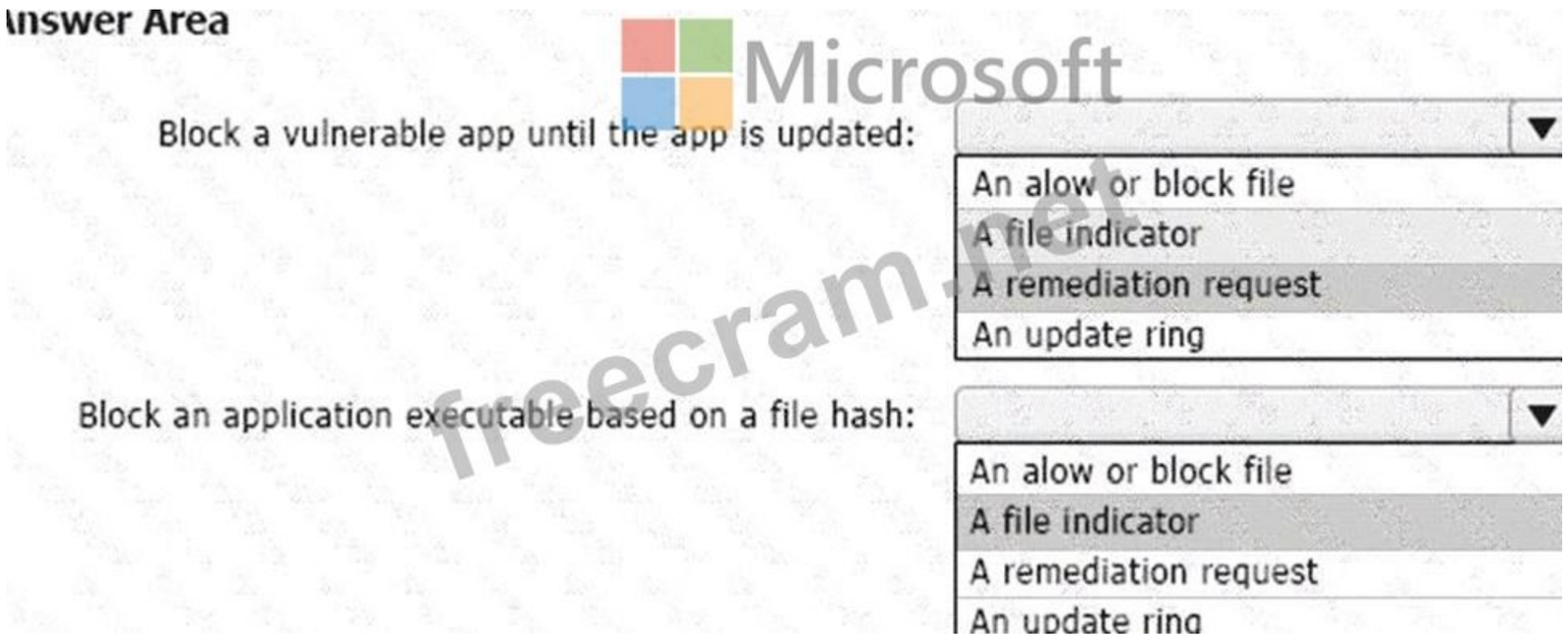
Block an application executable based on a file hash:

- An alow or block file
- A file indicator
- A remediation request
- An update ring

Answer:



Explanation:



Box 1: A remediation request

Block a vulnerable app until the app is updated.

Block vulnerable applications

How to block vulnerable applications

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

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

Select Request remediation.

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

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

Pick a Remediation due date and select Next.

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

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

Box 2: A file indicator

Block an application executable based on a file hash.

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

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

Reference:

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

NEW QUESTION: 122

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

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

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

* Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.

* User passwords must be 10 characters or more.

Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant.

Does this meet the goal?

A. No

B. Yes

Answer: (SHOW ANSWER)

NEW QUESTION: 123

HOTSPOT

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

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

You onboard a computer named computer1 to Microsoft Defender for Endpoint as shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.

Answer Area

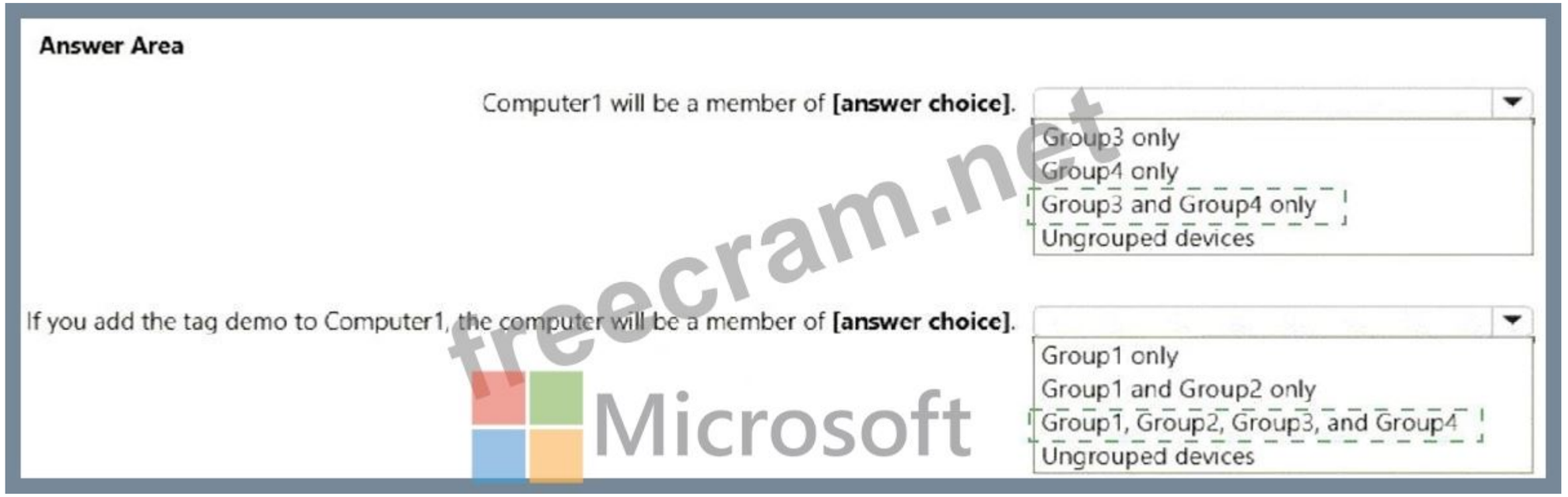
Computer1 will be a member of **[answer choice]**.

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

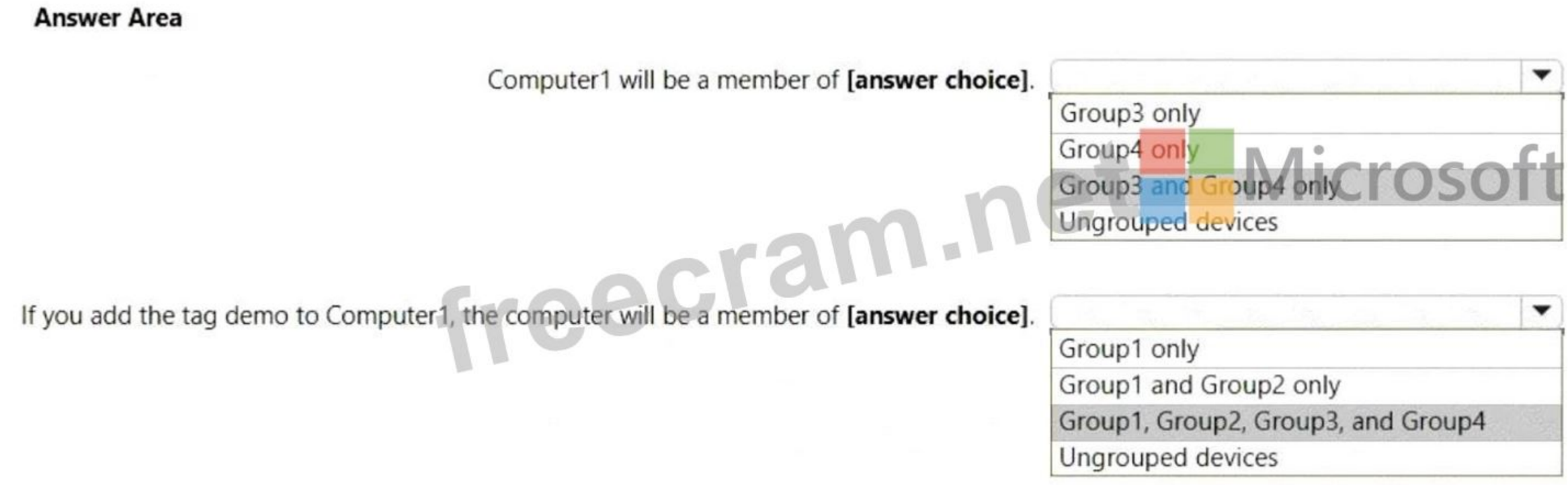
If you add the tag demo to Computer1, the computer will be a member of **[answer choice]**.

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

Answer:



Explanation:



Box 1: Group3 and Group4 only

Computer1 has no Demo Tag.

Computer1 is in the adatum domain and OS is Windows 10.

Box 2: Group1, Group2, Group3 and Group4

NEW QUESTION: 124

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

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

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

Which objects will sync to Azure AD?

A. Group1 only

B. User1 and User2 only

C. Group1 and User1 only

D. Group1, User1, and User2

Answer: (SHOW ANSWER)

Disabled accounts

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

The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found.

In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.

Reference:

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

NEW QUESTION: 125

You have a Microsoft 365 E5 subscription.

You need to configure threat protection tor Microsoft 365 to meet the following requirements:

* Limit a user named User 1 from sending more than 30 email messages per day.

* Prevent the delivery of a specific file based on the file hash.

Which two threat policies should you configure in Microsoft Defender for Office 365? To answer, select the appropriate threat policies in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft

Policies

	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Rules

	Tenant Allow/Block Lists	Manage allow or block entries for your organization.
	Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
	DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users
	Advanced delivery	Manage overrides for special system use cases.
	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
	Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own

Answer:

Answer Area

Policies

Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Rules

Tenant Allow/Block Lists	Manage allow or block entries for your organization.
Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users
Advanced delivery	Manage overrides for special system use cases.
Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own

Explanation:
Limit a user named User 1 from sending more than 30 email messages per day: Anti-spam policy The anti-spam policy in Microsoft Defender for Office 365 allows you to configure outbound spam settings, including limiting the number of email messages a user can send per day. This helps prevent spam and potential email abuse within the organization.
Prevent the delivery of a specific file based on the file hash: Safe Attachments policy The Safe Attachments policy in Microsoft Defender for Office 365 can be configured to block or quarantine emails with attachments that match specific file hashes. This ensures that potentially malicious files are not delivered to users' inboxes.

NEW QUESTION: 126
You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps.
You plan to perform a security audit of all the apps detected by Cloud Discovery.
You need to track which apps were audited. The solution must ensure that the list of audited apps can be displayed in the cloud app catalog.
A. Enable app governance.
B. Deploy Conditional Access App Control.

C. Define each app as a critical asset.
D. Apply a custom app tag to each app.
E. Generate a Cloud Discovery snapshot report.
Answer: (SHOW ANSWER)

NEW QUESTION: 127
You have a Microsoft 365 E5 subscription. The subscription contains a Microsoft SharePoint Online site named Site1. Site1 contains the following files:
* File.docx
* ImportantFile.docx
* Filejmportant.docx
From Microsoft Defender Cloud Apps, you create a file policy named Policy1 that has the filter shown in the following exhibit.

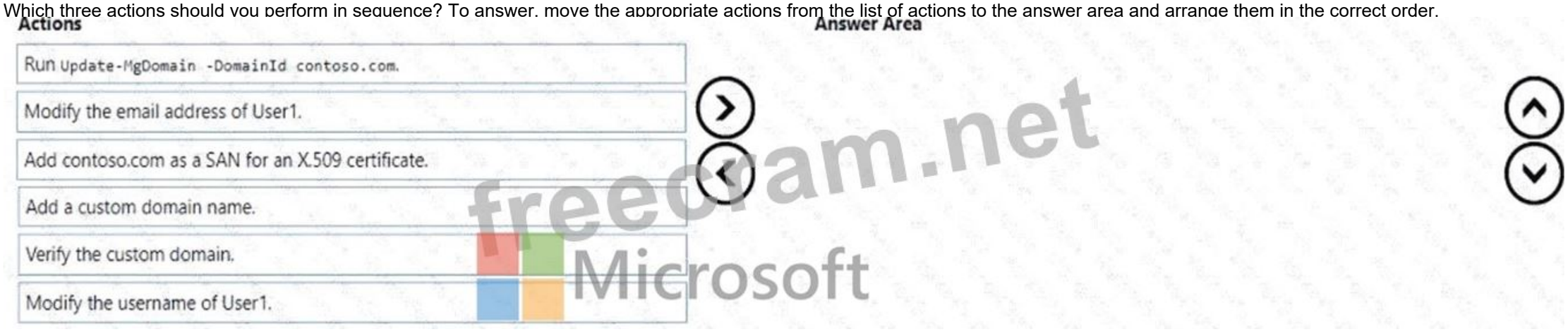
To which files will Policy1 apply?
A. ImportantFile.docx only
B. Filejmportant.docx only
C. File.docx, ImportantFile.docx, and Filejmportant.docx
D. ImportantFile.docx and Filejmportant.docx only
E. File.docx only
Answer: (SHOW ANSWER)

NEW QUESTION: 128
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview policies to meet the following requirements:
Identify documents that are stored in Microsoft Teams and SharePoint that contain Personally Identifiable Information (PII).
Report on shared documents that contain PII.
What should you create?
A. a data loss prevention (DLP) policy
B. a retention policy
C. an alert policy
D. a Microsoft Defender for Cloud Apps policy
Answer: (SHOW ANSWER)
Demonstrate data protection
Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities.
With DLP policies, you can automatically protect sensitive information across Microsoft 365.

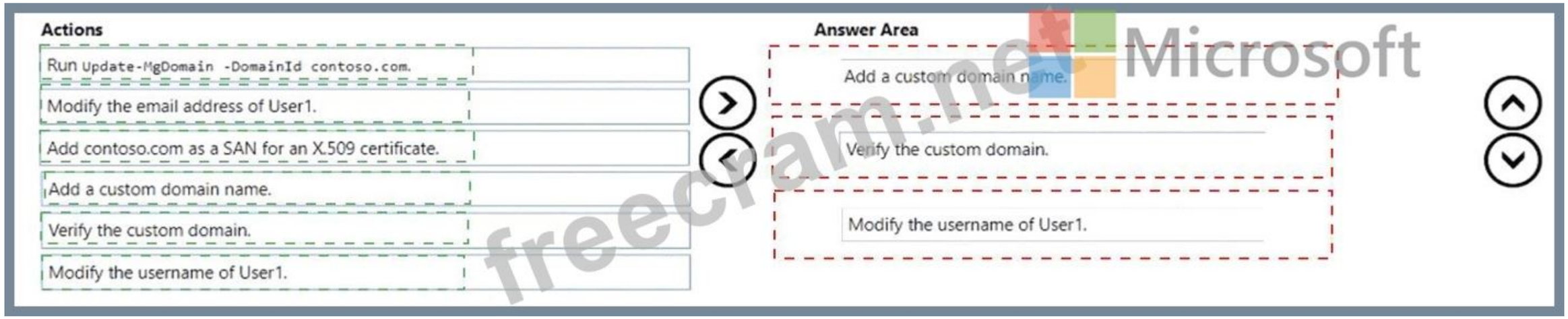
There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.
In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.
From the Security & Compliance tab of your browser, click Home.
Click Data loss prevention > Policy.
Click + Create a policy.
In Start with a template or create a custom policy, click Custom > Custom policy > Next.
In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b.
Description: Protect the personally identifiable information of European citizens Etc.
Reference:
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365- dev-test-environment

NEW QUESTION: 129
You have a Microsoft 365 E5 subscription.
You need to compare the current Safe Links configuration to the Microsoft recommended configurations.
What should you use?
A. Microsoft Purview
B. Azure AD Identity Protection
C. the configuration analyzer
D. Microsoft Secure Score
Answer: (SHOW ANSWER)

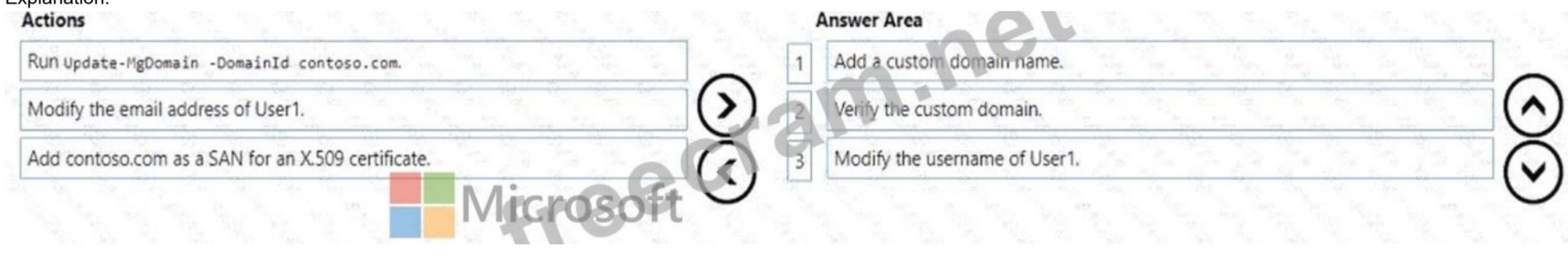
NEW QUESTION: 130
Your company has an Azure AD tenant named contoso.onmicrosoft.com.
You purchase a domain named contoso.com from a registrar and add all the required DNS records.
You create a user account named User1. User1 is configured to sign in as userl@contoso.onmicrosoft.com.
You need to configure 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: 131

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of	Device
User1	Group1	Device1
User2	Group1	Device2, Device3

The devices are configured as shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Joined
Device3	Android	Registered

You have a Conditional Access policy named CAPolicy1 that has the following settings:

1.Assignments

Users or workload identities: Group1

Cloud apps or actions: Office 365 SharePoint Online

Conditions

- Filter for devices: Exclude filtered devices from the policy

- Rule syntax: device.displayName -startsWith " Device "

2.Access controls

Grant

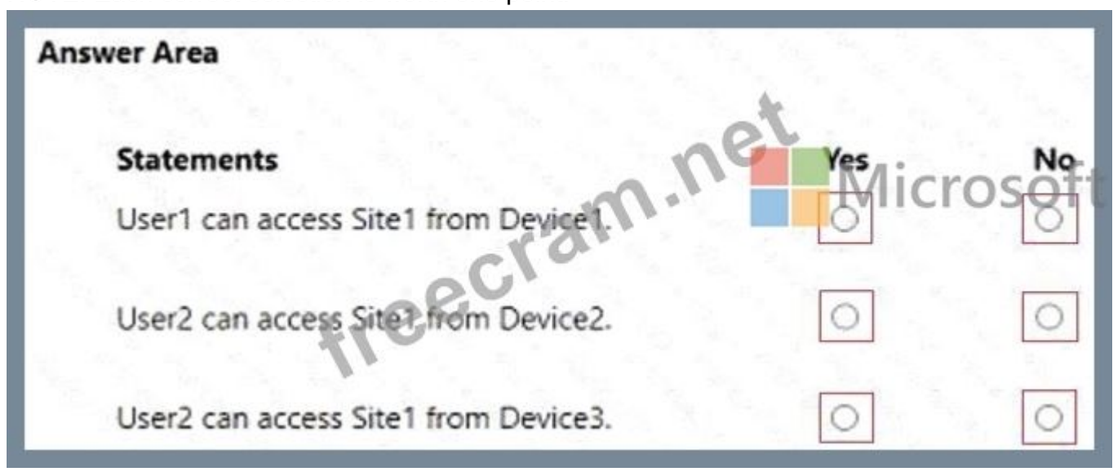
- Grant: Block access

Session: 0 controls selected

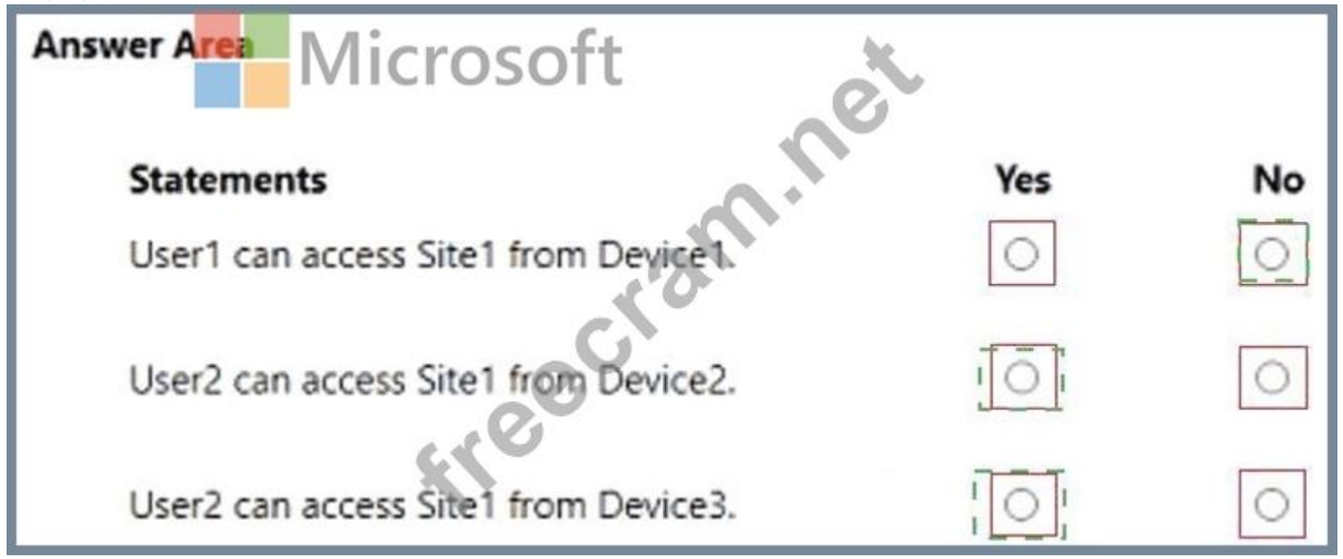
3.Enable policy: On

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:

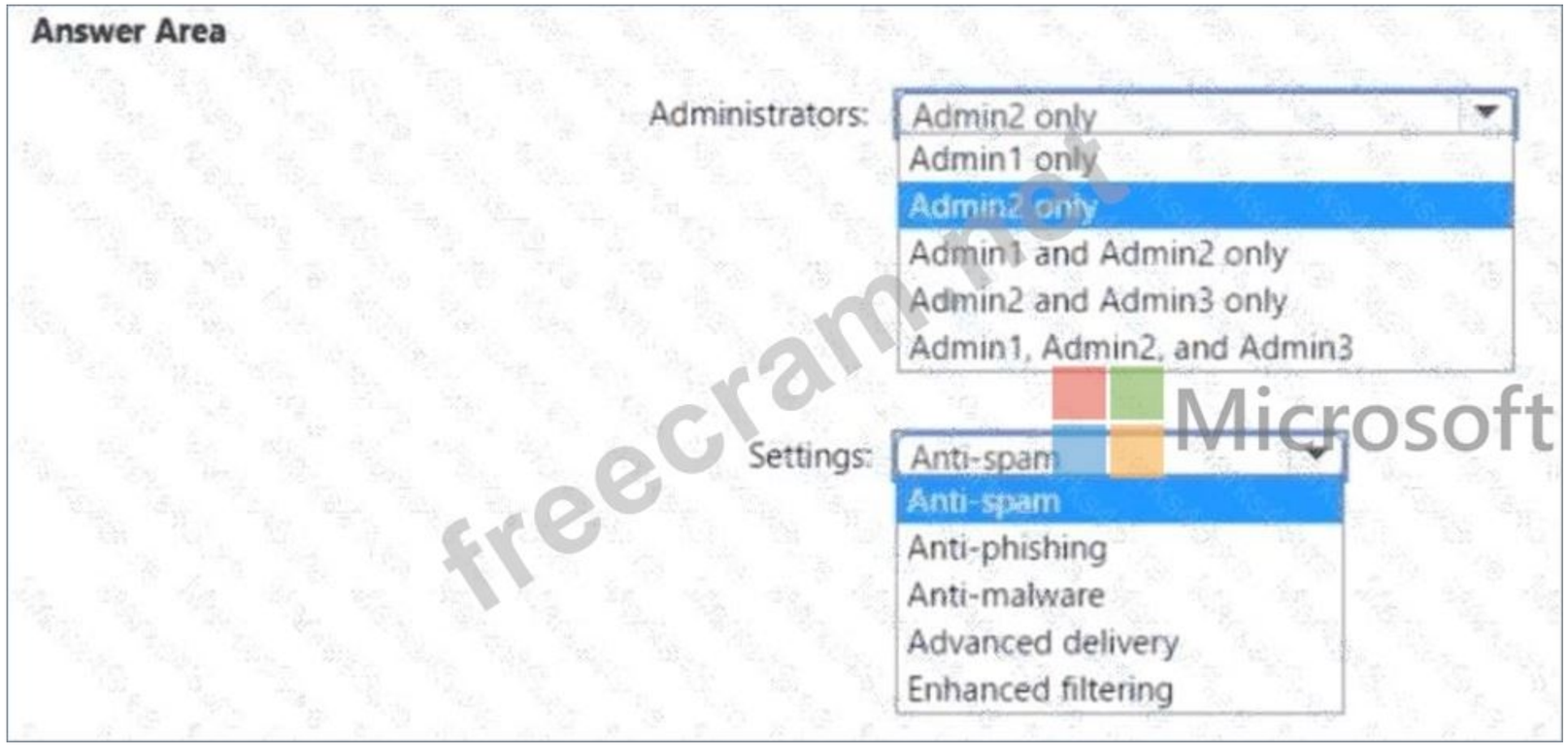


Explanation:

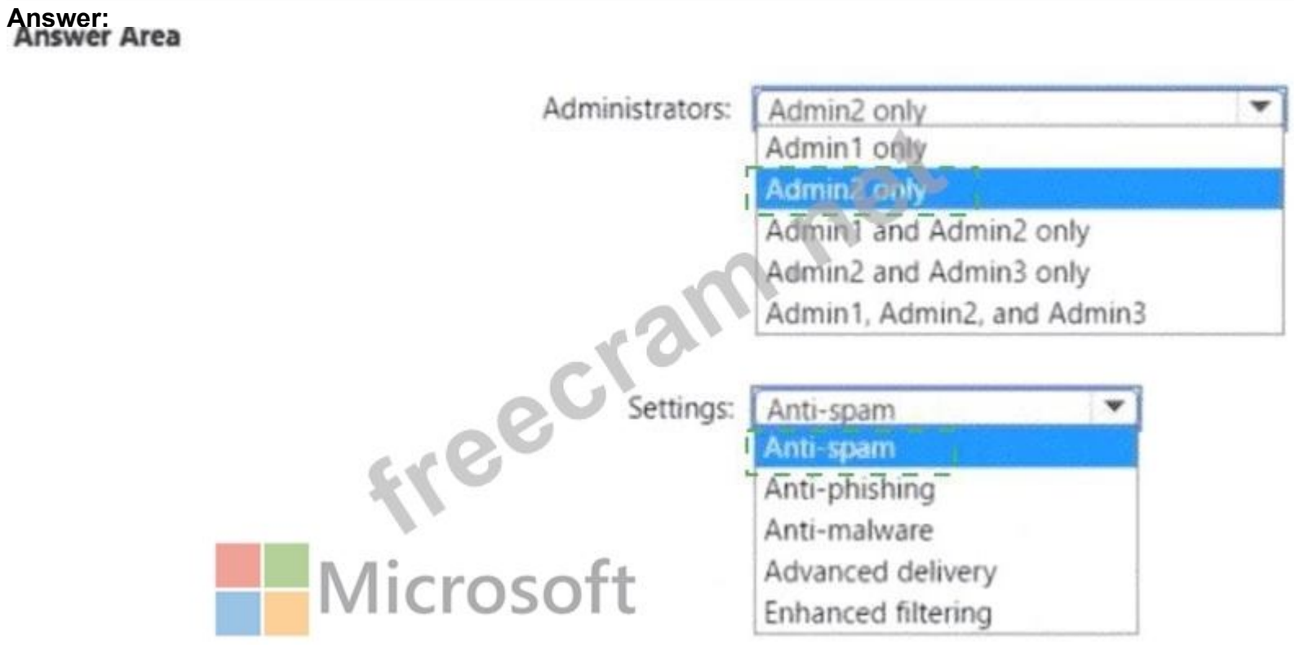
Answer Area

Box 1: No
User1 is member of Group1 and has Device1.
Device1 is not Azure AD joined.
Note: Requiring a hybrid Azure AD joined device is dependent on your devices already being hybrid Azure AD joined.
Box 2: Yes
User2 is member of Group1 and has devices Device2 and Device3.
Device2 is Azure AD joined.
Device2 is excluded from CAPolicy1 (which would block access to Site1).
Box 3: Yes
User2 is member of Group1 and has devices Device2 and Device3.
Device3 is Android and is Azure AD registered.
Device3 is excluded from CAPolicy1 (which would block access to Site1).
Note: On Windows 7, iOS, Android, macOS, and some third-party web browsers, Azure AD identifies the device using a client certificate that is provisioned when the device is registered with Azure AD.
When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-hybrid-azure-ad-join
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy- compliant-device

NEW QUESTION: 132
You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table.
User1 reports that after sending 1,000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:
* Which administrators can unblock User1
* What to configure to allow User1 to send at least 2,000 emails per day without being blocked What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Answer Area

NEW QUESTION: 133
Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 10.
You purchase a Microsoft 365 subscription.
You implement password hash synchronization and Azure AD Seamless Single Sign-On (Seamless SSO).
You need to ensure that users can use Seamless SSO from the Windows 10 computers.
What should you do?
A. Join the computers to Azure AD.
B. Deploy an Azure AD Connect staging server.
C. Create a conditional access policy in Azure AD.
D. Modify the Intranet zone settings by using Group Policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 134
You have a Microsoft 365 subscription that includes Microsoft Intune and Microsoft Defender XDR.
All users have devices that run Windows 11.
From the Microsoft Defender portal, you review the Microsoft Secure Score recommendations. One of the top recommendations is to block all Microsoft Office applications from creating child processes.
You need to increase the secure score by addressing the recommendation.
What should you do?
A. Create a policy for Office applications.
B. Select Safe Documents for Office clients.
C. Configure an endpoint detection and response (EDR) policy.
D. Create an attack surface reduction (ASR) policy.
Answer: (SHOW ANSWER)

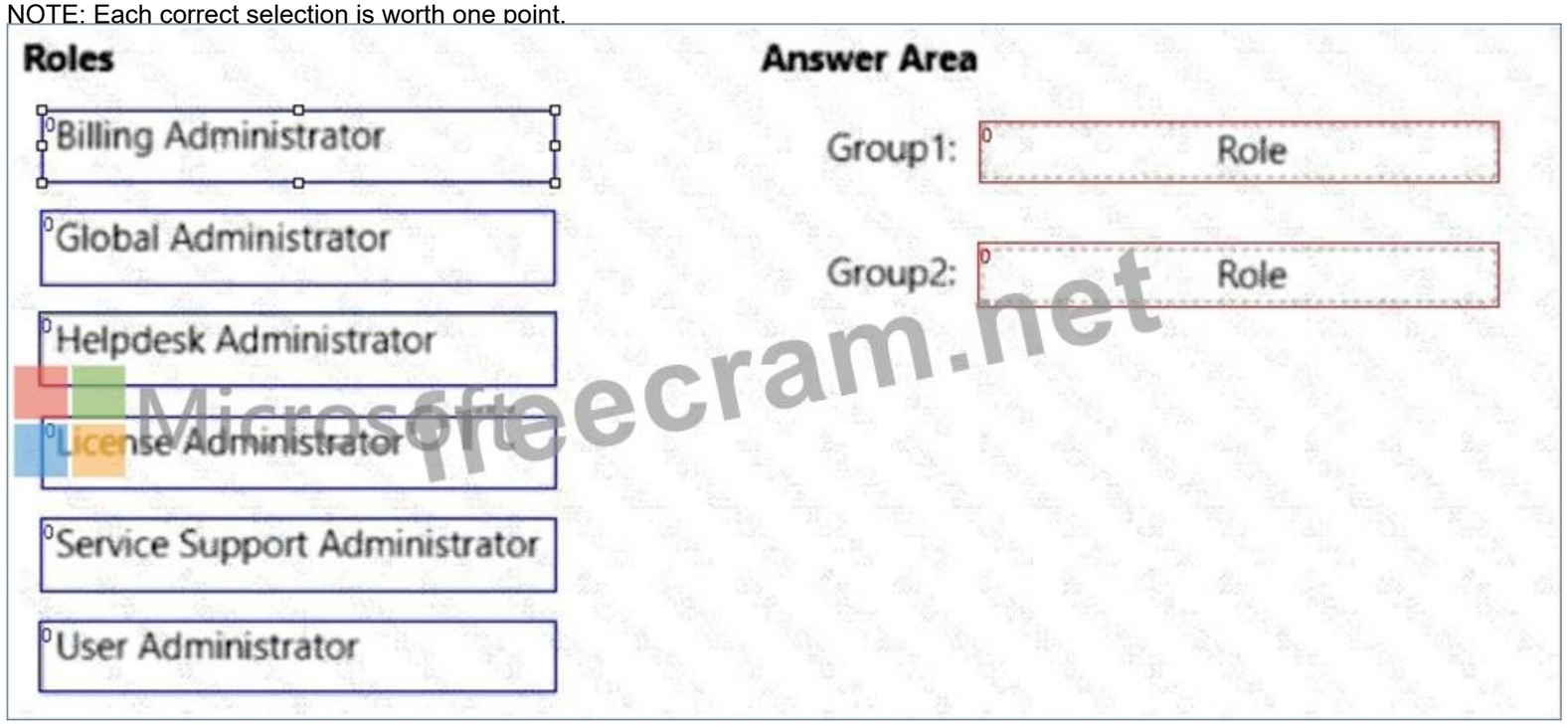
NEW QUESTION: 135
DRAG DROP
You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.
You need to ensure that each group can perform the tasks shown in the following table.

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.

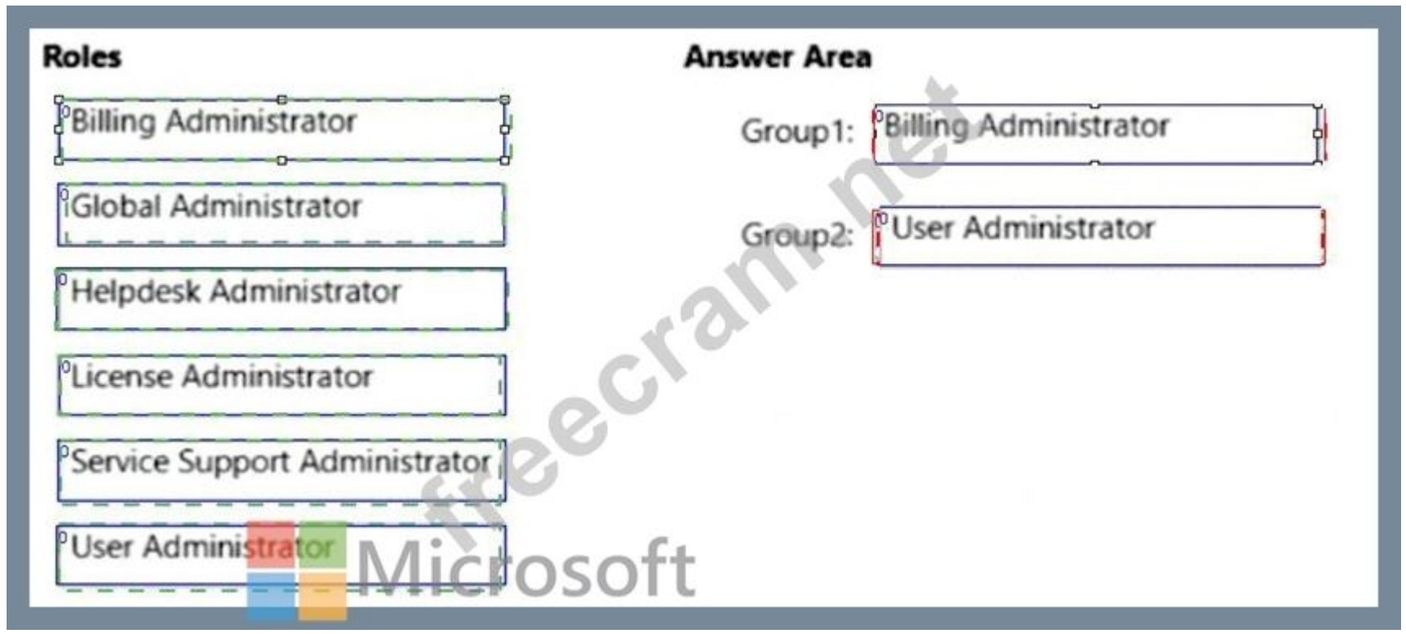
The solution must use the principle of least privilege.

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.

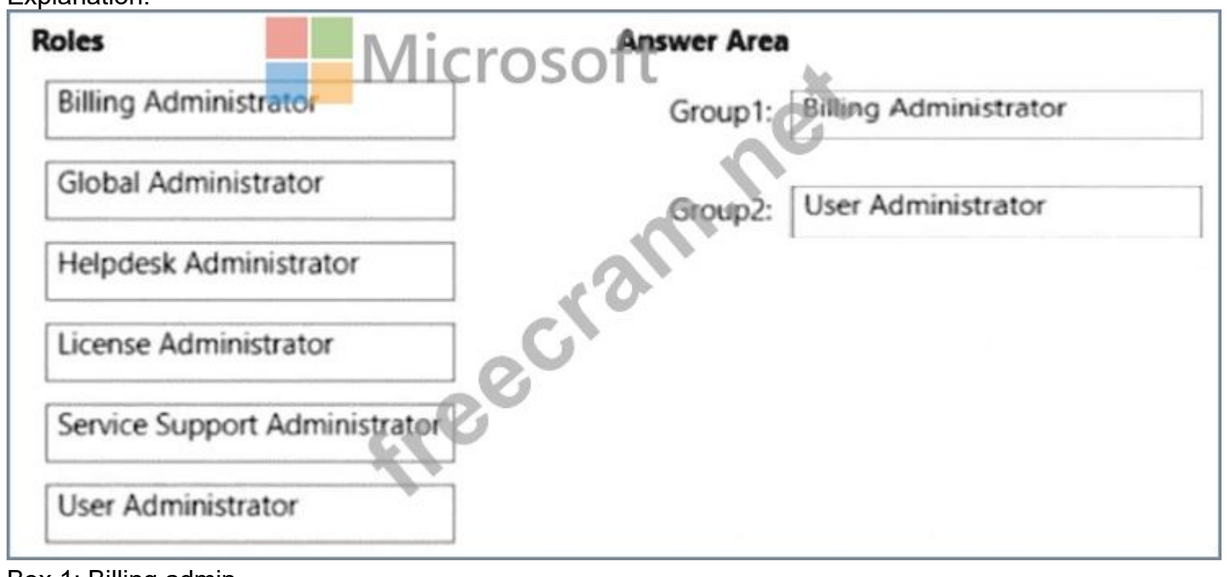
NOTE: Each correct selection is worth one point.



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: 136

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

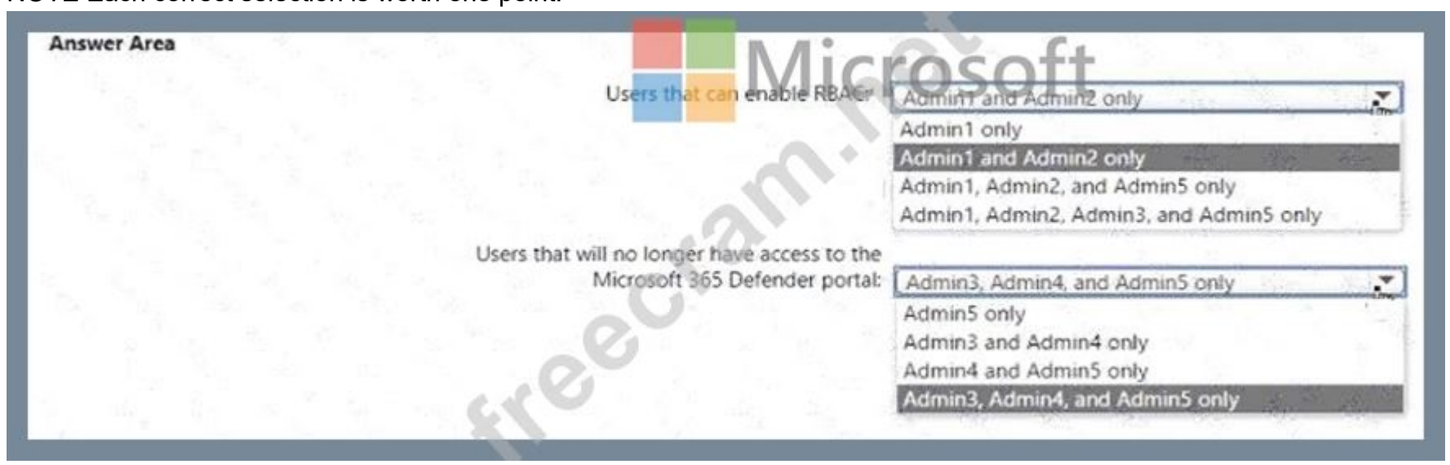
Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

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.

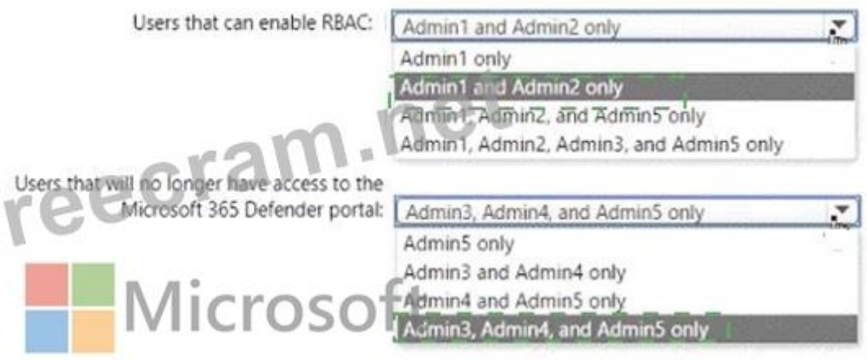
Which users can enable RBAC, and winch users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.



Answer:

Answer Area



Explanation:

NEW QUESTION: 137

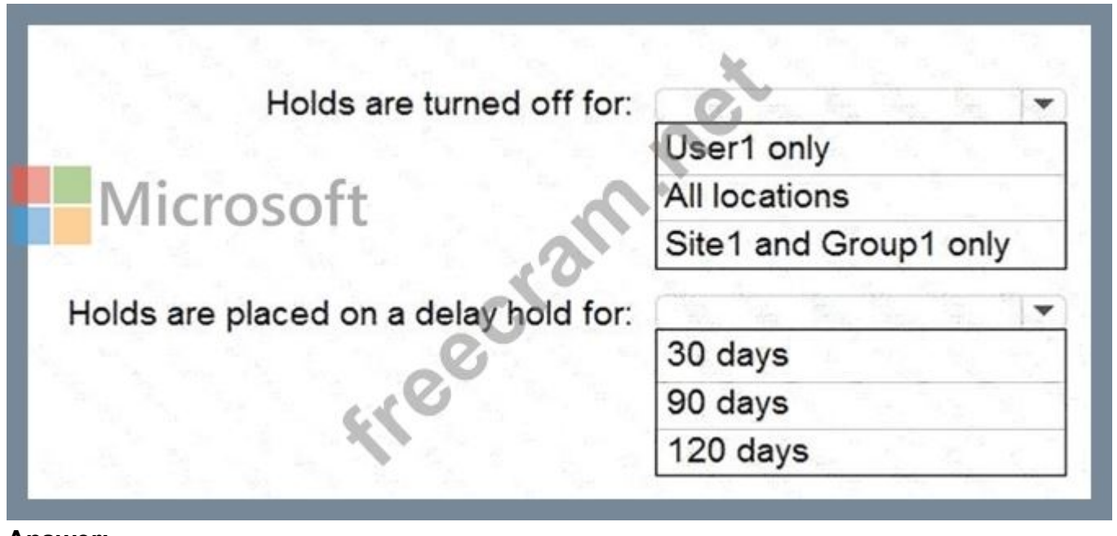
You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:

Name: Case1
Included content: Group1, User1, Site1

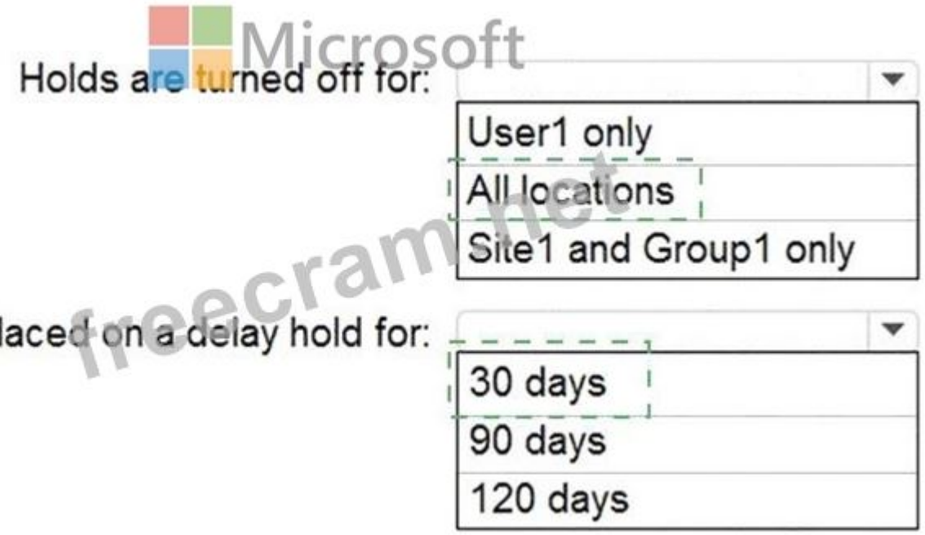
Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders The investigation for Case1 completes, and you close the case.

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

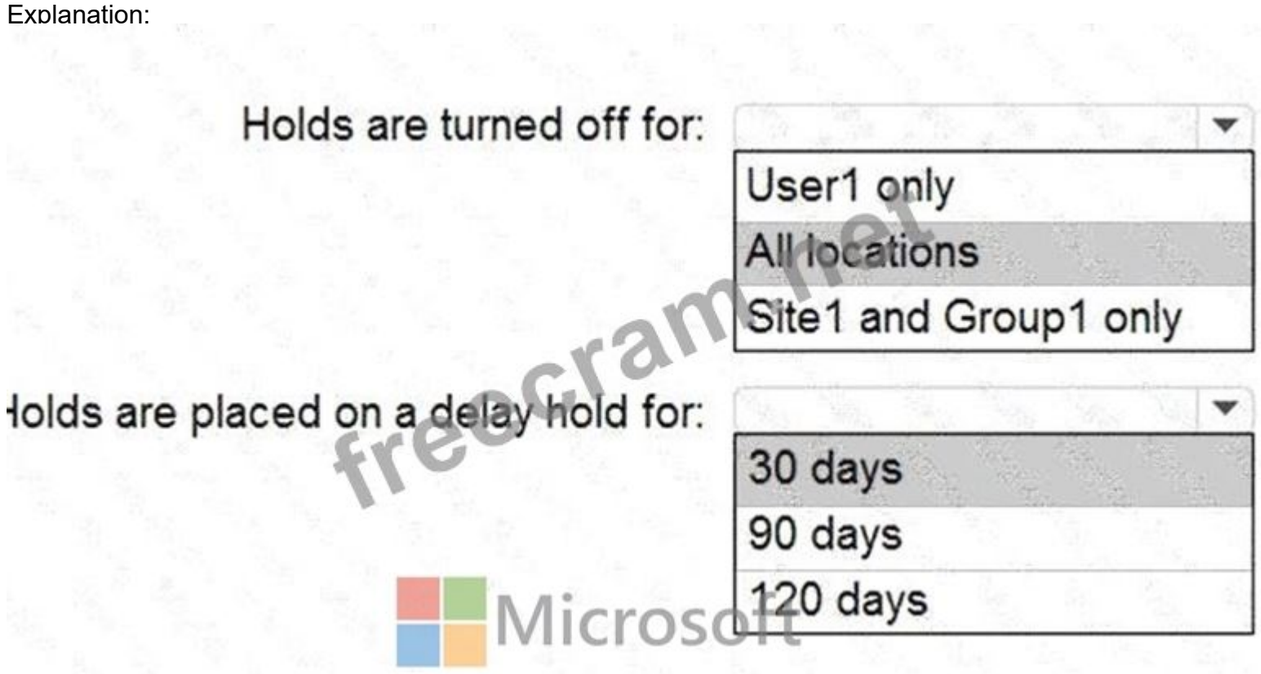
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

NEW QUESTION: 138
(You have a Microsoft 365 E5 subscription.
You are implementing Microsoft Defender for Cloud Apps.
You need to ensure that you can create OAuth app policies .
Solution: You configure Conditional Access app control .
Does this meet the goal?)
A. Yes

B. No

Answer: (SHOW ANSWER)

OAuth app policies are a feature of Microsoft Defender for Cloud Apps (MDCA) that allow you to:

* Monitor OAuth-connected apps
* Control app permissions
* Detect risky or overprivileged OAuth applications

Microsoft documentation clearly states that OAuth app policies are created and managed directly within Microsoft Defender for Cloud Apps , under Control # Policies # OAuth app policies .

Why Conditional Access app control does NOT meet the goal

Conditional Access app control is a different capability that:

* Integrates Microsoft Defender for Cloud Apps with Microsoft Entra Conditional Access
* Provides real-time session control for cloud apps
* Is used to control user actions (download, upload, copy, etc.) during app sessions Microsoft documentation explicitly distinguishes these features:
* Conditional Access app control is for session-based access control
* OAuth app policies are for app governance and permission monitoring

Configuring Conditional Access app control does not enable or affect the ability to create OAuth app policies .

NEW QUESTION: 139

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.

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

All users have Windows 10 Enterprise devices.

The Products & services settings in Microsoft Store for Business are 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
User2 can install the Microsoft Remote Desktop app from the private store.	○	○
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	○	○
User4 can manage the Microsoft Remote Desktop app from the private store.	○	○

Answer:

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

Explanation:

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

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

NEW QUESTION: 140

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. a Microsoft Intune device configuration profile
B. Microsoft Entra conditional access
C. a Microsoft Intune device compliance policy
D. Microsoft Entra password protection
Answer: (SHOW ANSWER)

NEW QUESTION: 141

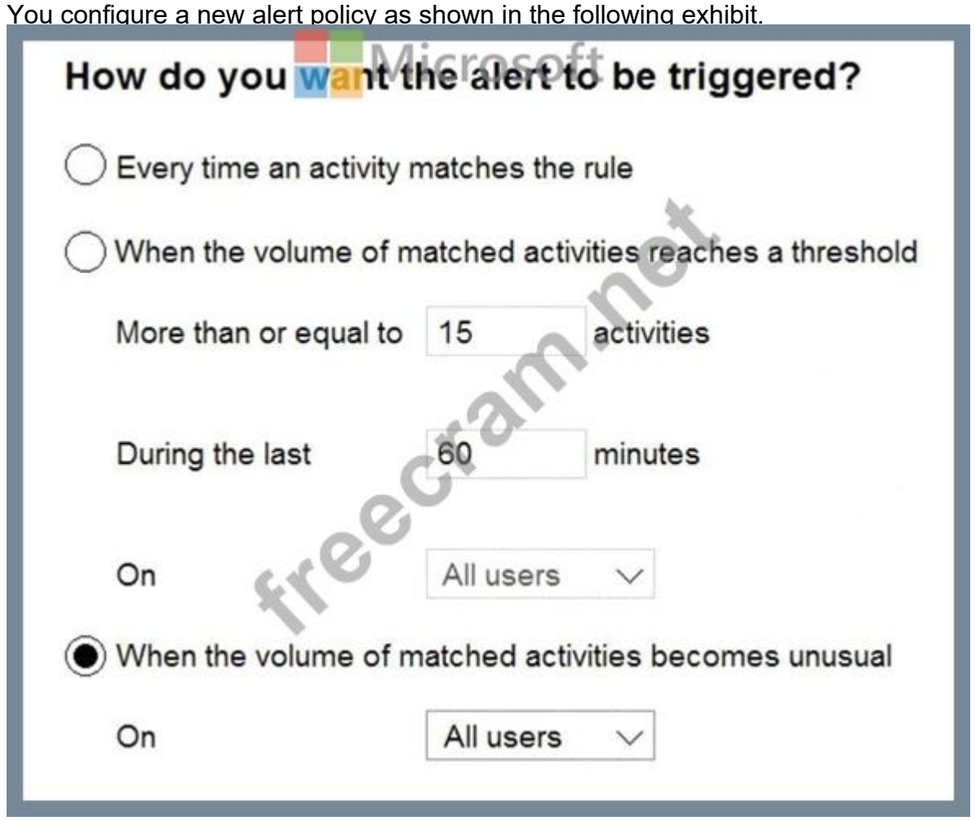
You have a Microsoft 365 E5 subscription.
You need to create Conditional Access policies to meet the following requirements:
All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.
Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.
All users must be blocked from signing in from outside the United States and Canada.
Only users in the R&D department must be blocked from signing in from both Android and iOS devices.
Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.
What is the minimum number of Conditional Access policies you should create?

A. 3
B. 4
C. 5
D. 6
E. 7
F. 8
Answer: (SHOW ANSWER)

* Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.
One Policy.
* Only users in the R&D department must be blocked from signing in from both Android and iOS devices.
One Policy.
* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.
One policy
* All users must be blocked from signing in from outside the United States and Canada.
Only users in the R&D department must be blocked from signing in from both Android One Policy Reference:
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

NEW QUESTION: 142
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.

How many days it will take to establish the baseline:

- 1
- 5
- 7
- 10

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

- Alerts will be triggered.
- Alerts will not be triggered.
- Alerts will be triggered only after the process to establish the baseline has been running for one day.

Answer:

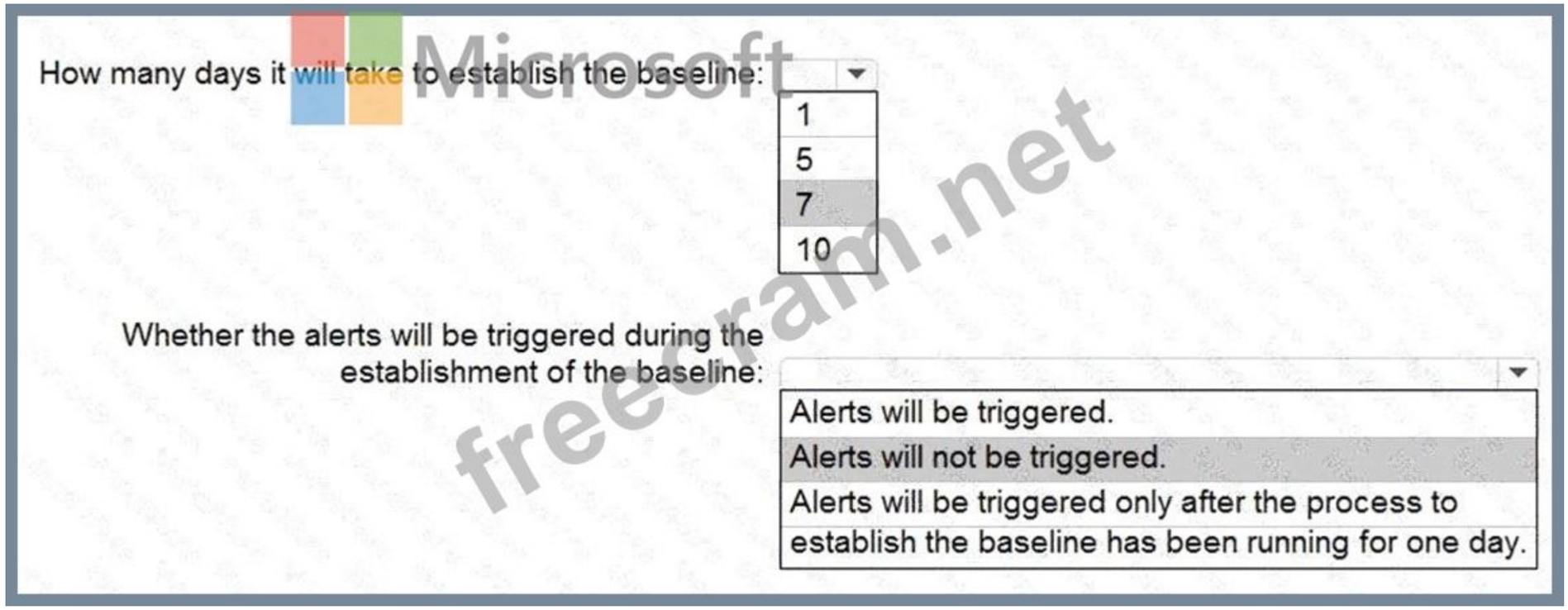
How many days it will take to establish the baseline:

- 1
- 5
- 7
- 10

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

- Alerts will be triggered.
- Alerts will not be triggered.
- Alerts will be triggered only after the process to establish the baseline has been running for one day.

Explanation:



ence:

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

NEW QUESTION: 143

You have a Microsoft 365 E5 subscription that.

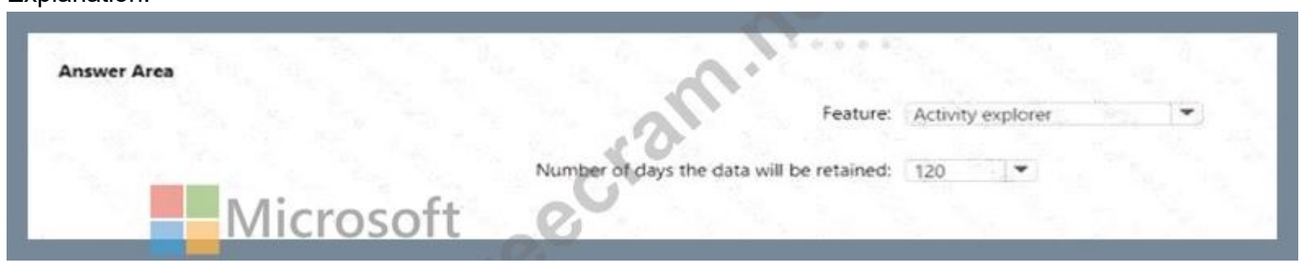
You need to identify whenever a sensitivity label is applied, changed, or removed within the subscription.

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:

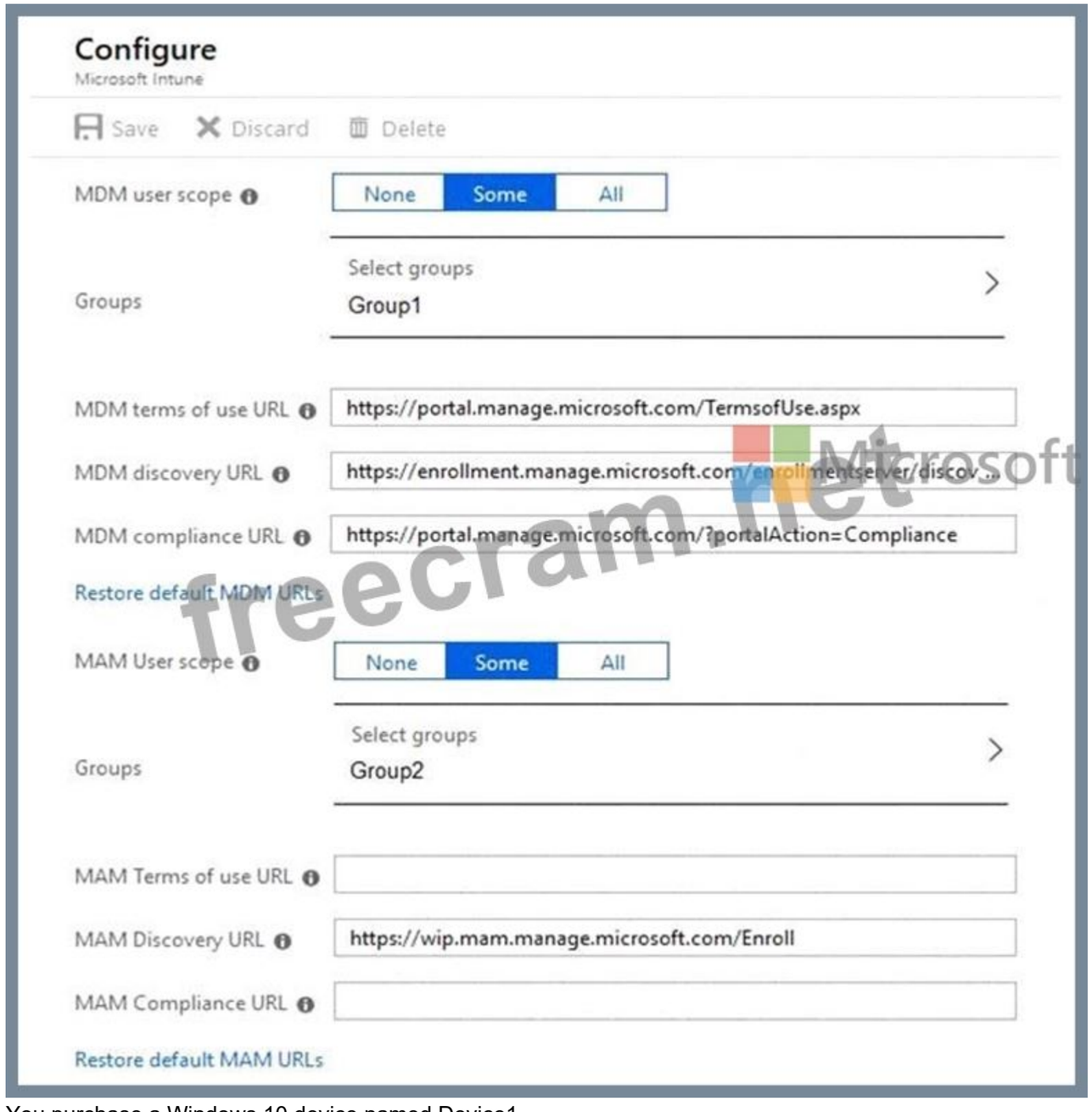


NEW QUESTION: 144

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.



You purchase a Windows 10 device named Device1.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

Answer:

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

Explanation:

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

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

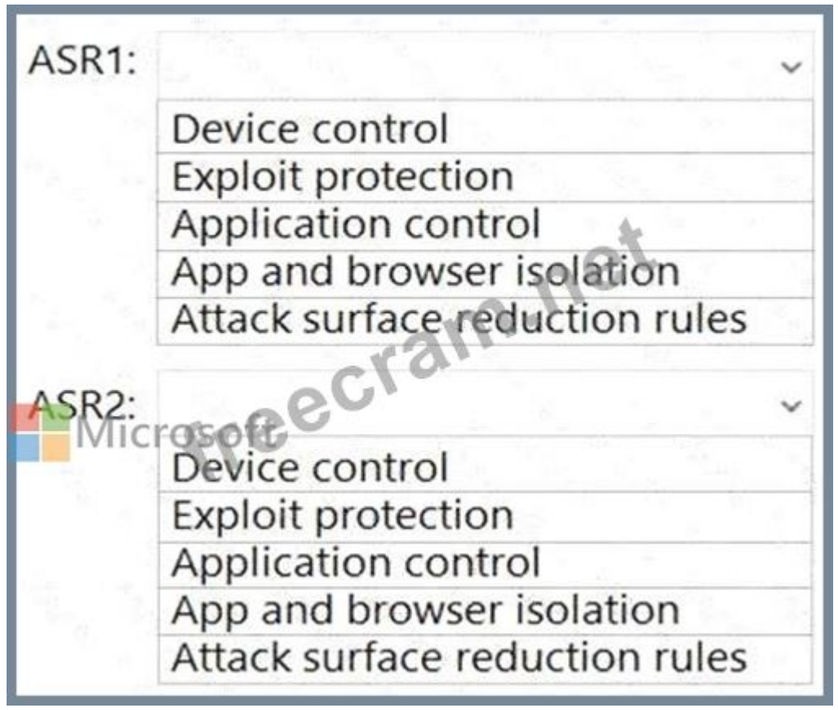
NEW QUESTION: 145
As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

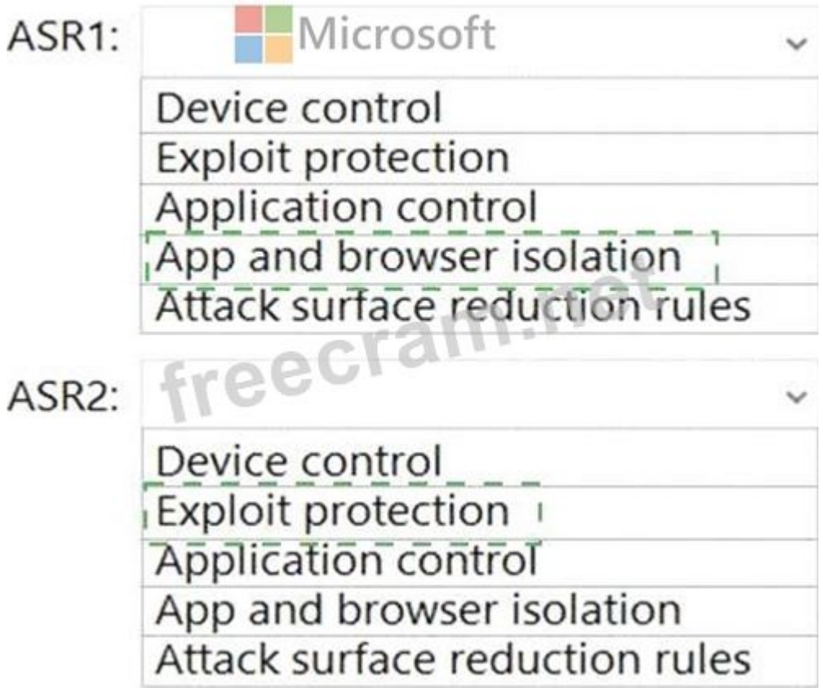
Explanation:

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

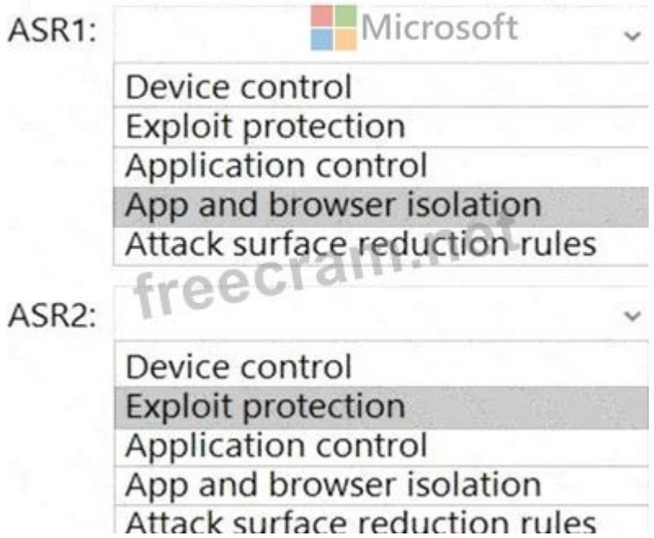
NEW QUESTION: 146
You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.
You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard. ASR2 will be used to configure Microsoft Defender SmartScreen.
Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

NEW QUESTION: 147
You have a Microsoft 365 E5 subscription that contains Windows 11 devices. All the devices are onboarded to Microsoft Defender for Endpoint.
You need to compare the configuration of the devices against industry standard benchmarks. What should you use?
A. Attack surface map
B. Security baselines assessment
C. Events
D. Initiatives
Answer: (SHOW ANSWER)

NEW QUESTION: 148
You have a Microsoft 365 E5 subscription.
You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:
* Support KQL for querying data.
* Retain report data for at least one year.
What should you include in the recommendation?
A. Microsoft 365 usage analytics
B. End point analytics
C. Azure Monitor workbooks
D. a security report in Microsoft 365 Defender
Answer: (SHOW ANSWER)

NEW QUESTION: 149
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: 150

You need to create the Microsoft Store for Business. Which user can create the store?

A. User2

B. User3

C. User4

D. User5

Answer: (SHOW ANSWER)

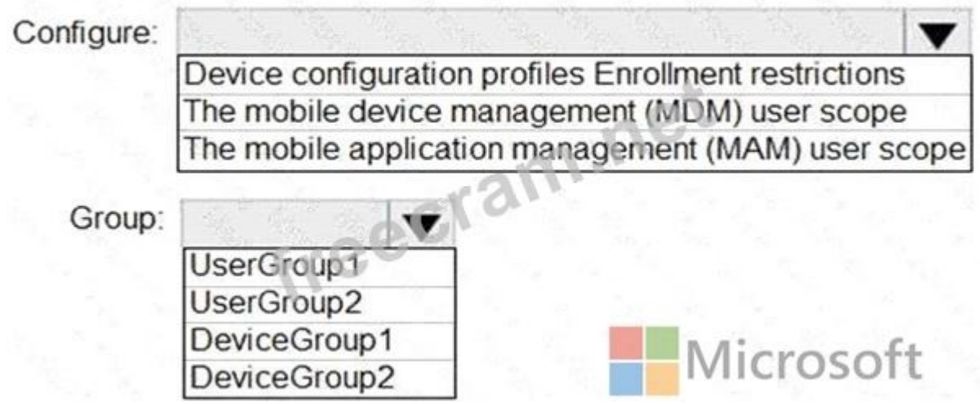
References:

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

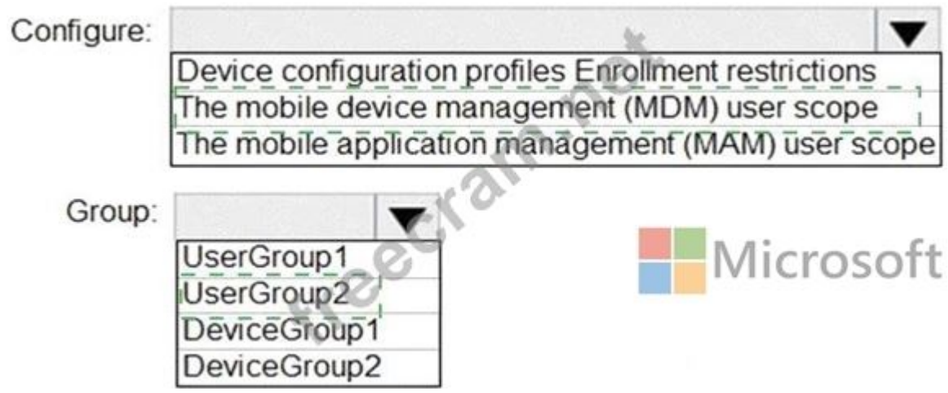
NEW QUESTION: 151

You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.

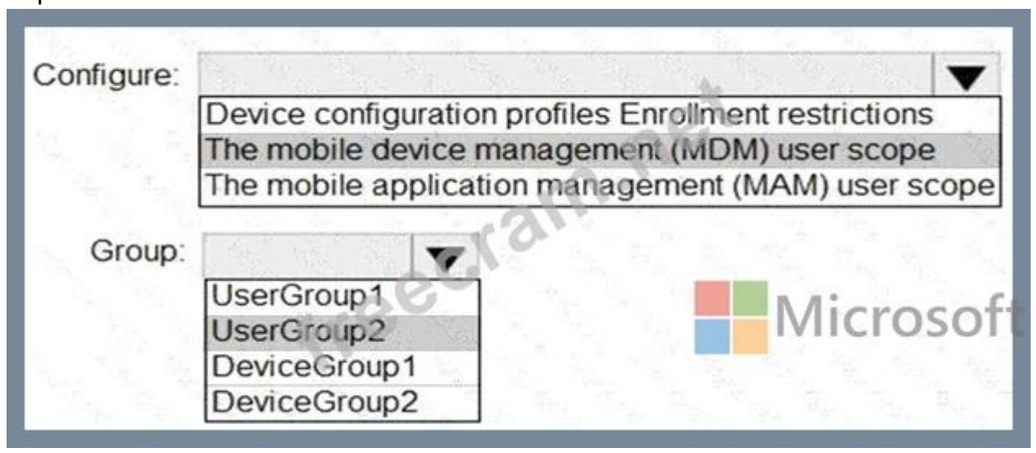
What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

NEW QUESTION: 152

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

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

From the Microsoft Defender portal, you create an anti-spam inbound policy named Policy1 that has the following settings:

* Include these users, groups and domains

o Users: User3 o Groups: Group1

* Exclude these users, groups and domains

o Users: User1

Policy1 has the following Bulk email threshold & spam properties settings:

* Mark as spam

o Empty messages: On o Object tags in HTML On o Sensitive words: Off o Backscatter On Policy1 has the following Actions settings:

* Message actions

o Spam: Move message to Junk Email folder

o High confidence spam: Move message to Junk Email folder

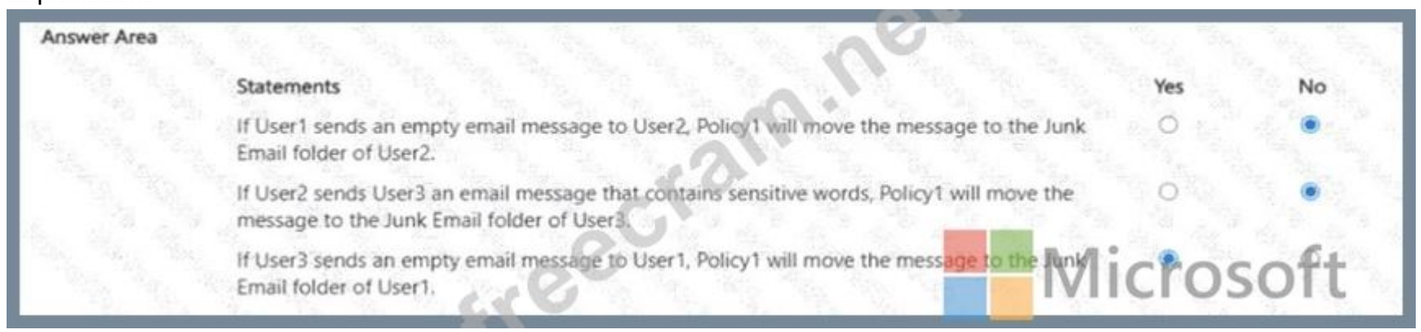
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 sends an empty email message to User2, Policy1 will move the message to the Junk Email folder of User2.	○	○
If User2 sends User3 an email message that contains sensitive words, Policy1 will move the message to the Junk Email folder of User3.	○	○
If User3 sends an empty email message to User1, Policy1 will move the message to the Junk Email folder of User1.	○	○

Explanation:



NEW QUESTION: 153
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: 154
You have a Microsoft 365 subscription.
You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.
To which location can the policy be applied?
A. SharePoint sites
B. OneDrive accounts
C. Teams chat and channel messages
D. Exchange email

Answer: D (LEAVE A REPLY)

NEW QUESTION: 155
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goats. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain.
You deploy a Microsoft Entra tenant.
Another administrator configures the domain to synchronize to the Microsoft Entra tenant.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.
You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.
Solution: From Microsoft Entra Connect, you modify the filtering settings.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)

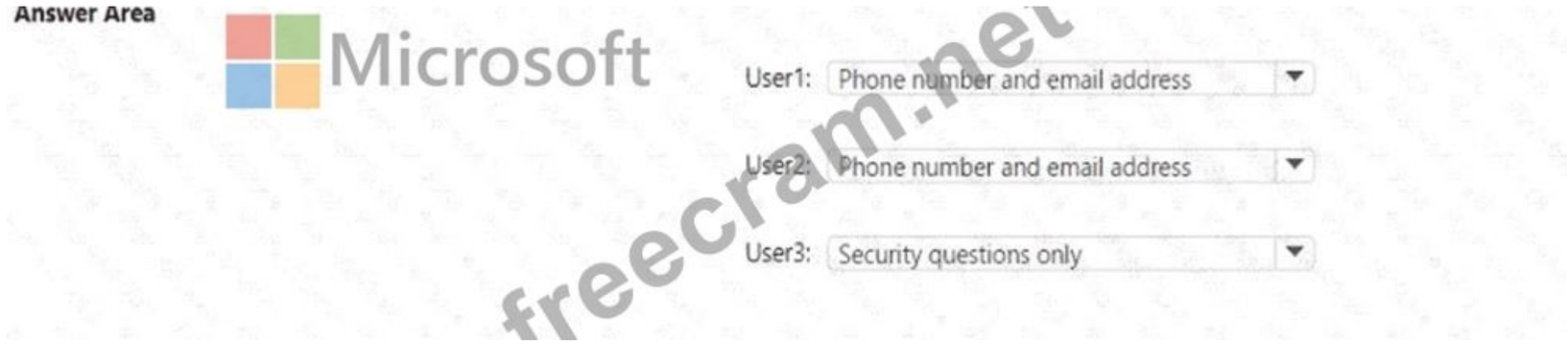
NEW QUESTION: 156
You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.
What information must be configured for each user before the user can perform a self-service password reset?
To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:



NEW QUESTION: 157
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)
You need to create a trusted location and a conditional access policy.

NEW QUESTION: 158
Your company has a Microsoft Entra tenant that contains the users shown in the following table.

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

The tenant includes a security group named Admin1. Admin1 will be used to manage administrative accounts.
External collaboration settings have default configuration.
You need to identify which users can perform the following administrative tasks:

Answer:

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

NEW QUESTION: 159
Your network contains an Active Directory domain and a Microsoft Entra tenant.
The network uses a firewall that contains a list of allowed outbound domains.

You begin to implement directory synchronization, but it fails.
The firewall currently allows only:
* microsoft.com
* office.com
You need to ensure that directory synchronization completes successfully.
What is the best approach to achieve the goal?
A. Deploy a Microsoft Entra Connect Sync sync server in staging mode.
B. From the firewall, modify the list of allowed outbound domains.
C. From Microsoft Entra Connect, modify the Customize synchronization options task.
D. From the firewall, allow the IP address range of the Azure data center for outbound communication.
Answer: (SHOW ANSWER)

NEW QUESTION: 160
You have a Microsoft 365 IS subscription and use Microsoft Defender for Cloud Apps. You register a cloud app named App1 in Microsoft Entra 10. You need to create an access policy for Appl. What should you do first?

A. Add a security Information and event management (SIEM) agent to Defender for Cloud Apps.
B. Create an app tag for App1.
C. Deploy Conditional Access AppControl toApp1.
D. Configure an app connector to Defender for Cloud Apps.
Answer: (SHOW ANSWER)

NEW QUESTION: 161
You have a Microsoft 365 E5 tenant that contains the resources shown in the following table.

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

To which resources can you apply a sensitivity label by using an auto-labeling policy?
A. Mailbox1 and Site1 only
B. Mailbox1, Account1, and Site1 only
C. Account1 and Site1 only
D. Mailbox1, Account1, Site1, and Channel1
E. Account1, Site1, and Channel1 only
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

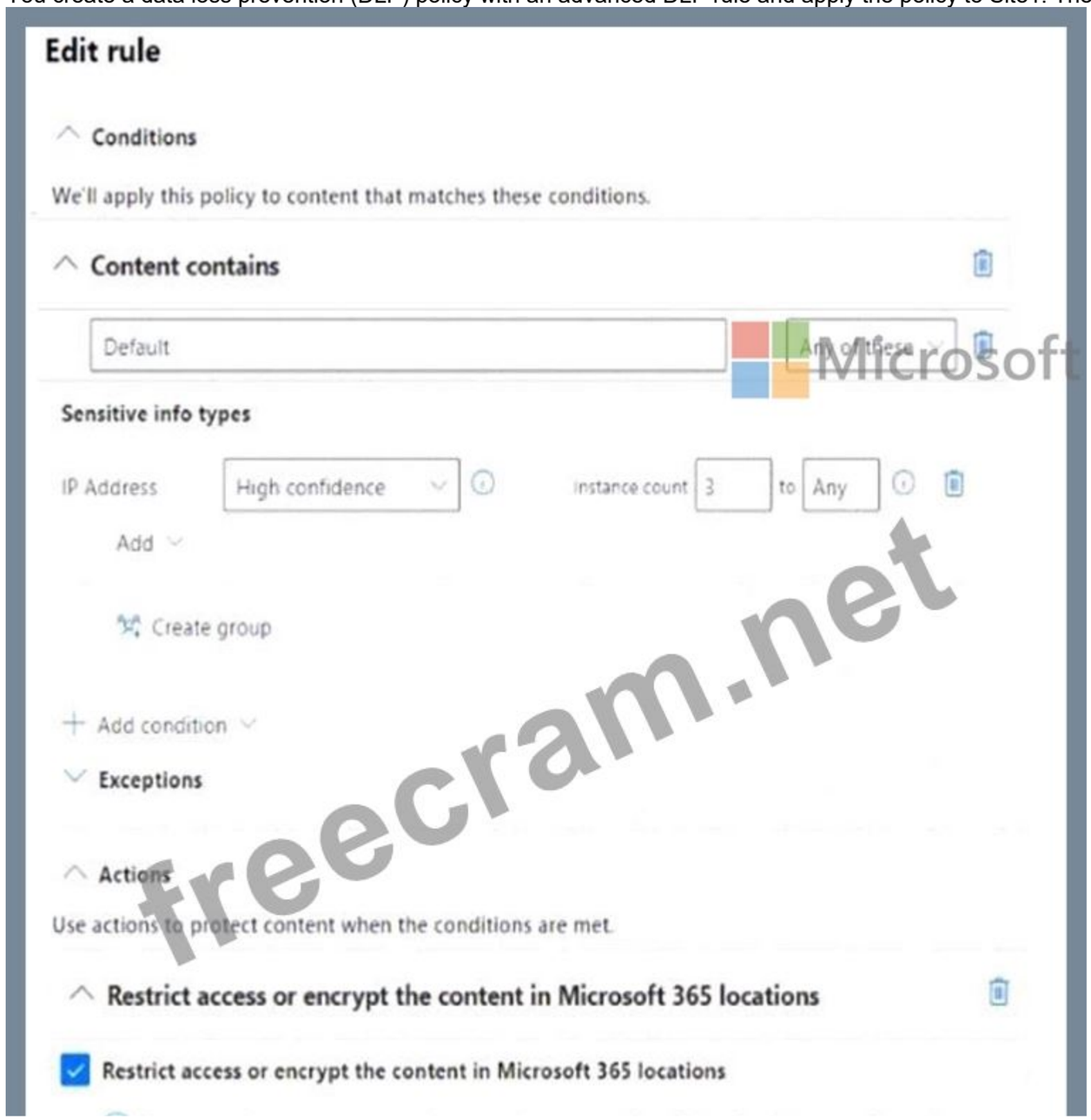
NEW QUESTION: 162
You have a Microsoft 365 E5 subscription that contains a SharePoint site named Site1. Site1 contains the files shown in the following table.

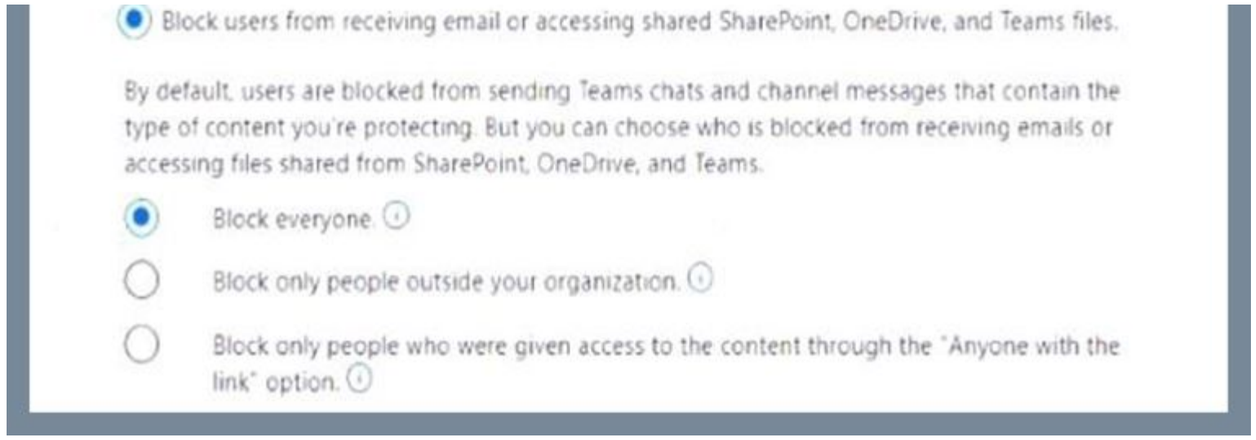
Name	Number of IP addresses in the file
File1	2
File2	5

You have the users shown in the following table.

Name	Role
User1	Site owners for Site1
User2	Site members for Site1
Admin1	SharePoint admins

You create a data loss prevention (DLP) policy with an advanced DLP rule and apply the policy to Site1. The DLP rule 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.

Answer Area

Statements	Yes	No
User1 can open File2.	○	○
User2 can open File1.	○	○
Admin1 can open File2.	○	○

Answer:

Explanation:

User1 can open File2: No

User2 can open File1: Yes

Admin1 can open File2: Yes

User1 can open File2: No

The DLP policy specifies that if a file contains 3 or more IP addresses, access to that content should be restricted. File2 contains 5 IP addresses, which exceeds the threshold set by the DLP policy. Therefore, User1, who is a site owner, will not be able to access File2 because it matches the conditions set in the DLP rule to block access.

User2 can open File1: Yes

File1 contains only 2 IP addresses, which is below the threshold of 3 set by the DLP policy. Since the DLP policy does not apply to files with fewer than 3 IP addresses, User2, who is a site member, can access File1 without any restrictions.

Admin1 can open File2: Yes

Admin1 is part of the SharePoint admins group, which typically has elevated privileges. Despite the DLP rule, SharePoint admins are generally not restricted by the same DLP rules that apply to regular

users. Therefore, Admin1 can access File2.

NEW QUESTION: 163

You have a Microsoft 365 subscription.

You need to be notified to your personal email address when a Microsoft Exchange Online service issue occurs. What should you do?

A. From the Microsoft 365 admin center, update the technical contact details.

B. From the Microsoft 365 admin center, customize the Service health settings.

C. From the Exchange admin center, create a contact.

D. From the Microsoft Outlook client configure an Inbox rule.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 164

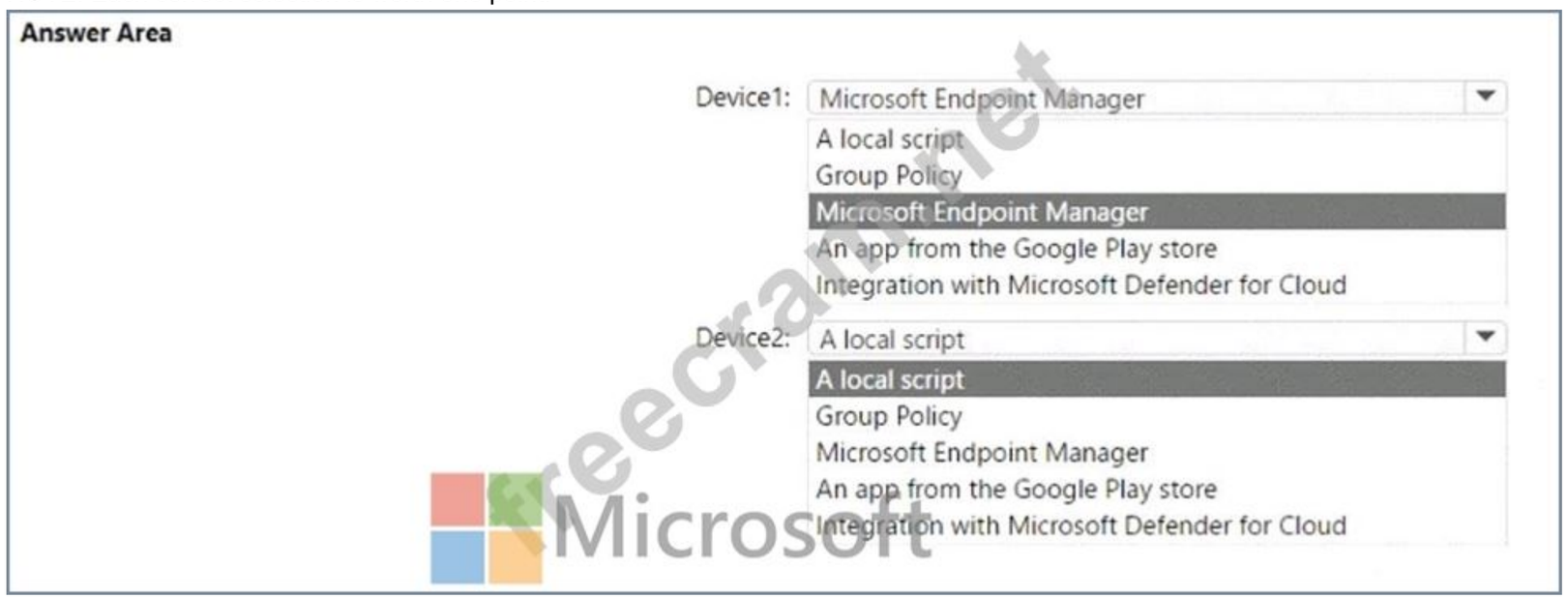
You have a Microsoft 365 E5 subscription that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

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

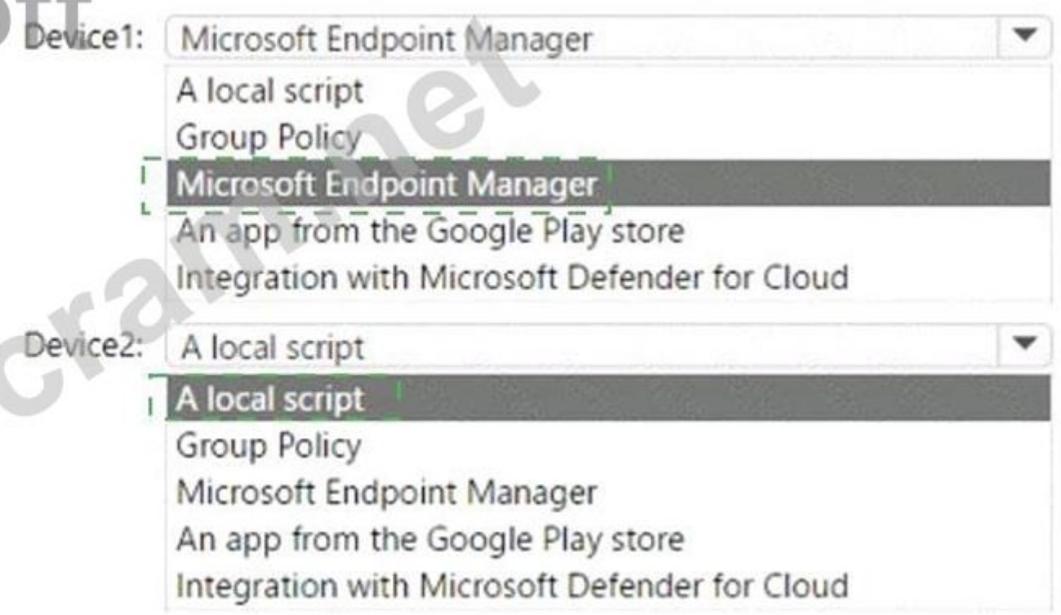
What should you use to onboard each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Answer Area



Explanation:

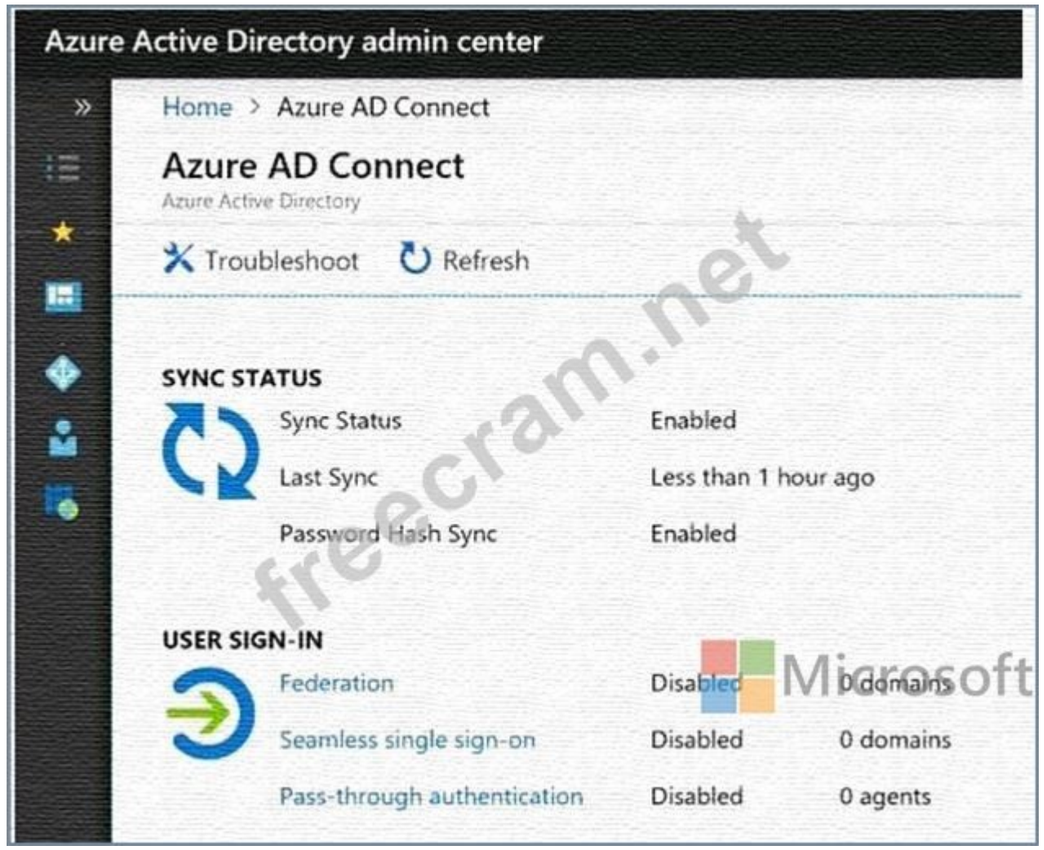
Answer Area

NEW QUESTION: 165

HOTSPOT

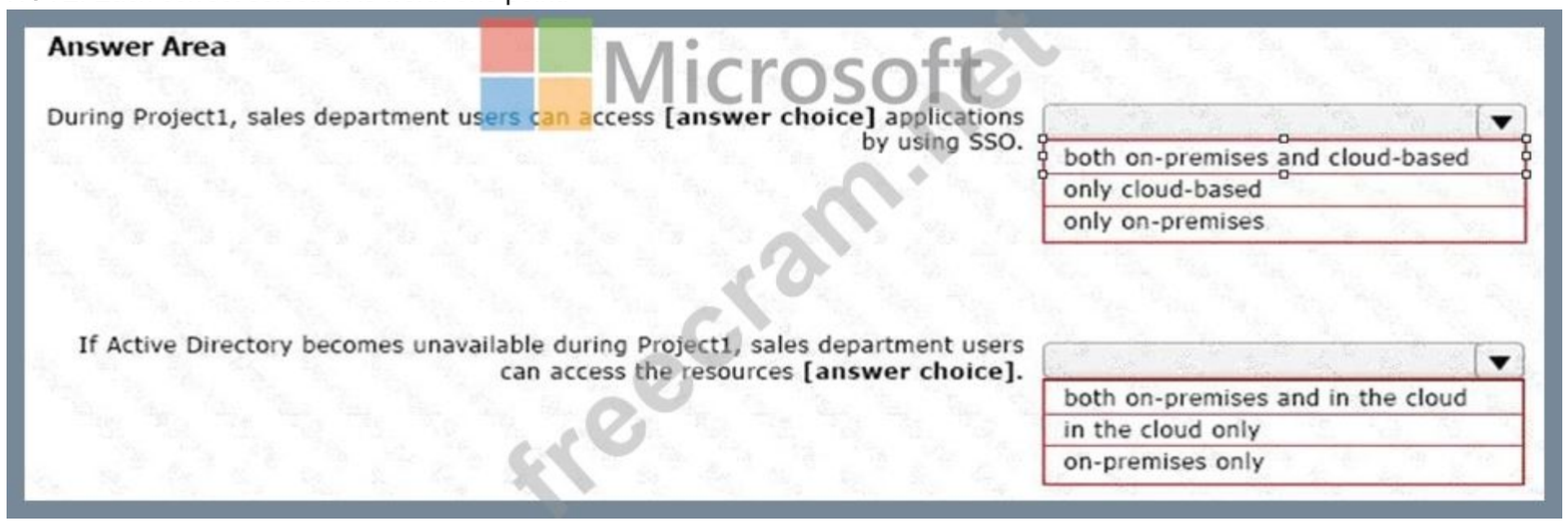
You create the Microsoft 365 tenant.

You implement Azure AD Connect 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:

Answer Area

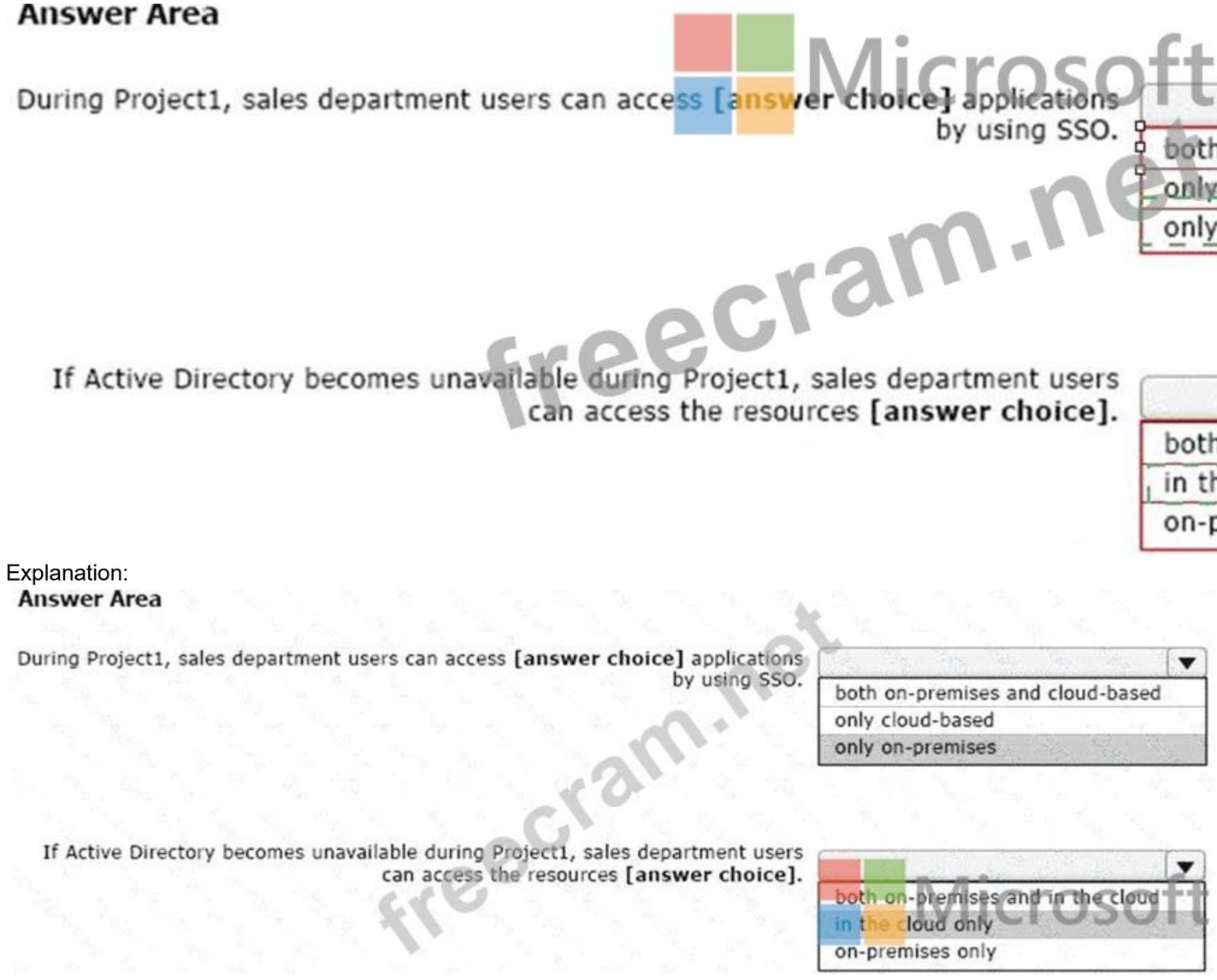
During Project1, sales department users can access [answer choice] applications by using SSO.

- both on-premises and cloud-based
- only cloud-based
- only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources **[answer choice]**.

- both on-premises and in the cloud
- in the cloud only
- on-premises only

Explanation:



Box 1: only on-premises

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

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

Box 2: in the cloud only

NEW QUESTION: 166

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. all the domains in the subscription

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

C. only Sub1.contoso221018.onmicrosoft.com

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

Answer: (SHOW ANSWER)

NEW QUESTION: 167

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

Name	Platform
Device1	Windows 11
Device2	macOS
Device3	Android
Device4	Linux

All the devices are onboarded to Microsoft Defender for Endpoint. You plan to deploy Endpoint data loss prevention (Endpoint DLP) policies. Which devices can be protected by using the DLP policies?

A. Device1 only

B. Device1, Device3, and Device 4 only

C. Device1, Device2, and Device 3 only

D. Device1, Device2, Device3, and Device4

E. Device1 and Device2 only

Answer: (SHOW ANSWER)

NEW QUESTION: 168

You have a Microsoft 365 E5 subscription.

You plan to create the data loss prevention (DLP) policies shown in the following table.

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

You need to create DLP rules for each policy.

Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

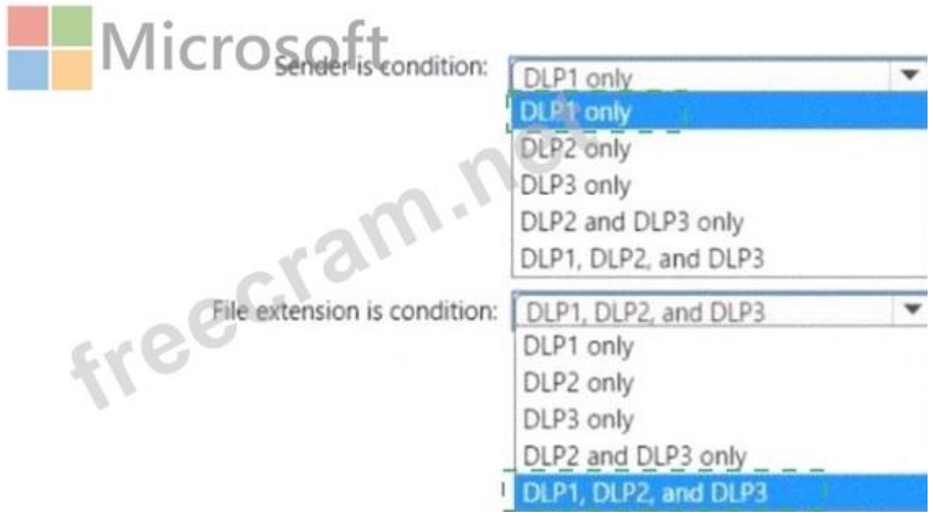
Answer Area

Sender is condition: DLP1 only
- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

File extension is condition: DLP1, DLP2, and DLP3
- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

Answer:

Answer Area



Explanation:

Answer Area

NEW QUESTION: 169

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

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

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

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

The policies use the settings shown in the following table.

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

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

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

Answer:

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

Explanation:

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

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

NEW QUESTION: 170

You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP).
You need to create a detection exclusion in Azure ATP.
Which tool should you use?

A. the Security & Compliance admin center
B. Microsoft Defender Security Center
C. the Microsoft 365 admin center
D. the Azure Advanced Threat Protection portal
E. the Cloud App Security portal

Answer: (SHOW ANSWER)

Reference:
https://docs.microsoft.com/en-us/defender-for-identity/what-is
https://docs.microsoft.com/en-us/defender-for-identity/excluding-entities-from-detections

NEW QUESTION: 171
You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

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

Per-user multifactor authentication is configured to use 131.107.5.0/24 as trusted IPs.
The tenant contains the named locations shown in the following table.

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

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

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

Answer:

Answer Area

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

Explanation:

NEW QUESTION: 172

You have a Microsoft 365 subscription.

You suspect that several Microsoft Office 365 applications or services were recently updated.

You need to identify which applications or services were recently updated.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. From the Microsoft 365 admin center review the Service health blade

B. From the Microsoft 365 admin center, review the Message center blade.

C. From the Microsoft 365 admin center review the Products blade.

D. From the Microsoft 365 Admin mobile agg, review the messages.

Answer: (SHOW ANSWER)

The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where Microsoft posts official messages with information including new and changed features, planned maintenance, or other important announcements.

The messages displayed in the Message center can also be viewed by using the Office 365 Admin mobile app.

Reference:

https://docs.microsoft.com/en-us/office365/admin/manage/message-center

https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app

NEW QUESTION: 173

You have a Microsoft 365 E5 subscription. You create a data loss prevention (DLP) policy named DLP1.
You need to ensure that endpoint rule actions are available in the advanced DLP rules for DLP1. To which location should you apply DLP1?
A. OneDrive accounts
B. Instances
C. Devices
D. On-premises repositories
Answer: C (LEAVE A REPLY)

NEW QUESTION: 174
You have a Microsoft 365 E5 subscription.
You need to ensure that an alert is generated when an app is registered in Microsoft Entra and is assigned the Directory.Readwrite.ALL Microsoft Graph permission.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

Explanation:

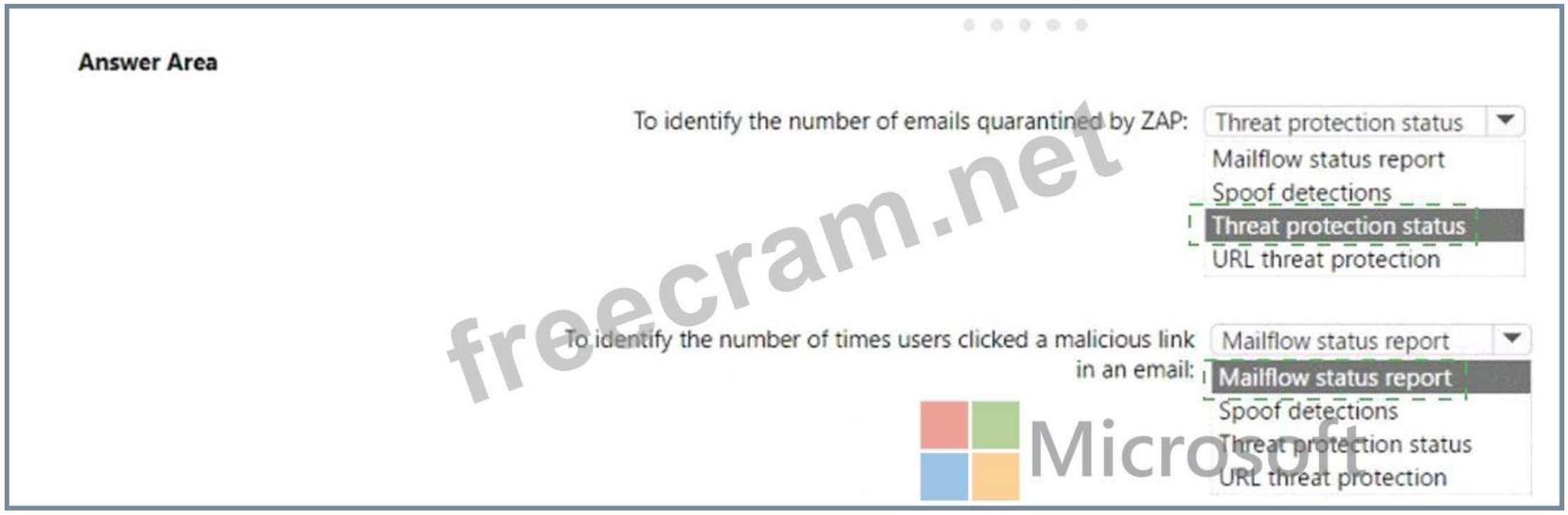
NEW QUESTION: 175
You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps. The subscription contains users that have Windows 11 devices.
You need to use the Cloud Discovery snapshot report to analyze cloud app usage on the devices. What should you do before generating a report?
A. Create an app discovery policy.
B. Deploy the Azure Monitor Agent on the devices.
C. Create an activity policy.
D. Export traffic logs from firewalls and proxies.
Answer: (SHOW ANSWER)

NEW QUESTION: 176
You have a Microsoft 365 E5 subscription.
You create a new data loss prevention (DLP) policy named DLP1 that protects financial data from being shared by using Microsoft Teams messages. You apply DLP1 to the users in the finance department.
An incident is raised when a finance department user named User1 shares financial data in a Teams channel that includes external members.
When User1 uses Teams to send the same message in a 1:1 chat or a private channel, the message is blocked as expected.
You need to ensure that User1 is prevented from sharing financial data in Teams channels that include external members.
What should you do?
A. Edit the Locations settings of DLP1.

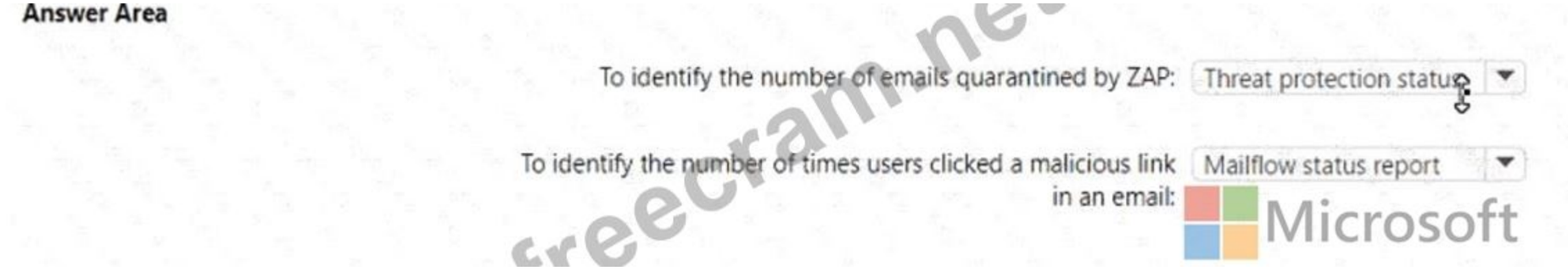
B. Edit the policy rules of DLP1.
C. Edit the settings of the team that contains the channel.
D. Modify the licenses assigned to User1.
Answer: (SHOW ANSWER)

NEW QUESTION: 177
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.
The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.
You need to identify the following information:
* The number of email messages quarantined by zero-hour auto purge (ZAP)
* The number of times users clicked a malicious link in an email message Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer:



Explanation:



NEW QUESTION: 178

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*

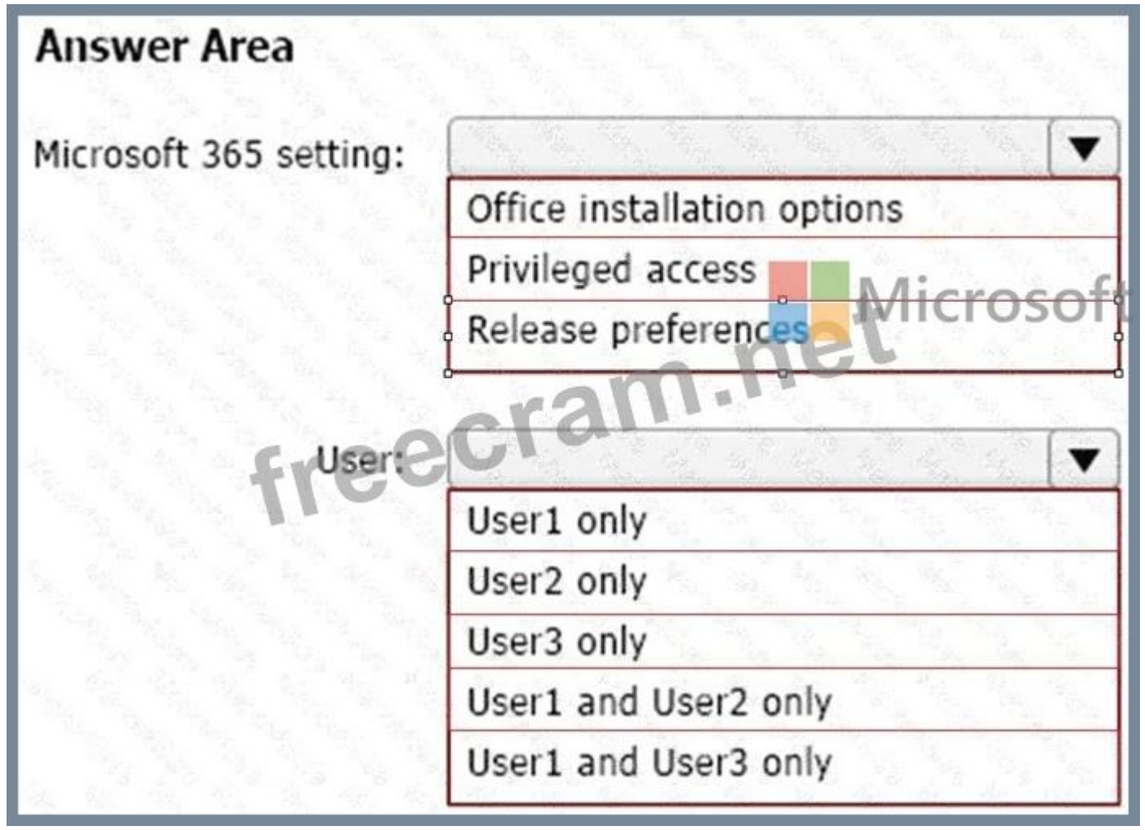
You plan to provide User4 with early access to Microsoft 365 feature and service updates.

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:

Answer Area

Microsoft

Microsoft 365 setting:

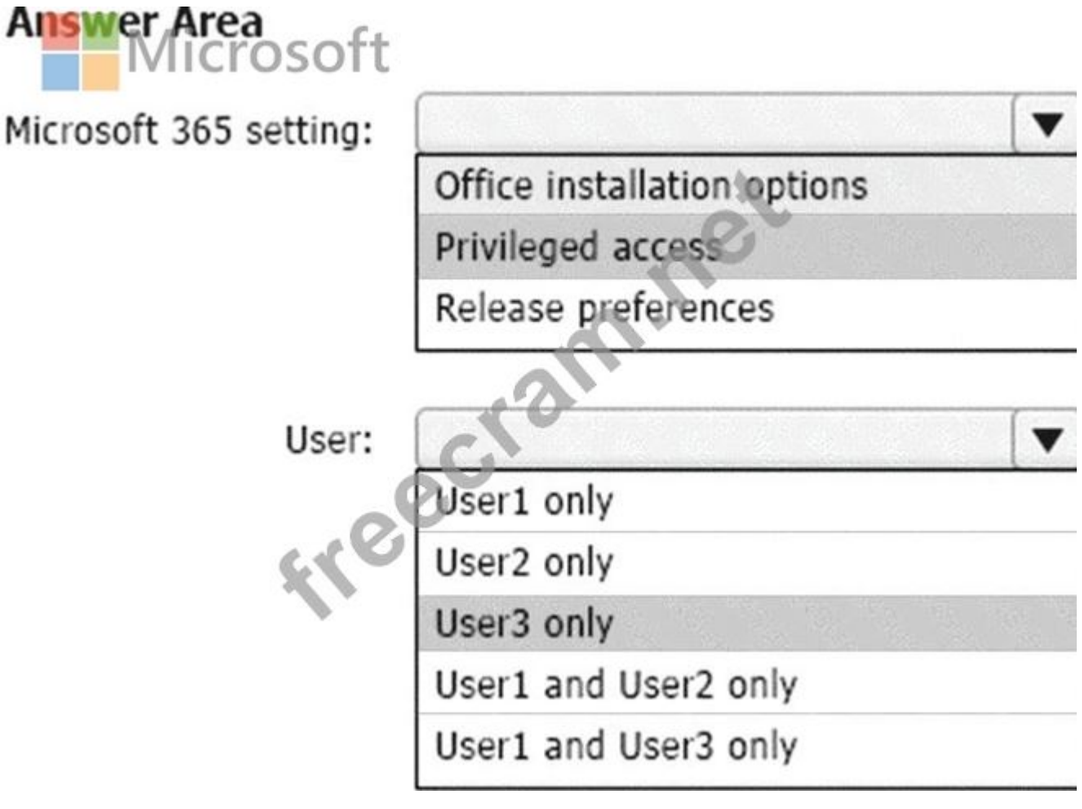
- Office installation options
- Privileged access
- Release preferences

User:

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

Explanation:

Answer Area



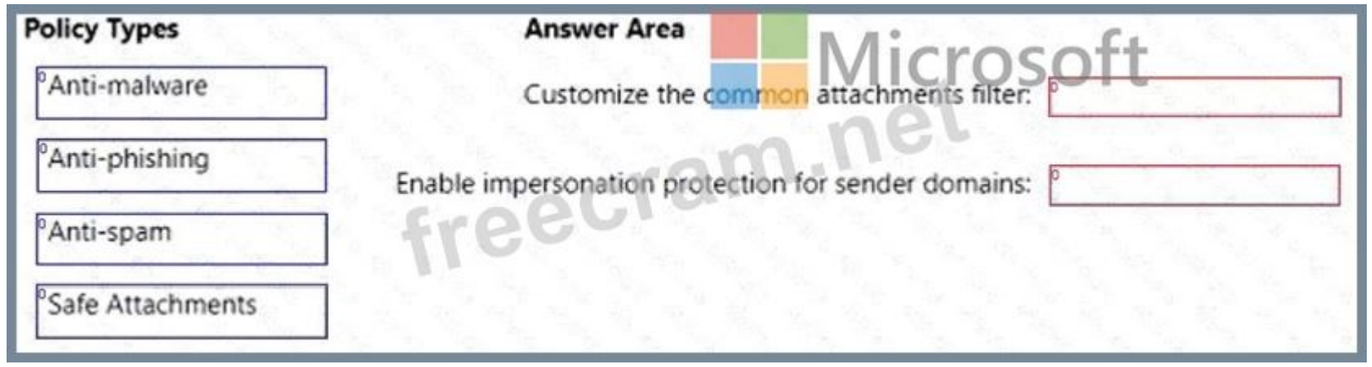
NEW QUESTION: 179
You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:
* Windows 10
* Android
* iOS
On which devices can you configure the Endpoint DLP policies?
A. Windows 10 only
B. Windows 10 and Android only
C. Windows 10 and macO Sonly
D. Windows 10, Android, and iOS
Answer: (SHOW ANSWER)
Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide

NEW QUESTION: 180
You have a Microsoft 365 E5 subscription.
You create the users shown in the following table.

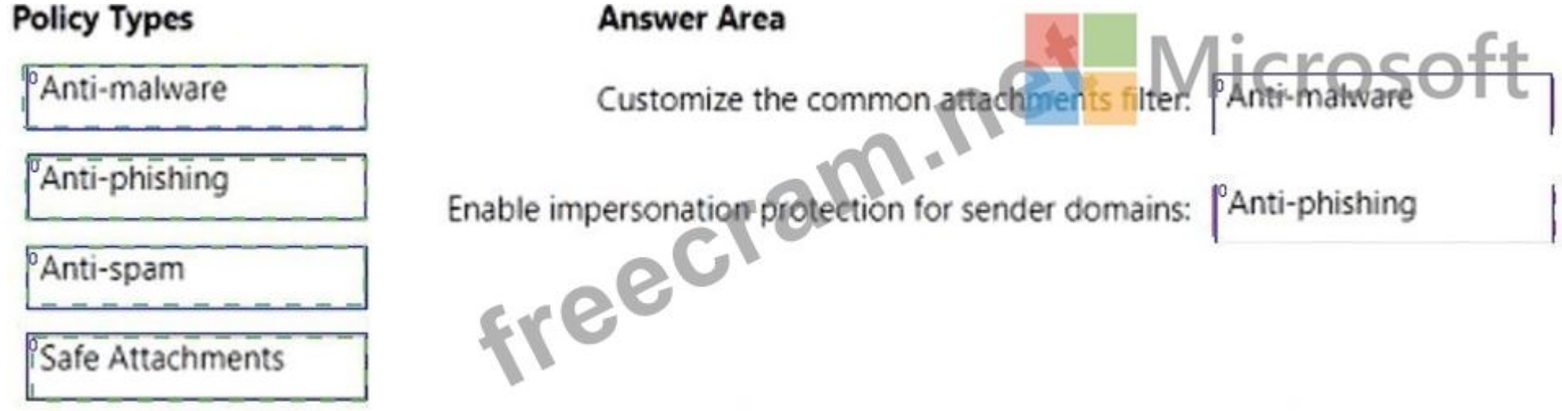
Name	Assigned role
Admin1	Security Administrator
Admin2	Security Operator
Admin3	Security Reader

You plan to use Microsoft Entra ID Protection.
Which users will be added automatically to the Users at risk detected alerts list?
A. Admin1 only
B. Admin1, Admin2, and Admin3
C. Admin2 only
D. Admin1 and Admin2 only
E. Admin1 and Admin3 only
Answer: (SHOW ANSWER)

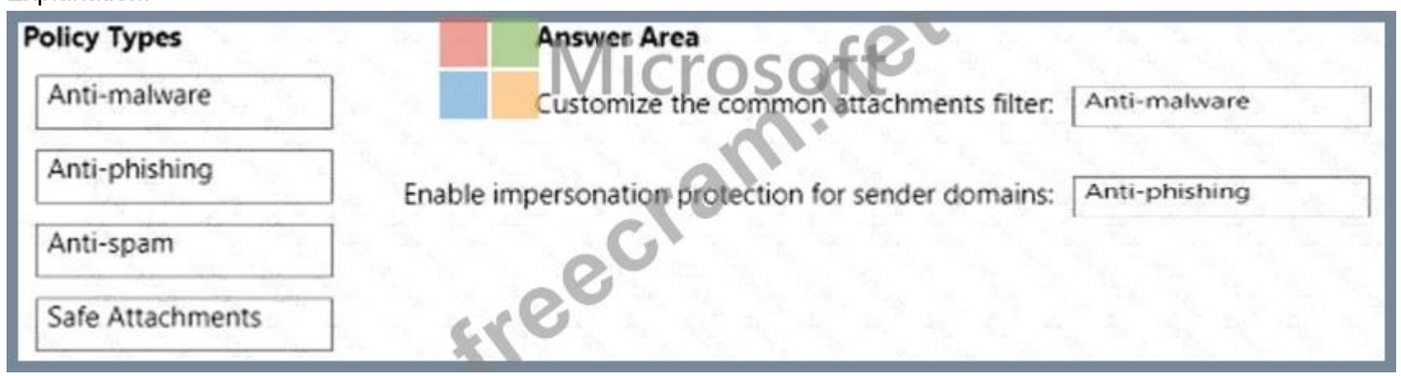
NEW QUESTION: 181
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You need to configure policies to meet the following requirements:
Customize the common attachments filter.
Enable impersonation protection for sender domains.
Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Box 1: Anti-malware

Customize the common attachments filter.

See step 5 below.

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

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

On the Name your policy page, configure these settings:

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

Description: Enter an optional description for the policy.

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

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

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

Protection settings section:

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

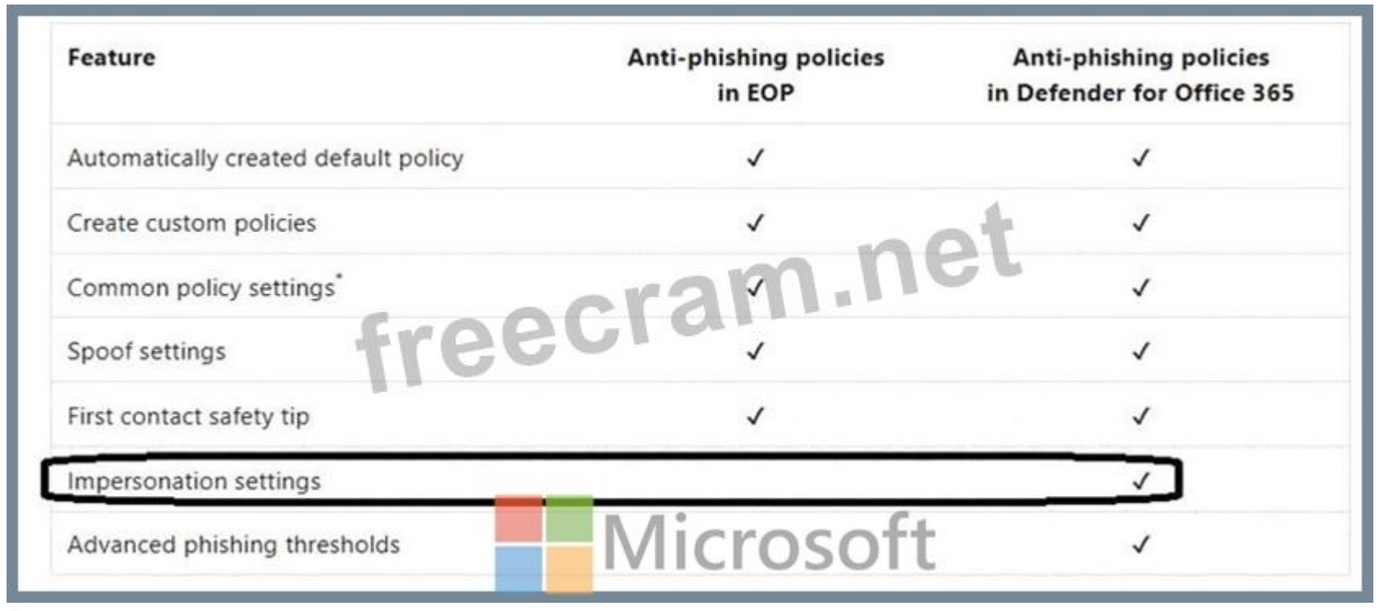
6. Etc.

Box 2: Anti-phishing

Enable impersonation protection for sender domains.

Anti-phishing policies in Microsoft 365

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



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

NEW QUESTION: 182
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: 183
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. Security Reader
B. Global Administrator
C. Owner
D. User Administrator
Answer: (SHOW ANSWER)

NEW QUESTION: 184
You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs.
What should you do?
A. From PowerShell, run the Add-ADSyncConnectorAttnbuteinclusion cmdlet.
B. From the Microsoft Azure AD Connect wizard, select Manage federation.
C. From PowerShell, run the start-ADSyncSyncCycle cmdlet.
D. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.
Answer: (SHOW ANSWER)

NEW QUESTION: 185
You have a Microsoft 365 subscription That contains two administrative units named AU1 and AU2.
The subscription contains the users shown in the following table.

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

The subscription contains the groups shown in the following table.

Name	Members	Administrative unit
Group1	User3	AU2
Group2	User2 User3	AU1

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

Answer Area

Statements	Yes	No
User1 can reset the password of User2.	○	○
User2 can modify the membership of Group1.	○	○
User1 can reset the password of User3.	○	○

Answer:

Explanation:

NEW QUESTION: 186

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

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

What should you configure?

A. group expiration policies

B. access reviews

C. Conditional Access policies

D. retention policies

Answer: (SHOW ANSWER)

NEW QUESTION: 187

You have a Microsoft 365 E5 tenant.

You configure a device compliance policy as shown in the following exhibit.

Compliance settings Edit

Microsoft Defender ATP

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

Device Health

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

System Security

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

Actions for noncompliance Edit

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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.

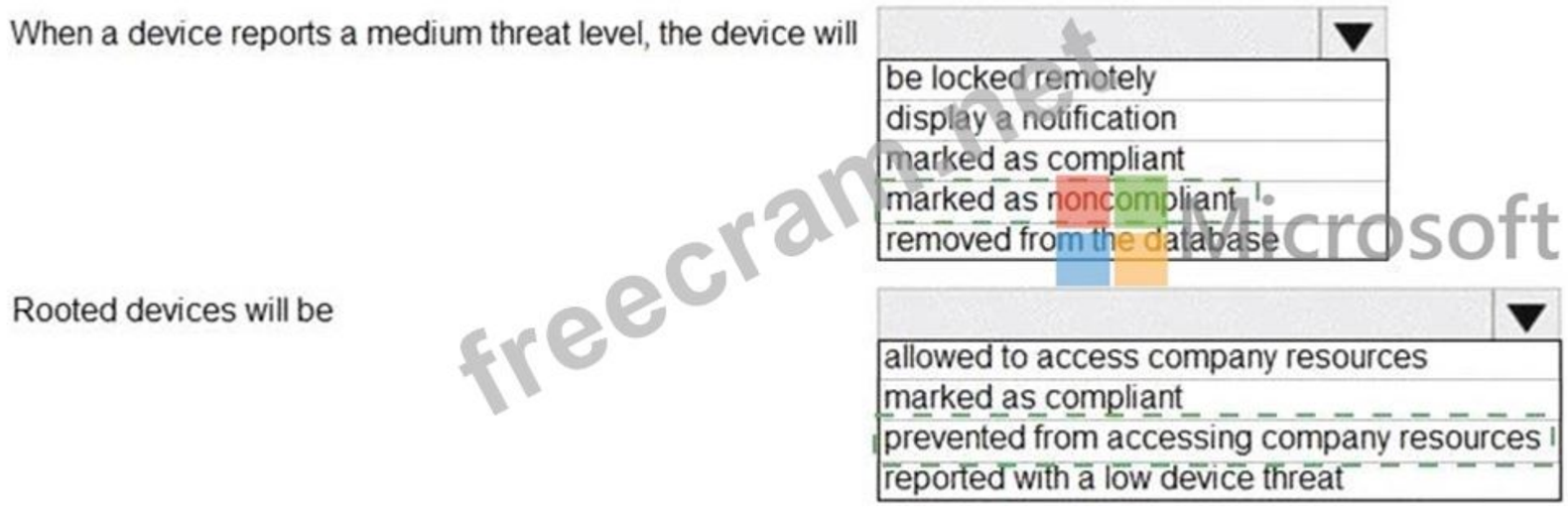
When a device reports a medium threat level, the device will

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

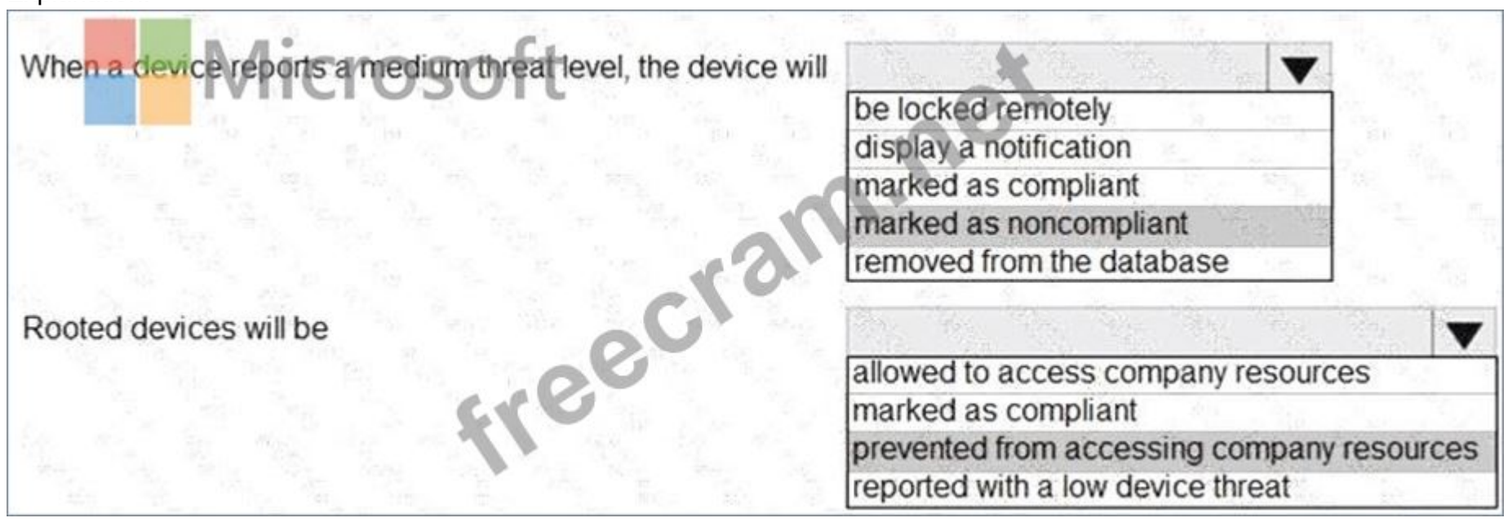
Rooted devices will be

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

Answer:



Explanation:



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

NEW QUESTION: 188
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

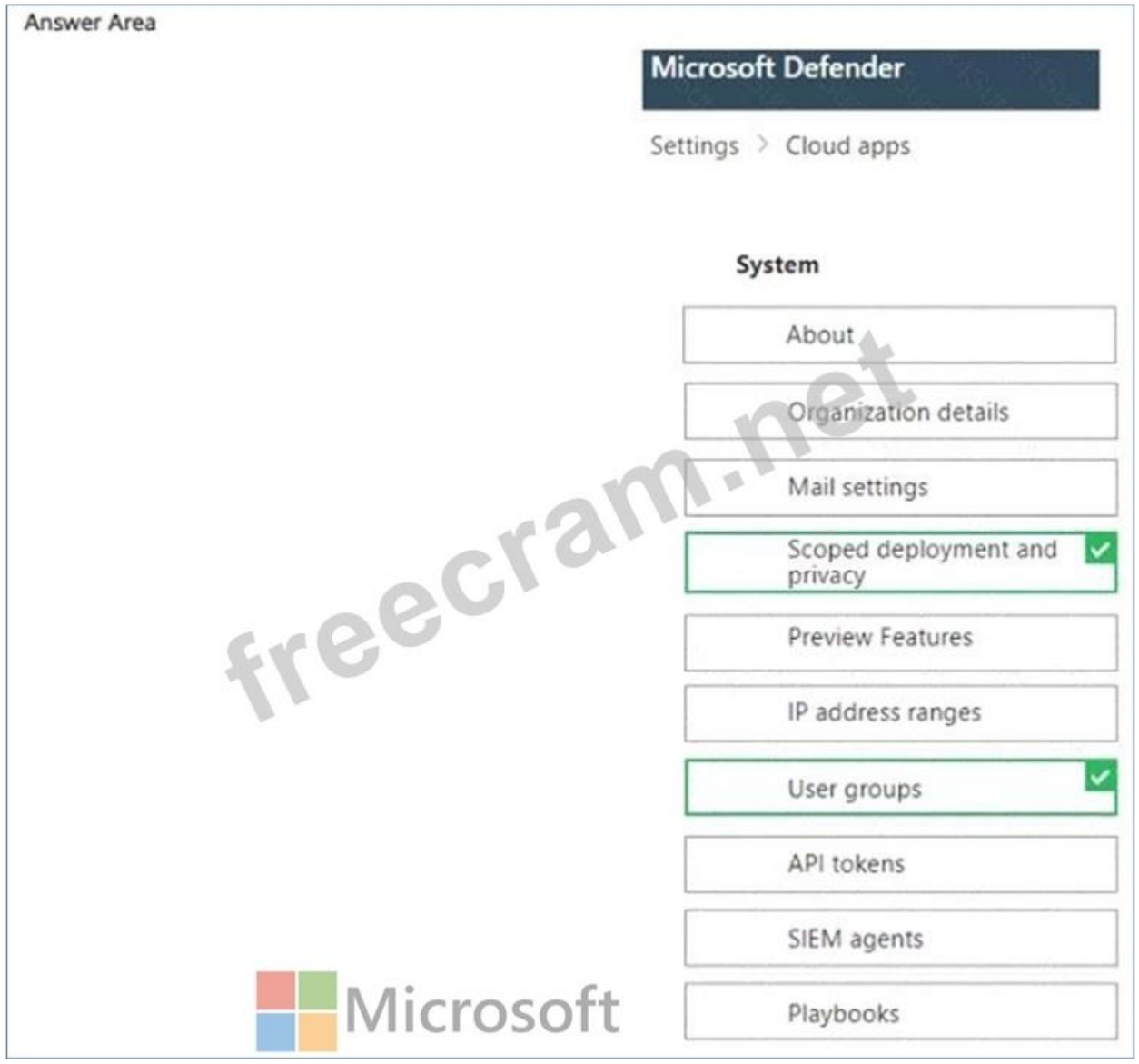
Answer: (SHOW ANSWER)

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: 189

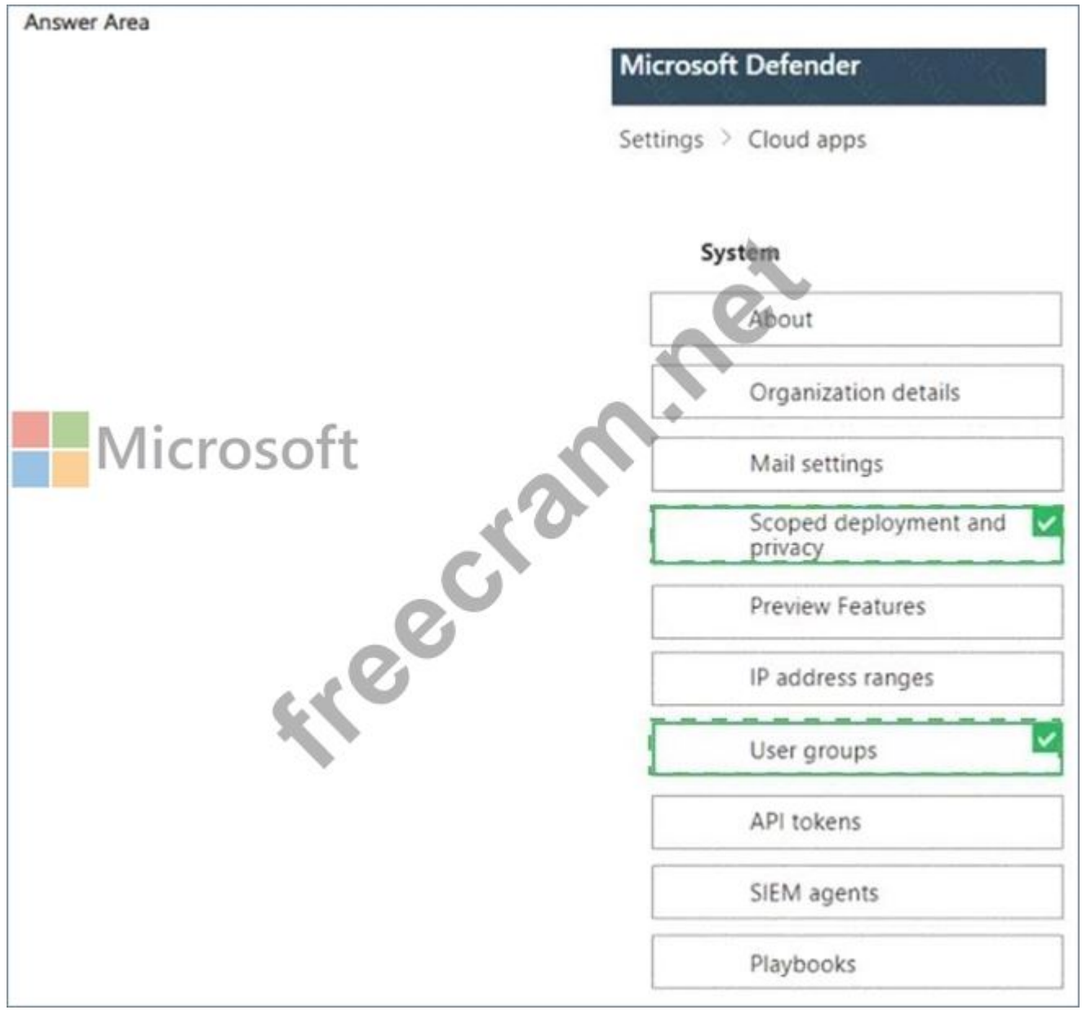
You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table.
User1 reports that after sending 1.000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:
* Which administrators can unblock User1
* What to configure to allow User1 to send at least 2.000 emails per day without being blocked What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



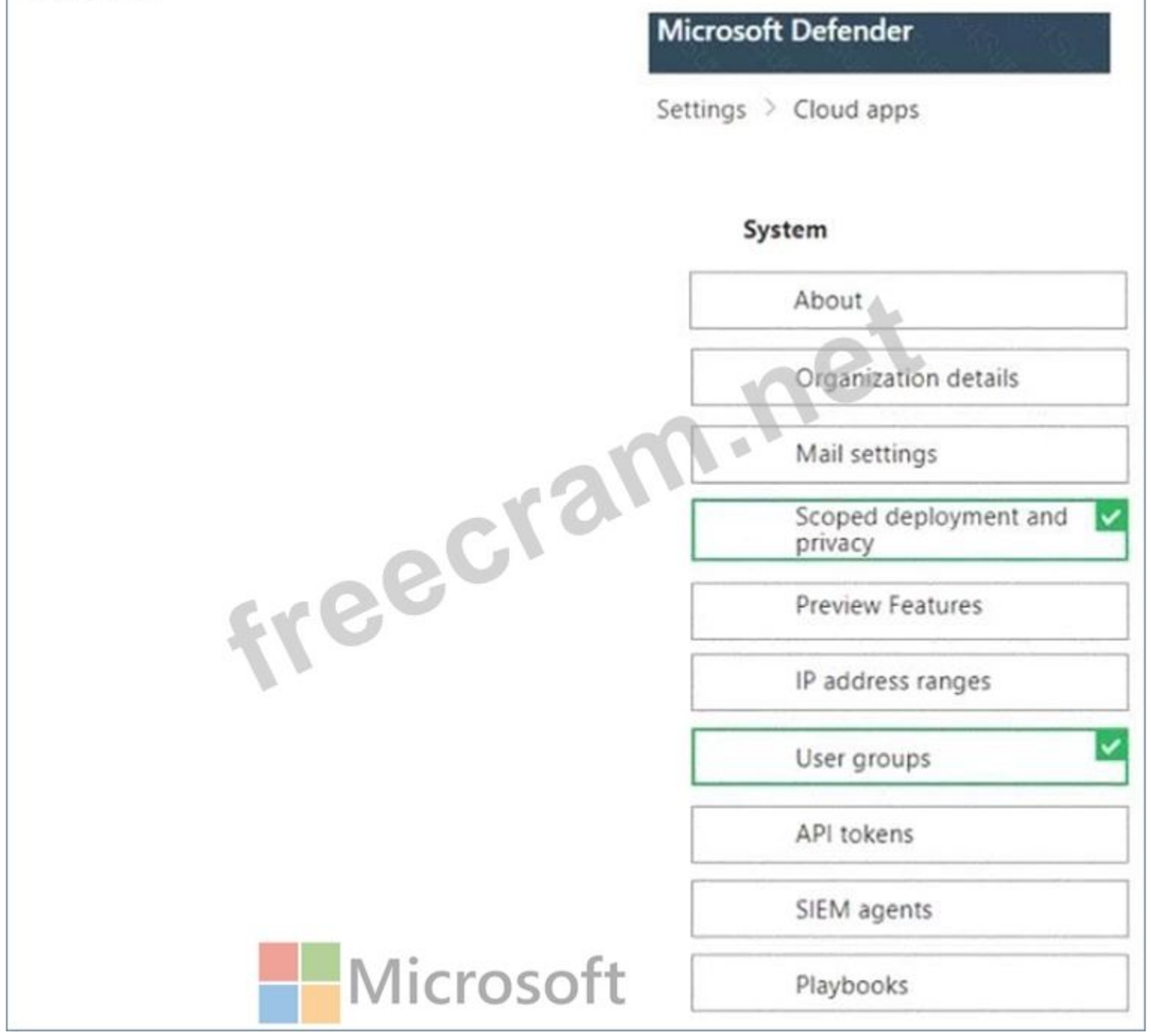
Answer:

Answer Area



Explanation:

Answer Area



NEW QUESTION: 190

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

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

You need to configure group-based licensing to meet the following requirements:

To all users, deploy an Office 365 E3 license without the Power Automate license option.

To all users, deploy an Enterprise Mobility + Security E5 license.

To the users in the research department only, deploy a Power BI Pro license.
To the users in the marketing department only, deploy a Visio Plan 2 license.
What is the minimum number of deployment groups required?
A. 1
B. 2
C. 3
D. 4
E. 5
Answer: (SHOW ANSWER)
One for all users, one for the research department, and one for the marketing department.
Note: What are Deployment Groups?
With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers on- premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.
Reference:
https://devblogs.microsoft.com/devops/deployment-groups-is-now-generally-available-sharing-of-targets-and- more

NEW QUESTION: 191
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)
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: 192
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 Defender for CloudUse the

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

NEW QUESTION: 193
You have a Microsoft 365 E5 subscription and use Microsoft Defender for Endpoint Defender for Endpoint has tamper protection enabled.
You have a device named Device1 that is onboarded to Defender for Endpoint. You need to configure antivirus and real-time protection for Device1.
What should you do in the Microsoft Defender portal?
A. Create a device group.
B. Initiate a live response session.
C. Isolate Device1.
D. Enable troubleshooting mode.
Answer: (SHOW ANSWER)

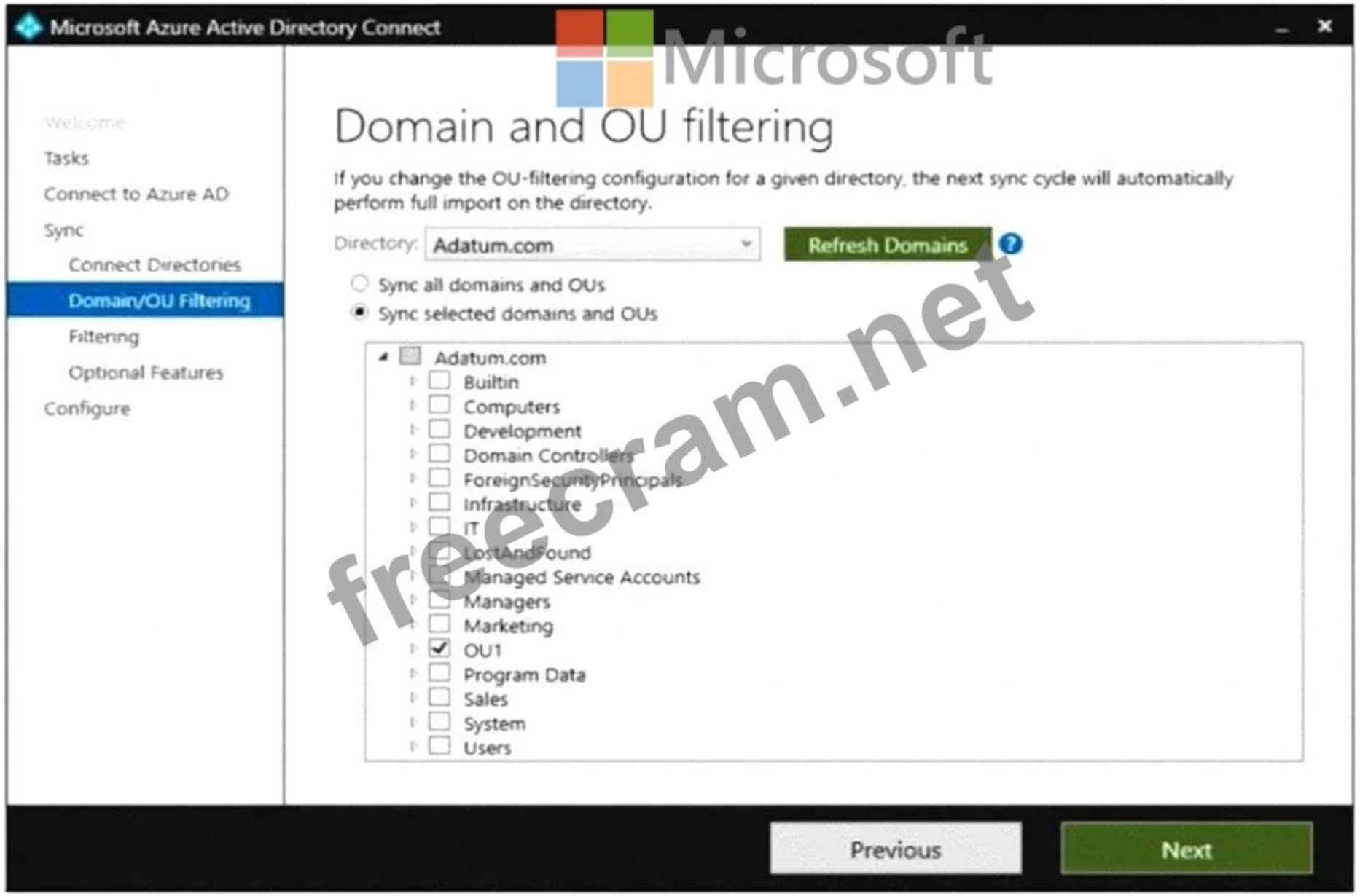
NEW QUESTION: 194
HOTSPOT
Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.
The domain contains the users shown in the following table.

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.

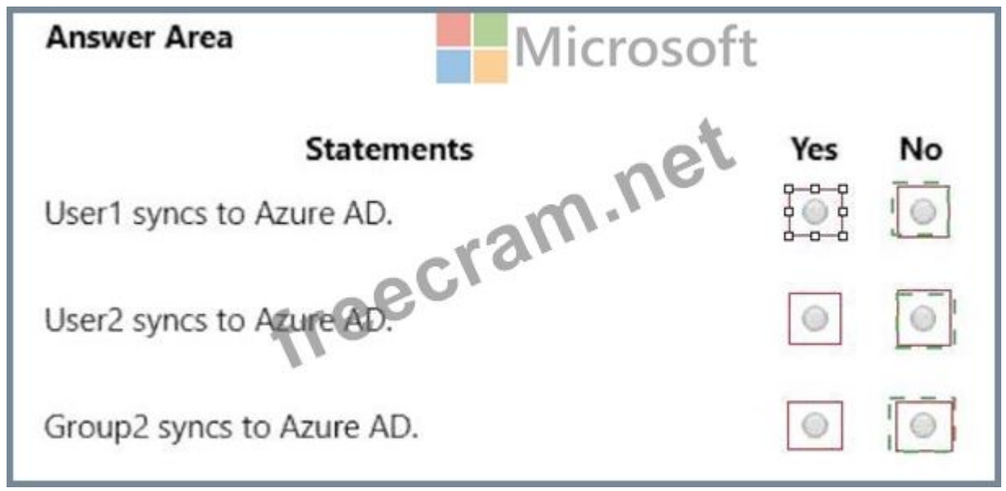
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

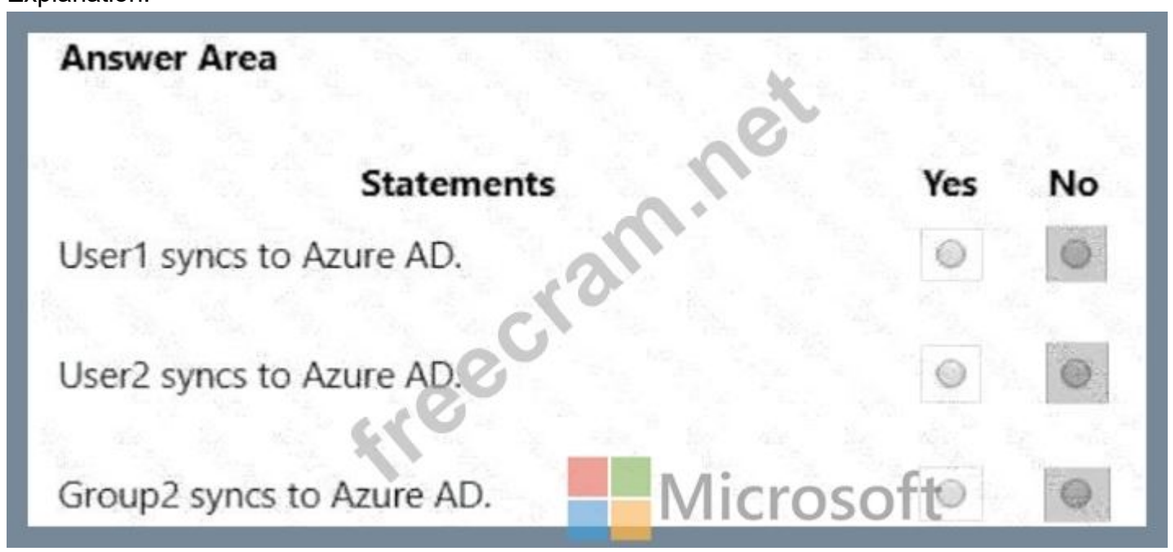
Answer Area

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

Answer:



Explanation:



NEW QUESTION: 195

You have a Microsoft 365 subscription that uses Microsoft Defender XDR

From Automatic remediation in the Microsoft Defender portal, you set Automation level to Semi - require approval for non-temp folders for the endpoints.

You need to identify the impact of the Automation level setting on the endpoints.

Which two actions will occur based on the remediation settings? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Devices will be remediated automatically if a threat is detected in the \windows\ folder.

B. Devices will be remediated automatically if a threat is detected in the \users\"\downloads\" folder.

C. Devices will be remediated automatically if a threat is detected in the \program files (X86) \" folder.

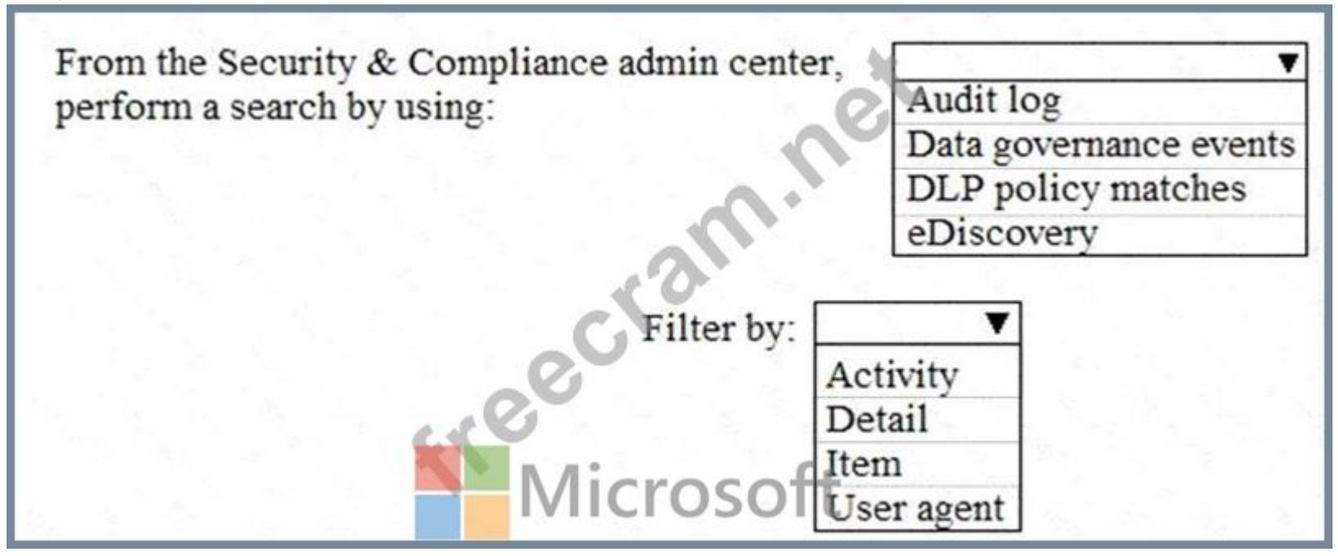
D. Devices will be remediated only after end-user approval.

Answer: A,C (LEAVE A REPLY)

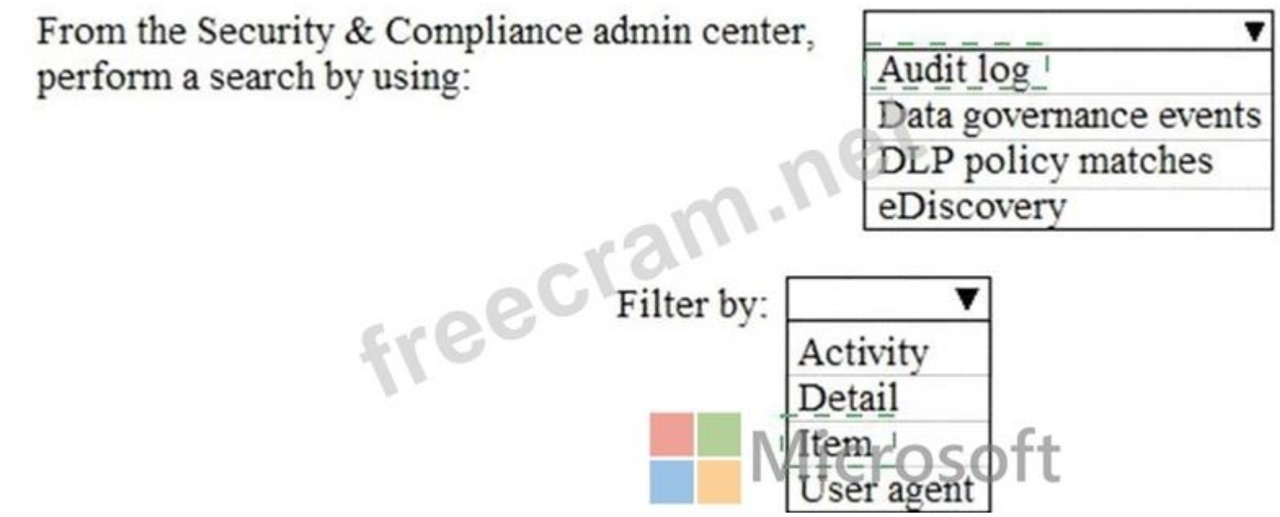
NEW QUESTION: 196

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

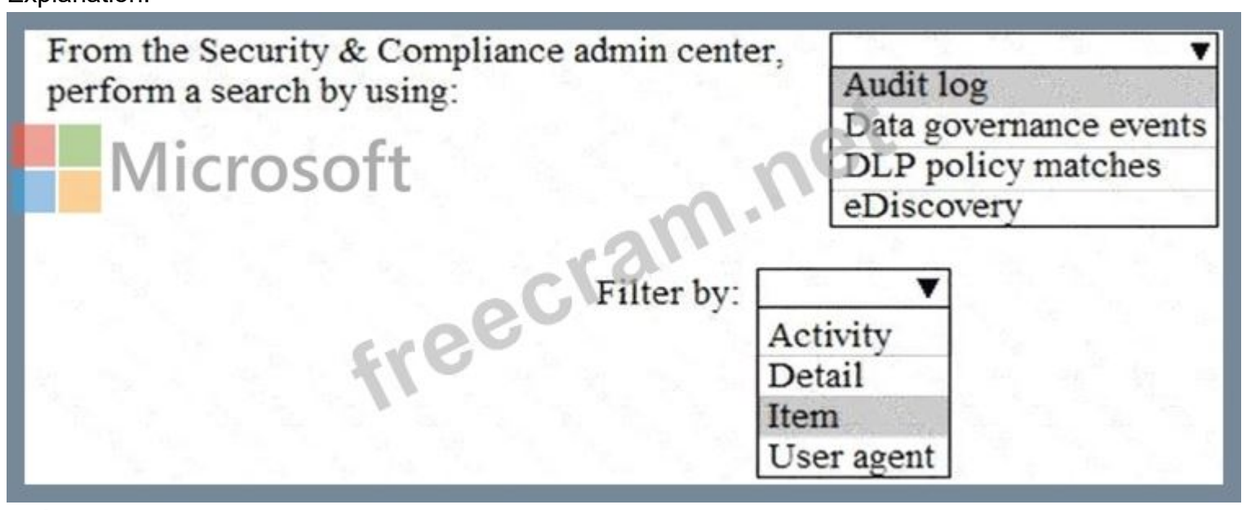
NEW QUESTION: 197
You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



Explanation:



References:

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

Topic 3, Litware Inc.Case Study

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

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

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

To start the case study

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

Overview

General Overviews

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

Environment

Existing Environment

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

Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

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

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

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

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

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

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

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

Problem Statements

Litware identifies the following issues:

Users open email attachments that contain malicious content.

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

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

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

Requirements

Planned Changes

Litware plans to implement the following changes:

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

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

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

Grant User2 permissions to review the audit logs of he litware.com tenant.
Deploy new devices to the Seattle office as shown in the following table.

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

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

NEW QUESTION: 198
You have a Microsoft 365 subscription that contains the users in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.

Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	Group3

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

Answer:

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

Explanation:

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

NEW QUESTION: 199
You have a Microsoft 365 ES subscription.
You integrate Microsoft Defender for Endpoint with Microsoft Intune.
You need to ensure that devices automatically onboard to Defender for Endpoint when they are enrolled In Intune.
Solution: You create an endpoint detection and response (EDR) policy.
Does this meet the goal?
A. No
B. Yes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 200
You have an Azure subscription and a Microsoft 365 E5 subscription.
You are licensed to use Microsoft Defender XDR
You need to monitor activities from suspicious IP addresses and unusual administrative activities in Azure.
What should you use to monitor the activities, and what should you use to integrate Azure with Microsoft Defender XDR? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

NEW QUESTION: 201

Your network contains three Active Directory forests. There are forests trust relationships between the forests.

You create a Microsoft Entra tenant

You plan to sync the on-premises Active Directory to the Microsoft Entra tenant.

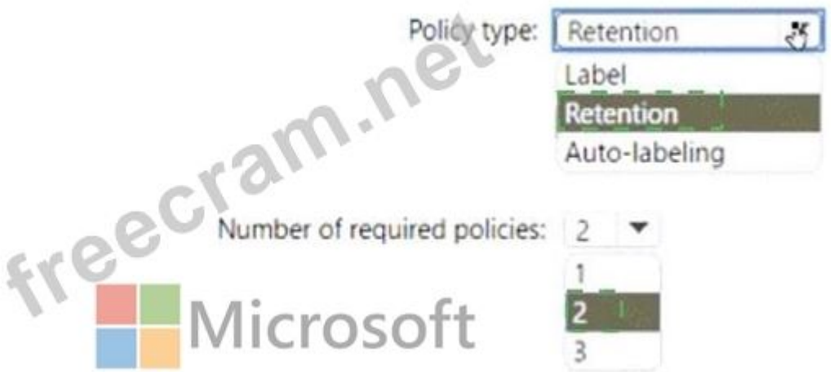
You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete and as quickly as possible if a single server fails.

What should you include in the recommendation?

A. six Microsoft Entra Connect sync servers and three Microsoft Entra Connect sync servers in staging mode
B. three Microsoft Entra Connect sync servers and three Microsoft Entra Connect sync servers in staging mode
C. three Microsoft Entra Connect sync servers and one Microsoft Entra Connect sync server in staging mode
D. one Microsoft Entra Connect sync server and one Microsoft Entra Connect sync server in staging mode
Answer: (SHOW ANSWER)

NEW QUESTION: 202
You need to configure the information governance settings to meet the technical requirements.
Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:
Answer Area



Explanation:

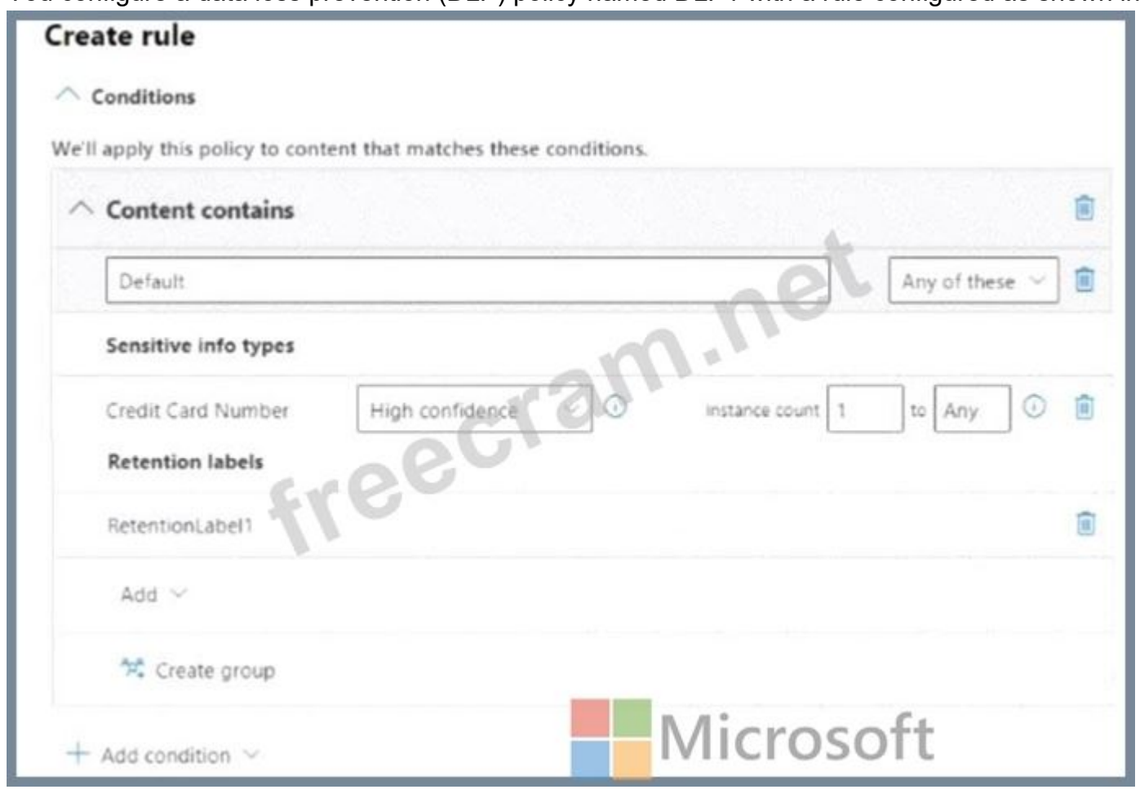
Answer Area

Policy type: Retention

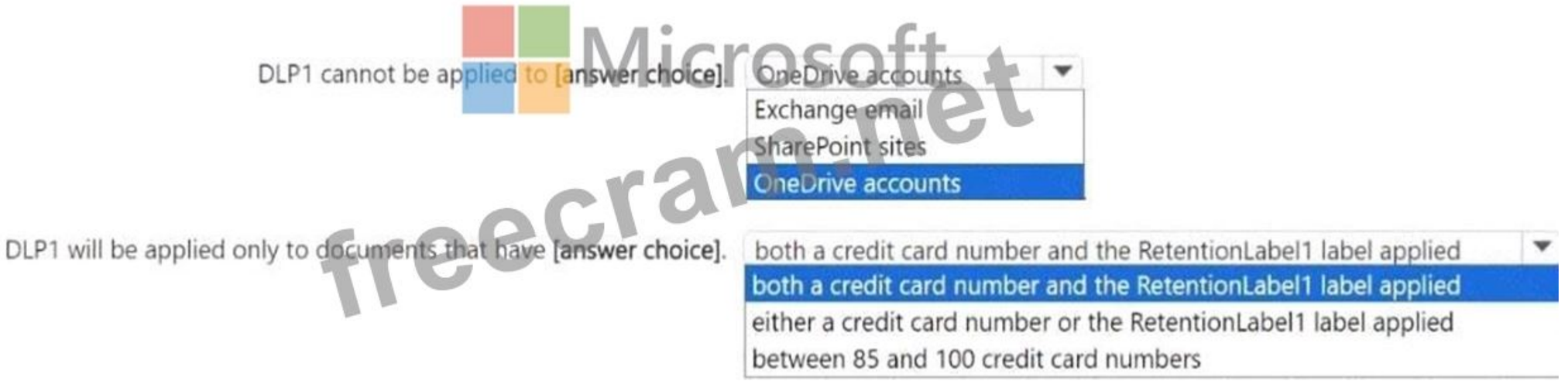
Number of required policies: 2

NEW QUESTION: 203

You configure a data loss prevention (DLP) policy named DLP1 with a rule configured as shown in the following exhibit.

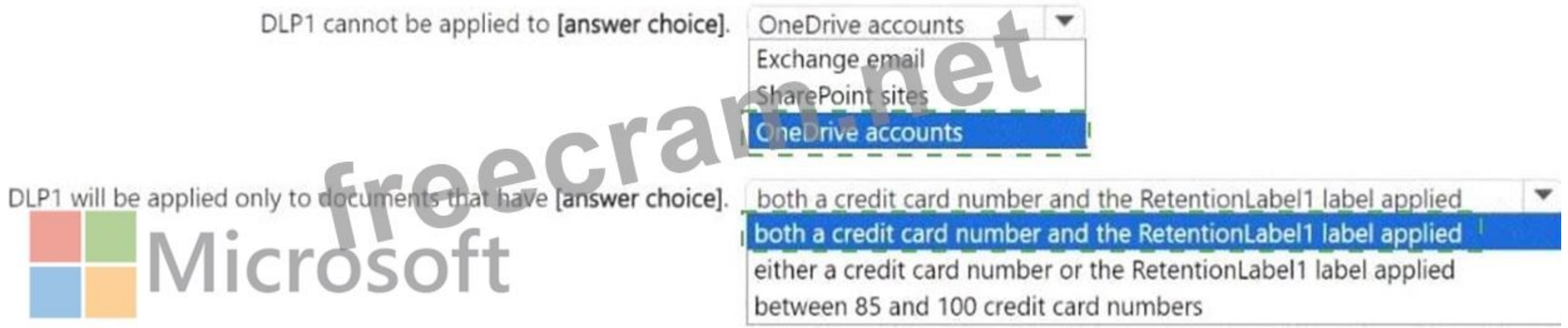


Answer Area

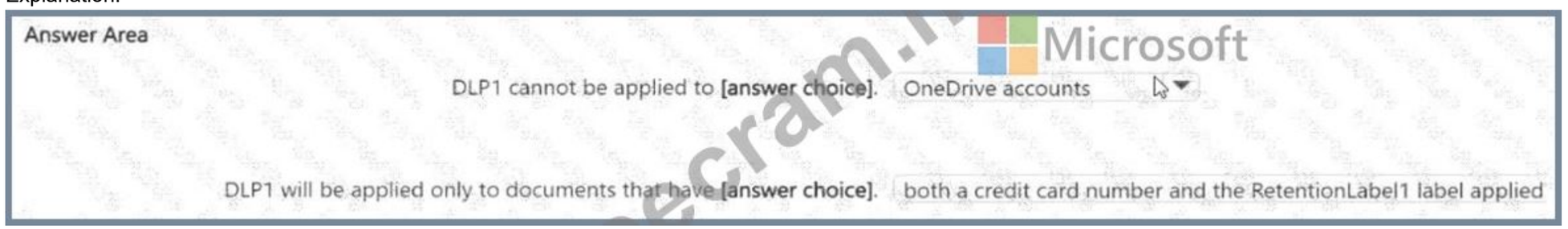


Answer:

Answer Area



Explanation:



NEW QUESTION: 204

You have a Microsoft 365 E5 tenant.

You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.

You need to deploy the policy.

What should you do first?

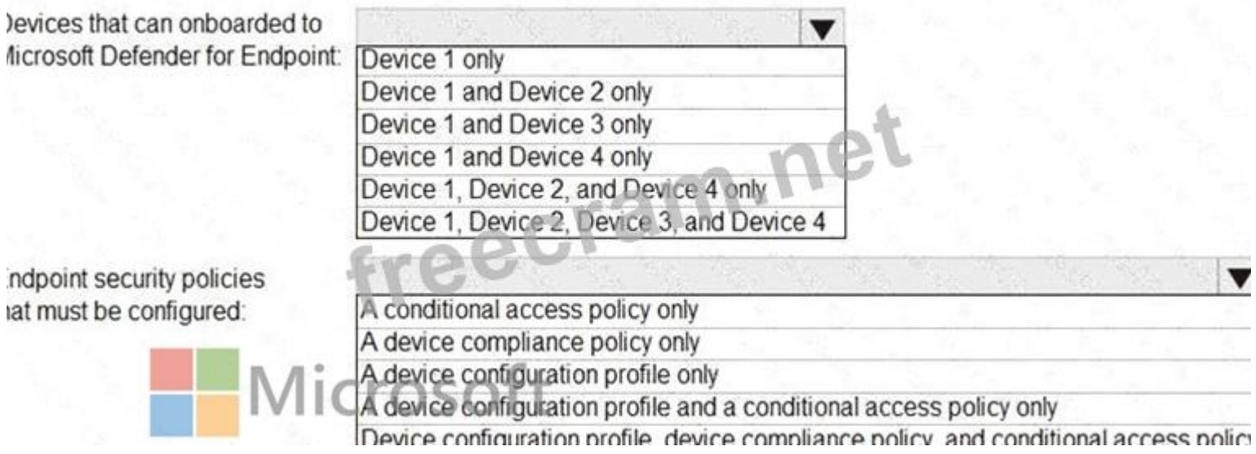
A. Review the sensitive information in Activity explorer

B. Turn on the policy
C. Run the policy in simulation mode
D. Configure Azure Information Protection analytics
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

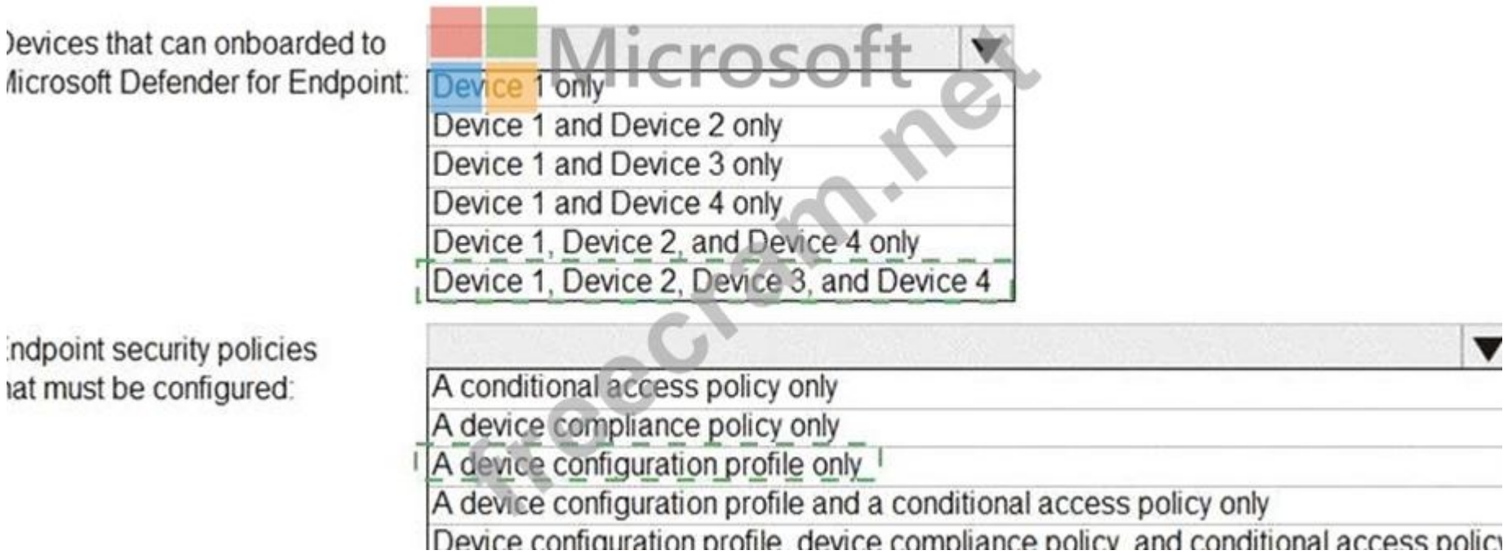
NEW QUESTION: 205
You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.
You have devices enrolled in Microsoft Intune as shown in the following table.

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

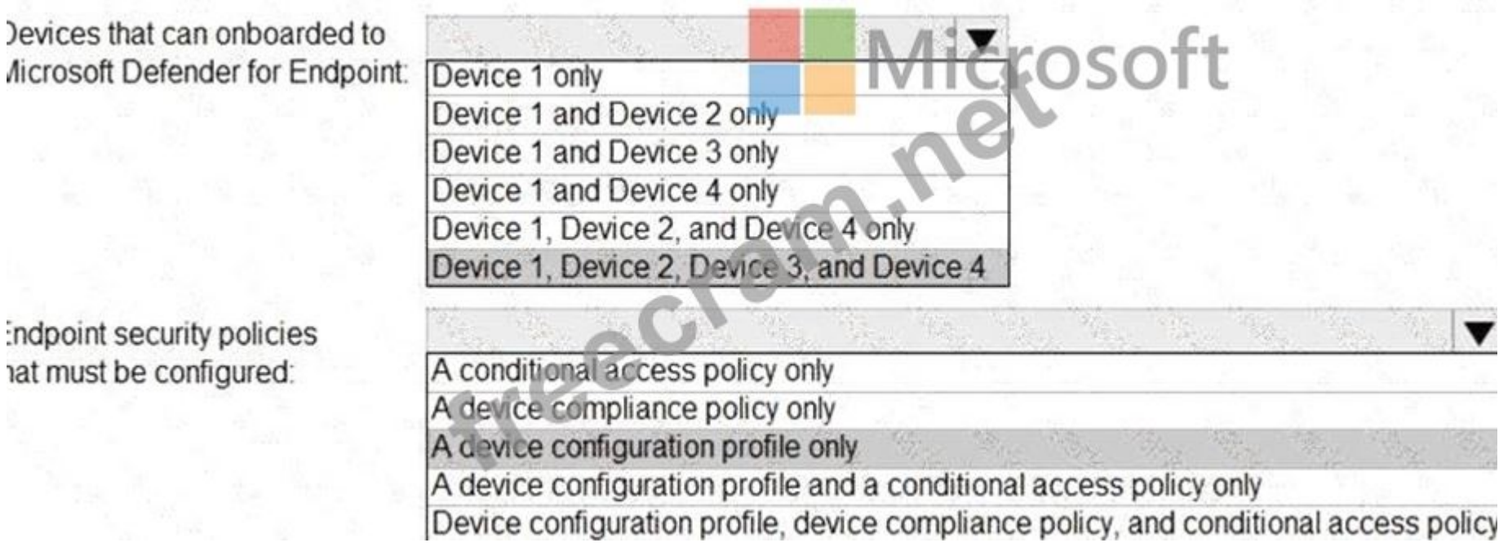
You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant.
Noncompliant devices must be blocked from accessing corporate resources.
You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies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



Answer:



Explanation:



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

NEW QUESTION: 206
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: 207
You have a Microsoft 365 ES tenant.
You have the alerts 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 Area

Answer:

Explanation:
Answer Area

NEW QUESTION: 208
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: 209
Your on-premises network contains an Active Directory domain.
You have a Microsoft 365 subscription.
You need to sync the domain with the subscription. The solution must meet the following requirements:
On-premises Active Directory password complexity policies must be enforced.
Users must be able to use self-service password reset (SSPR) in Azure AD.
What should you use?
A. password hash synchronization
B. Azure AD Identity Protection
C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
D. pass-through authentication
Answer: (SHOW ANSWER)
Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.
This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.
Note: Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time by using either Azure AD Connect or Azure AD Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.
Password writeback is supported in environments that use the following hybrid identity models:
Password hash synchronization
Pass-through authentication
Active Directory Federation Services
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback
NEW QUESTION: 210

You have a Microsoft 36S E5 subscription.

You have devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

Name	Platform
Device1	Windows 11
Computer2	Windows 11
Device3	Android

You create the device groups shown in the following table.

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

IP address indicators are defined as shown in the following table.

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

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
Defender for Endpoint blocks access to IP address 20.30.40.50 from Device1.	○	○
Defender for Endpoint blocks access to IP address 2.23.10.15 from Computer2.	○	○
Defender for Endpoint blocks access to IP address 131.107.10.50 from Device3.	○	○

Answer:

Answer Area

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

Explanation:

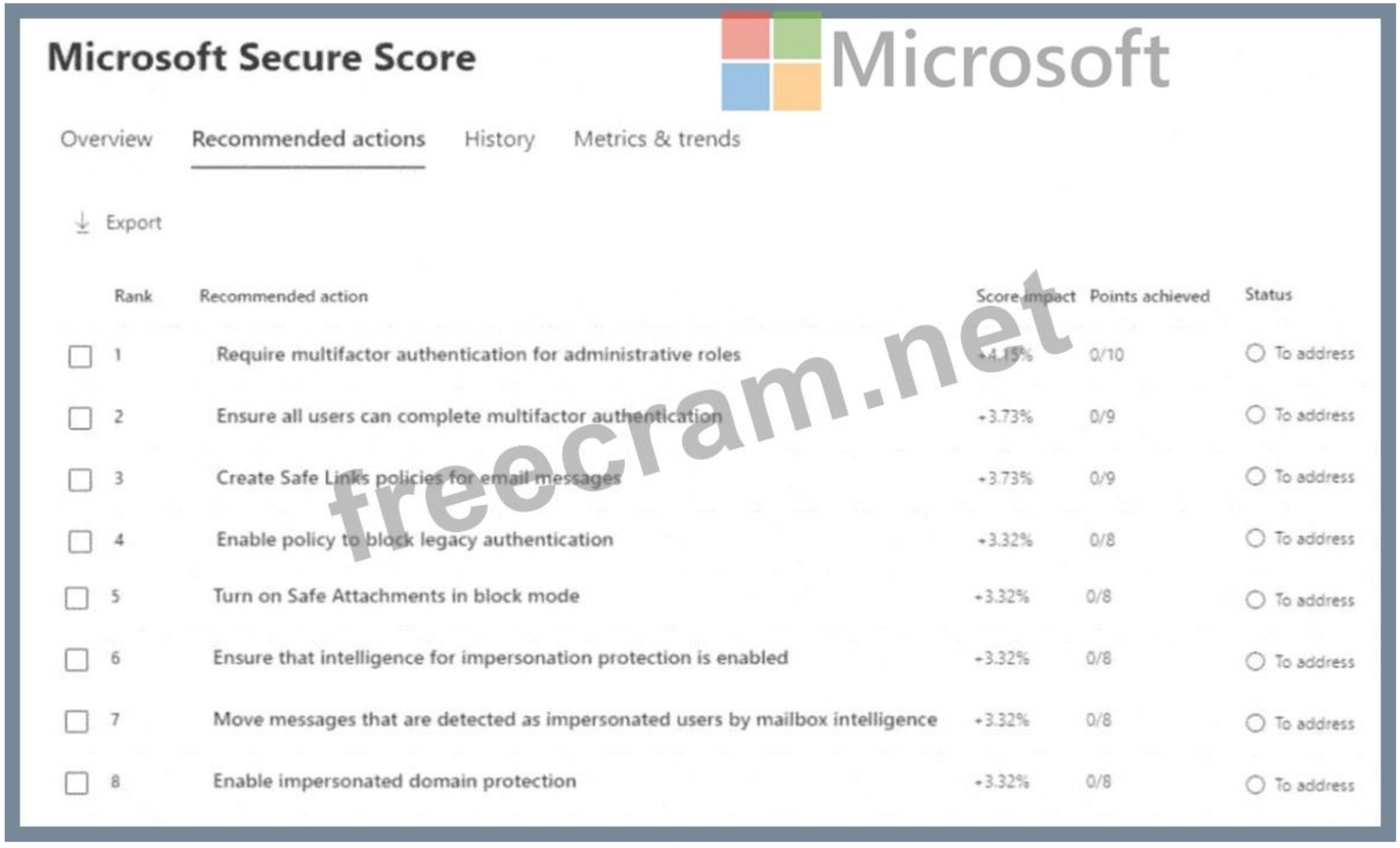
Answer Area

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

NEW QUESTION: 211

You have a Microsoft 365 E5 subscription.

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



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

How does the change affect the Secure Score?

A. increases by 9 points

B. increases by 1 point

C. decreases by 9 points

D. decreases by 1 point

E. remains the same

Answer: (SHOW ANSWER)

NEW QUESTION: 212

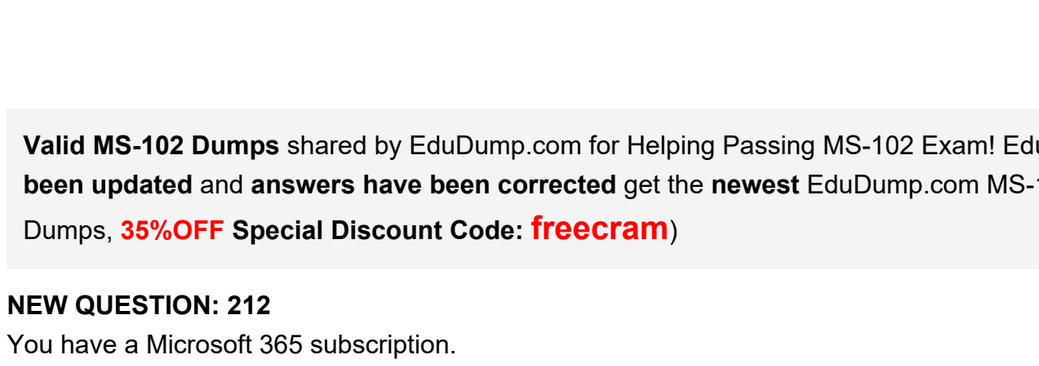
You have a Microsoft 365 subscription.

You need to identify all users that have an Enterprise Mobility + Security plan, and then provide a list of the users in the CSV format.

Which settings should you use in the Microsoft 365 admin center, and which option should you select? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:

NEW QUESTION: 213

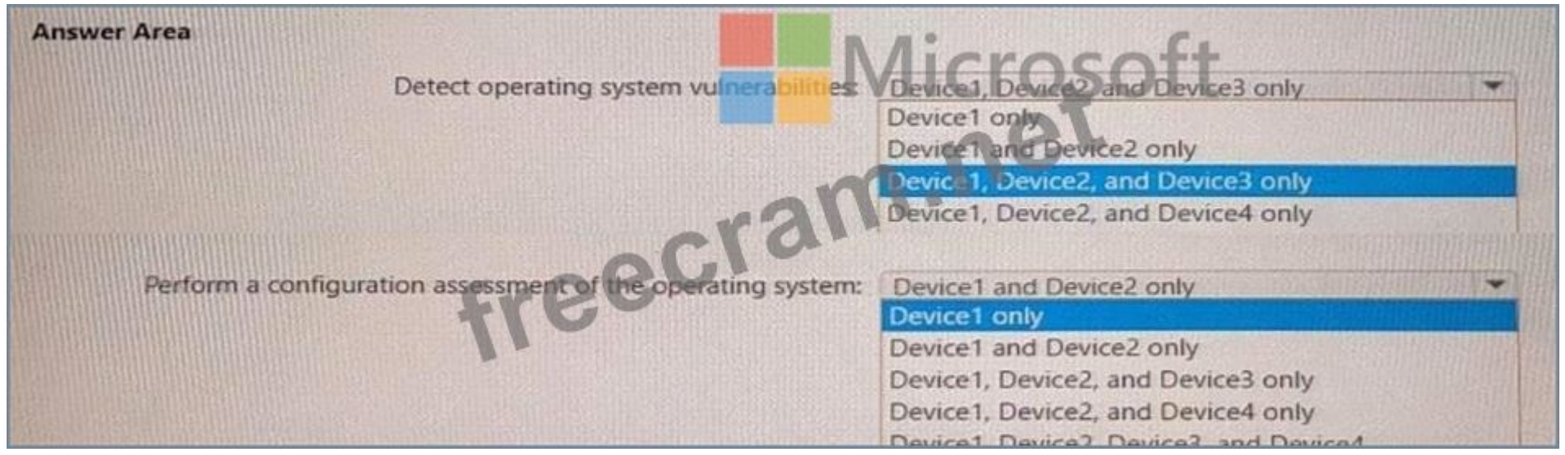
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

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

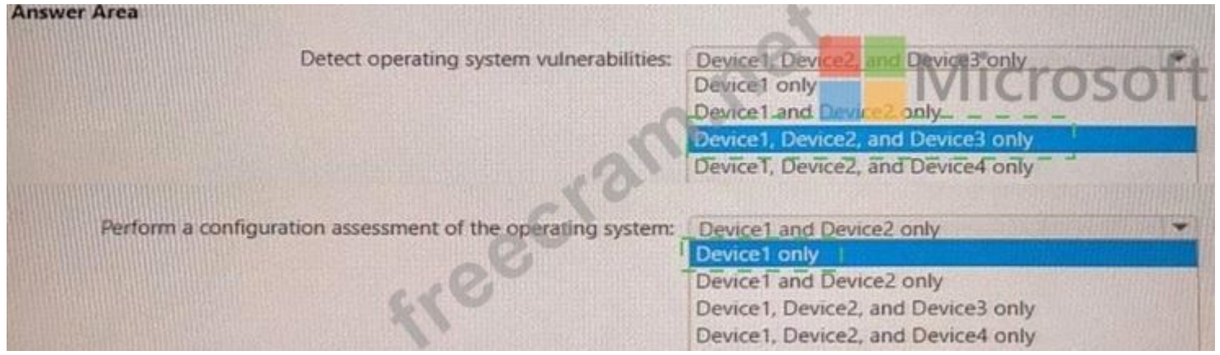
All the devices are onboarded To Microsoft Defender for Endpoint

You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:

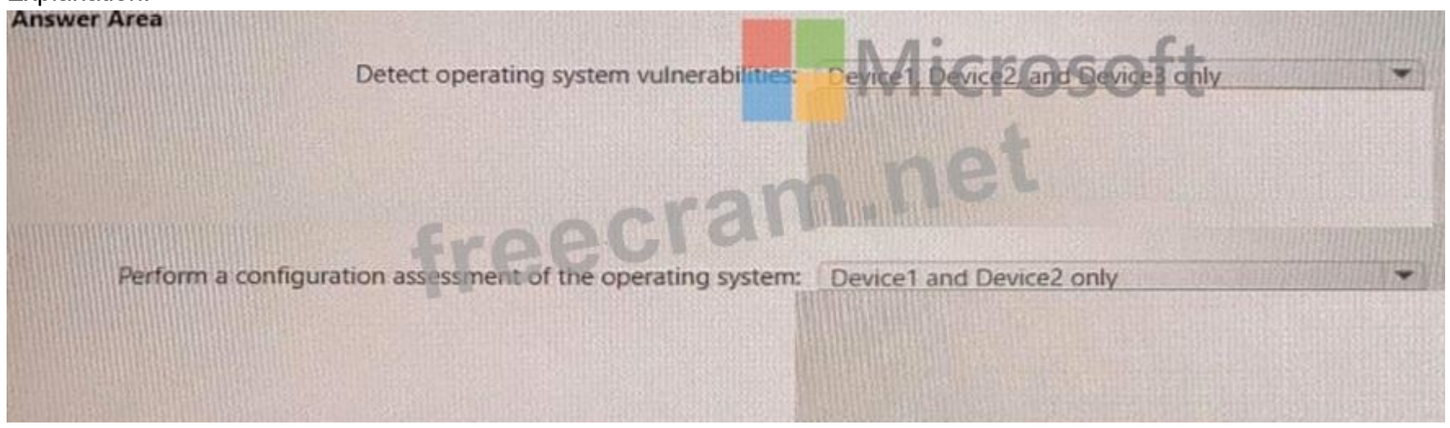
* Detect operating system vulnerabilities.



Answer:



Explanation:



NEW QUESTION: 214

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: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

NEW QUESTION: 215
You have a Microsoft 365 subscription that includes Microsoft Defender XDR.
From the Microsoft Defender portal, you review the Microsoft Secure Score improvement actions shown in the following table.

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

You plan to update the status of the improvement actions as shown in the following table.

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

How many points will the Secure Score increase after the update?
A. 16
B. 13
C. 0
D. 7
E. 4
Answer: (SHOW ANSWER)

NEW QUESTION: 216
You have a Microsoft 365 E5 subscription that contains the groups shown in the following exhibit.

To which groups can you assign Microsoft 365 E5 licenses?

A. Group2, Group3, and Group4 only

B. Group3 and Group4 only

C. Group 1, Group2. and Group3 only

D. Group! and Group2 only

E. Group2 and Group3 only

Answer: (SHOW ANSWER)

NEW QUESTION: 217

HOTSPOT

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

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

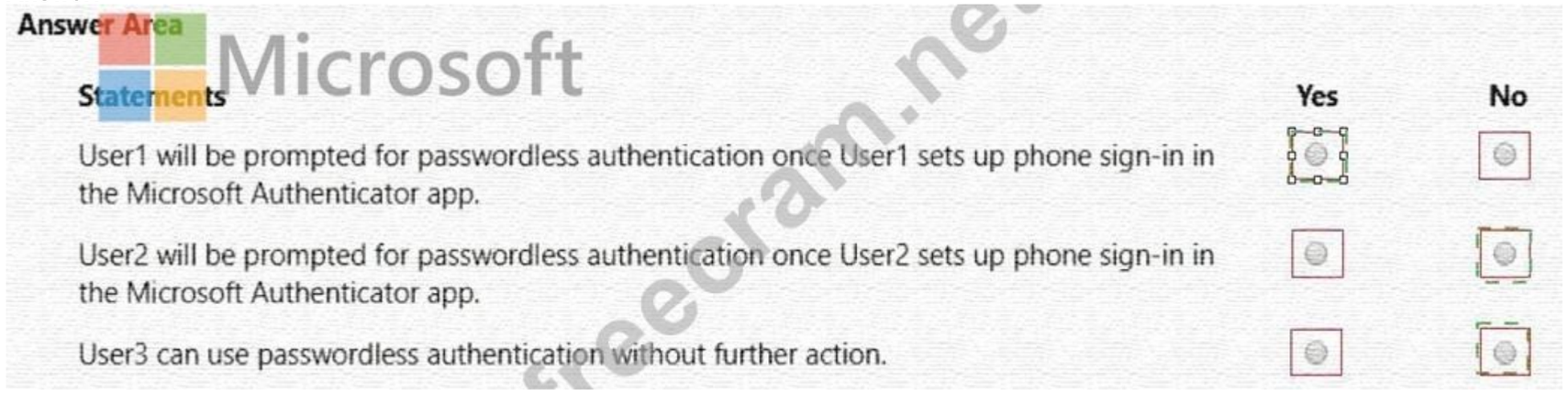
You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.

Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.

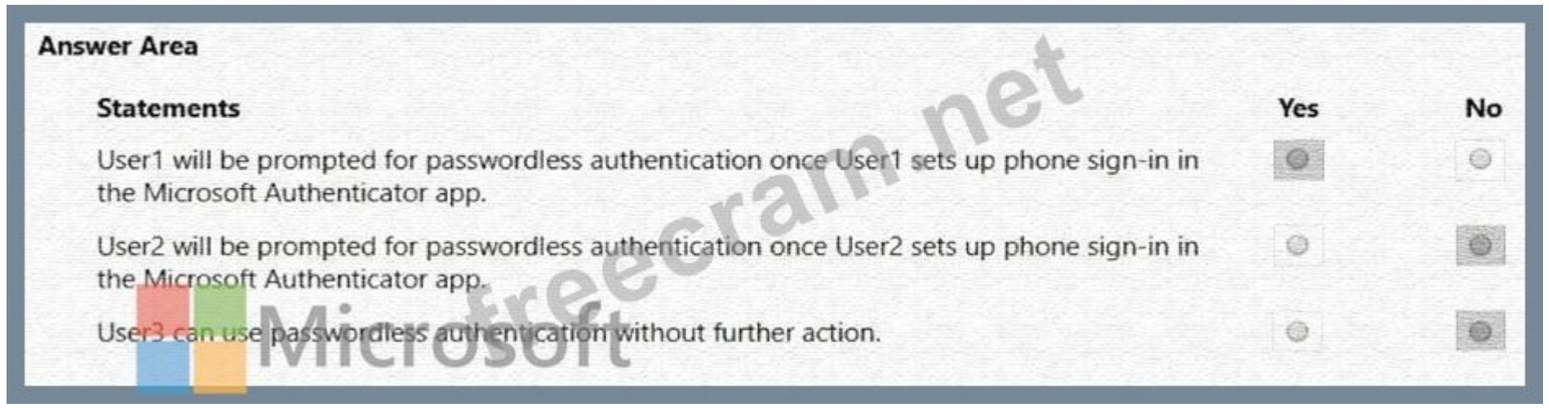
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:



Box 1: Yes

User1 is member of Group1.

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

Note: Microsoft Authenticator can be used to sign in to any Azure AD account without using a password.

Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology.

This authentication technology can be used on any device platform, including mobile. This technology can also be used with any app or website that integrates with Microsoft Authentication Libraries.

Box 2: No

User2 is member of Group2.

The Microsoft Authenticator authentication method policy is configured for Group1, not for Group2.

Box 3: No

User3 is member of Group1.

User3 has no MFA method registered.

User3 must choose an authentication method.

Note: Enable passwordless phone sign-in authentication methods

Azure AD lets you choose which authentication methods can be used during the sign-in process. Users then register for the methods they ' d like to use.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless- phone

NEW QUESTION: 218

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

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

You plan to implement Microsoft Defender for Endpoint.

You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.

You need to identify which user can view security incidents from the Microsoft 365 Defender portal.

Which user should you identify?
A. User3
B. User4
C. User1
D. User2
Answer: (SHOW ANSWER)

NEW QUESTION: 219
You have a Microsoft 365 E5 subscription that is linked to a Microsoft Entra tenant named contoso.com.
You purchase 100 Microsoft 365 Business Voice add-on licenses.
You need to ensure that the members of a group named Voice are assigned a Microsoft 365 Business Voice add-on license automatically.
What should you do?
A. From the Licenses page of the Microsoft 365 admin center, assign the licenses.
B. From the Microsoft Entra admin center, modify the settings of the Voice group.
C. From the Microsoft 365 admin center, modify the settings of the Voice group.
Answer: (SHOW ANSWER)

NEW QUESTION: 220
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. Insider risk management policies
B. Data Subject Requests (DSRs)
C. Communication compliance policies
D. Audit log retention policies
Answer: (SHOW ANSWER)

NEW QUESTION: 221
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

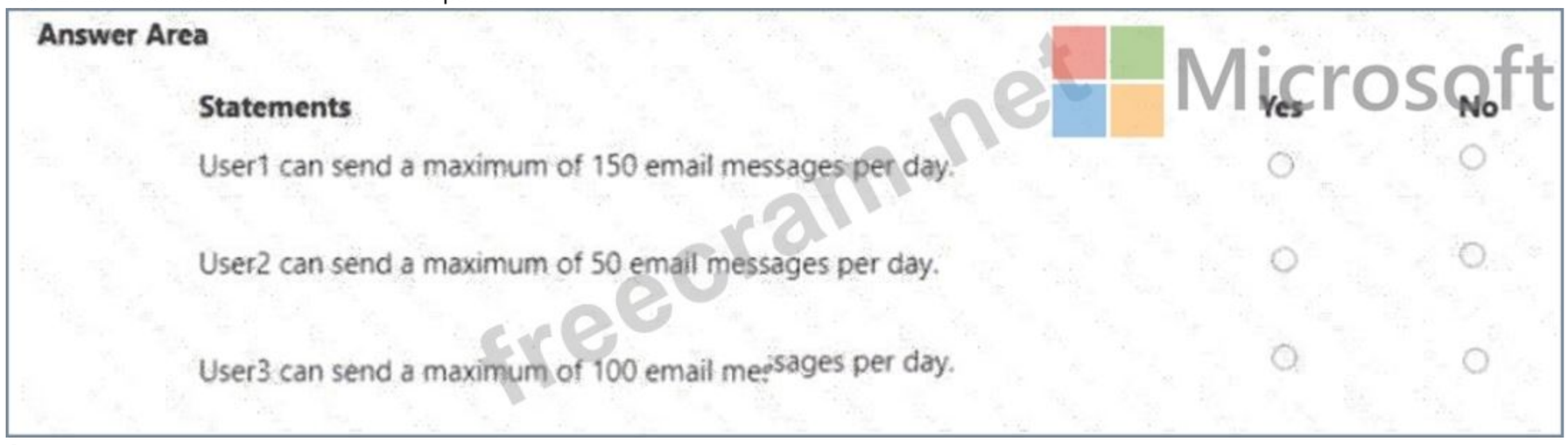
Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

The subscription has the following two anti-spam policies:
* Name: AntiSpam1
* Priority: 0
* Induce these users, groups and domains
o Users: User3
o Groups: Group1

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

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

NEW QUESTION: 222

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: 223

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.

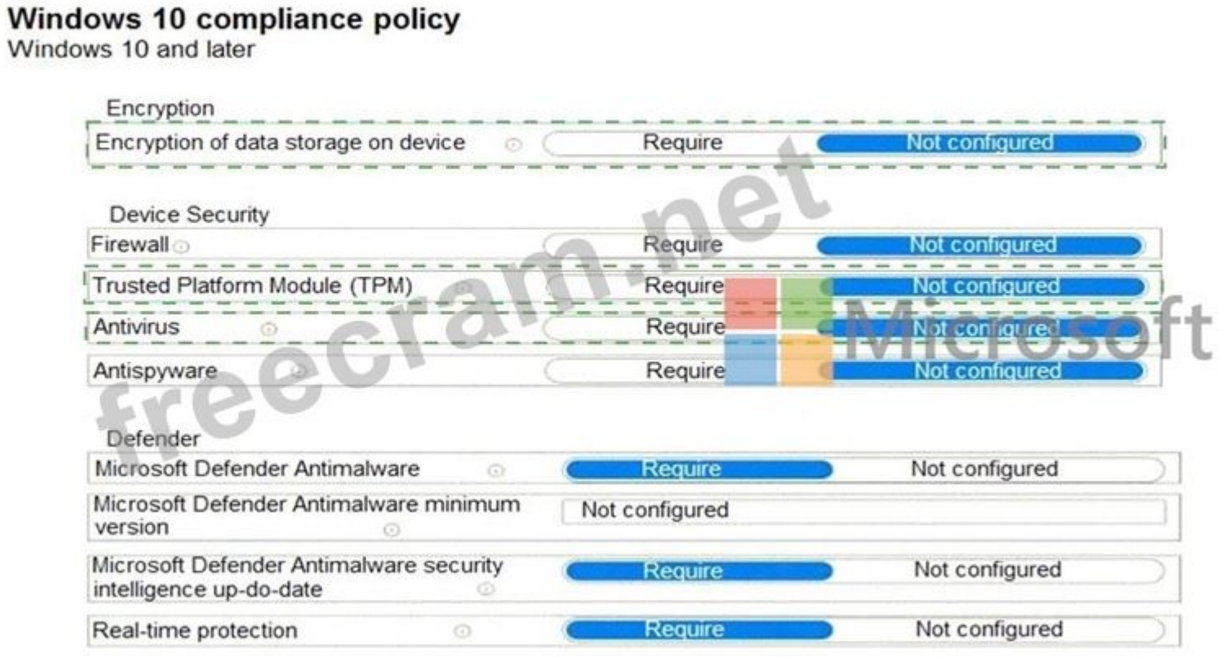
Answer Area

Windows 10 compliance policy
Windows 10 and later

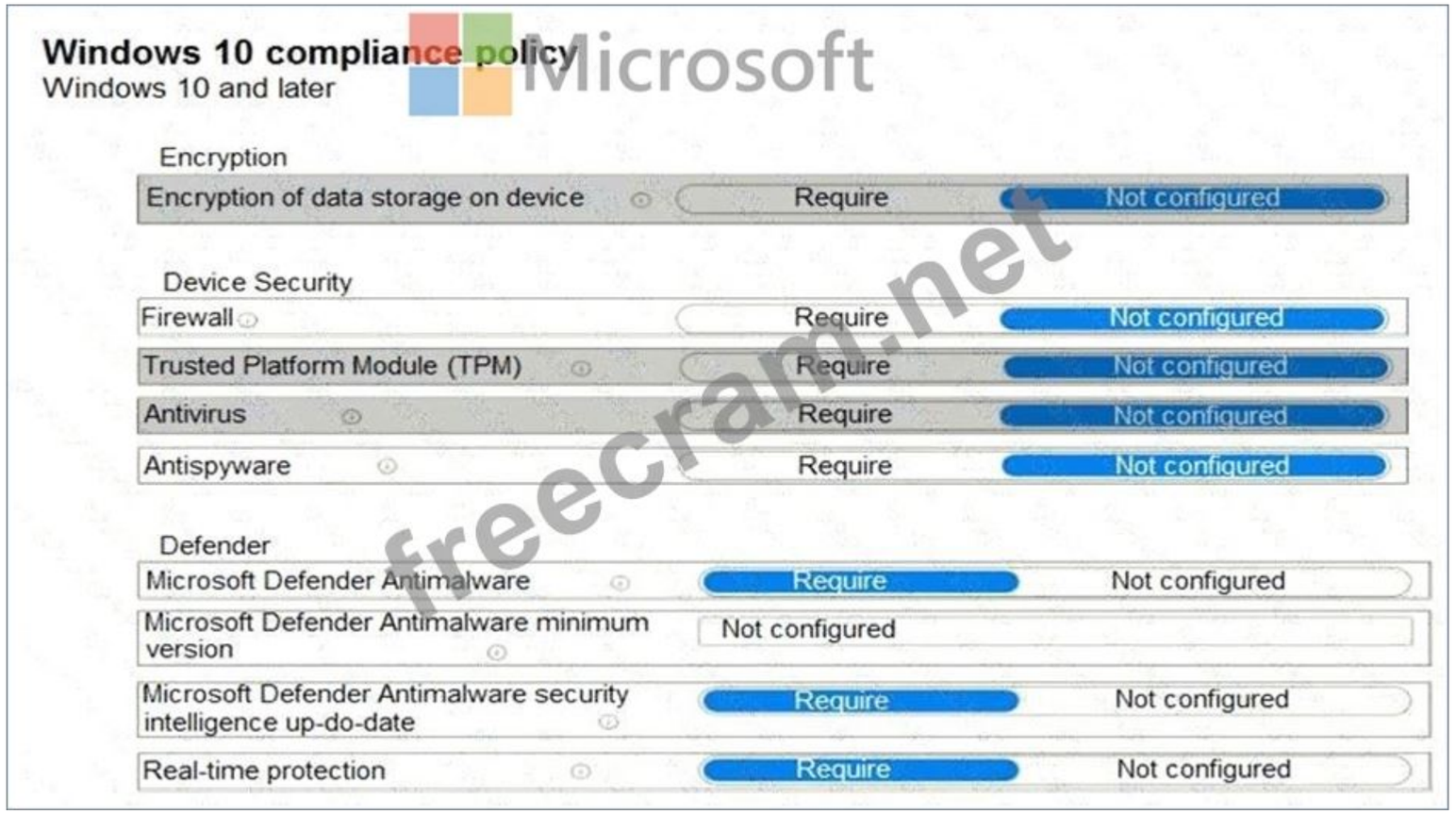
Encryption		
Encryption of data storage on device	Require	Not configured
Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured
Defender		
Microsoft Defender Antimalware	Require	Not configured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

Answer:

Answer Area



Explanation:



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

NEW QUESTION: 224
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	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

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

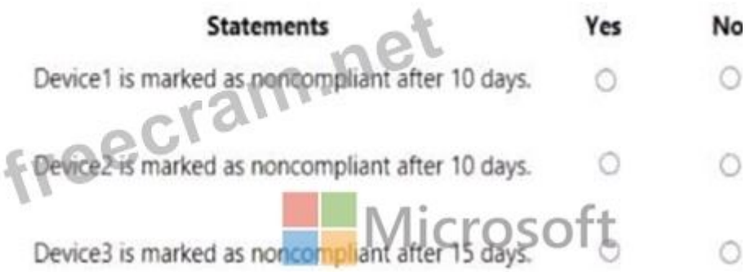
Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Not configured	15	Yes

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

Name	Assigned to
Policy2	Group2
Policy3	Group3

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

Answer Area



Answer:

Explanation:

Answer Area

NEW QUESTION: 225
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

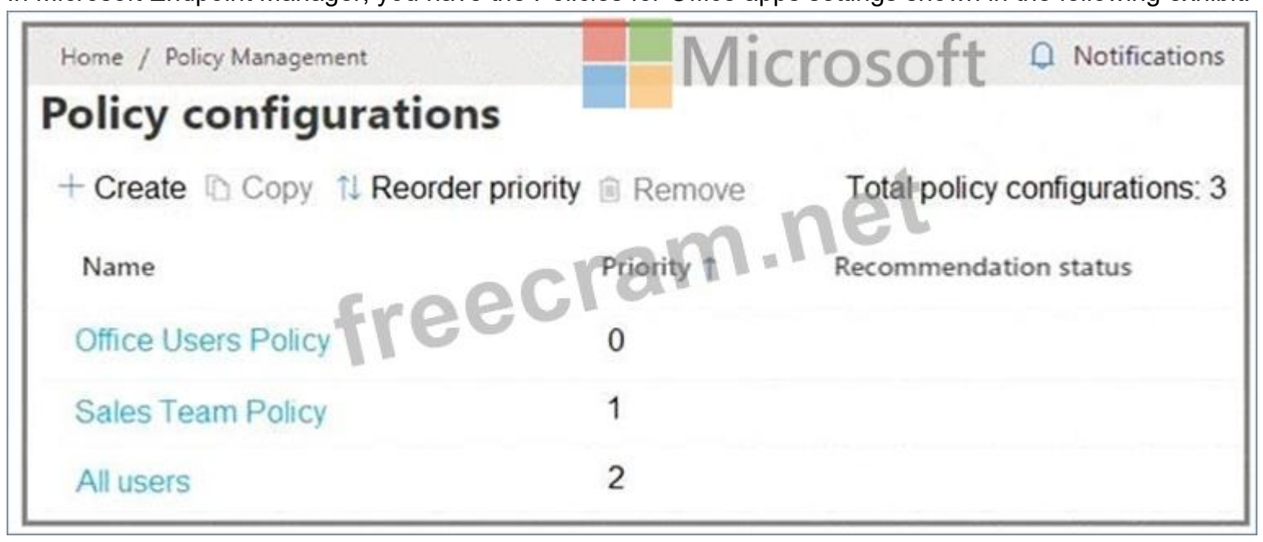
NEW QUESTION: 226

You have a Microsoft 365 E5 subscription that contains a user named User1.
You have a Conditional Access policy applied to a cloud-based app named App1. App1 has Conditional Access App Control deployed.
You need to create a Microsoft Defender for Cloud Apps policy to block User1 from printing from App1.
A. Cloud Discovery anomaly detection policy
B. OAuth app policy
C. Activity policy
D. Session policy
Answer: (SHOW ANSWER)

NEW QUESTION: 227
You have a Microsoft 365 subscription that contains three groups named All users, Sales team, and Office users, and two users shown in the following table.

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

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

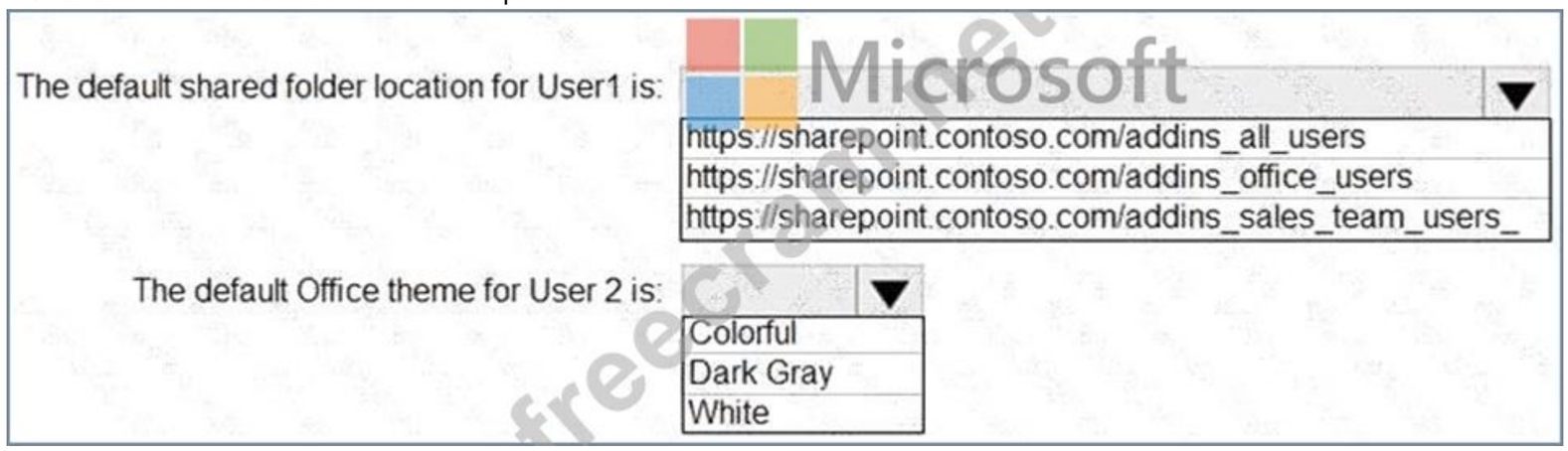


The policies use the settings shown in the following table.

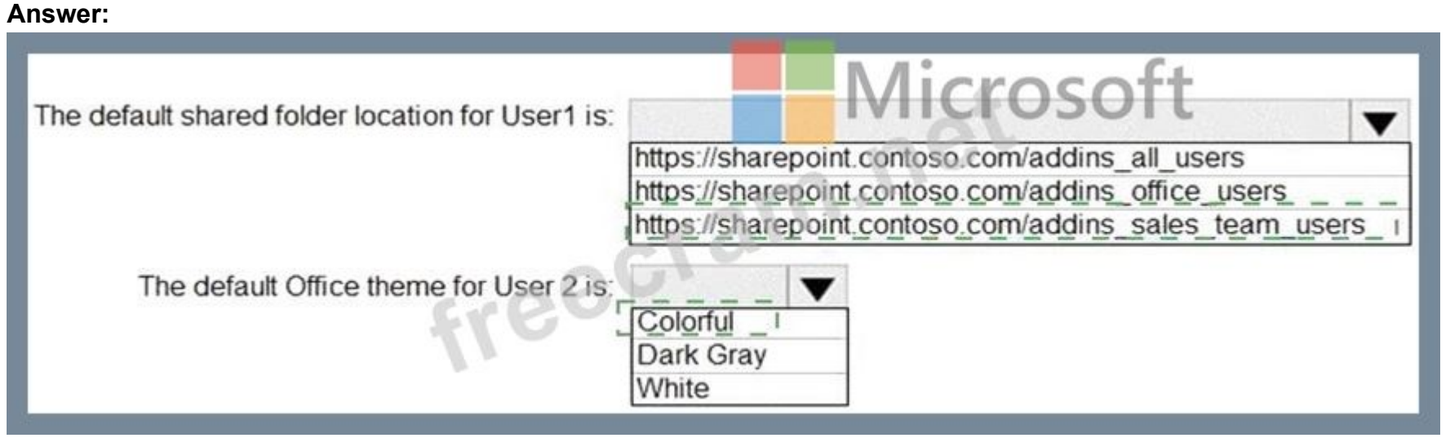
Policy	Default Shared Folder Location	Default Office Theme
All users	https://sharepoint.contoso.com/addins_all_users	Colorful
Office Users Policy	https://sharepoint.contoso.com/addins_office_users	White
Sales Team Policy	https://sharepoint.contoso.com/addins_sales_team_users_	Dark Gray

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

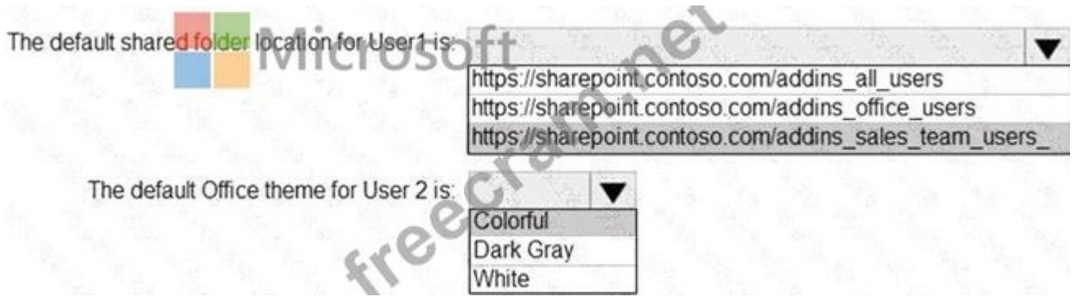
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

NEW QUESTION: 228
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 raise the domain functional level to Windows Server 2019. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)

NEW QUESTION: 229
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

At 08:00. you create an incident notification rule that has the following configurations:
* Name: Notification!
* Notification settings
o Notify on alert seventy: Low
o Device group scope: All (3)
o Details: First notification per incident
* Recipients: Userl@contoso.com, User2@contoso.com

At 08:02. you create an incident notification rule that has the following configurations:
* Name: Notification
* Notification settings
o Notify on alert severity: Low. Medium
o Device group scope: DevtceGroup1, DeviceGroup2
* Recipients: Userl@contoso.com
in Microsoft 365 Defender, alerts are logged as shown in the following table.

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

For each of the following statements, select Yes if the statement is true. Otherwise, select No1.
NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

Answer Area

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

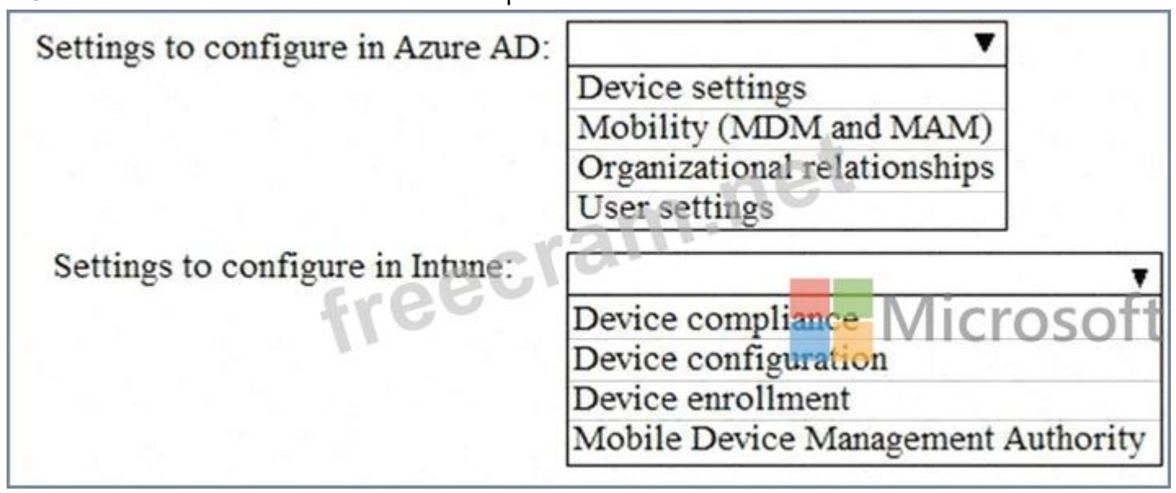
Explanation:

NEW QUESTION: 230

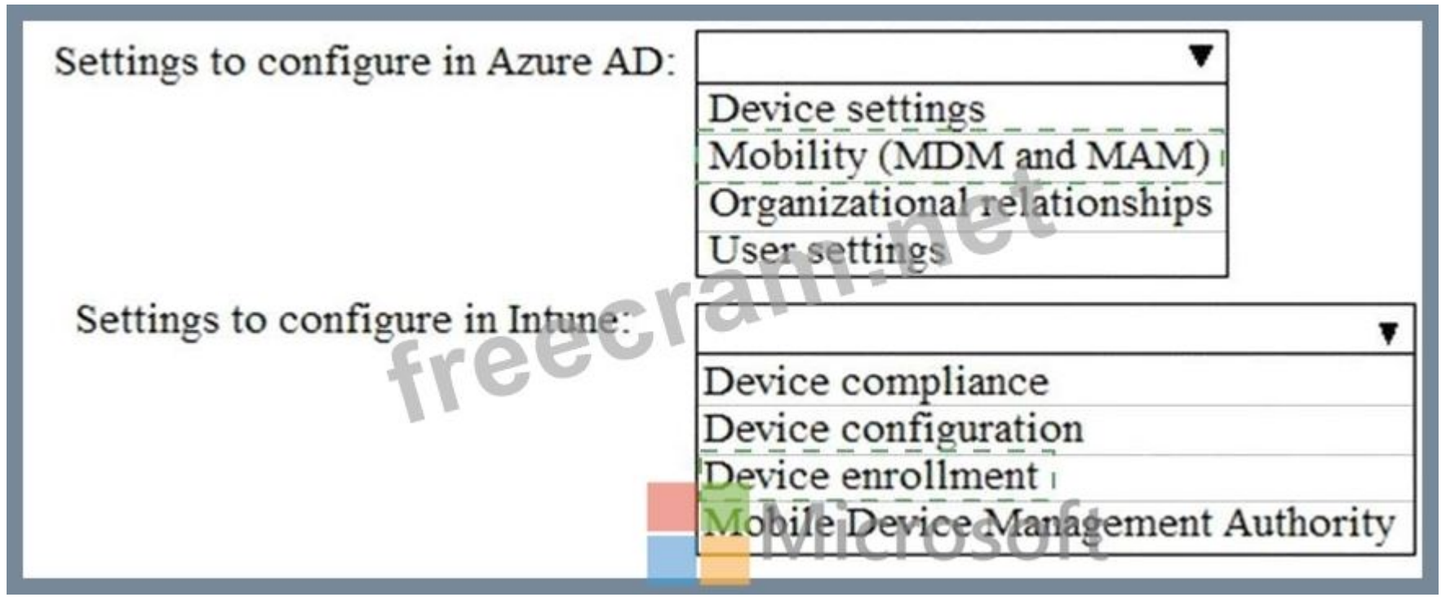
You need to meet the Intune requirements for the Windows 10 devices.

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

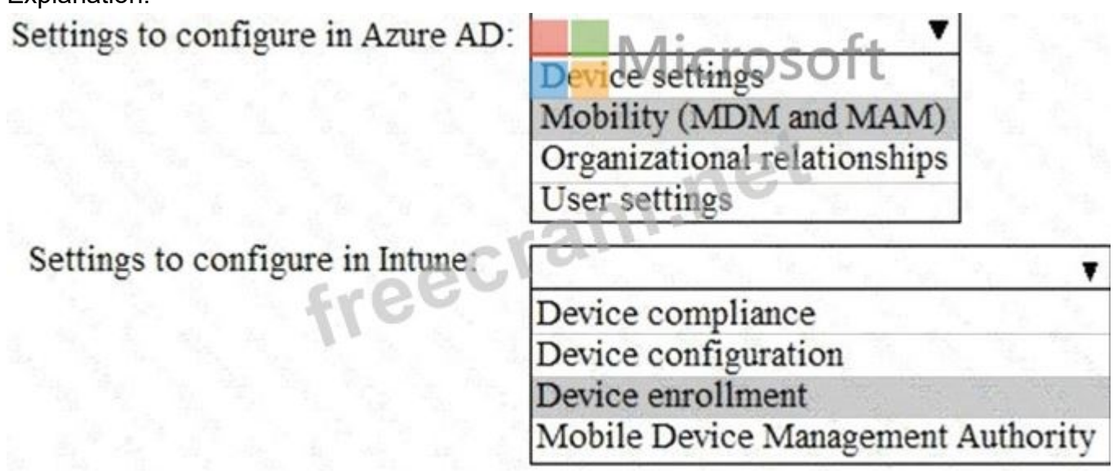
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

NEW QUESTION: 231
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
A Built-in protection preset security policy is applied to the subscription.
Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. Safe Links
B. Anti-malware
C. Safe Attachments
D. Anti-phishing
E. Anti-spam

Answer: (SHOW ANSWER)

NEW QUESTION: 232

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. 2

B. 4

C. 1

D. 3

Answer: (SHOW ANSWER)

NEW QUESTION: 233

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 policy

B. a sensitive info type

C. a data loss prevention (DLP) policy

D. a retention label

E. a retention label policy

F. a sensitivity label

Answer: (SHOW ANSWER)

NEW QUESTION: 234

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)

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.

Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

NEW QUESTION: 235
You have a Microsoft 365 E5 subscription.
You plan to configure multi-factor authentication (MFA).
You need to select an authentication method for users. The solution must ensure that each time a user is prompted for MFA, the application name that requires MFA is provided.
What should you select?
A. Microsoft Authenticator
B. email OTP
C. SMS
D. a FID02 security key
E. a voice call
Answer: (SHOW ANSWER)

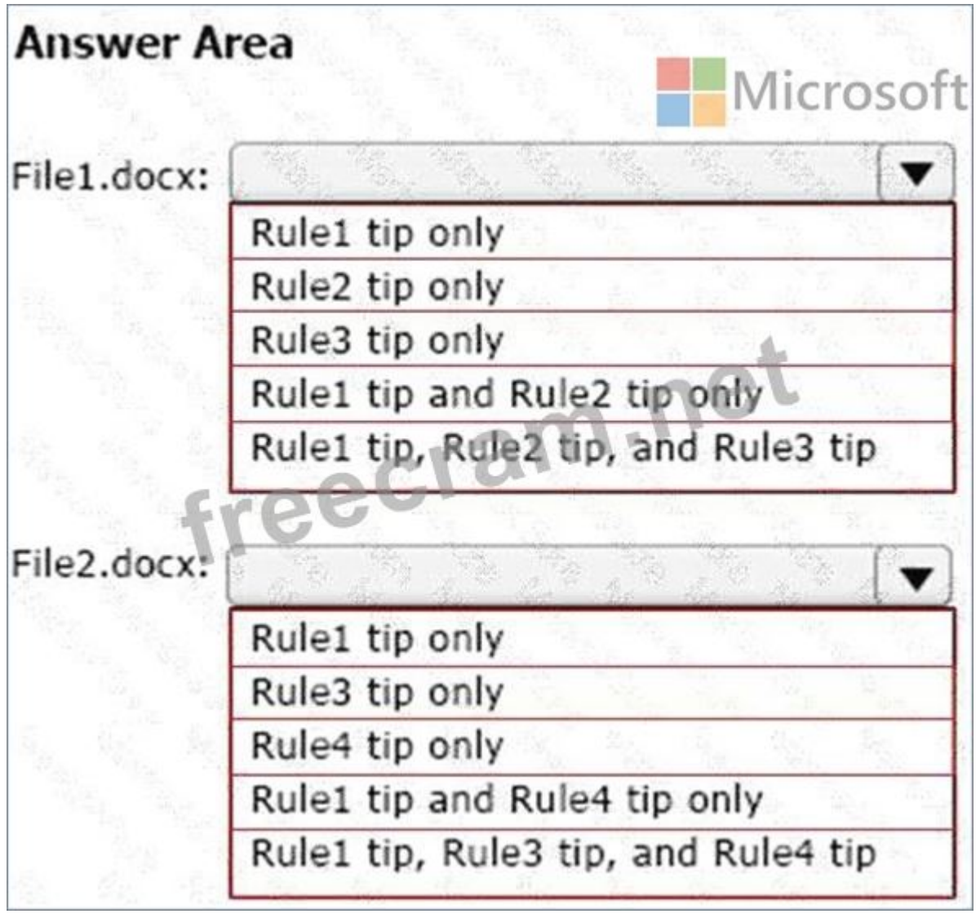
NEW QUESTION: 236
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

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

Site1 contains the files shown in the following table.

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

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



Answer:

Answer Area

File1.docx:

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

File2.docx:

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

Explanation:

Answer Area

File1.docx:

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

File2.docx:

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

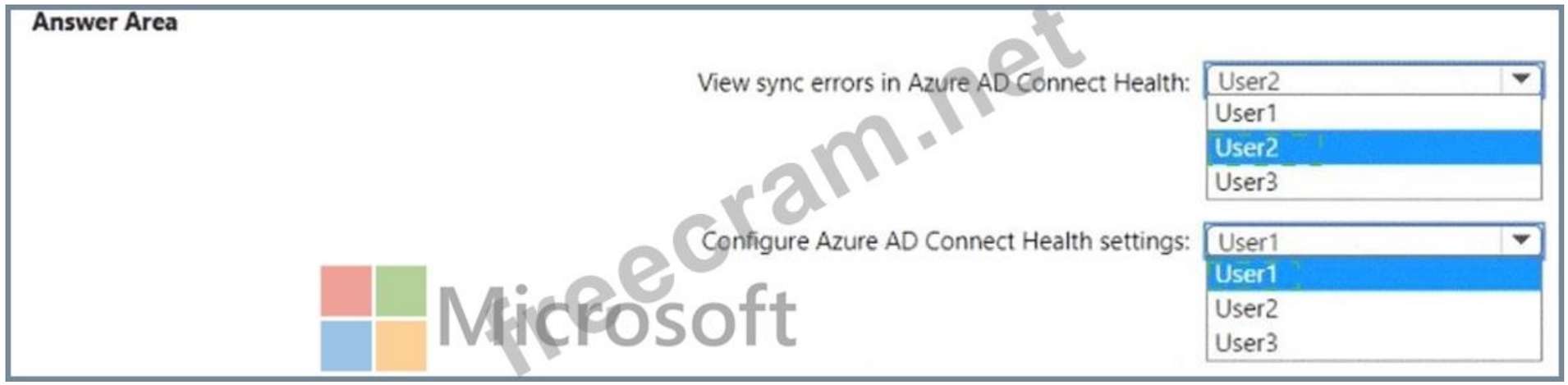
Box 1: Rule1 tip only
File1 matches Rule1, Rule2, and Rule3.
Rule1 has the highest priority.
Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can ' t have the same priority value.
Box 2: Rule1 tip only
Note: User Override support
The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can ' t be overridden).
It ' s possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.
If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp
https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips

NEW QUESTION: 237
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:



Explanation:

NEW QUESTION: 238
You have a Microsoft 365 E5 subscription.
You need to use Microsoft Defender for Cloud Apps to monitor user mailbox activities. What should you do?
A. Create an app connector for Microsoft 365.
B. Create an access policy.
C. Create an activity policy.
D. Enable mailbox audit logging.
Answer: (SHOW ANSWER)

NEW QUESTION: 239
You need to configure just in time access to meet the technical requirements.
What should you use?
A. entitlement management
B. access reviews
C. Azure AD Identity Protection
D. Azure AD Privileged Identity Management (PIM)
Answer: (SHOW ANSWER)

NEW QUESTION: 240
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 and Device4
B. Device1, Device2, Device3, and Device4
C. Device1 only
D. Device1, Device3, and Device4
Answer: (SHOW ANSWER)

NEW QUESTION: 241
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. information barriers
B. administrator units in Azure Active Directory (Azure AD)
C. communication compliance policies
D. moderated distribution groups
Answer: (SHOW ANSWER)

Valid MS-102 Dumps shared by EduDump.com for Helping Passing MS-102 Exam! EduDump.com now offer the **newest MS-102 exam dumps**, the EduDump.com MS-102 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com MS-102 dumps with Test Engine here: https://www.edudump.com/exams/Microsoft/MS-102/premium/ (**598** Q&As Dumps, **35%OFF Special Discount Code: freecram**)