MS-500.prepaway.premium.exam.115q

Number: MS-500
Passing Score: 800
Time Limit: 120 min
File Version: 5.0

MS-500

Microsoft 365 Security Administration

Version 5.0

Testlet 1

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
Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment

Network Infrastructure
The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements
Fabrikam identifies the following issues:

- Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.
- Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements

Planned Changes
Fabrikam plans to implement the following changes:

- Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory
- Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

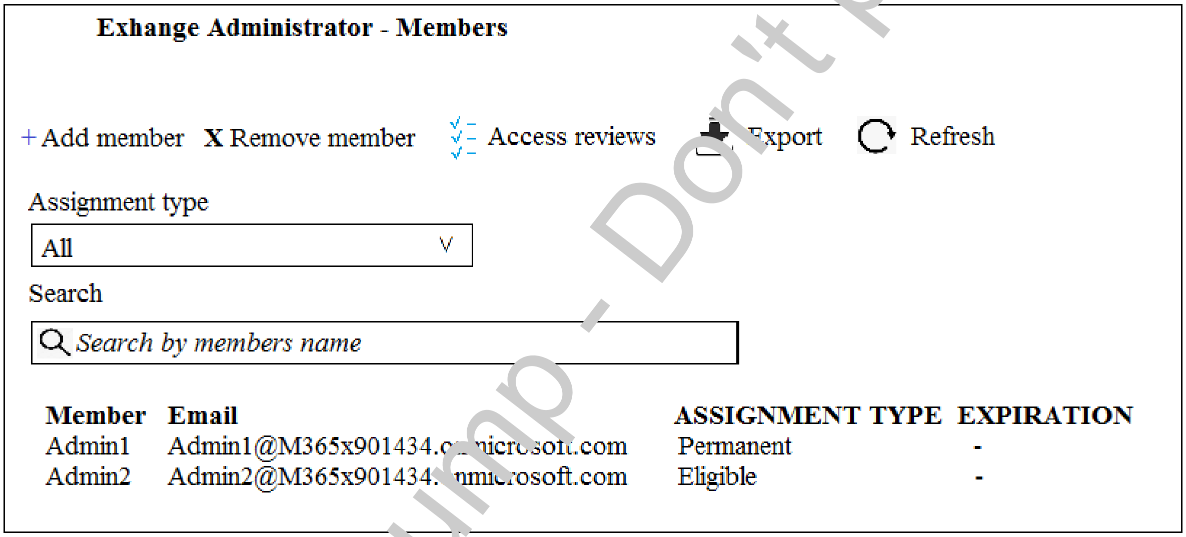
Application Administration
Fabrikam identifies the following application requirements for managing workload applications:

- User administrators will work from different countries
- User administrators will use the Azure Active Directory admin center
- Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements
Fabrikam identifies the following security requirements:

- Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed
- Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement
- Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send invitations
- Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory
- Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location
- The location of the user administrators must be audited when the administrators authenticate to Azure AD
- Email messages that include attachments containing malware must be delivered without the attachment
- The principle of least privilege must be used whenever possible

QUESTION 1
An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.



Exhange Administrator - Members

Assignment type: All

Search: *Search by members name*

Member	Email	ASSIGNMENT TYPE	EXPIRATION
Admin1	Admin1@M365x901434.onmicrosoft.com	Permanent	-
Admin2	Admin2@M365x901434.onmicrosoft.com	Eligible	-

What should you do to meet the security requirements?

A. Change the Assignment Type for Admin2 to **Permanent**
B. From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
C. From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
D. Change the Assignment Type for Admin1 to **Eligible**

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
You need to recommend a solution for the user administrators that meets the security requirements for auditing.

Which blade should you recommend using from the Azure Active Directory admin center?

A. Sign-ins
B. Azure AD Identity Protection
C. Authentication methods
D. Access review

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

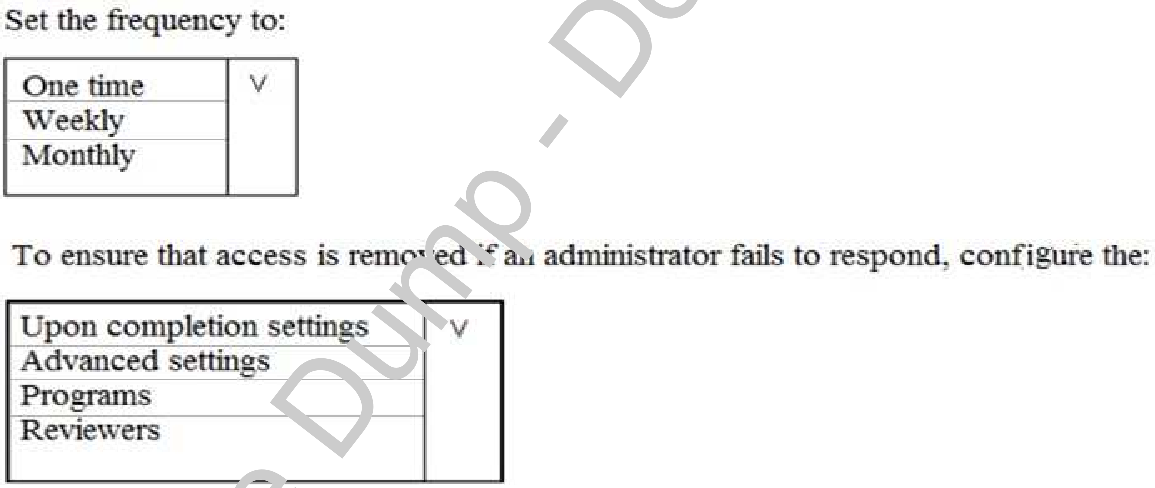
QUESTION 3
HOTSPOT

You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Set the frequency to:

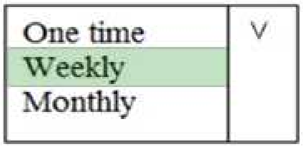
One time Weekly Monthly	V

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings Advanced settings Programs Reviewers	V

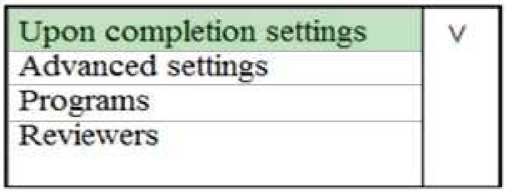
Correct Answer:

Set the frequency to:



One time
[✓ Weekly]
Monthly

To ensure that access is removed if an administrator fails to respond, configure the:



[✓ Upon completion settings]
Advanced settings
Programs
Reviewers

Section: [none]
Explanation

Explanation/Reference:

QUESTION 4
You need to recommend a solution to protect the sign-ins of Admin1 and Admin2.

What should you include in the recommendation?

A. a device compliance policy
B. an access review
C. a user risk policy
D. a sign-in risk policy

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy

QUESTION 5
You need to resolve the issue that targets the automated email messages to the IT team.

Which tool should you run first?

A. Synchronization Service Manager
B. Azure AD Connect wizard
C. Synchronization Rules Editor
D. IdFix

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:

https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization

Testlet 2

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.

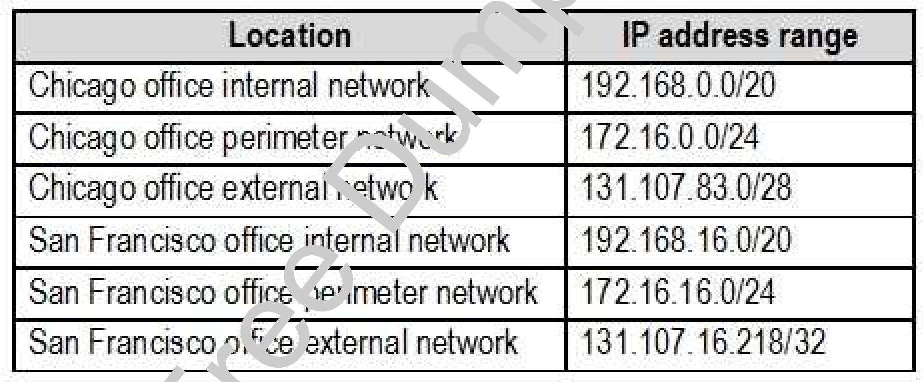
Overview
Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment

Internal Network Infrastructure
The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.



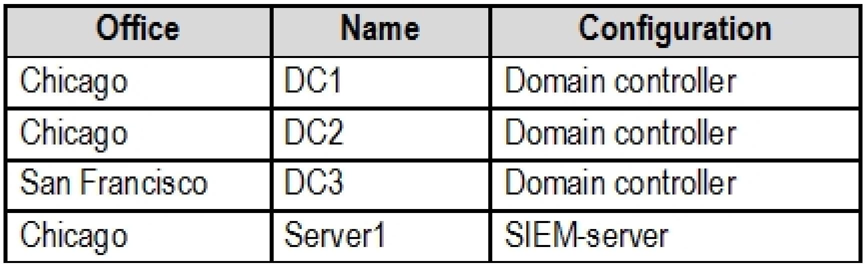
Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

- Windows Server 2016
- Windows 10 Enterprise
- Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.



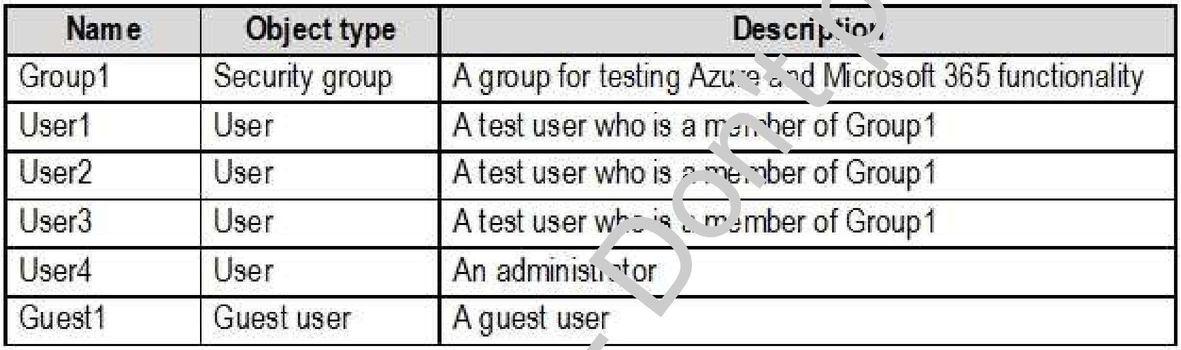
Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure
Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.



Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Planned Changes
Litware plans to implement the following changes:

- Migrate the email system to Microsoft Exchange Online
- Implement Azure AD Privileged Identity Management

Security Requirements
Litware identities the following security requirements:

- Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
- Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
- Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
- Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
- Implement a permanent eligible assignment of the Compliance administrator role for User1
- Configure domain-joined servers to ensure that they report sensor data to Windows Defender ATP
- Prevent access to Azure resources for the guest user accounts by default
- Ensure that all domain-joined computers are registered to Azure AD

Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.

You identify the following requirements for testing MFA:

- Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA

must **NOT** be used on the Chicago office internal network.
- If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
- Any disruption of legitimate authentication attempts must be minimized.

General Requirements
Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

QUESTION 1
You need to create Group2.

What are two possible ways to create the group?

A. an Office 365 group in the Microsoft 365 admin center
B. a mail-enabled security group in the Microsoft 365 admin center
C. a security group in the Microsoft 365 admin center
D. a distribution list in the Microsoft 365 admin center
E. a security group in the Azure AD admin center

Correct Answer: CE
Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
Which IP address space should you include in the Trusted IP MFA configuration?

A. 131.107.83.0/28
B. 192.168.16.0/20
C. 172.16.0.0/24
D. 192.168.0.0/20

Correct Answer: B
Section: [none]
Explanation

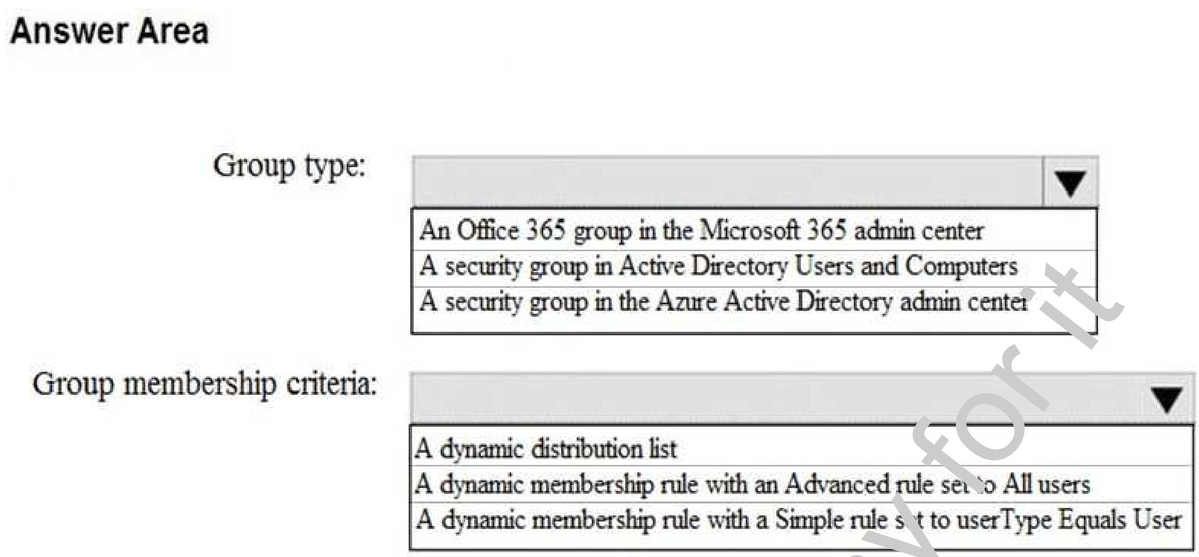
Explanation/Reference:

QUESTION 3
HOTSPOT

How should you configure Group3? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

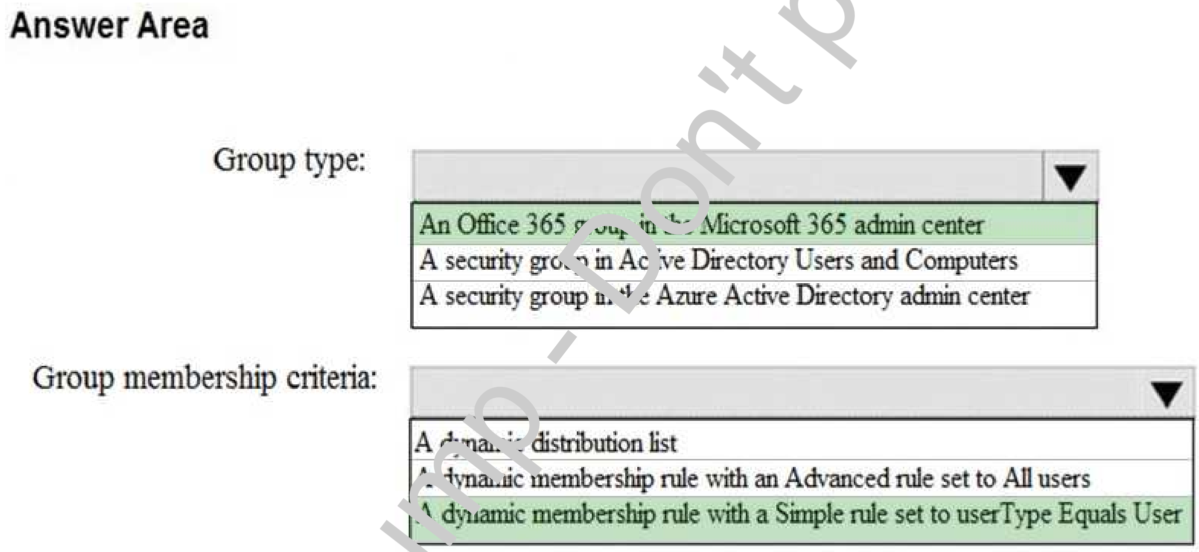
Group type:

- An Office 365 group in the Microsoft 365 admin center
- A security group in Active Directory Users and Computers
- A security group in the Azure Active Directory admin center

Group membership criteria:

- A dynamic distribution list
- A dynamic membership rule with an Advanced rule set to All users
- A dynamic membership rule with a Simple rule set to userType Equals User

Correct Answer:



Answer Area

Group type:

- [✓ An Office 365 group in the Microsoft 365 admin center]
- A security group in Active Directory Users and Computers
- A security group in the Azure Active Directory admin center

Group membership criteria:

- A dynamic distribution list
- A dynamic membership rule with an Advanced rule set to All users
- [✓ A dynamic membership rule with a Simple rule set to userType Equals User]

Section: [none]
Explanation

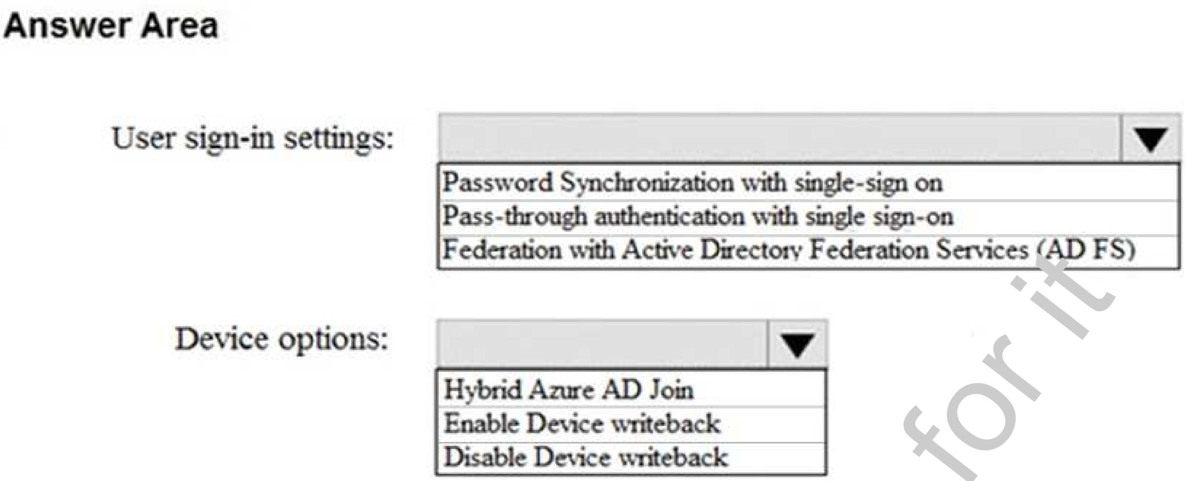
Explanation/Reference:

QUESTION 4
HOTSPOT

How should you configure Azure AD Connect? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

User sign-in settings: ▼

Password Synchronization with single-sign on

Pass-through authentication with single sign-on

Federation with Active Directory Federation Services (AD FS)

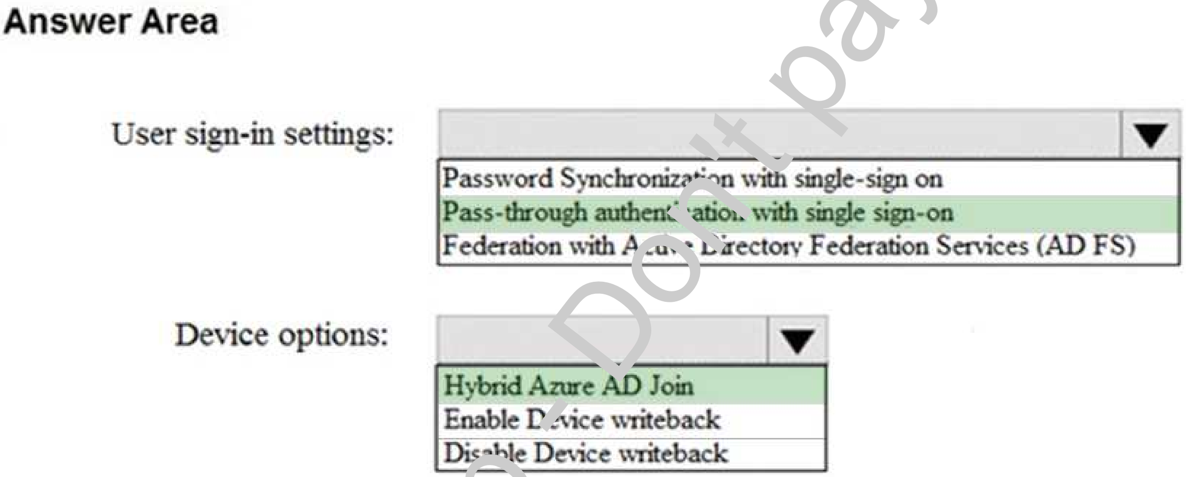
Device options: ▼

Hybrid Azure AD Join

Enable Device writeback

Disable Device writeback

Correct Answer:



Answer Area

User sign-in settings: ▼

Password Synchronization with single-sign on

[✓ Pass-through authentication with single sign-on]

Federation with Active Directory Federation Services (AD FS)

Device options: ▼

[✓ Hybrid Azure AD Join]

Enable Device writeback

Disable Device writeback

Section: [none]
Explanation

Explanation/Reference:

QUESTION 5
You need to create Group3

What are two possible ways to create the group?

A. an Office 365 group in the Microsoft 365 admin center
B. a mail-enabled security group in the Microsoft 365 admin center
C. a security group in the Microsoft 365 admin center
D. a distribution list in the Microsoft 365 admin center
E. a security group in the Azure AD admin center

Correct Answer: AD
Section: [none]
Explanation

Explanation/Reference:

Testlet 3

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.

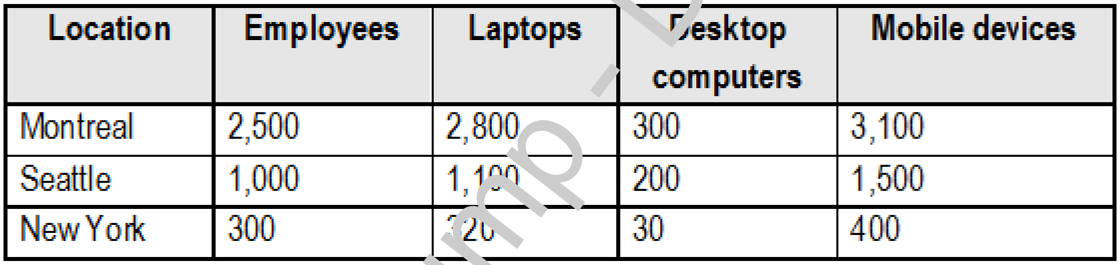
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

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

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

The company has the offices shown in the following table.



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

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment

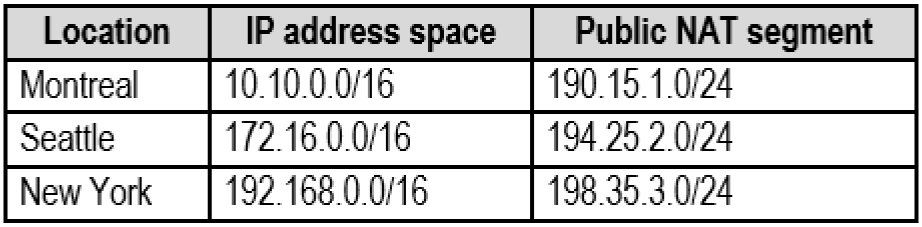
Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

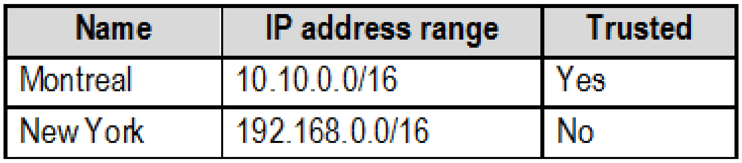
Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.



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

Named locations are defined in Azure AD as shown in the following table.

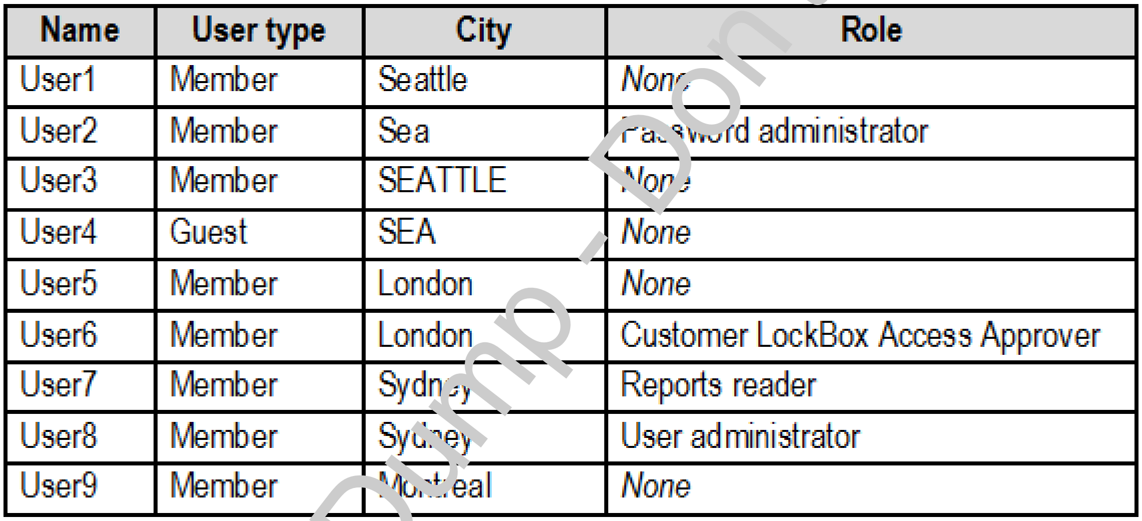


Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

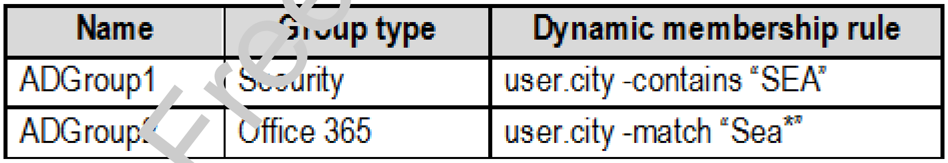
Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.



Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

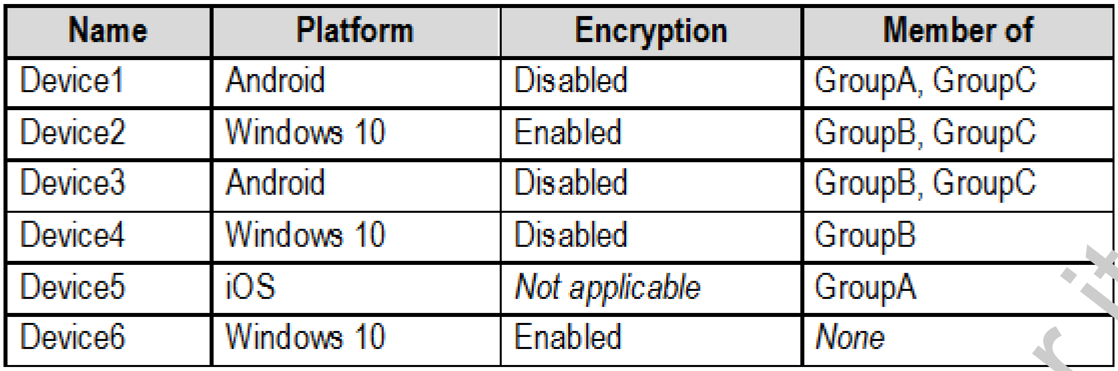


Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

Customer Lockbox is enabled in Microsoft 365.

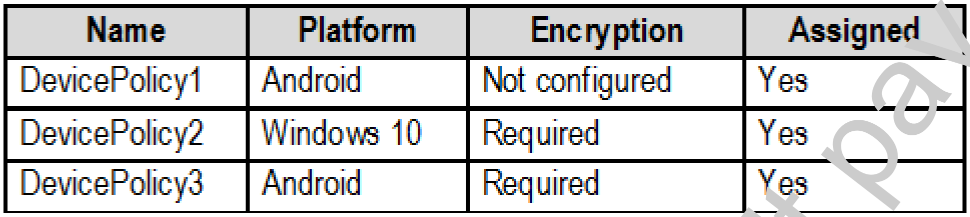
Microsoft Intune Configuration

The devices enrolled in Intune are configured as shown in the following table.



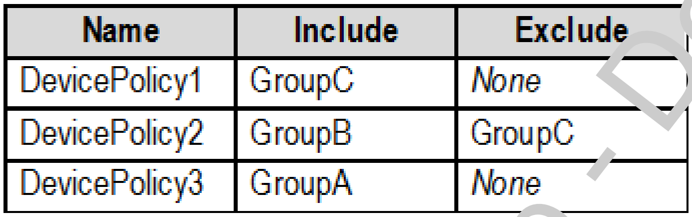
Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

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



Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

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



Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to **Compliant**.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

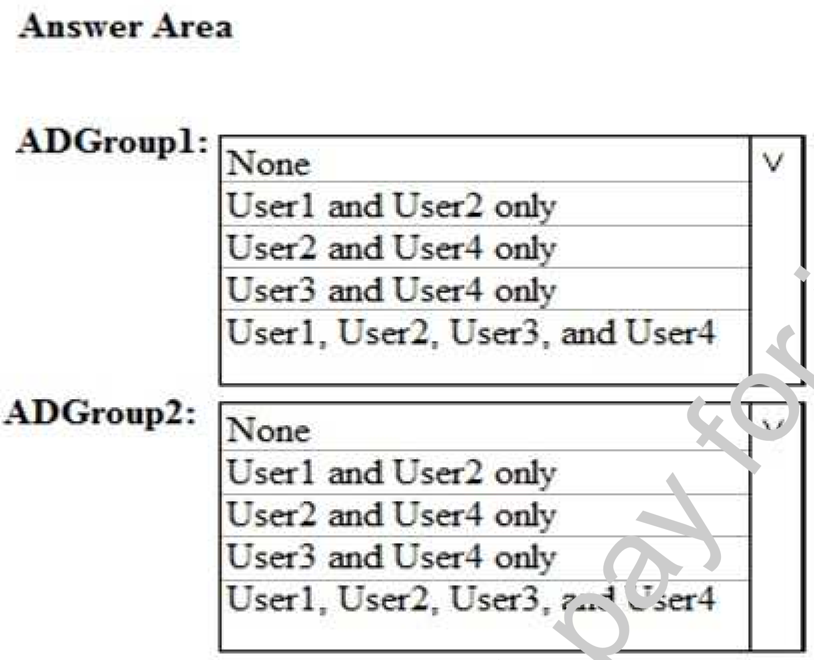
- Use the principle of least privilege
- Enable User1 to assign the Reports reader role to users
- Ensure that User6 approves Customer Lockbox requests as quickly as possible
- Ensure that User9 can enable and configure Azure AD Privileged Identity Management

QUESTION 1
HOTSPOT

Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

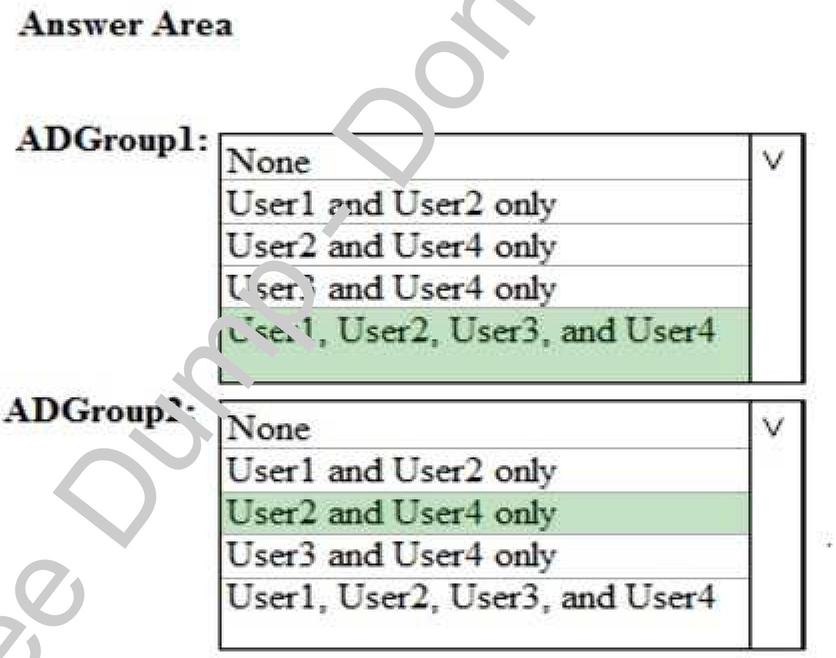
ADGroup1:

- None
- User1 and User2 only
- User2 and User4 only
- User3 and User4 only
- User1, User2, User3, and User4

ADGroup2:

- None
- User1 and User2 only
- User2 and User4 only
- User3 and User4 only
- User1, User2, User3, and User4

Correct Answer:



Answer Area

ADGroup1:

- None
- User1 and User2 only
- User2 and User4 only
- User3 and User4 only
- [✓ User1, User2, User3, and User4]

ADGroup2:

- None
- User1 and User2 only
- [✓ User2 and User4 only]
- User3 and User4 only
- User1, User2, User3, and User4

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

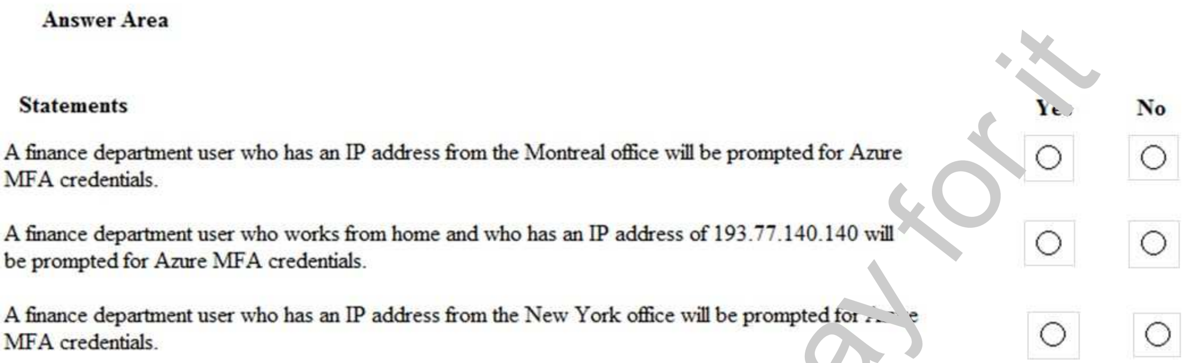
QUESTION 2
HOTSPOT

You are evaluating which finance department users will be prompted for Azure MFA credentials.

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

NOTE: Each correct selection is worth one point.

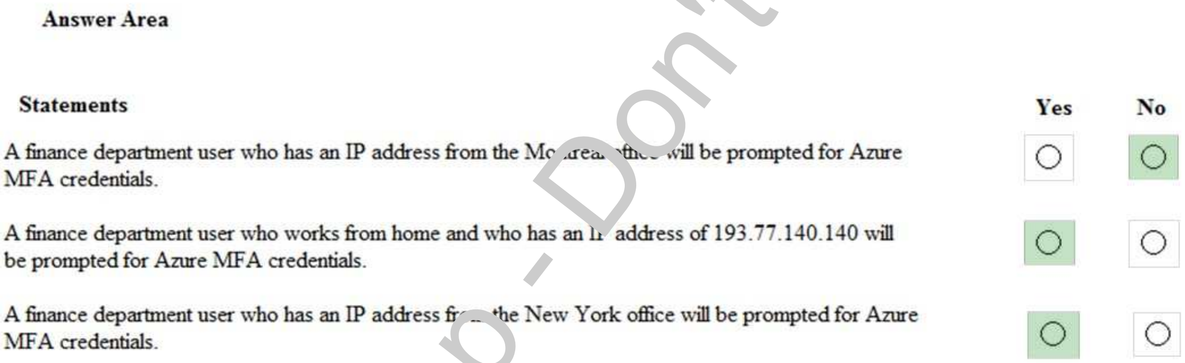
Hot Area:



Answer Area

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	○	○
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	○	○
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	○	[✓ ○]
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	[✓ ○]	○
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	[✓ ○]	○

Section: [none]
Explanation

Explanation/Reference:

QUESTION 3
Which user passwords will User2 be prevented from resetting?

A. User6 and User7
B. User4 and User6
C. User4 only
D. User7 and User8
E. User8 only

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 4
You need to meet the technical requirements for User9. What should you do?

A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9
B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9
C. Assign the Security administrator role to User9
D. Assign the Global administrator role to User9

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 5
Which role should you assign to User1?

A. Global administrator
B. User administrator
C. Privileged role administrator
D. Security administrator

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

Question Set 4

QUESTION 1
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Azure AD app and attribute filtering settings.

Does that meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled

- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Password Hash Synchronization settings.

Does that meet the goal?

A. Yes

B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps

QUESTION 3
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Source Anchor settings.

Does that meet the goal?

A. Yes

B. No

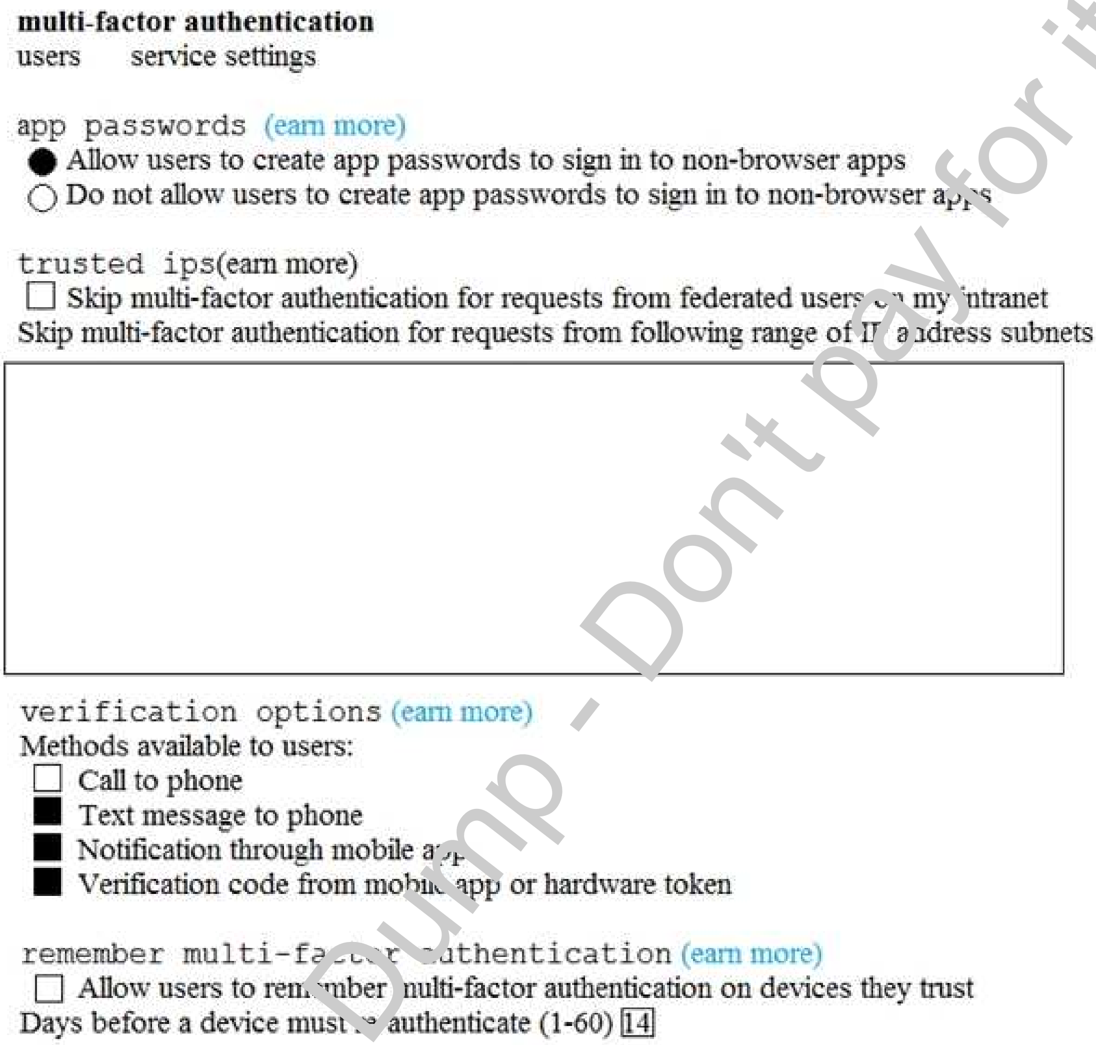
Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 4
HOTSPOT

You have a Microsoft 365 subscription that uses a default domain name of contoso.com.

The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Click the **Exhibit** tab.)



multi-factor authentication
users   service settings

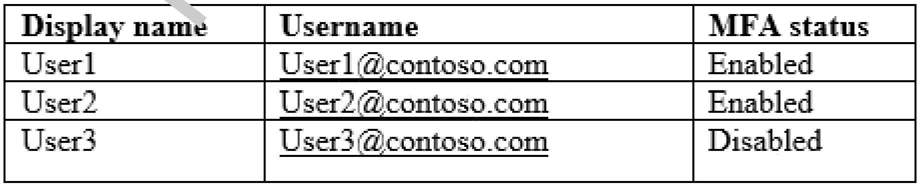
app passwords (earn more)
● Allow users to create app passwords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips(earn more)
□ Skip multi-factor authentication for requests from federated users on my intranet
Skip multi-factor authentication for requests from following range of IP address subnets

verification options (earn more)
Methods available to users:
□ Call to phone
■ Text message to phone
■ Notification through mobile app
■ Verification code from mobile app or hardware token

remember multi-factor authentication (earn more)
□ Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60) 14

In contoso.com, you create the users shown in the following table.

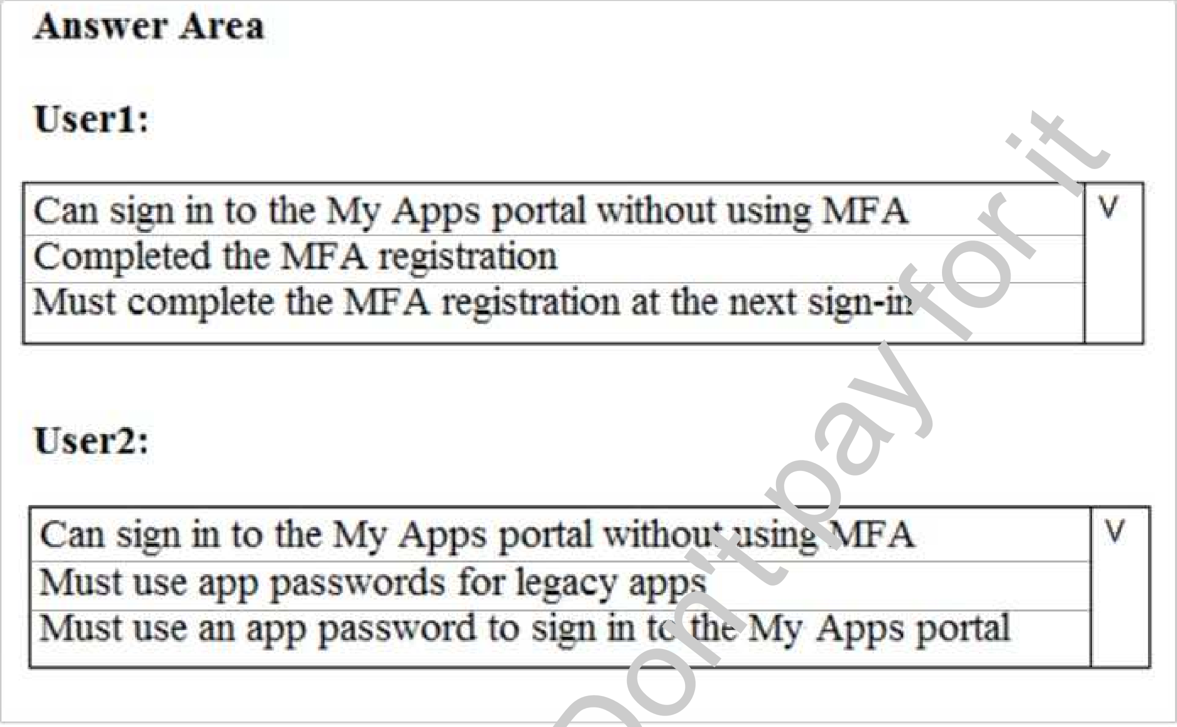


Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

What is the effect of the configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

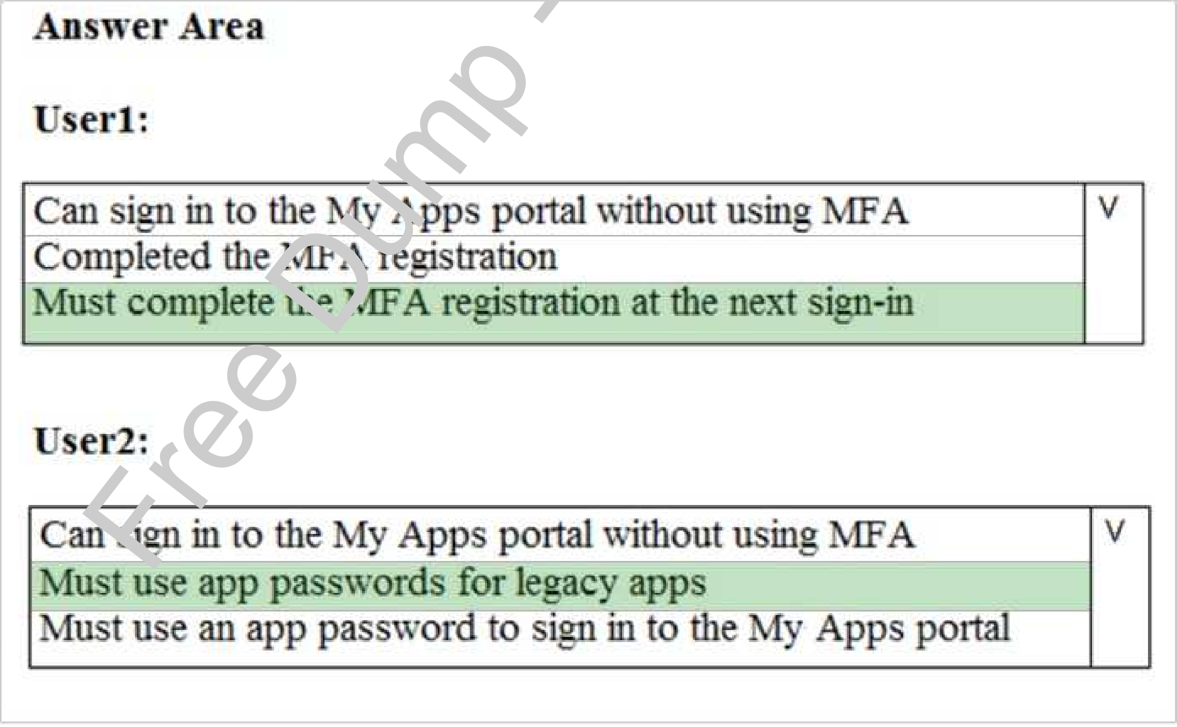
User1:

Can sign in to the My Apps portal without using MFA
Completed the MFA registration
Must complete the MFA registration at the next sign-in

User2:

Can sign in to the My Apps portal without using MFA
Must use app passwords for legacy apps
Must use an app password to sign in to the My Apps portal

Correct Answer:



Answer Area

User1:

Can sign in to the My Apps portal without using MFA
Completed the MFA registration
[✓ Must complete the MFA registration at the next sign-in]

User2:

Can sign in to the My Apps portal without using MFA
[✓ Must use app passwords for legacy apps]
Must use an app password to sign in to the My Apps portal

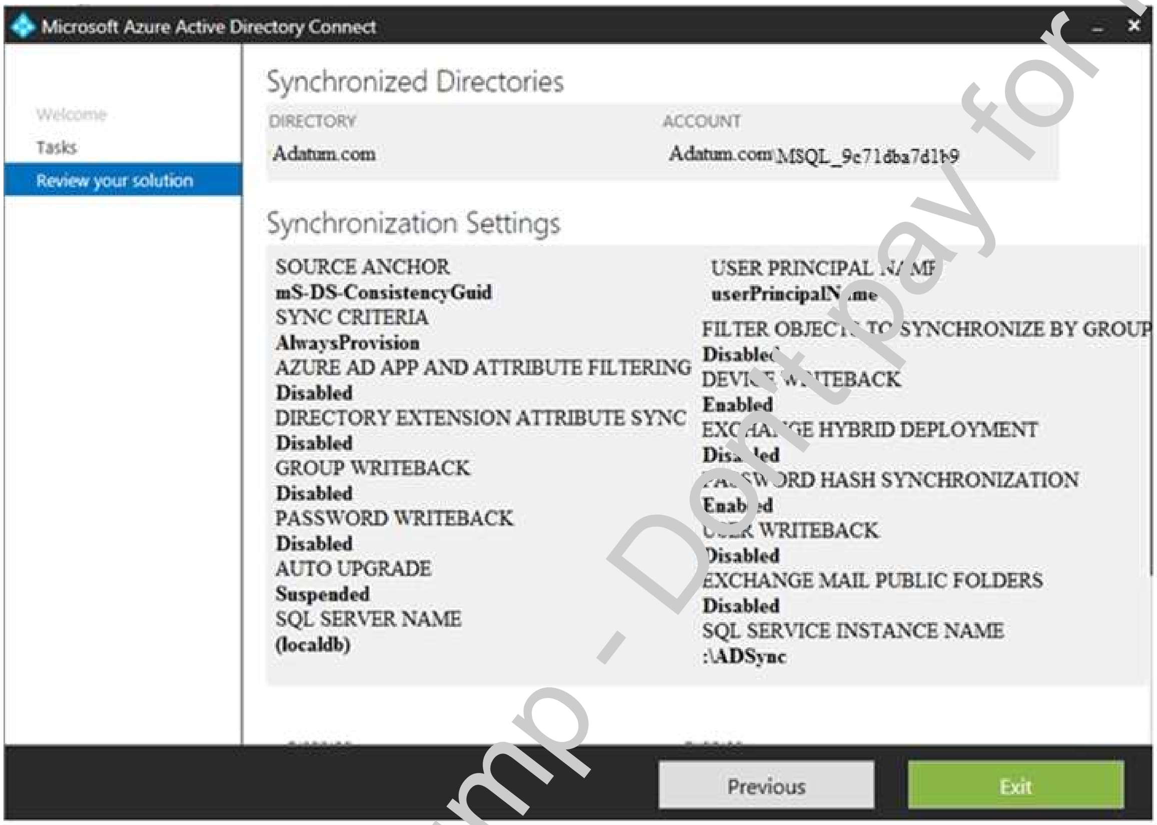
Section: [none]

Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

QUESTION 5
HOTSPOT

You configure Microsoft Azure Active Directory (Azure AD) Connect as shown in the following exhibit.



Synchronized Directories

DIRECTORY	ACCOUNT
Adatum.com	Adatum.com\MSQL_9c71dba7d1b9

Synchronization Settings

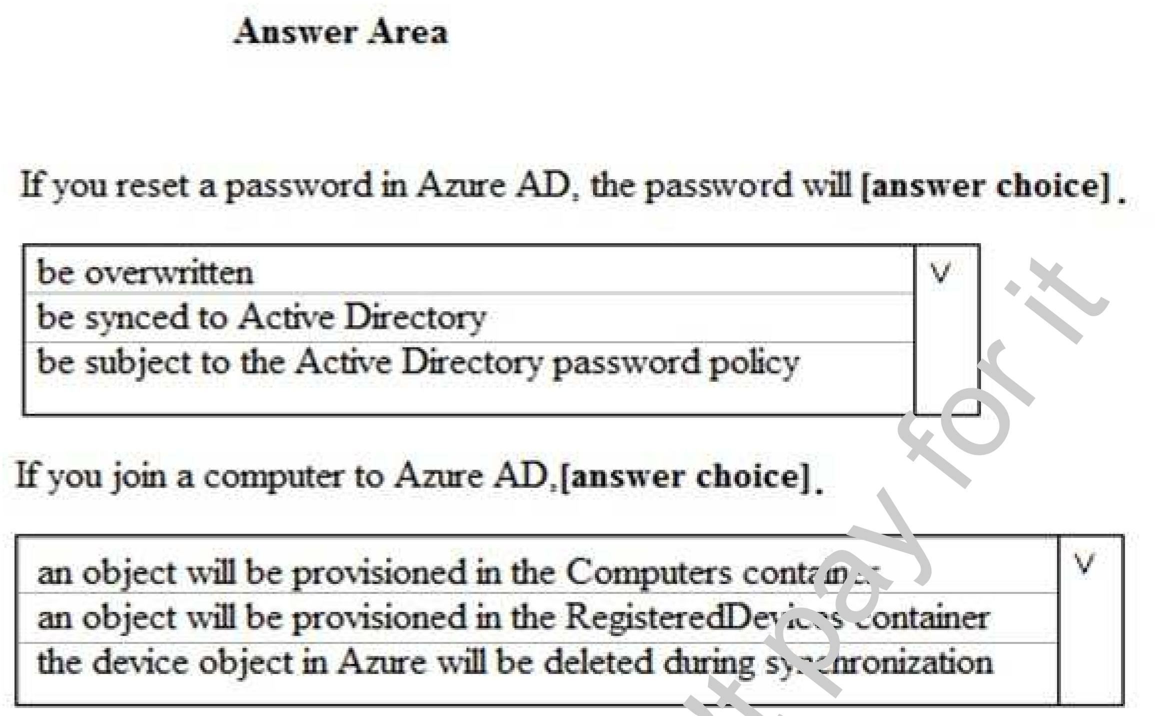
SOURCE ANCHOR
mS-DS-ConsistencyGuid
SYNC CRITERIA
AlwaysProvision
AZURE AD APP AND ATTRIBUTE FILTERING
Disabled
DIRECTORY EXTENSION ATTRIBUTE SYNC
Disabled
GROUP WRITEBACK
Disabled
PASSWORD WRITEBACK
Disabled
AUTO UPGRADE
Suspended
SQL SERVER NAME
(localdb)

USER PRINCIPAL NAME
userPrincipalName
FILTER OBJECTS TO SYNCHRONIZE BY GROUP
Disabled
DEVICE WRITEBACK
Enabled
EXCHANGE HYBRID DEPLOYMENT
Disabled
PASSWORD HASH SYNCHRONIZATION
Enabled
USER WRITEBACK
Disabled
EXCHANGE MAIL PUBLIC FOLDERS
Disabled
SQL SERVICE INSTANCE NAME
.\ADSync

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.

Hot Area:



Answer Area

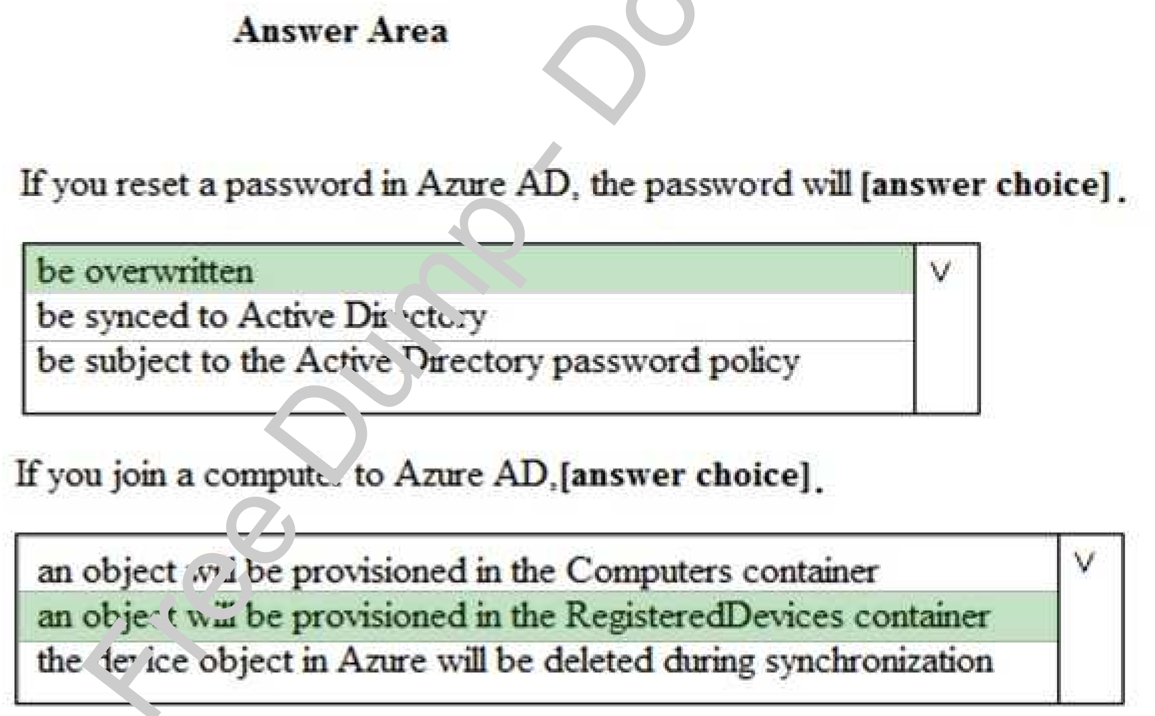
If you reset a password in Azure AD, the password will **[answer choice]**.

- be overwritten
- be synced to Active Directory
- be subject to the Active Directory password policy

If you join a computer to Azure AD,**[answer choice]**.

- an object will be provisioned in the Computers container
- an object will be provisioned in the RegisteredDevices container
- the device object in Azure will be deleted during synchronization

Correct Answer:



Answer Area

If you reset a password in Azure AD, the password will **[answer choice]**.

- [✓ be overwritten]
- be synced to Active Directory
- be subject to the Active Directory password policy

If you join a computer to Azure AD,**[answer choice]**.

- an object will be provisioned in the Computers container
- [✓ an object will be provisioned in the RegisteredDevices container]
- the device object in Azure will be deleted during synchronization

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback

QUESTION 6
You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune.

You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on-premises network.

What should you do first?

A. From the Azure Active Directory admin center, create a new certificate
B. Enable Application Proxy in Azure AD
C. From Active Directory Administrative Center, create a Dynamic Access Control policy
D. From the Azure Active Directory admin center, configure authentication methods

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity-windows10

QUESTION 7
You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you create a new user.

You plan to assign the Reports reader role to the user.

You need to see the permissions of the Reports reader role.

Which admin center should you use?

A. Azure Active Directory
B. Cloud App Security
C. Security & Compliance
D. Microsoft 365

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 8
You have a Microsoft 365 subscription.

You need to ensure that all users who are assigned the Exchange administrator role have multi-factor authentication (MFA) enabled by default.

What should you use to achieve the goal?

A. Security & Compliance permissions
B. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management

C. Microsoft Azure AD group management
D. Microsoft Office 365 user management

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 9
Your company has a Microsoft 365 subscription.

The company does not permit users to enroll personal devices in mobile device management (MDM).

Users in the sales department have personal iOS devices.

You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.

The users must be prevented from backing up the app's data to iCloud.

What should you create?

A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
B. an app protection policy in Microsoft Intune
C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
D. a device compliance policy in Microsoft Intune

Correct Answer: B
Section: [none]
Explanation

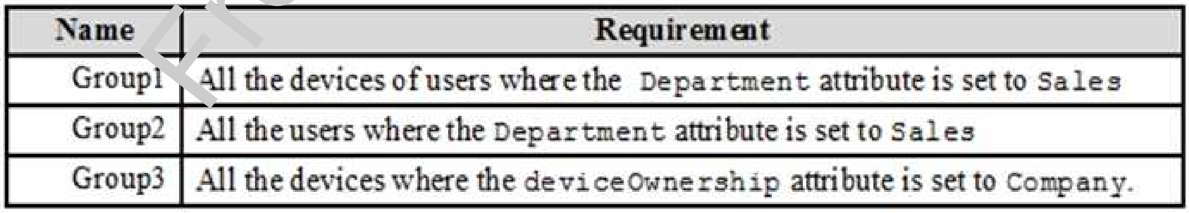
Explanation/Reference:

QUESTION 10
HOTSPOT

You have a Microsoft 365 E5 subscription.

Users and device objects are added and removed daily. Users in the sales department frequently change their device.

You need to create three following groups:



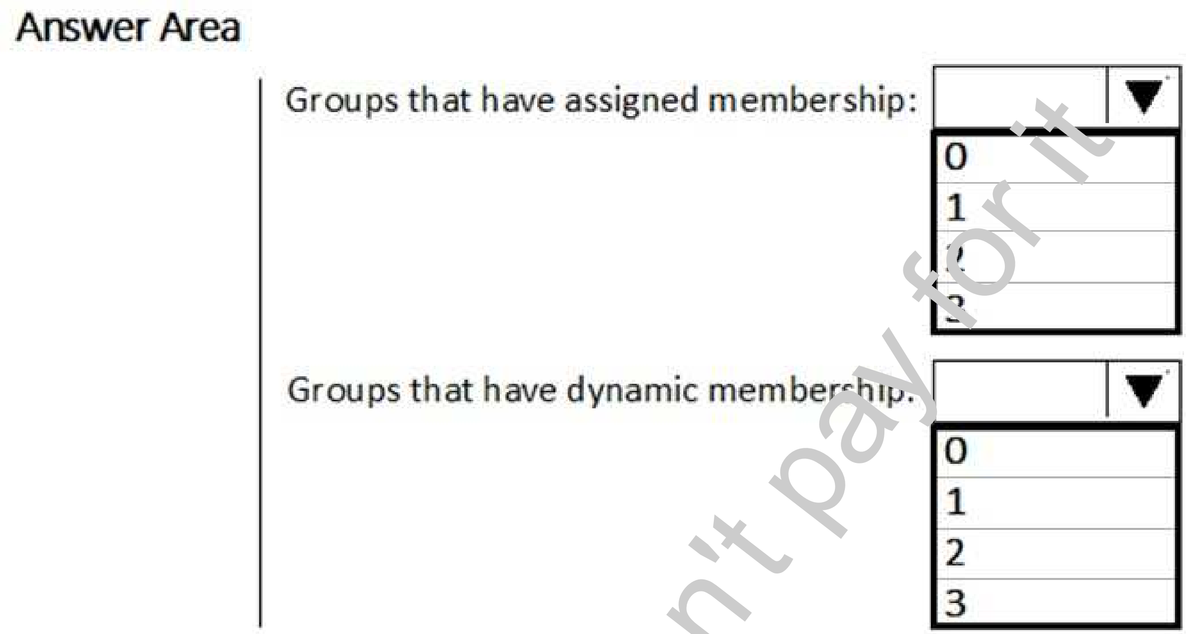
Name	Requirement
Group1	All the devices of users where the `Department` attribute is set to `Sales`
Group2	All the users where the `Department` attribute is set to `Sales`
Group3	All the devices where the `deviceOwnership` attribute is set to `Company.`

The solution must minimize administrative effort.

What is the minimum number of groups you should create for each type of membership? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

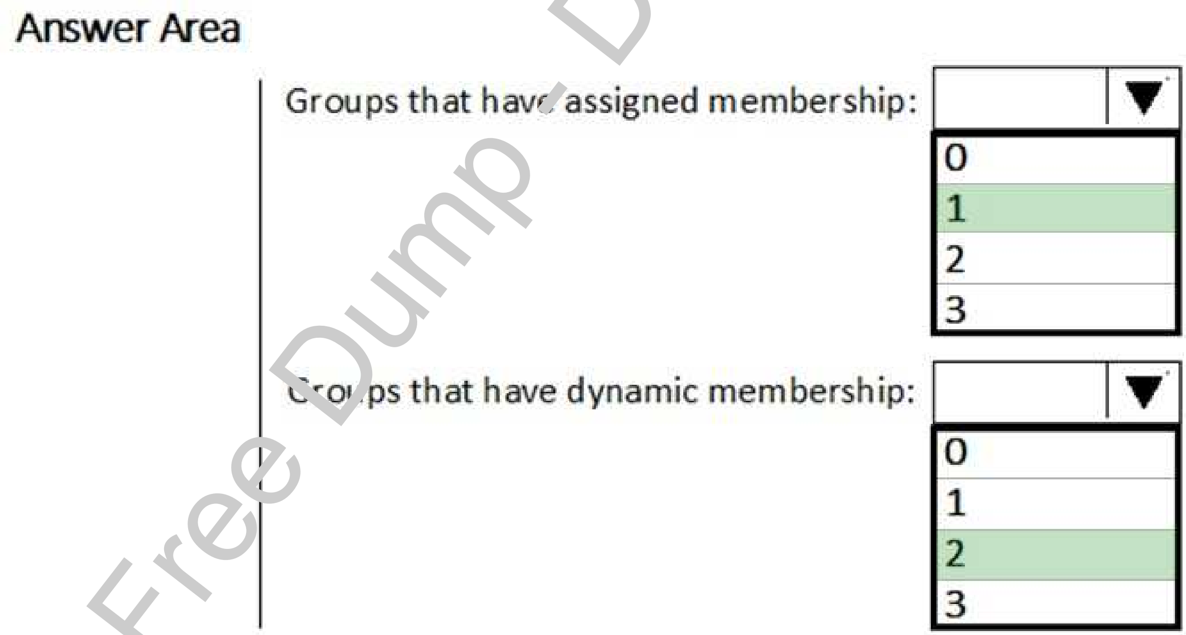
Groups that have assigned membership:

0
1
2
3

Groups that have dynamic membership:

0
1
2
3

Correct Answer:



Answer Area

Groups that have assigned membership:

0
[✓ 1]
2
3

Groups that have dynamic membership:

0
1
[✓ 2]
3

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Group 1 has to be assigned because you can't create a device group based on the device owners' attributes.

Group 2 can be dynamic because a user does have a department attribute.
Group 3 can be dynamic because a device does have a deviceownership attribute.

References:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dynamic-membership.md

QUESTION 11
Your company has a main office and a Microsoft 365 subscription.

You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.

What should you include in the configuration?

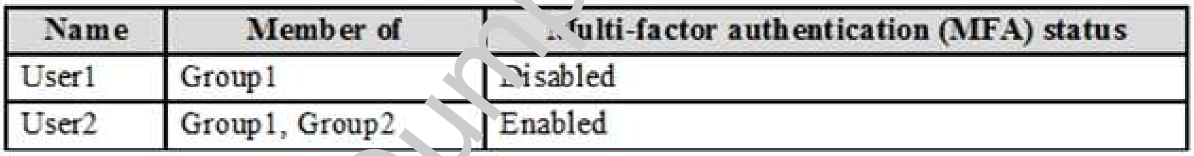
A. a user risk policy
B. a sign-in risk policy
C. a named location in Azure Active Directory (Azure AD)
D. an Azure MFA Server

Correct Answer: C
Section: [none]
Explanation

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

QUESTION 12
HOTSPOT

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



Name	Member of	Multi-factor authentication (MFA) status
User1	Group1	Disabled
User2	Group1, Group2	Enabled

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

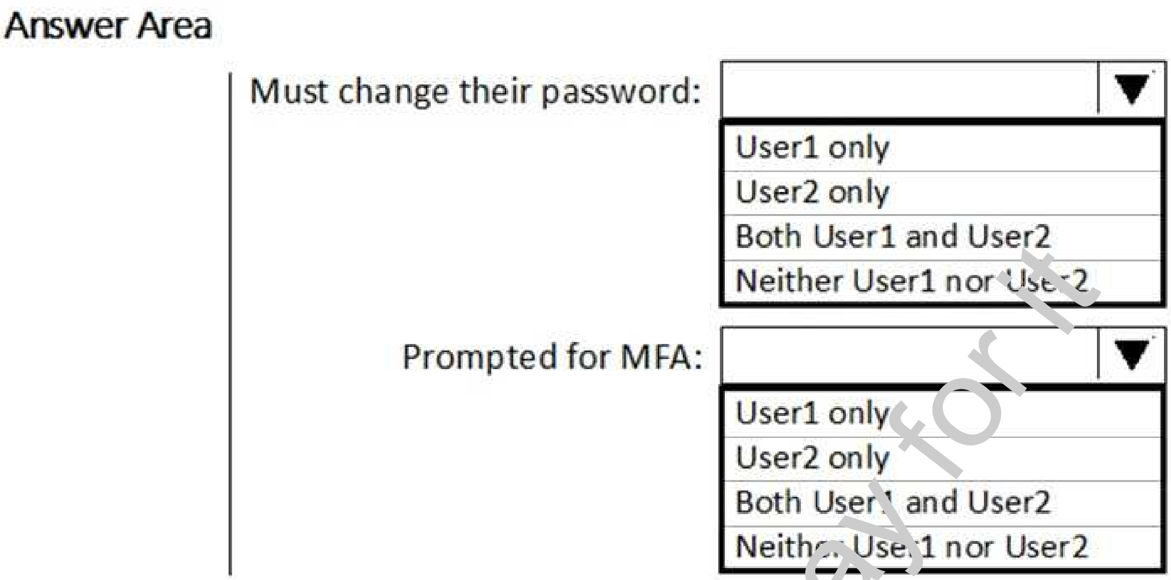
- Assignments: Include Group1, Exclude Group2
- Conditions: Sign-in risk of Low and above
- Access: Allow access, Require password change

You need to identify how the policy affects User1 and User2.

What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

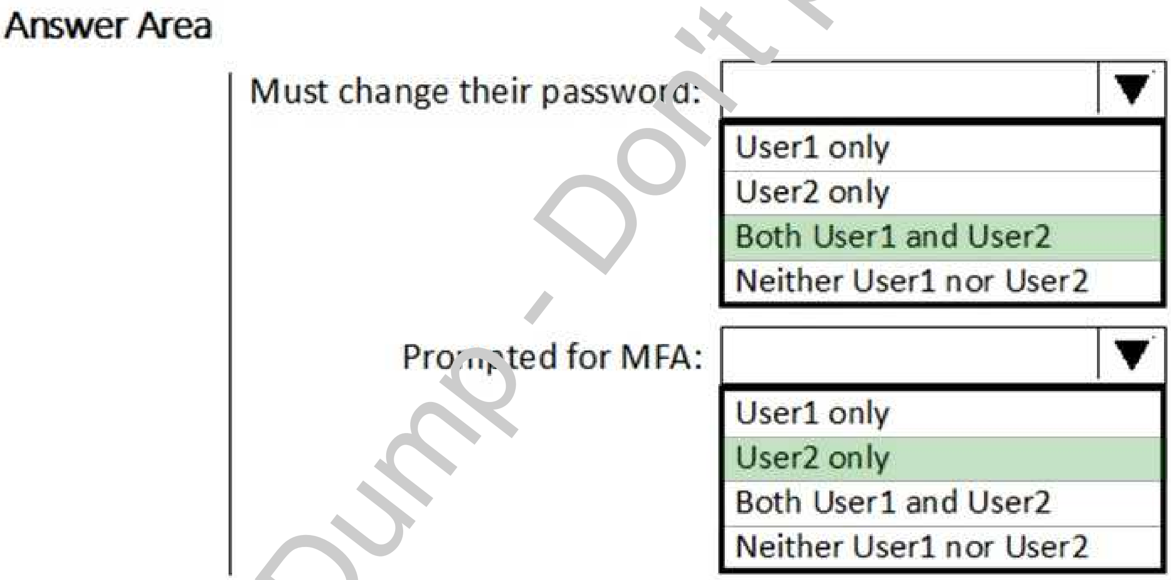
Must change their password:

- User1 only
- User2 only
- Both User1 and User2
- Neither User1 nor User2

Prompted for MFA:

- User1 only
- User2 only
- Both User1 and User2
- Neither User1 nor User2

Correct Answer:



Answer Area

Must change their password:

- User1 only
- User2 only
- [✓ Both User1 and User2]
- Neither User1 nor User2

Prompted for MFA:

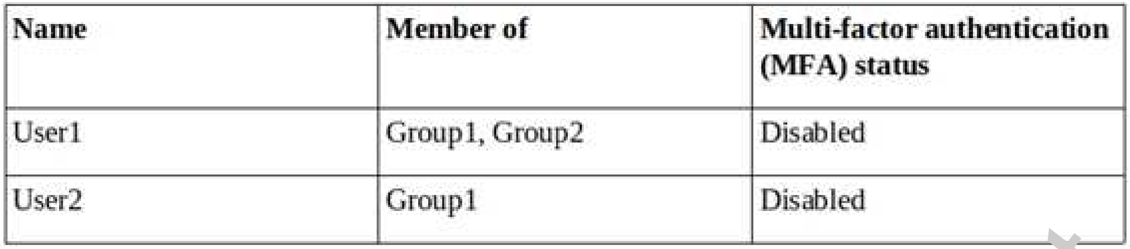
- User1 only
- [✓ User2 only]
- Both User1 and User2
- Neither User1 nor User2

Section: [none]
Explanation

Explanation/Reference:

QUESTION 13
HOTSPOT

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



Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

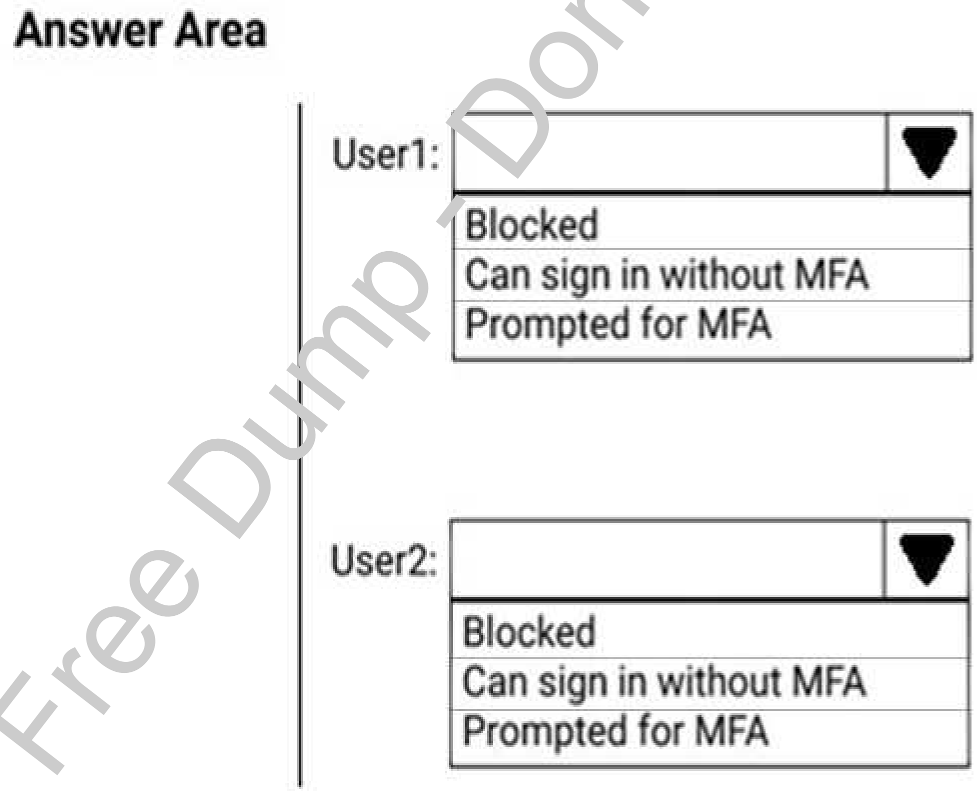
- Assignments: Include Group1, Exclude Group2
- Conditions: Sign-in risk of Low and above
- Access: Allow access, Require password multi-factor authentication

You need to identify how the policy affects User1 and User2.

What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

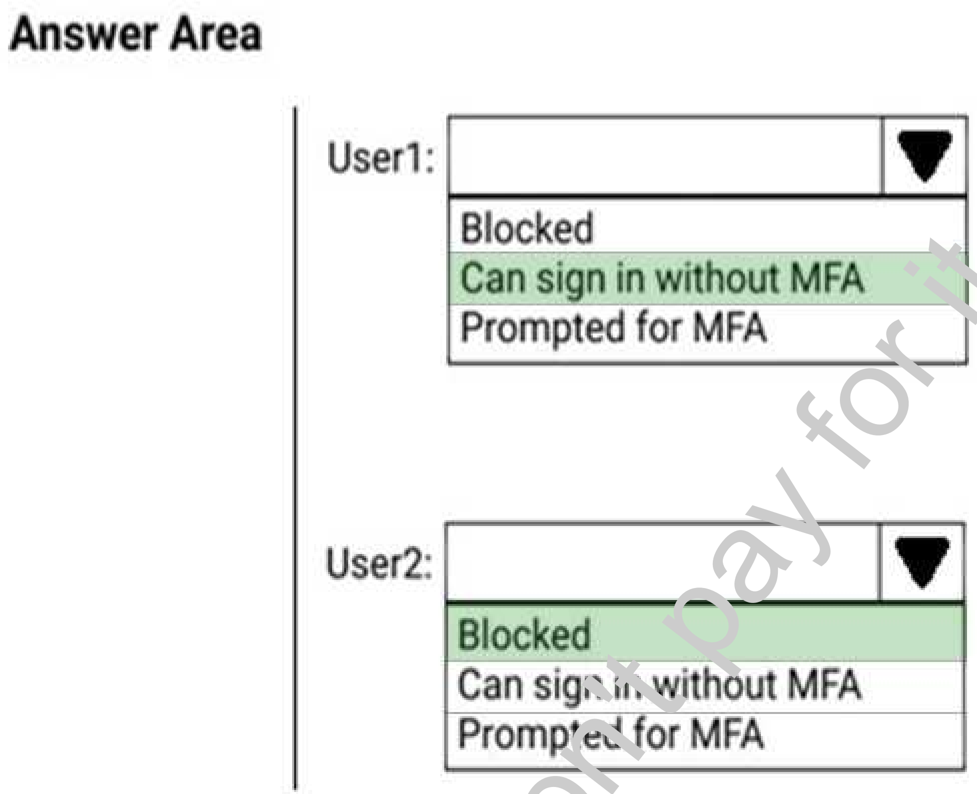


Answer Area

User1:
- Blocked
- Can sign in without MFA
- Prompted for MFA

User2:
- Blocked
- Can sign in without MFA
- Prompted for MFA

Correct Answer:



Answer Area

User1:
- Blocked
- [✓ Can sign in without MFA]
- Prompted for MFA

User2:
- [✓ Blocked]
- Can sign in without MFA
- Prompted for MFA

Section: [none]
Explanation

Explanation/Reference:

QUESTION 14
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 questions 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 an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server.

You need to view Azure AD Connect events.

You use the Security event log on Server1.

Does that meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

QUESTION 15
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 questions 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 an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server.

You need to view Azure AD Connect events.

You use the Directory Service event log on Server1.

Does that meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

QUESTION 16
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions 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 an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server.

You need to view Azure AD Connect events.

You use the System event log on Server1.

Does that meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

QUESTION 17
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 questions 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 an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server.

You need to view Azure AD Connect events.

You use the Application event log on Server1.

Does that meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

QUESTION 18
You have a Microsoft 365 E5 subscription without a Microsoft Azure subscription.

Some users are required to use an authenticator app to access Microsoft SharePoint Online.

You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.

What should you do?

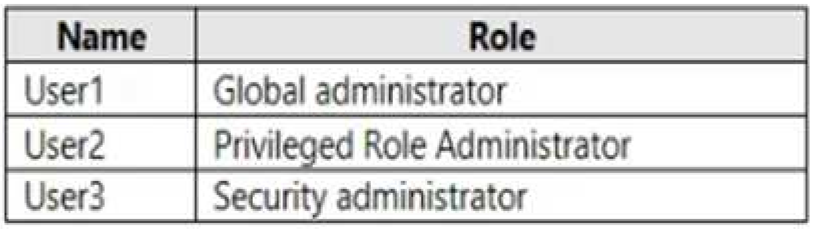
A. From the Security & Compliance admin center, download a report.
B. From Azure Log Analytics, query the logs.
C. From the Azure Active Directory admin center, view the audit logs.
D. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 19
HOTSPOT

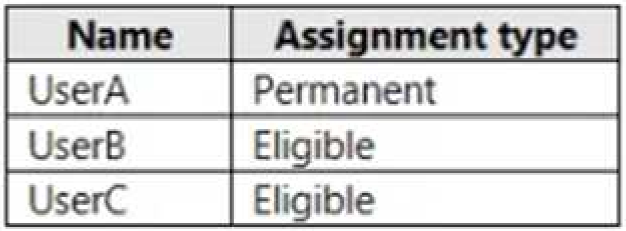
You have a Microsoft 365 subscription that contains the users shown in the following table.



Name	Role
User1	Global administrator
User2	Privileged Role Administrator
User3	Security administrator

You implement Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

From PIM, you review the Application Administrator role and discover the users shown in the following table.



Name	Assignment type
UserA	Permanent
UserB	Eligible
UserC	Eligible

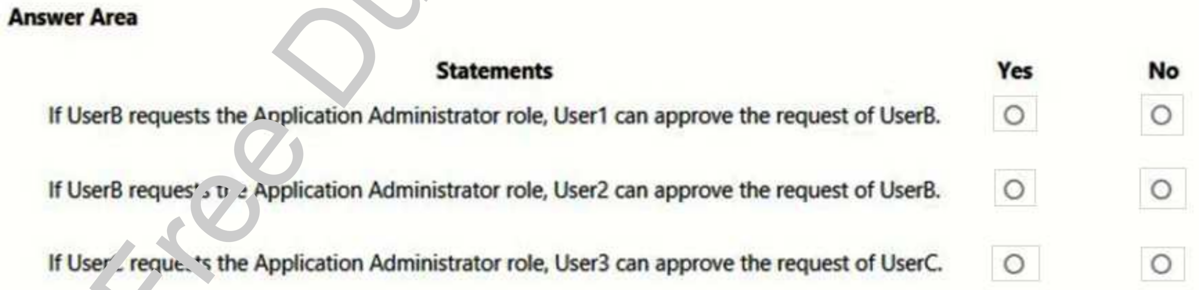
The Application Administrator role is configured to use the following settings in PIM:

- Maximum activation duration: 1 hour
- Notifications: Disable
- Incident/Request ticket: Disable
- Multi-Factor Authentication: Disable
- Require approval: Enable
- Selected approver: No results

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

NOTE: Each correct selection is worth one point.

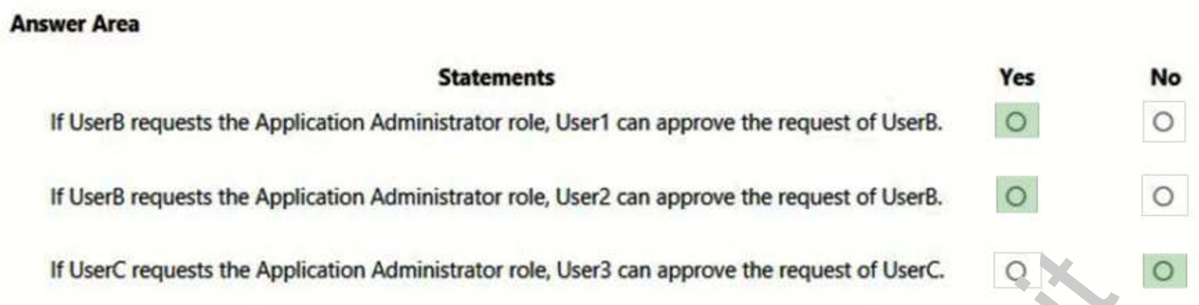
Hot Area:



Answer Area

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	○	○
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	○	○
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	[✓ ○]	○
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	[✓ ○]	○
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	○	[✓ ○]

Section: [none]
Explanation

Explanation/Reference:

Testlet 1

Overview
Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment

Network Infrastructure
The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements
Fabrikam identifies the following issues:

- Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.
- Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements

Planned Changes
Fabrikam plans to implement the following changes:

- Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory
- Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration
Fabrikam identifies the following application requirements for managing workload applications:

- User administrators will work from different countries
- User administrators will use the Azure Active Directory admin center
- Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements
Fabrikam identifies the following security requirements:

- Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed
- Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement
- Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send invitations
- Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory
- Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location
- The location of the user administrators must be audited when the administrators authenticate to Azure AD
- Email messages that include attachments containing malware must be delivered without the attachment
- The principle of least privilege must be used whenever possible

QUESTION 1

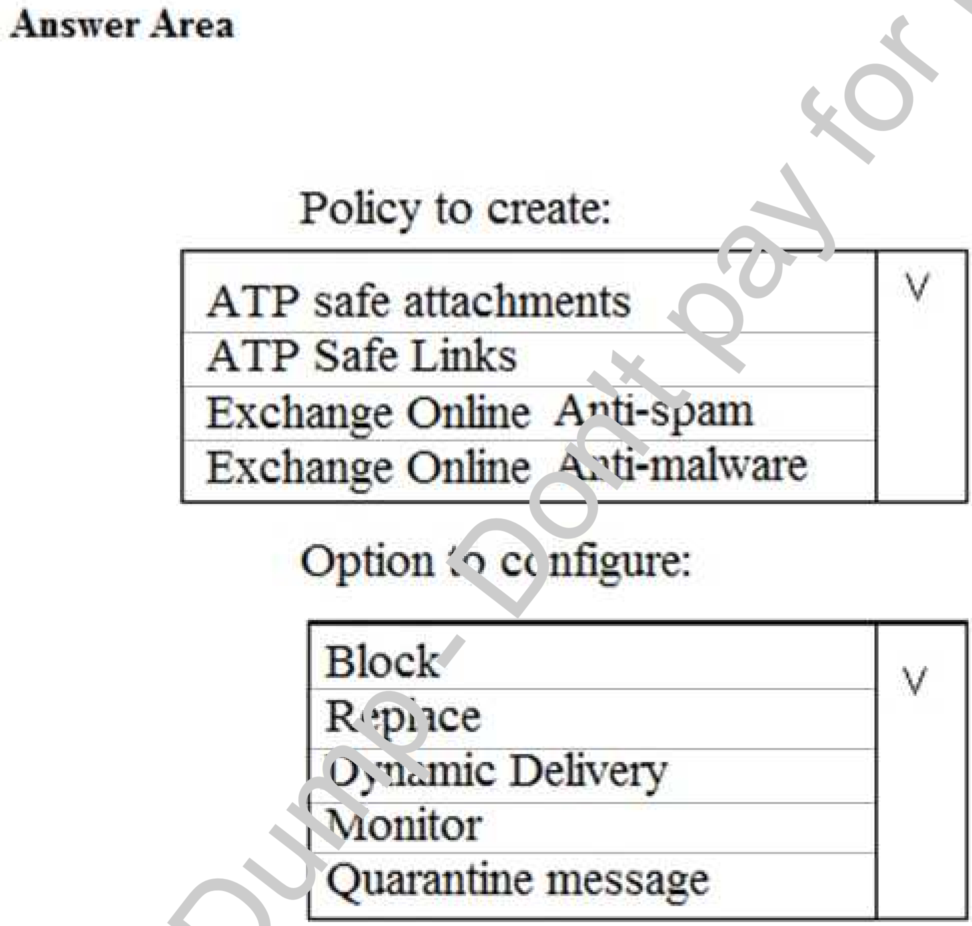
HOTSPOT

You need to recommend an email malware solution that meets the security requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

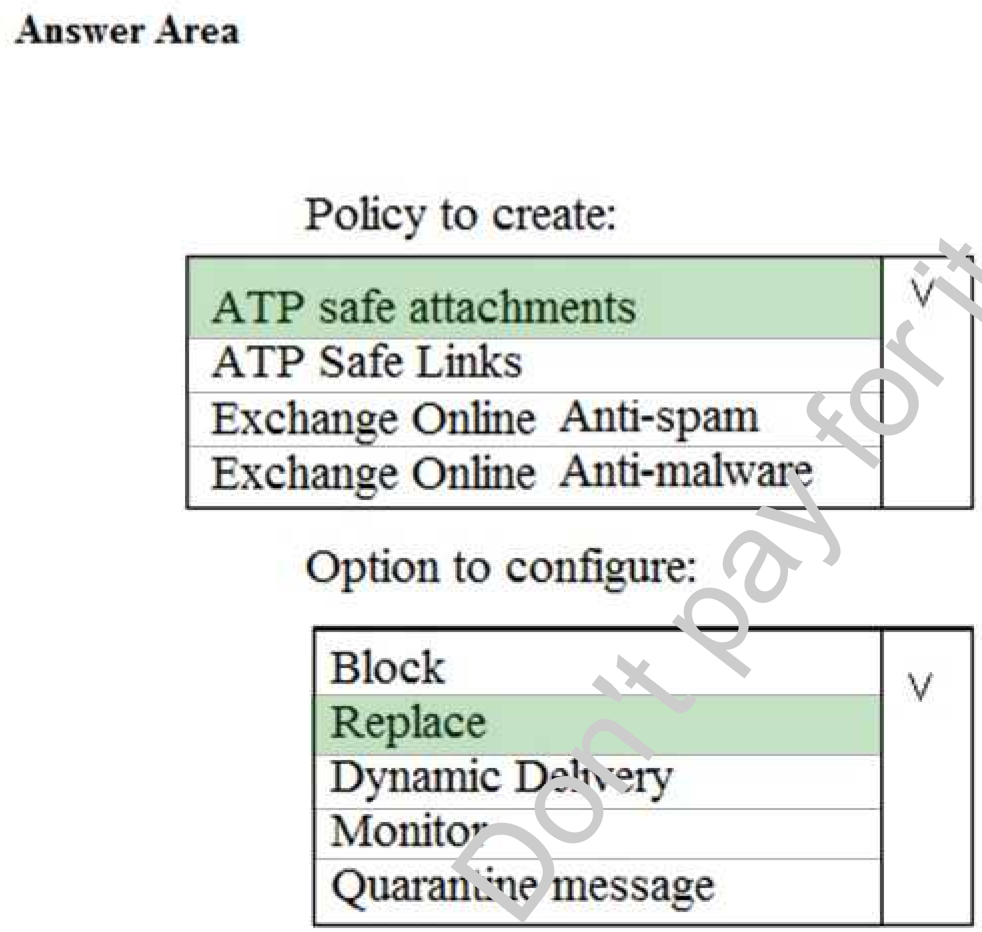
Policy to create:

- ATP safe attachments
- ATP Safe Links
- Exchange Online Anti-spam
- Exchange Online Anti-malware

Option to configure:

- Block
- Replace
- Dynamic Delivery
- Monitor
- Quarantine message

Correct Answer:



Answer Area

Policy to create:

- [✓ ATP safe attachments]
- ATP Safe Links
- Exchange Online Anti-spam
- Exchange Online Anti-malware

Option to configure:

- Block
- [✓ Replace]
- Dynamic Delivery
- Monitor
- Quarantine message

Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
HOTSPOT

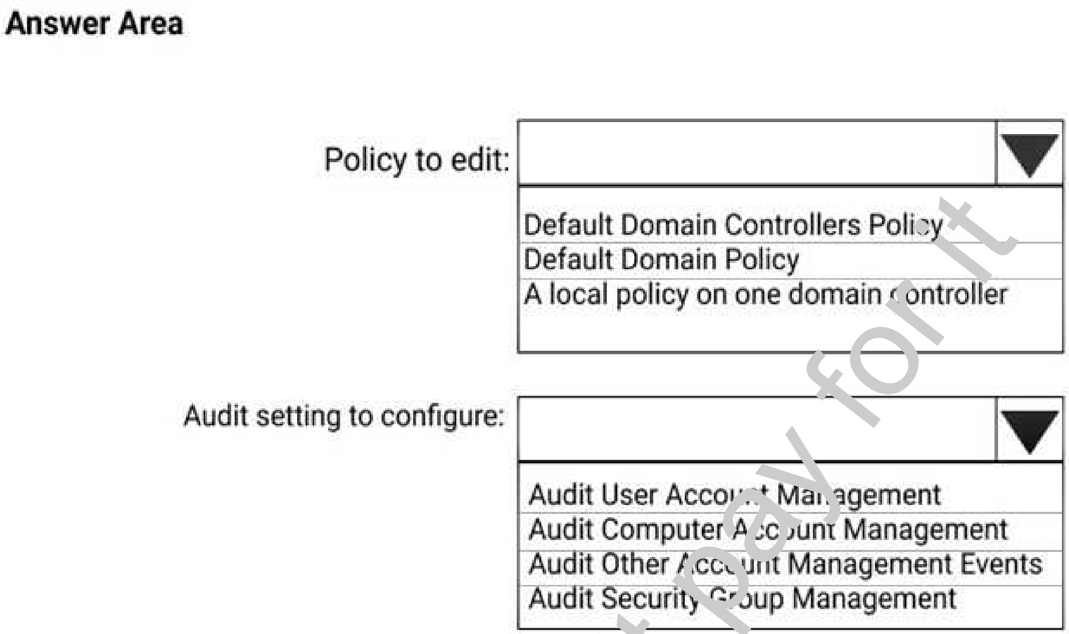
You install Azure ATP sensors on domain controllers.

You add a member to the Domain Admins group. You view the timeline in Azure ATP and discover that information regarding the membership change is missing.
You need to meet the security requirements for Azure ATP reporting.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

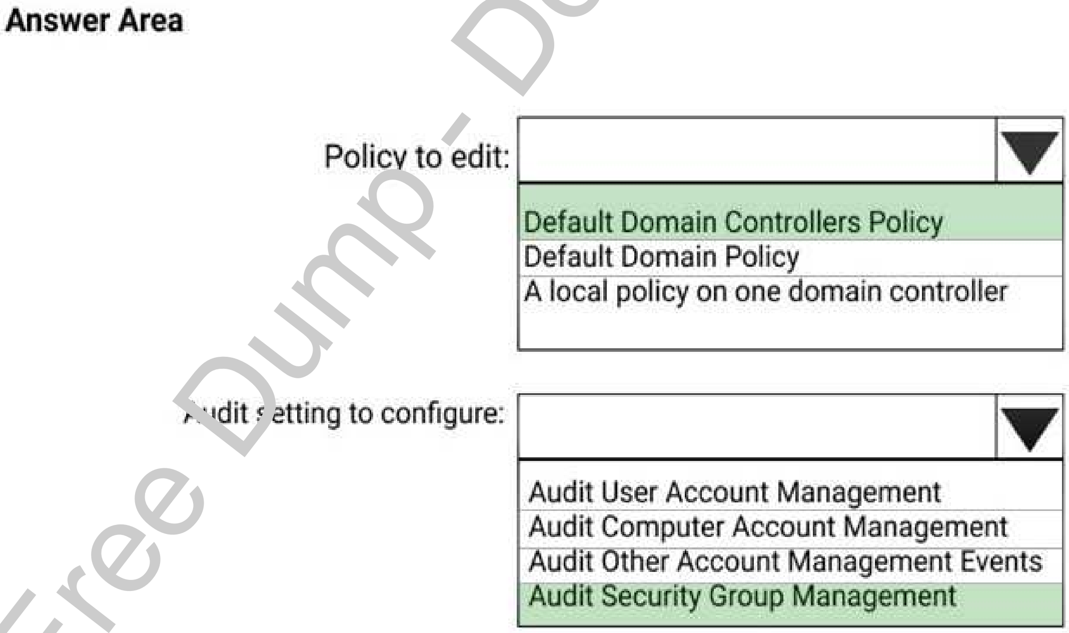
Policy to edit:

- Default Domain Controllers Policy
- Default Domain Policy
- A local policy on one domain controller

Audit setting to configure:

- Audit User Account Management
- Audit Computer Account Management
- Audit Other Account Management Events
- Audit Security Group Management

Correct Answer:



Answer Area

Policy to edit:

- [✓ Default Domain Controllers Policy]
- Default Domain Policy
- A local policy on one domain controller

Audit setting to configure:

- Audit User Account Management
- Audit Computer Account Management
- Audit Other Account Management Events
- [✓ Audit Security Group Management]

Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-advanced-audit-policy

Testlet 2

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.

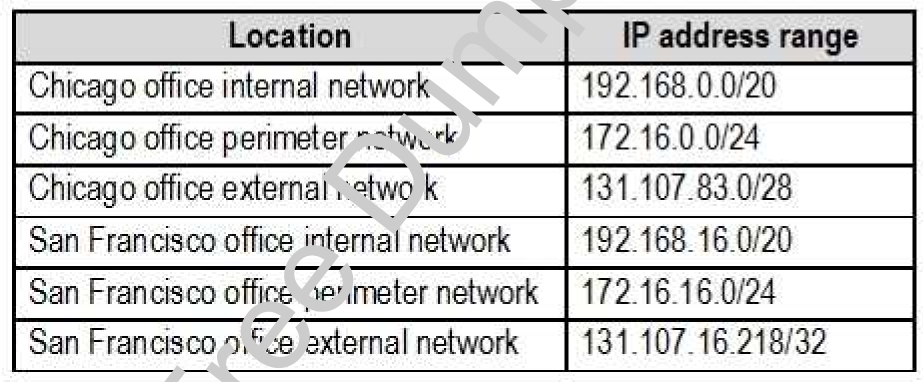
Overview
Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment

Internal Network Infrastructure
The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.



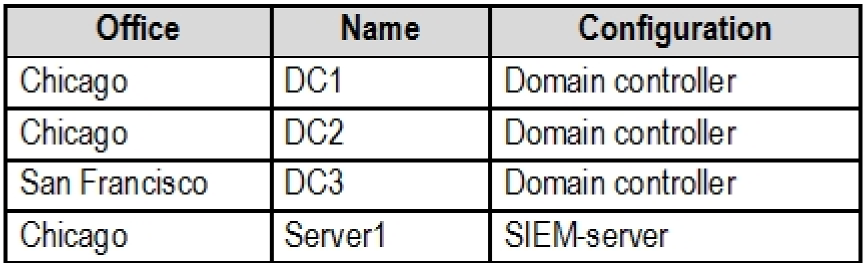
Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

- Windows Server 2016
- Windows 10 Enterprise
- Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.



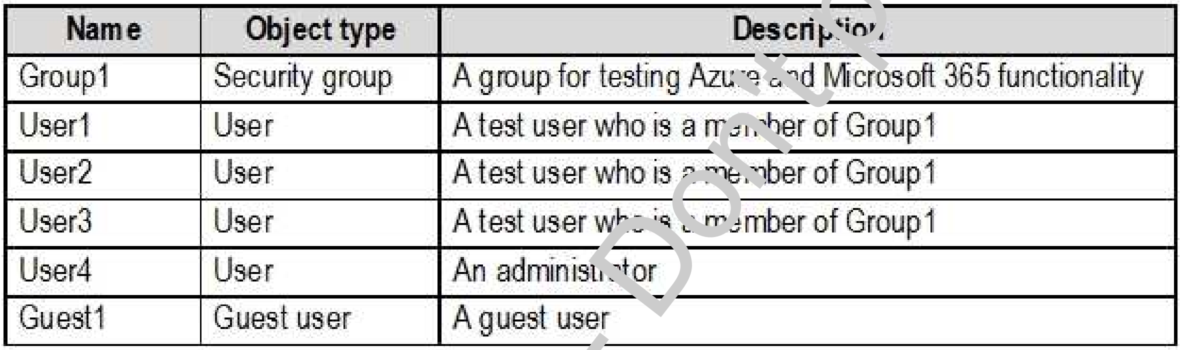
Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure
Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.



Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Planned Changes
Litware plans to implement the following changes:

- Migrate the email system to Microsoft Exchange Online
- Implement Azure AD Privileged Identity Management

Security Requirements
Litware identities the following security requirements:

- Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
- Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
- Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
- Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
- Implement a permanent eligible assignment of the Compliance administrator role for User1
- Configure domain-joined servers to ensure that they report sensor data to Windows Defender ATP
- Prevent access to Azure resources for the guest user accounts by default
- Ensure that all domain-joined computers are registered to Azure AD

Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.

You identify the following requirements for testing MFA:

- Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must **NOT** be used on the Chicago office internal network.

- If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
- Any disruption of legitimate authentication attempts must be minimized.

General Requirements
Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

QUESTION 1
DRAG DROP

You need to configure threat detection for Active Directory. The solution must meet the security requirements.

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.

Select and Place:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
You need to enable and configure Windows Defender ATP to meet the security requirements. What should you do?

A. Configure port mirroring
B. Create the `ForceDefenderPassiveMode` registry setting
C. Download and install the Microsoft Monitoring Agent
D. Run `WindowsDefenderATPOnboardingScript.cmd`

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

Testlet 3

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.

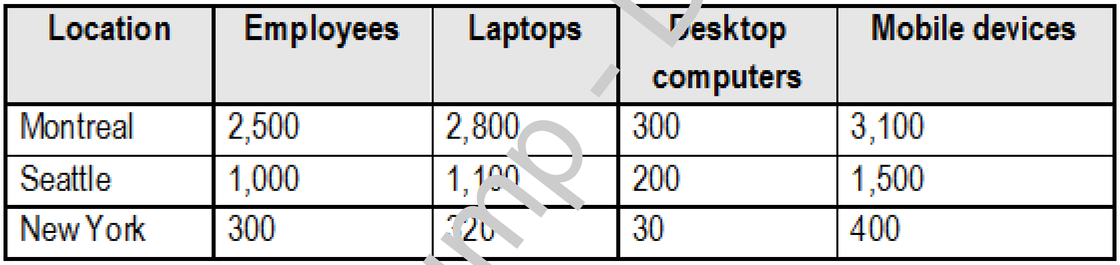
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

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

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

The company has the offices shown in the following table.



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

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment

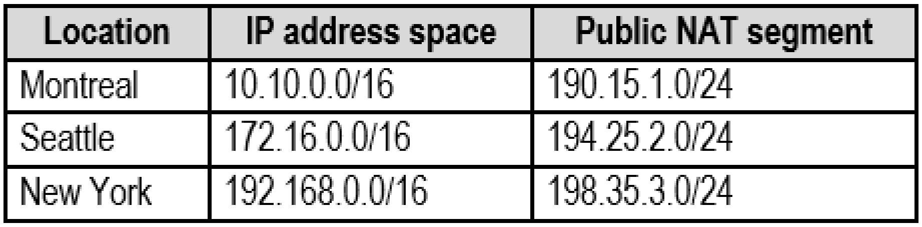
Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

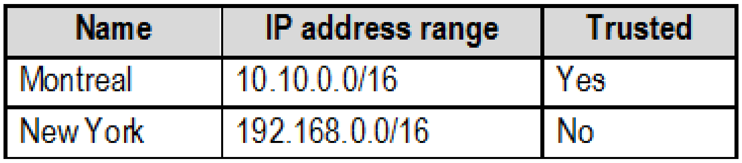
Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.



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

Named locations are defined in Azure AD as shown in the following table.

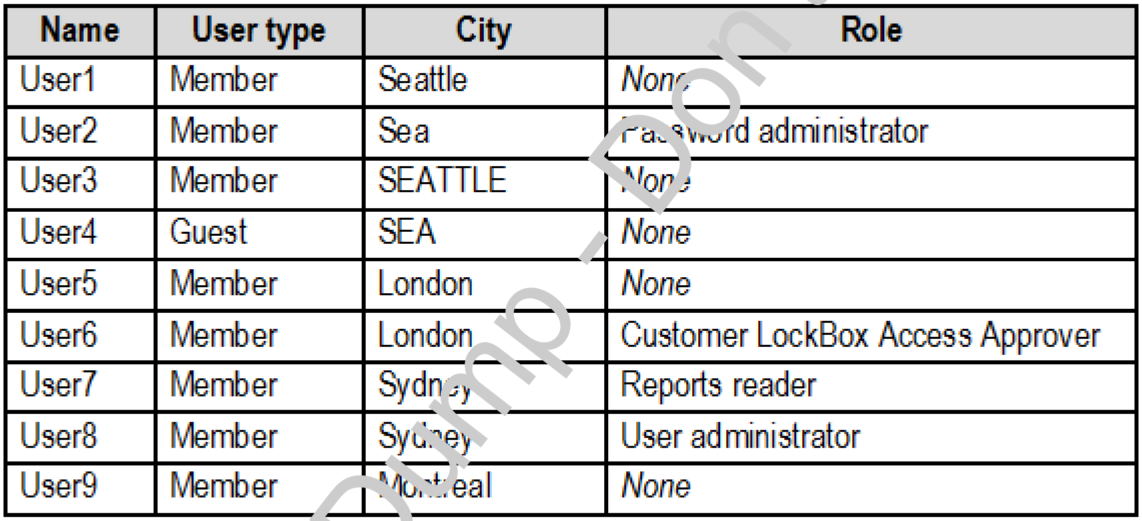


Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

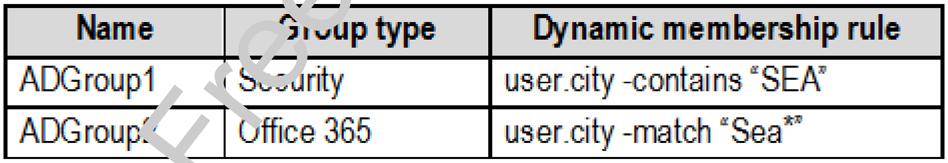
Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.



Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

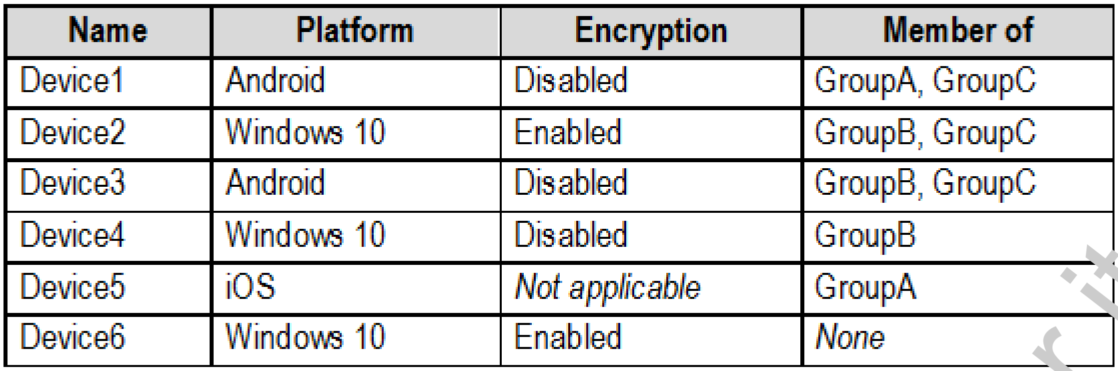


Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains “SEA”
ADGroup2	Office 365	user.city -match “Sea*”

Customer Lockbox is enabled in Microsoft 365.

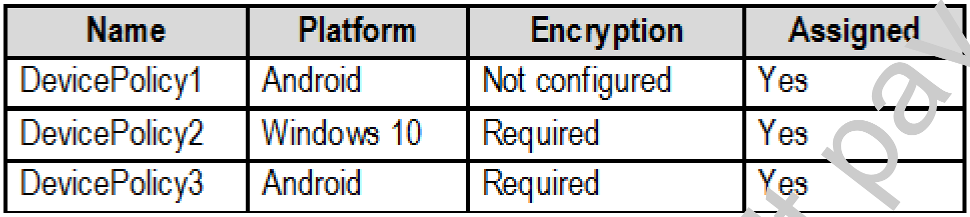
Microsoft Intune Configuration

The devices enrolled in Intune are configured as shown in the following table.



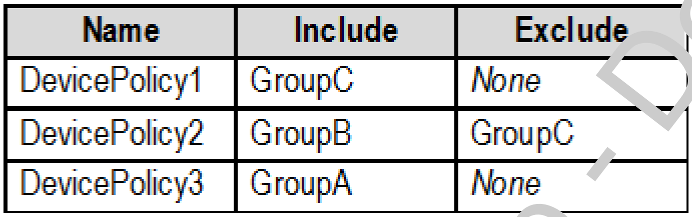
Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

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



Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

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



Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to **Compliant**.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

- Use the principle of least privilege
- Enable User1 to assign the Reports reader role to users
- Ensure that User6 approves Customer Lockbox requests as quickly as possible
- Ensure that User9 can enable and configure Azure AD Privileged Identity Management

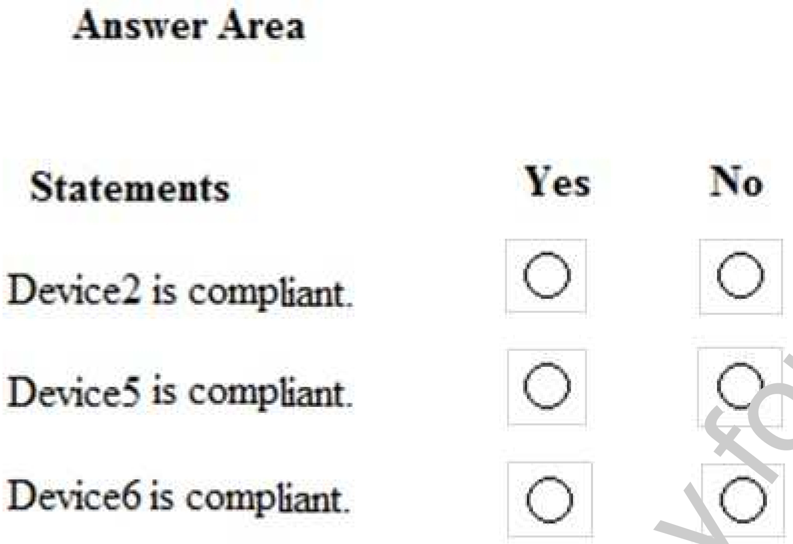
QUESTION 1
HOTSPOT

You are evaluating which devices are compliant in Intune.

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

NOTE: Each correct selection is worth one point.

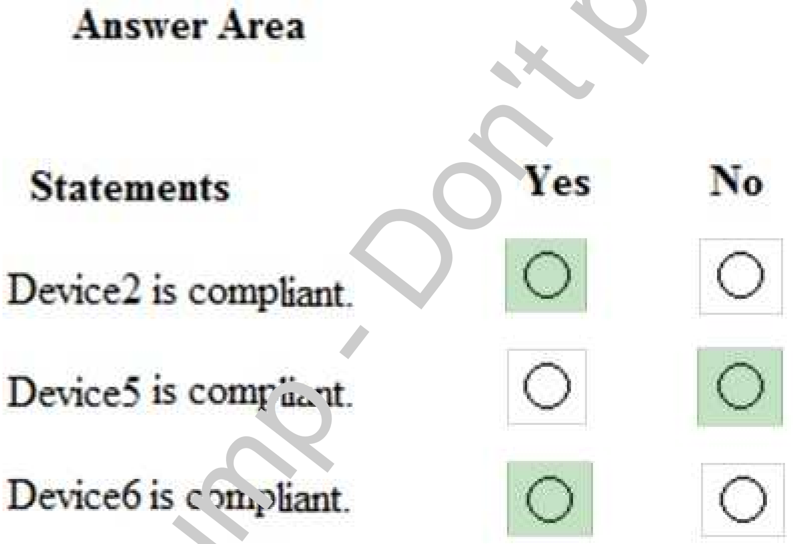
Hot Area:



Answer Area

Statements	Yes	No
Device2 is compliant.	○	○
Device5 is compliant.	○	○
Device6 is compliant.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Device2 is compliant.	[✓ ○]	○
Device5 is compliant.	○	[✓ ○]
Device6 is compliant.	[✓ ○]	○

Section: [none]
Explanation

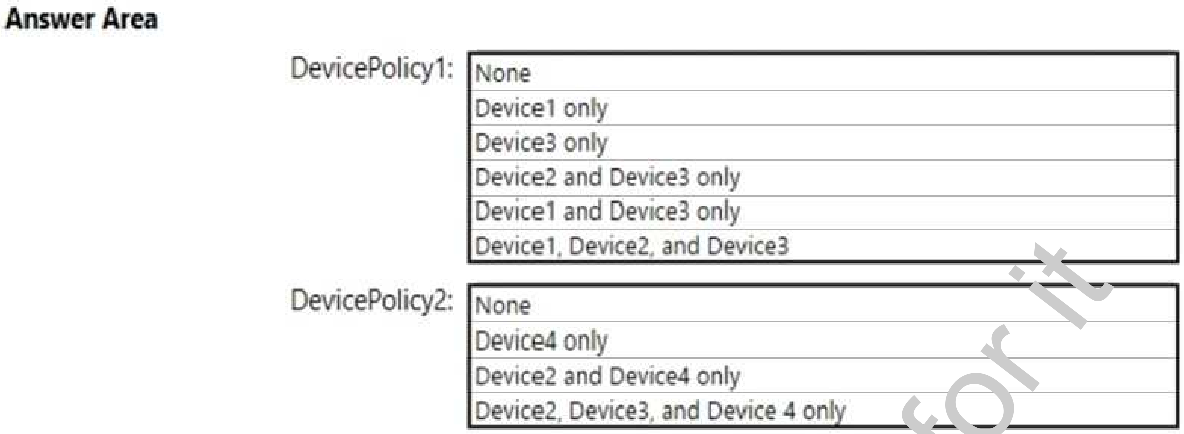
Explanation/Reference:

QUESTION 2
HOTSPOT

Which policies apply to which devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

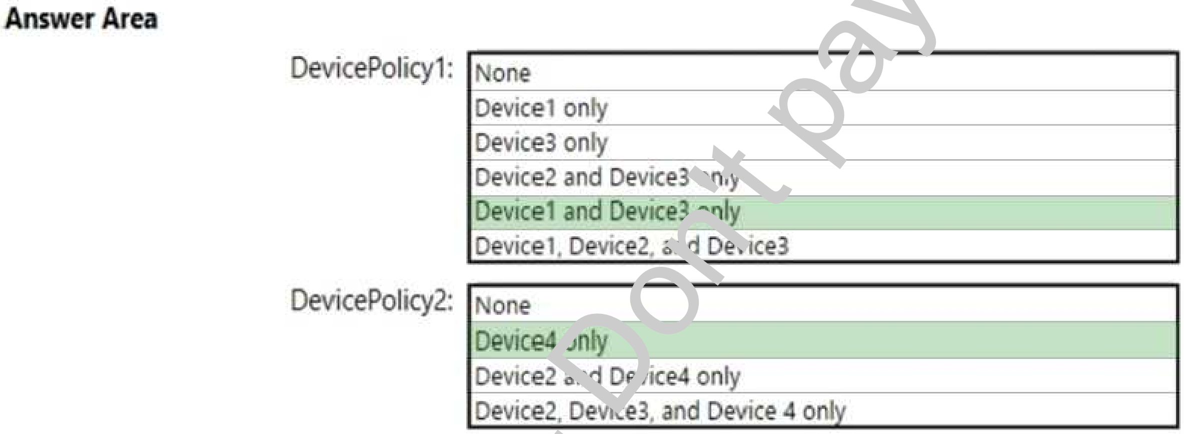


Answer Area

DevicePolicy1:
- None
- Device1 only
- Device3 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device3

DevicePolicy2:
- None
- Device4 only
- Device2 and Device4 only
- Device2, Device3, and Device 4 only

Correct Answer:



Answer Area

DevicePolicy1:
- None
- Device1 only
- Device3 only
- Device2 and Device3 only
- [✓ Device1 and Device3 only]
- Device1, Device2, and Device3

DevicePolicy2:
- None
- [✓ Device4 only]
- Device2 and Device4 only
- Device2, Device3, and Device 4 only

Section: [none]
Explanation

Explanation/Reference:

Question Set 4

QUESTION 1
You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription.

You need to allow a user named User1 to view ATP reports in the Threat management dashboard.

Which role provides User1 with the required role permissions?

A. Security reader
B. Message center reader
C. Compliance administrator
D. Information Protection administrator
E. Service administrator
F. Exchange administrator

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-are-needed-to-view-the-atp-reports

QUESTION 2
You have a Microsoft 365 Enterprise E5 subscription.

You use Windows Defender Advanced Threat Protection (Windows Defender ATP). You plan to use Microsoft Office 365 Attack simulator.

What is a prerequisite for running Attack simulator?

A. Enable multi-factor authentication (MFA)
B. Configure Advanced Threat Protection (ATP)
C. Create a Conditional Access App Control policy for accessing Office 365
D. Integrate Office 365 Threat Intelligence and Windows Defender ATP

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

QUESTION 3
You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.

Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.

You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members.

The email addresses that you intend to spoof belong to the Executive group members.

What should you do first?

A. From the Azure ATP admin center, configure the primary workspace settings
B. From the Microsoft Azure portal, configure the user risk policy settings in Azure AD Identity Protection
C. Enable MFA for the Research group members
D. Migrate the Executive group members to Exchange Online

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

QUESTION 4
You have a Microsoft 365 E5 subscription.

You implement Advanced Threat Protection (ATP) safe attachments policies for all users.

User reports that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to receive email messages that contain attachments. The solution must ensure that all attachments are scanned for malware. Attachments that have malware must be blocked.

What should you do from ATP?

A. Set the action to **Block**
B. Add an exception
C. Add a condition
D. Set the action to **Dynamic Delivery**

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-previewing

QUESTION 5
HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed.

You have a Microsoft Azure subscription.

You are deploying Azure Advanced Threat Protection (ATP)

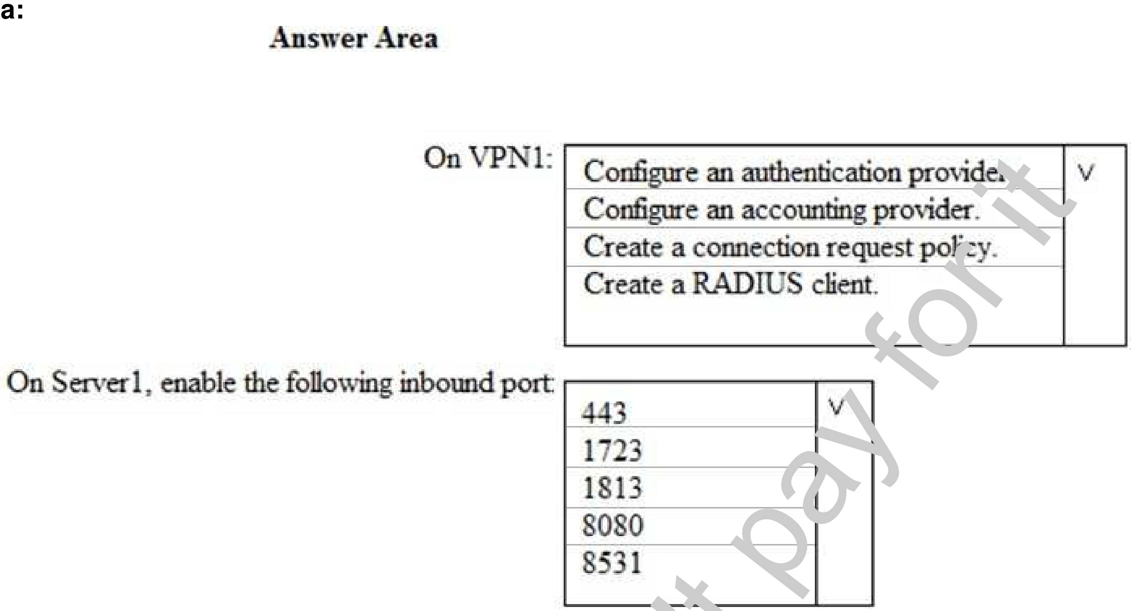
You install an Azure ATP standalone sensor on a server named Server1 that runs Windows Server 2016.

You need to integrate the VPN and Azure ATP.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

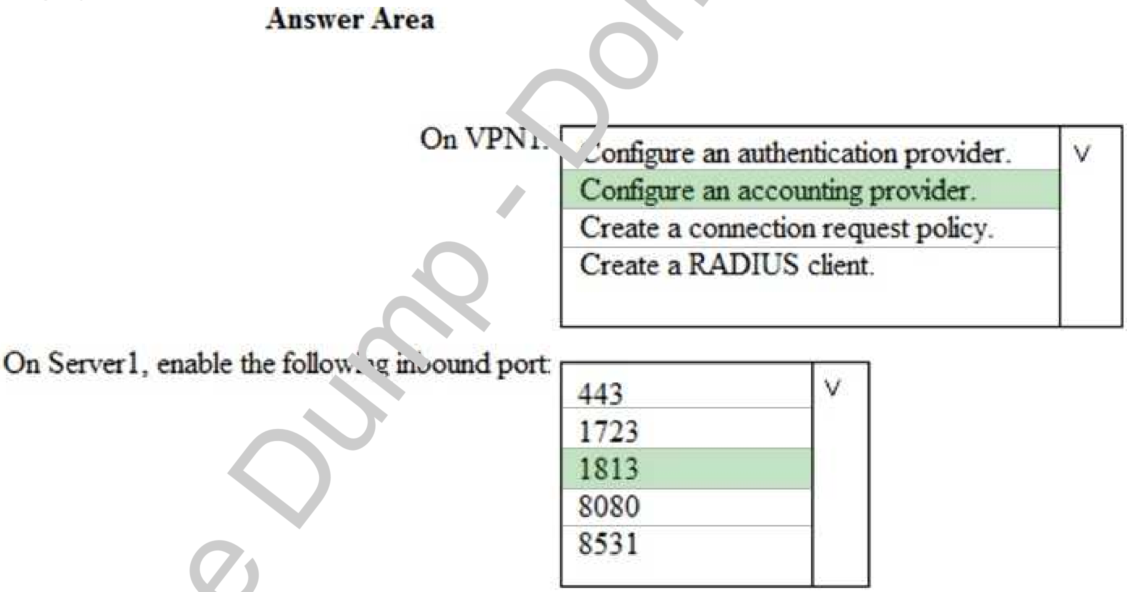
On VPN1:

- Configure an authentication provider.
- Configure an accounting provider.
- Create a connection request policy.
- Create a RADIUS client.

On Server1, enable the following inbound port:

- 443
- 1723
- 1813
- 8080
- 8531

Correct Answer:



Answer Area

On VPN1:

- Configure an authentication provider.
- [✓ Configure an accounting provider.]
- Create a connection request policy.
- Create a RADIUS client.

On Server1, enable the following inbound port:

- 443
- 1723
- [✓ 1813]
- 8080
- 8531

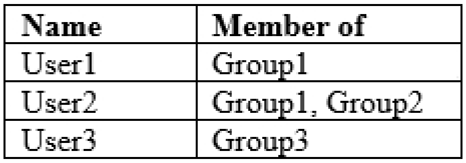
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn

QUESTION 6
HOTSPOT

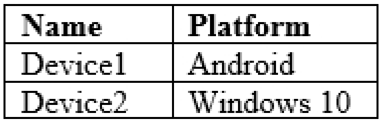
You have a Microsoft 365 subscription that uses a default domain name of contoso.com.

Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Intune has two devices enrolled as shown in the following table:



Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.

You create an app protection policy named ProtectionPolicy1 that has the following settings:

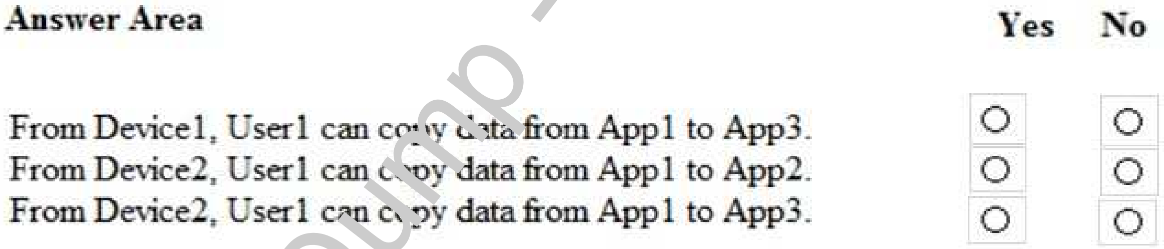
- Protected apps: App1
- Exempt apps: App2
- Windows Information Protection mode: Block

You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1.

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

NOTE: Each correct selection is worth one point.

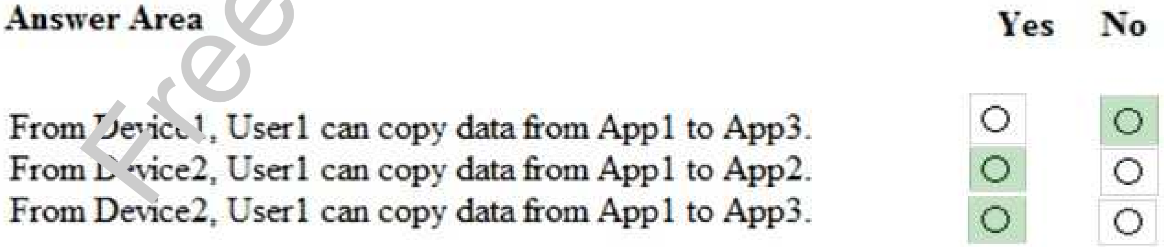
Hot Area:



Answer Area

	Yes	No
From Device1, User1 can copy data from App1 to App3.	○	○
From Device2, User1 can copy data from App1 to App2.	○	○
From Device2, User1 can copy data from App1 to App3.	○	○

Correct Answer:



Answer Area

	Yes	No
From Device1, User1 can copy data from App1 to App3.	○	[✓ ○]
From Device2, User1 can copy data from App1 to App2.	[✓ ○]	○
From Device2, User1 can copy data from App1 to App3.	[✓ ○]	○

Section: [none]
Explanation

Explanation/Reference:

QUESTION 7
You have a Microsoft 365 tenant.

You have 500 computers that run Windows 10.

You plan to monitor the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP) after the computers are enrolled in Microsoft Intune.

You need to ensure that the computers connect to Windows Defender ATP.

How should you prepare Intune for Windows Defender ATP?

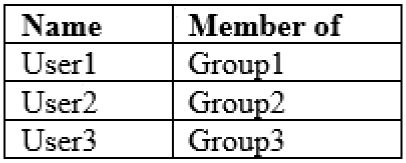
A. Configure an enrollment restriction
B. Create a device configuration profile
C. Create a conditional access policy
D. Create a Windows Autopilot deployment profile

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/intune/advanced-threat-protection

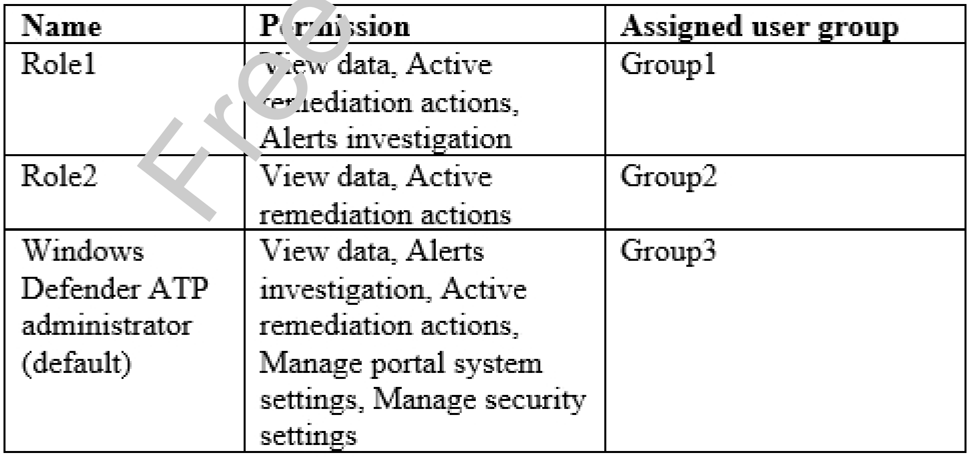
QUESTION 8
HOTSPOT

Your company has a Microsoft 365 subscription that contains the users shown in the following table.



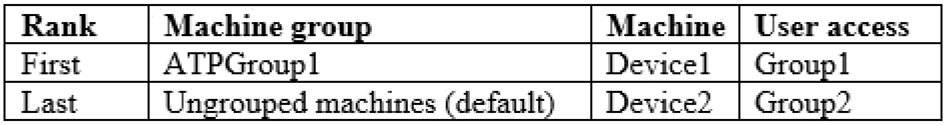
Name	Member of
User1	Group1
User2	Group2
User3	Group3

The company implements Windows Defender Advanced Threat Protection (Windows Defender ATP). Windows Defender ATP includes the roles shown in the following table:



Name	Permission	Assigned user group
Role1	View data, Active remediation actions, Alerts investigation	Group1
Role2	View data, Active remediation actions	Group2
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Windows Defender ATP contains the machine groups shown in the following table:

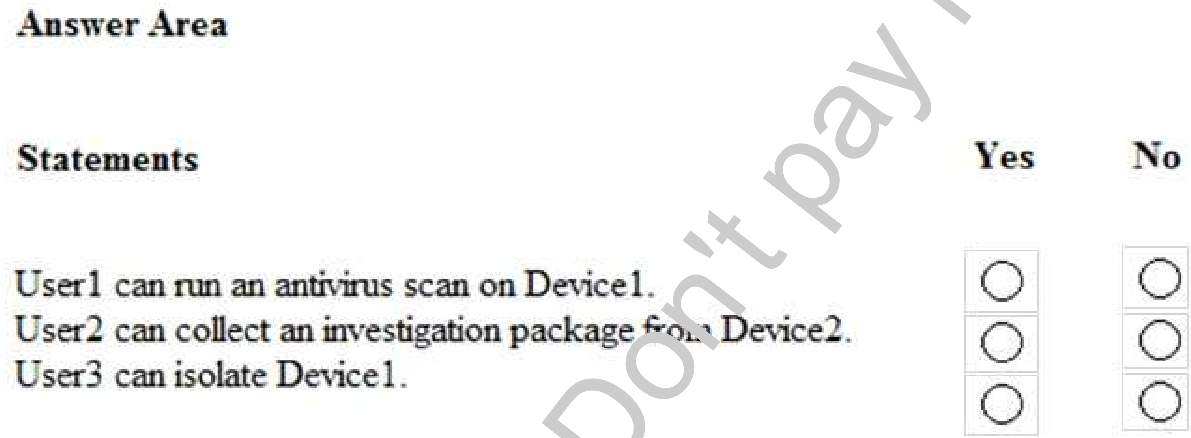


Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

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

NOTE: Each correct selection is worth one point.

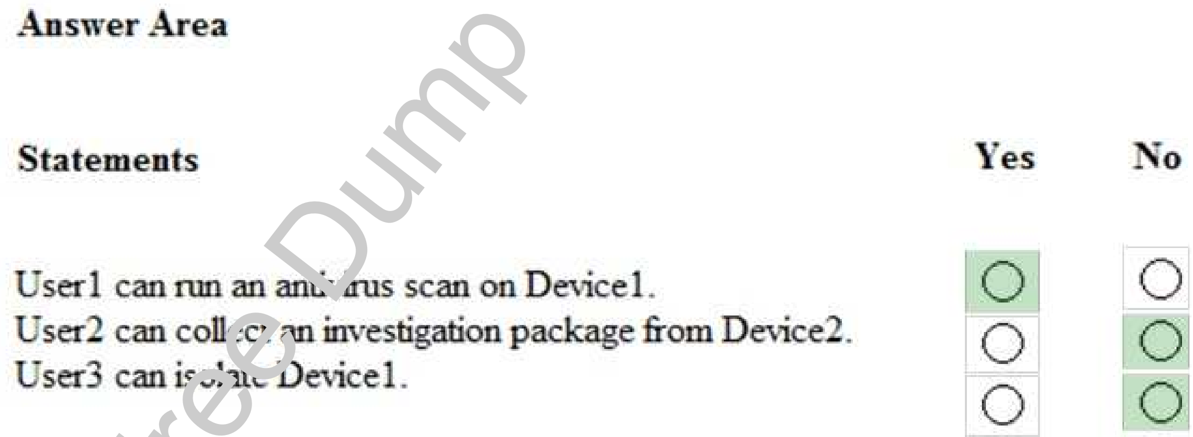
Hot Area:



Answer Area

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

Correct Answer:



Answer Area

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

Section: [none]
Explanation

Explanation/Reference:

QUESTION 9
Your company uses Microsoft Azure Advanced Threat Protection (ATP).

You enable the delayed deployment of updates for an Azure ATP sensor named Sensor1.

How long after the Azure ATP cloud service is updated will Sensor1 be updated?

A. 7 days
B. 24 hours
C. 1 hour
D. 48 hours
E. 12 hours

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Note: The delay period was 24 hours. In ATP release 2.62, the 24 hour delay period has been increased to 72 hours.

QUESTION 10
DRAG DROP

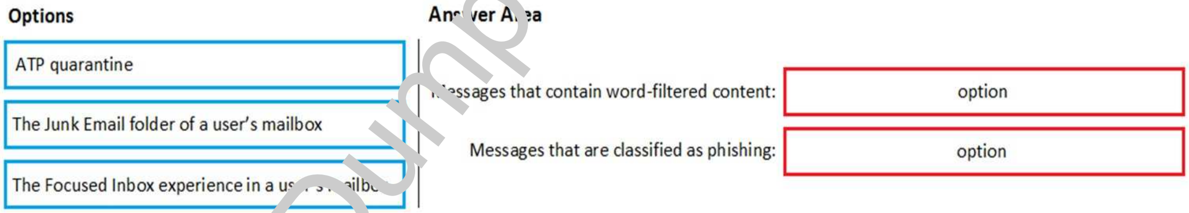
You have a Microsoft 365 subscription. All users use Microsoft Exchange Online.

Microsoft 365 is configured to use the default policy settings without any custom rules.

You manage message hygiene.

Where are suspicious email messages placed by default? To answer, drag the appropriate location to the correct message types. Each option 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.

Select and Place:



Options

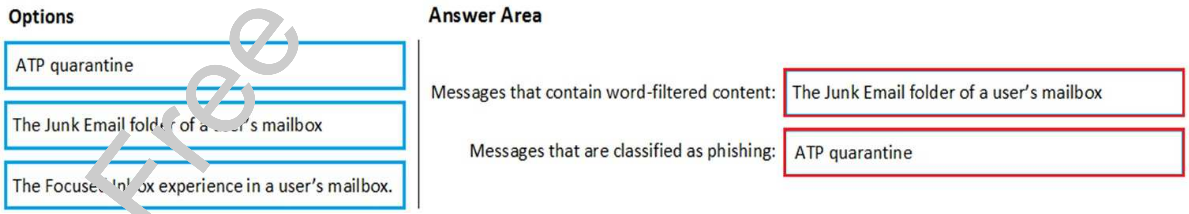
- ATP quarantine
- The Junk Email folder of a user's mailbox
- The Focused Inbox experience in a user's mailbox

Answer Area

Messages that contain word-filtered content: option

Messages that are classified as phishing: option

Correct Answer:



Options

- ATP quarantine
- The Junk Email folder of a user's mailbox
- The Focused Inbox experience in a user's mailbox.

Answer Area

Messages that contain word-filtered content: The Junk Email folder of a user's mailbox

Messages that are classified as phishing: ATP quarantine

Section: [none]
Explanation

Explanation/Reference:

QUESTION 11
You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy.

You need to configure the retention duration for the attachments in quarantine.

Which type of threat management policy should you create?

A. ATP anti-phishing
B. DKIM
C. Anti-spam
D. Anti-malware

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files#BKMK_ModQuarantineTime

QUESTION 12
Your company has 500 computers.

You plan to protect the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP). Twenty of the computers belong to company executives.

You need to recommend a remediation solution that meets the following requirements:

- Windows Defender ATP administrators must manually approve all remediation for the executives
- Remediation must occur automatically for all other users

What should you recommend doing from Windows Defender Security Center?

A. Configure 20 system exclusions on automation allowed/block lists
B. Configure two alert notification rules
C. Download an offboarding package for the computers of the 20 executives
D. Create two machine groups

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/machine-groups-windows-defender-advanced-threat-protection

QUESTION 13
You have a Microsoft 365 Enterprise E5 subscription.

You use Windows Defender Advanced Threat Protection (Windows Defender ATP).

You need to integrate Microsoft Office 365 Threat Intelligence and Windows Defender ATP.
Where should you configure the integration?

A. From the Microsoft 365 admin center, select **Settings**, and then select **Services & add-ins**.

B. From the Security & Compliance admin center, select **Threat management**, and then select **Explorer**.
C. From the Microsoft 365 admin center, select **Reports**, and then select **Security & Compliance**.
D. From the Security & Compliance admin center, select **Threat management** and then select **Threat tracker**.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-office-365-ti-with-wdatp

QUESTION 14
Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.

The security logs of the servers are collected by using a third-party SIEM solution.

You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.

You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.

What should you do?

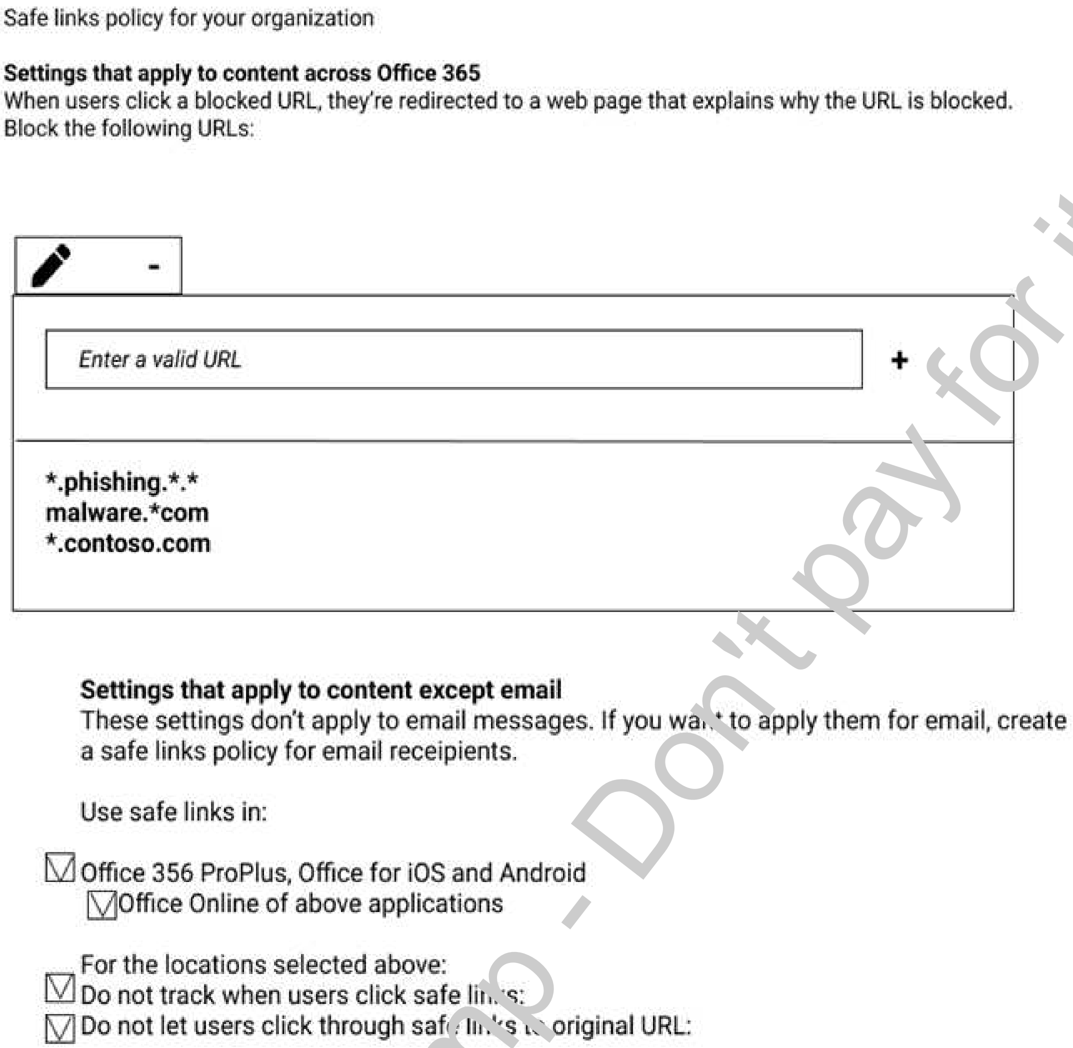
A. Configure auditing in the Office 365 Security & Compliance center.
B. Turn off Delayed updates for the Azure ATP sensors.
C. Modify the Domain synchronizer candidate's settings on the Azure ATP sensors.
D. Integrate SIEM and Azure ATP.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5

QUESTION 15
You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com.

You create a safe links policy as shown in the following exhibit.



Safe links policy for your organization

Settings that apply to content across Office 365
When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.
Block the following URLs:

.phishing.*.
malware.*com
***.contoso.com**

Settings that apply to content except email
These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email receipients.

Use safe links in:

☑ Office 356 ProPlus, Office for iOS and Android
☑ Office Online of above applications

For the locations selected above:
☑ Do not track when users click safe links:
☑ Do not let users click through safe links to original URL:

Which URL can a user safely access from Microsoft Word Online?

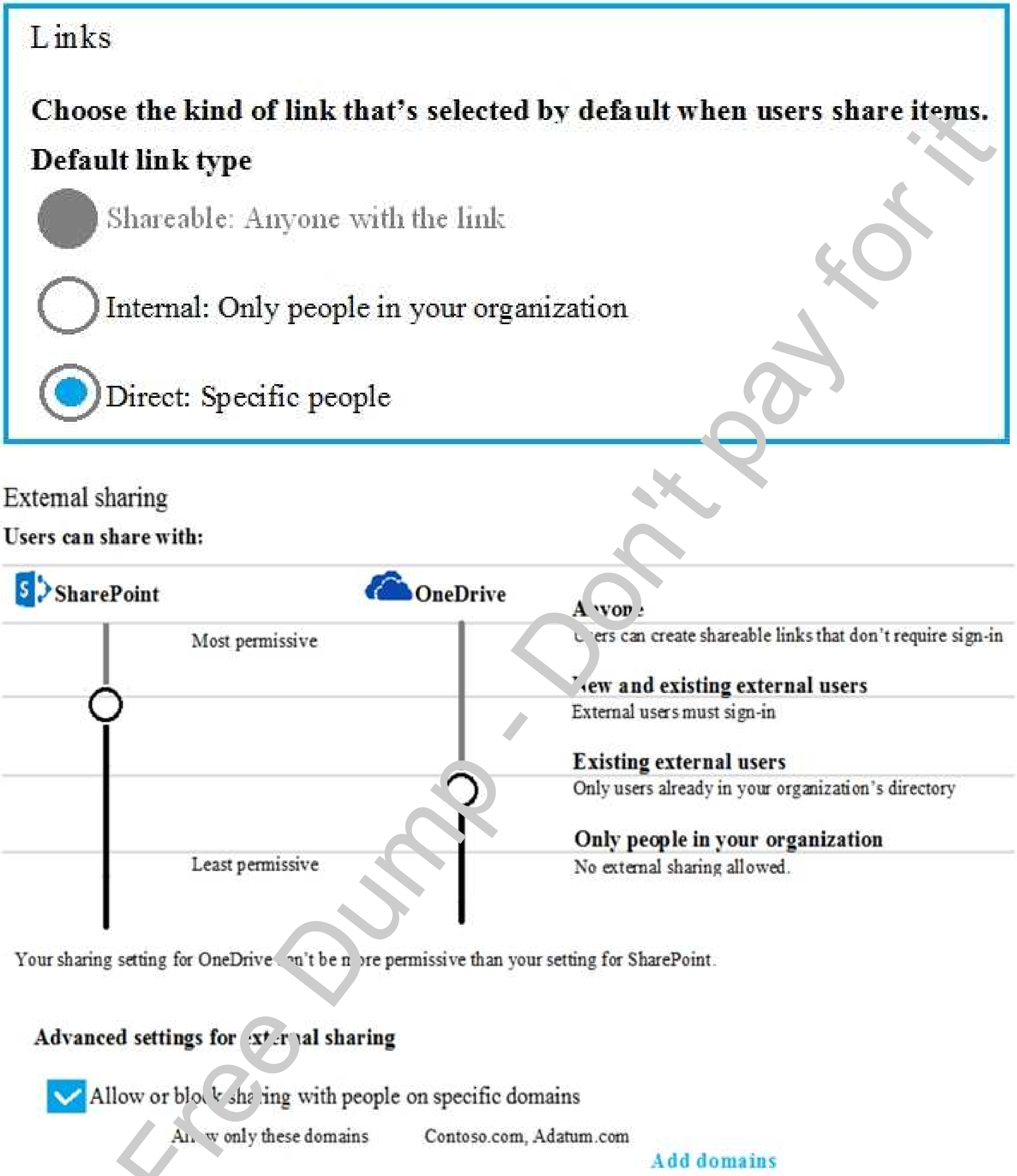
A. fabrikam.phishing.fabrikam.com
B. malware.fabrikam.com
C. fabrikam.contoso.com
D. www.malware.fabrikam.com

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-a-custom-blocked-urls-list-wtih-atp

QUESTION 16
HOTSPOT

You have a Microsoft 365 subscription that uses a default name of litwareinc.com.
You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.



Links

Choose the kind of link that's selected by default when users share items.

Default link type

● Shareable: Anyone with the link

○ Internal: Only people in your organization

◉ Direct: Specific people

External sharing

Users can share with:

SharePoint		OneDrive	
	Most permissive		**Anyone** Users can create shareable links that don't require sign-in
○			**New and existing external users** External users must sign-in
		○	**Existing external users** Only users already in your organization's directory
	Least permissive		**Only people in your organization** No external sharing allowed.

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

☑ Allow or block sharing with people on specific domains

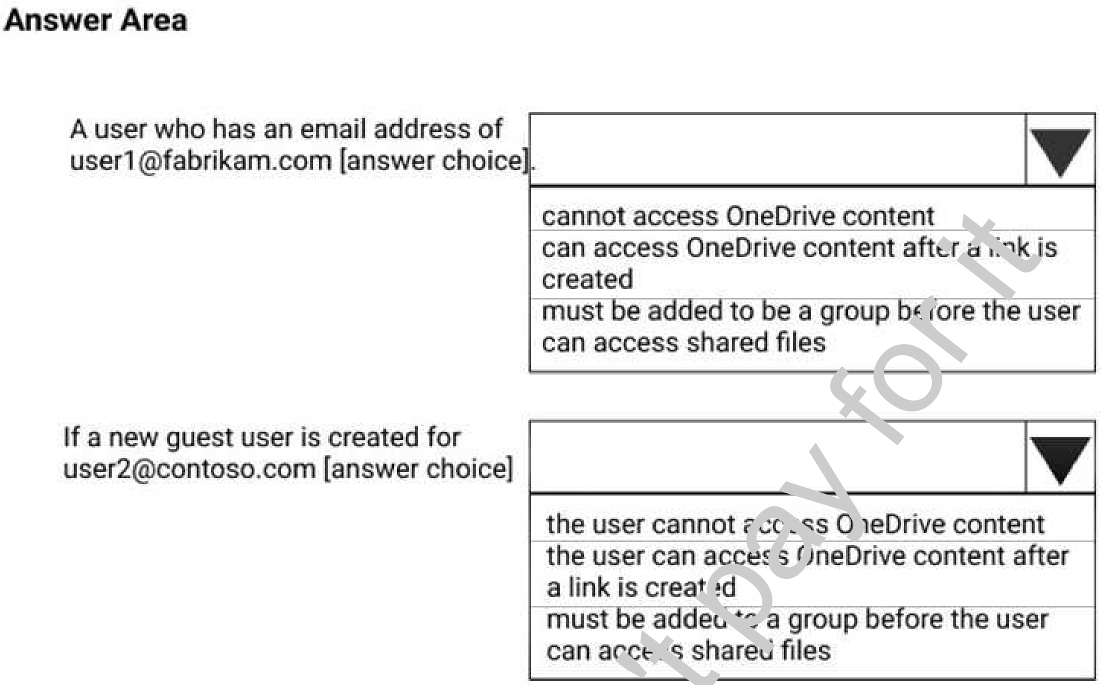
Allow only these domains Contoso.com, Adatum.com

Add domains

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.

Hot Area:



Answer Area

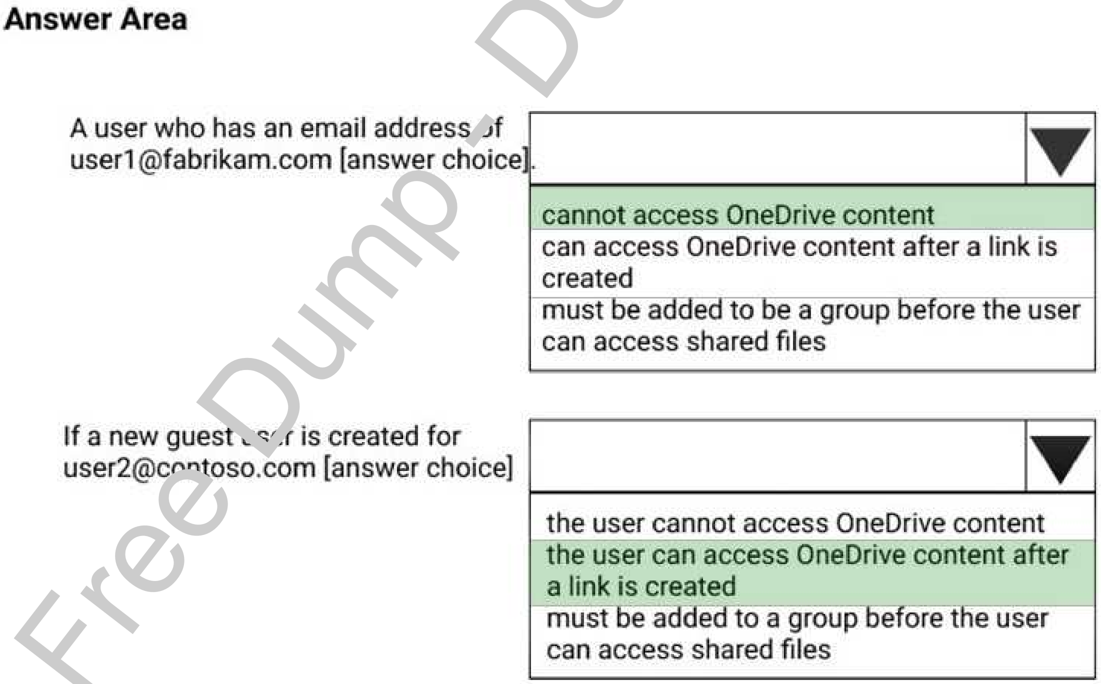
A user who has an email address of user1@fabrikam.com [answer choice].

- cannot access OneDrive content
- can access OneDrive content after a link is created
- must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

- the user cannot access OneDrive content
- the user can access OneDrive content after a link is created
- must be added to a group before the user can access shared files

Correct Answer:



Answer Area

A user who has an email address of user1@fabrikam.com [answer choice].

- [✓ cannot access OneDrive content]
- can access OneDrive content after a link is created
- must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

- the user cannot access OneDrive content
- [✓ the user can access OneDrive content after a link is created]
- must be added to a group before the user can access shared files

Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/onedrive/manage-sharing

QUESTION 17
Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.

The security logs of the servers are collected by using a third-party SIEM solution.

You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.

You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.

What should you do?

A. Configure Event Forwarding on the domain controllers
B. Configure auditing in the Office 365 Security & Compliance center.
C. Turn on Delayed updates for the Azure ATP sensors.
D. Enable the Audit account management Group Policy setting for the servers.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

QUESTION 18
Several users in your Microsoft 365 subscription report that they received an email message without attachment.

You need to review the attachments that were removed from the messages.

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

NOTE: Each correct selection is worth one point.

A. the Exchange admin center
B. the Azure ATP admin center
C. Outlook on the web
D. the Security & Compliance admin center
E. Microsoft Azure Security Center

Correct Answer: AD
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages-and-files

QUESTION 19
You have a Microsoft 365 subscription that contains several Windows 10 devices. The devices are managed by using Microsoft Intune.

You need to enable Windows Defender Exploit Guard (Windows Defender EG) on the devices.

Which type of device configuration profile should you use?

A. Endpoint protection
B. Device restrictions
C. Identity protection
D. Windows Defender ATP

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

QUESTION 20
DRAG DROP

You have a Microsoft 365 E5 subscription.

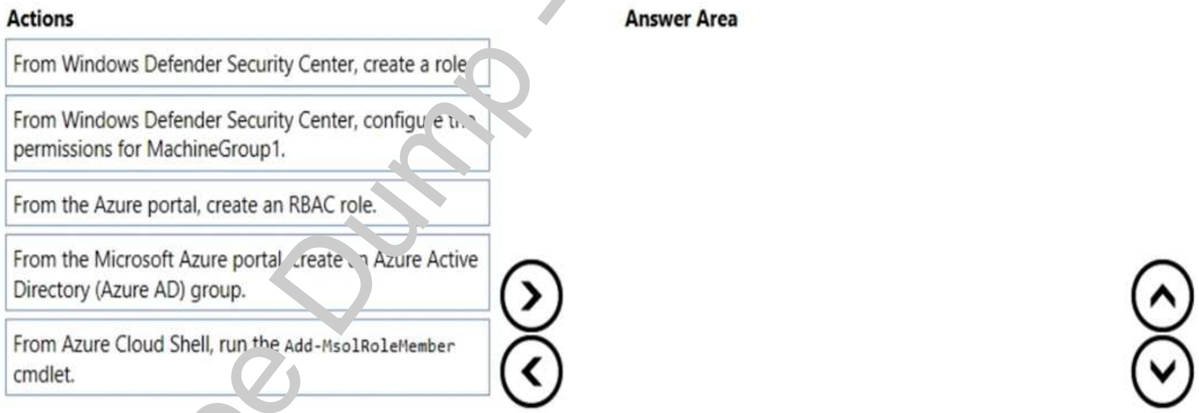
All computers run Windows 10 and are onboarded to Windows Defender Advanced Threat Protection (Windows Defender ATP).

You create a Windows Defender machine group named MachineGroup1.

You need to enable delegation for the security settings of the computers in MachineGroup1.

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.

Select and Place:

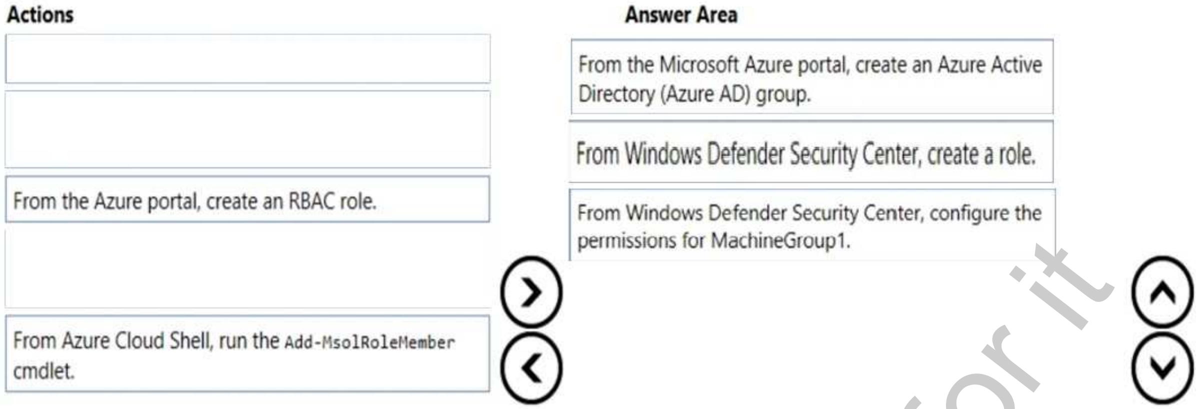


Actions

- From Windows Defender Security Center, create a role.
- From Windows Defender Security Center, configure the permissions for MachineGroup1.
- From the Azure portal, create an RBAC role.
- From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
- From Azure Cloud Shell, run the `Add-MsolRoleMember` cmdlet.

Answer Area

Correct Answer:



Actions

From the Azure portal, create an RBAC role.

From Azure Cloud Shell, run the `Add-MsolRoleMember` cmdlet.

Answer Area

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From Windows Defender Security Center, create a role.

From Windows Defender Security Center, configure the permissions for MachineGroup1.

Section: [none]
Explanation

Explanation/Reference:

QUESTION 21
You have a hybrid Microsoft Exchange Server organization. All users have Microsoft 365 E5 licenses.

You plan to implement an Advanced Threat Protection (ATP) anti-phishing policy.

You need to enable mailbox intelligence for all users.

What should you do first?

A. Configure attribute filtering in Microsoft Azure Active Directory Connect (Azure AD Connect)
B. Purchase the ATP add-on
C. Select **Directory extension attribute sync** in Microsoft Azure Active Directory Connect (Azure AD Connect)
D. Migrate the on-premises mailboxes to Exchange Online

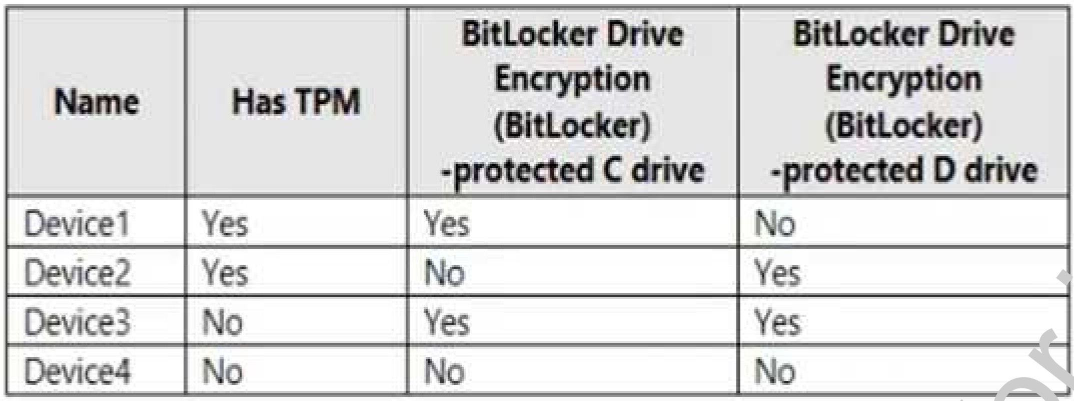
Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies

QUESTION 22
HOTSPOT

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

Four Windows 10 devices are joined to the tenant as shown in the following table.

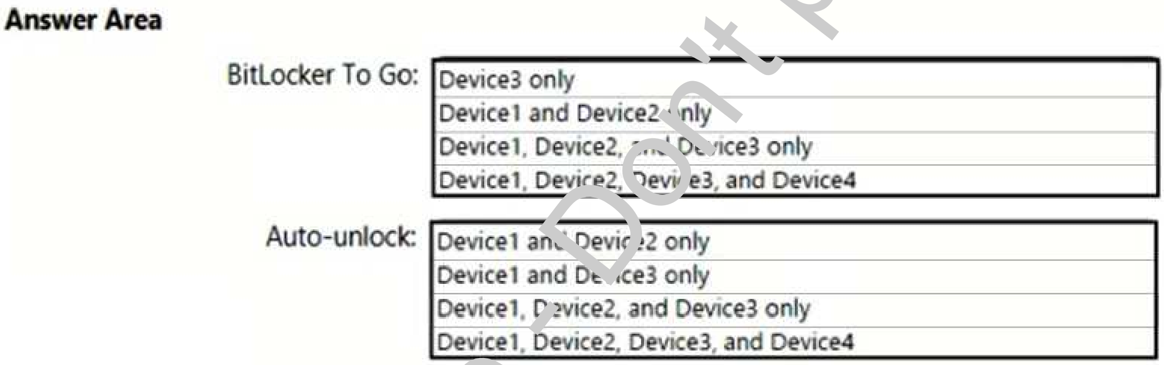


Name	Has TPM	BitLocker Drive Encryption (BitLocker) -protected C drive	BitLocker Drive Encryption (BitLocker) -protected D drive
Device1	Yes	Yes	No
Device2	Yes	No	Yes
Device3	No	Yes	Yes
Device4	No	No	No

On which devices can you use BitLocker To Go and on which devices can you turn on auto-unlock? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

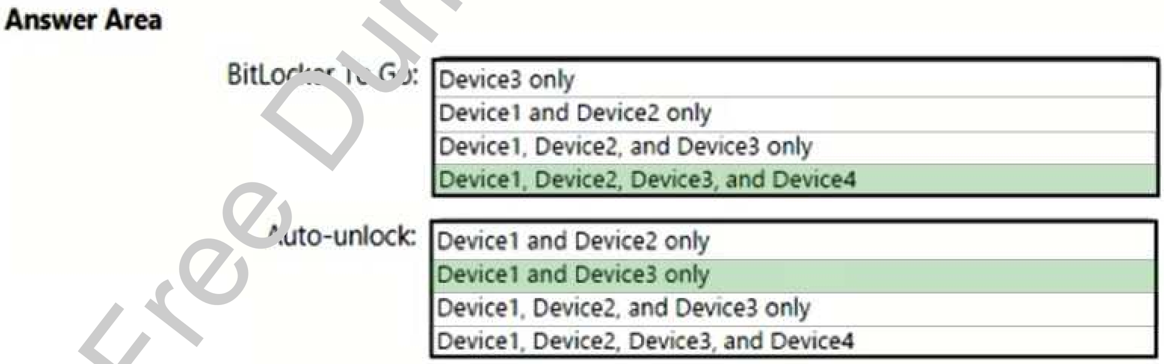


Answer Area

BitLocker To Go:
- Device3 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, Device3, and Device4

Auto-unlock:
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2, and Device3 only
- Device1, Device2, Device3, and Device4

Correct Answer:



Answer Area

BitLocker To Go:
- Device3 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- [✓ Device1, Device2, Device3, and Device4]

Auto-unlock:
- Device1 and Device2 only
- [✓ Device1 and Device3 only]
- Device1, Device2, and Device3 only
- Device1, Device2, Device3, and Device4

Section: [none]
Explanation

Explanation/Reference:

Testlet 1

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

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment

Network Infrastructure

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements

Fabrikam identifies the following issues:

- Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.
- Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements

Planned Changes

Fabrikam plans to implement the following changes:

- Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory
- Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration

Fabrikam identifies the following application requirements for managing workload applications:

- User administrators will work from different countries

- User administrators will use the Azure Active Directory admin center
- Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements

Fabrikam identifies the following security requirements:

- Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed
- Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement
- Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send invitations
- Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory
- Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location
- The location of the user administrators must be audited when the administrators authenticate to Azure AD
- Email messages that include attachments containing malware must be delivered without the attachment
- The principle of least privilege must be used whenever possible

QUESTION 1

You need to recommend a solution that meets the technical and security requirements for sharing data with the partners.

What should you include in the recommendation? (Choose two.) Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create an access review

B. Assign the Global administrator role to User1

C. Assign the Guest inviter role to User1

D. Modify the External collaboration settings in the Azure Active Directory admin center

Correct Answer: CD

Section: [none]

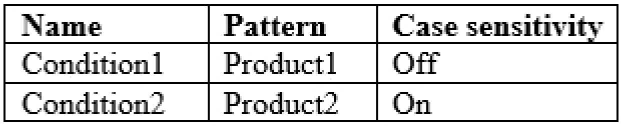
Explanation

Explanation/Reference:

Question Set 2

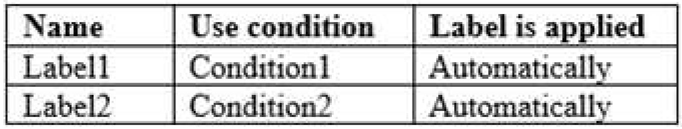
QUESTION 1
HOTSPOT

You have the Microsoft Azure Information Protection conditions shown in the following table.



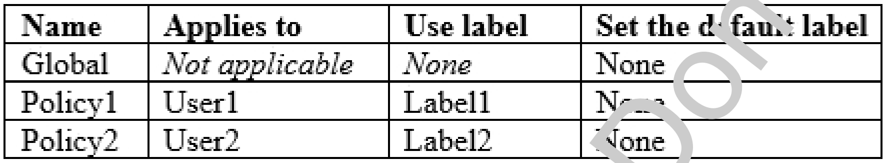
Name	Pattern	Case sensitivity
Condition1	Product1	Off
Condition2	Product2	On

You have the Azure Information Protection labels shown in the following table.



Name	Use condition	Label is applied
Label1	Condition1	Automatically
Label2	Condition2	Automatically

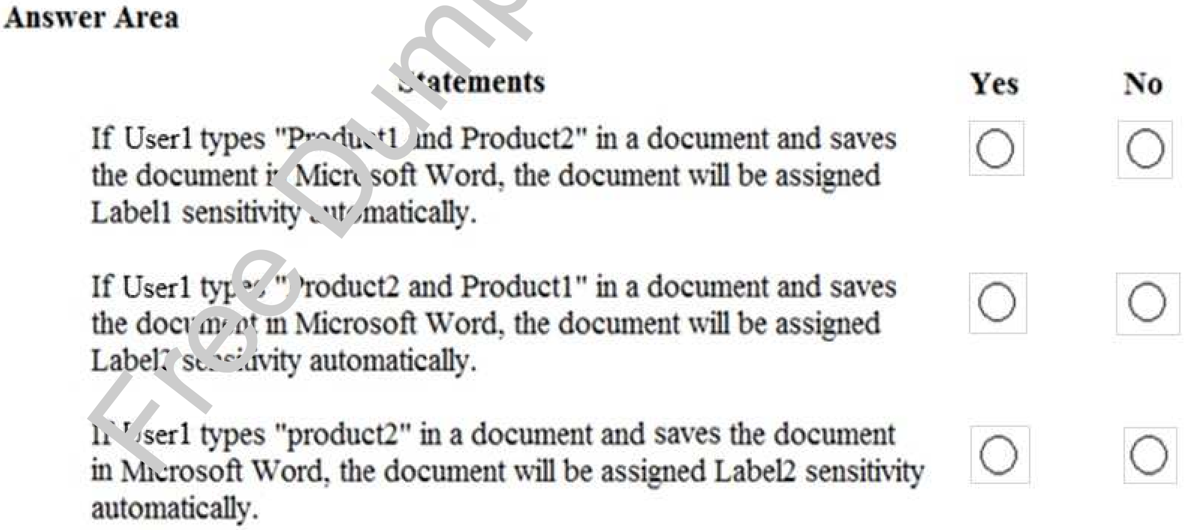
You have the Azure Information Protection policies shown in the following table.



Name	Applies to	Use label	Set the default label
Global	*Not applicable*	*None*	None
Policy1	User1	Label1	None
Policy2	User2	Label2	None

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

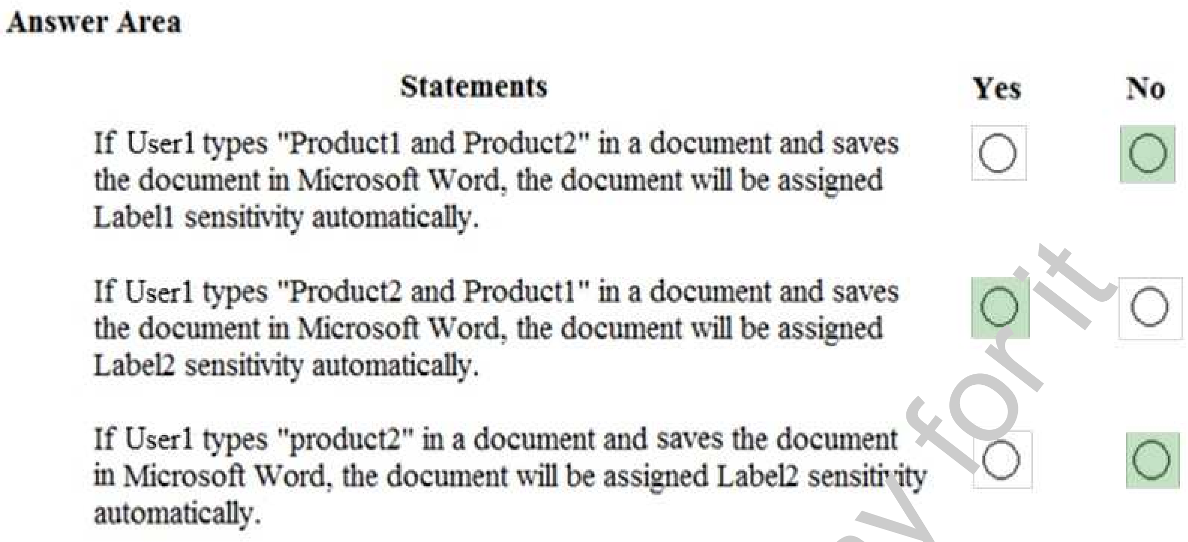
Hot Area:



Answer Area

Statements	Yes	No
If User1 types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	○
If User1 types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○
If User1 types "product2" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
If User1 types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	●
If User1 types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	●	○
If User1 types "product2" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	●

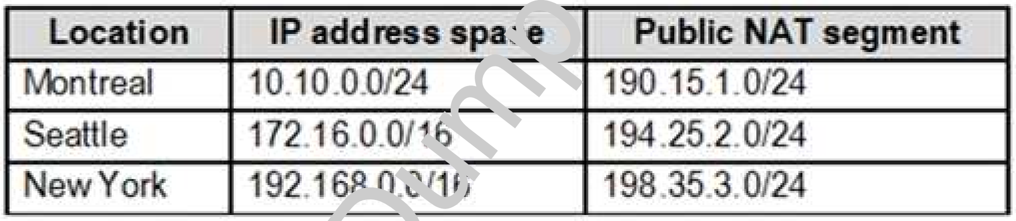
Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
HOTSPOT

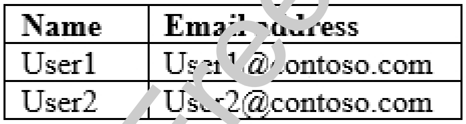
Your company has a Microsoft 365 subscription, a Microsoft Azure subscription, and an Azure Active Directory (Azure AD) tenant named contoso.com.

The company has the offices shown in the following table.



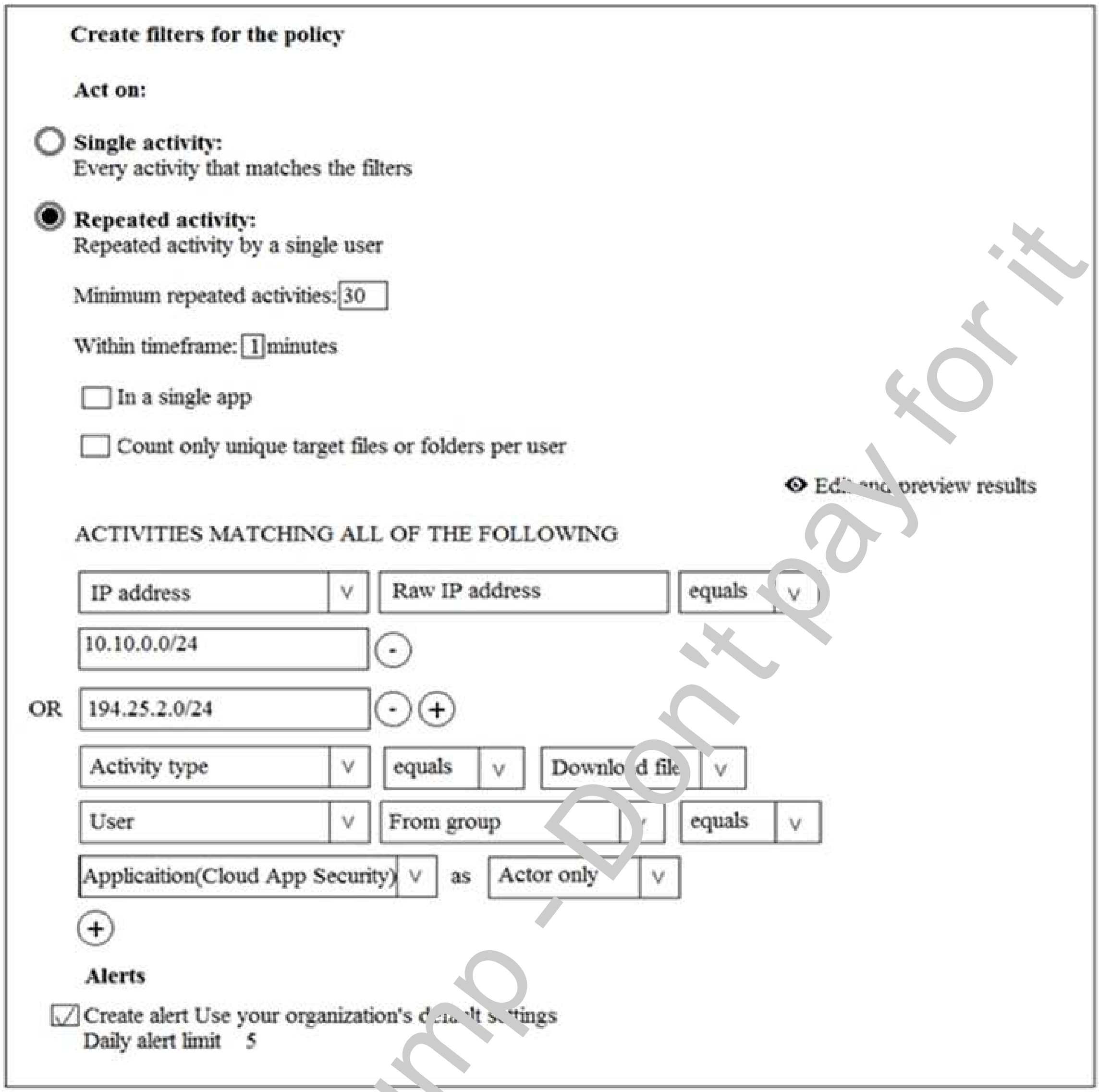
Location	IP address space	Public NAT segment
Montreal	10.10.0.0/24	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

The tenant contains the users shown in the following table.



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

You create the Microsoft Cloud App Security policy shown in the following exhibit.



Create filters for the policy

Act on:

○ **Single activity:**
Every activity that matches the filters

● **Repeated activity:**
Repeated activity by a single user

Minimum repeated activities: 30

Within timeframe: 1 minutes

□ In a single app

□ Count only unique target files or folders per user

Edit and preview results

ACTIVITIES MATCHING ALL OF THE FOLLOWING

IP address | Raw IP address | equals
10.10.0.0/24
OR 194.25.2.0/24
Activity type | equals | Download file
User | From group | equals
Applicaition(Cloud App Security) as Actor only

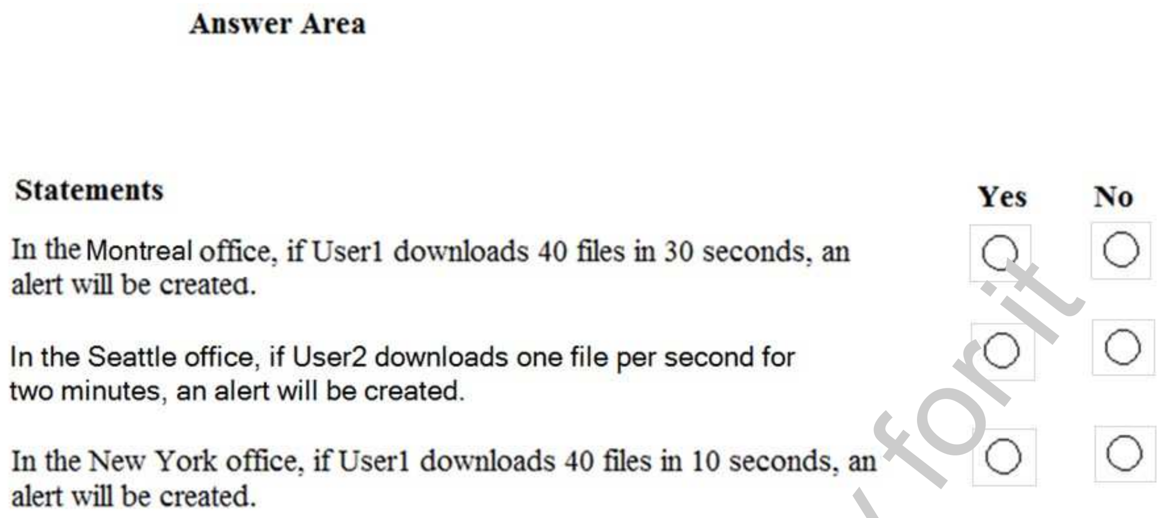
Alerts

☑ Create alert Use your organization's default settings
Daily alert limit 5

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

NOTE: Each correct selection is worth one point.

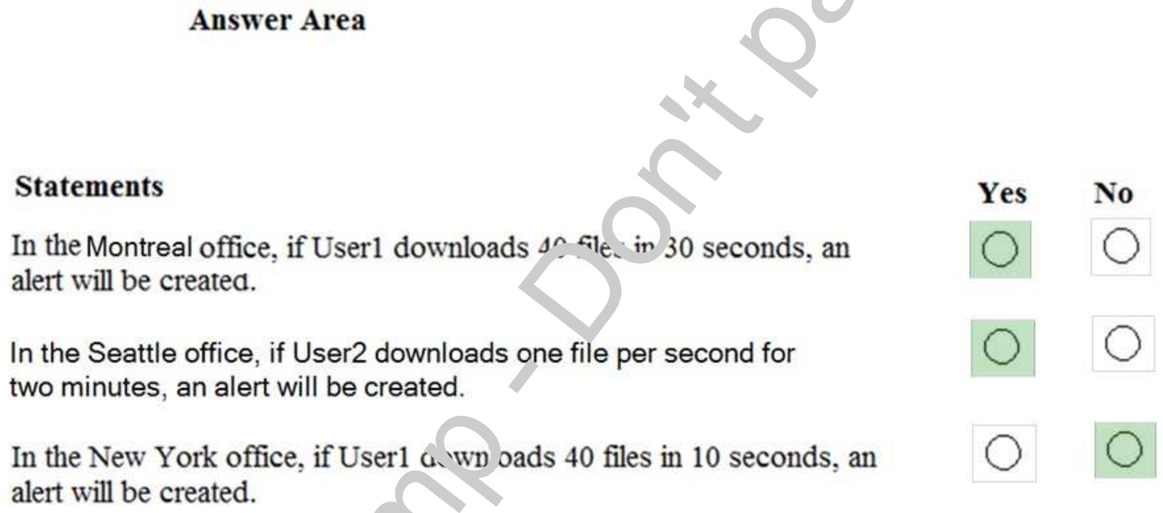
Hot Area:



Answer Area

Statements	Yes	No
In the Montreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	○	○
In the Seattle office, if User2 downloads one file per second for two minutes, an alert will be created.	○	○
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
In the Montreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	●	○
In the Seattle office, if User2 downloads one file per second for two minutes, an alert will be created.	●	○
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	○	●

Section: [none]
Explanation

Explanation/Reference:

QUESTION 3
HOTSPOT

You have a Microsoft 365 subscription.

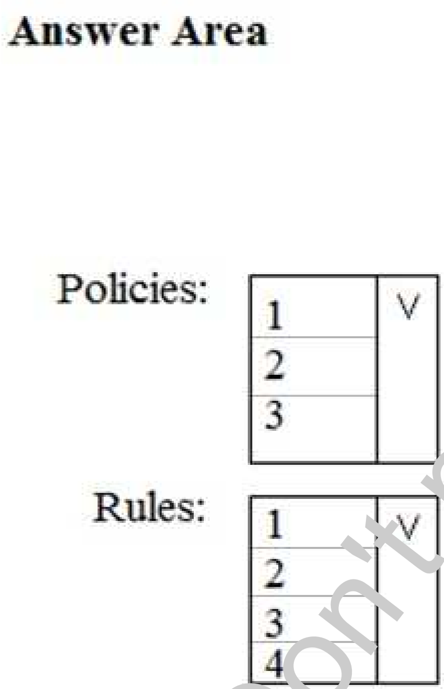
You identify the following data loss prevention (DLP) requirements:

- Send notifications to users if they attempt to send attachments that contain EU social security numbers
- Prevent any email messages that contain credit card numbers from being sent outside your organization
- Block the external sharing of Microsoft OneDrive content that contains EU passport numbers
- Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

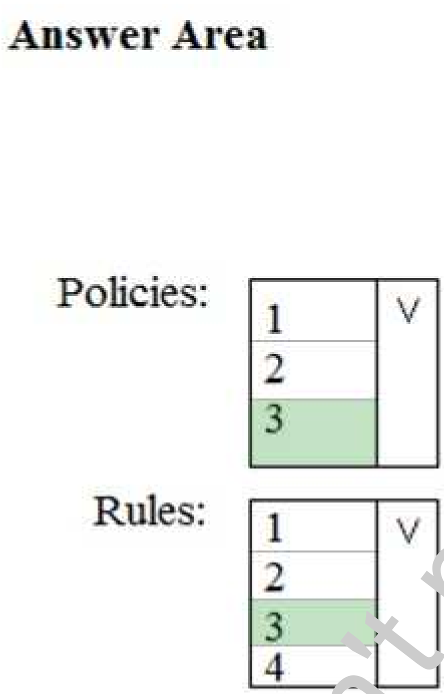


Answer Area

Policies:

Rules:

Correct Answer:



Answer Area

Policies:

1
2
[✓ 3]

Rules:

1
2
[✓ 3]
4

Section: [none]
Explanation

Explanation/Reference:

QUESTION 4
You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

You need to prevent the users from downloading, printing, and syncing files.

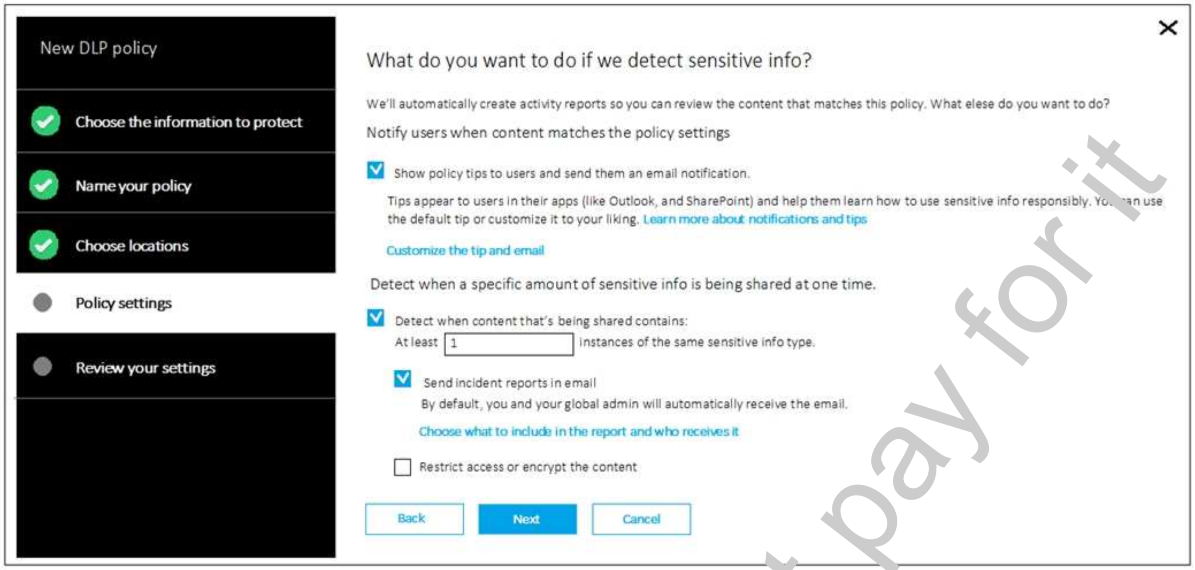
What should you do?

A. Run the `Set-SPODataConnectionSetting` cmdlet and specify the `AssignmentCollection` parameter
B. From the SharePoint admin center, configure the Access control settings
C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

QUESTION 5
You create a data loss prevention (DLP) policy as shown in the following exhibit:



What do you want to do if we detect sensitive info?

We'll automatically create activity reports so you can review the content that matches this policy. What elese do you want to do?

Notify users when content matches the policy settings

☑ Show policy tips to users and send them an email notification.

Tips appear to users in their apps (like Outlook, and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. Learn more about notifications and tips

Customize the tip and email

Detect when a specific amount of sensitive info is being shared at one time.

☑ Detect when content that's being shared contains:

At least 1 instances of the same sensitive info type.

☑ Send incident reports in email

By default, you and your global admin will automatically receive the email.

Choose what to include in the report and who receives it

☐ Restrict access or encrypt the content

What is the effect of the policy when a user attempts to send an email messages that contains sensitive information?

A. The user receives a notification and can send the email message
B. The user receives a notification and cannot send the email message
C. The email message is sent without a notification
D. The email message is blocked silently

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

QUESTION 6
You have a Microsoft 365 subscription.

You need to create data loss prevention (DLP) queries in Microsoft SharePoint Online to find sensitive data stored in sites.

Which type of site collection should you create first?

A. Records Center
B. eDiscovery Center
C. Enterprise Search Center
D. Document Center

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bb-b944-448d-b83d-8fec4abcc24c

QUESTION 7
You have a Microsoft 365 subscription that includes a user named User1.

You have a conditional access policy that applies to Microsoft Exchange Online. The conditional access policy is configured to use Conditional Access App Control.

You need to create a Microsoft Cloud App Security policy that blocks User1 from printing from Exchange Online.

Which type of Cloud App Security policy should you create?

A. an app permission policy
B. an activity policy
C. a Cloud Discovery anomaly detection policy
D. a session policy

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad

QUESTION 8
HOTSPOT

You have a Microsoft 365 E5 subscription.

From Microsoft Azure Active Directory (Azure AD), you create a security group named Group1. You add 10 users to Group1.

You need to apply app enforced restrictions to the members of Group1 when they connect to Microsoft Exchange Online from non-compliant devices, regardless of their location.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-conditional-access

QUESTION 9
Note: This question is part of 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 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.

You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them.

Solution: You create a new label in the global policy and instruct the user to resend the email message.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 10
Note: This question is part of 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 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection. You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them.

Solution: You modify the encryption settings of the label.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 11
Note: This question is part of 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 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection. You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them.

Solution: You modify the content expiration settings of the label.

Does this meet the goal?

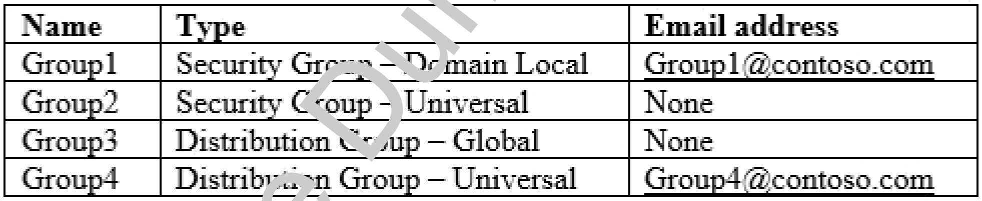
A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

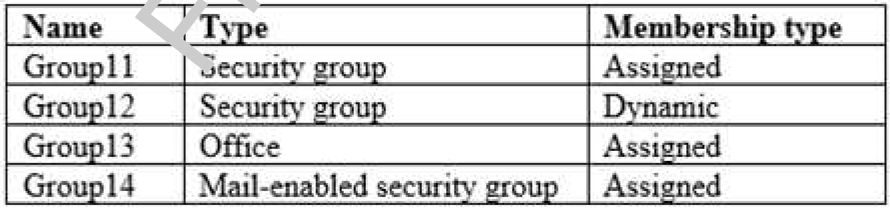
QUESTION 12
HOTSPOT

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



Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.



Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Office	Assigned
Group14	Mail-enabled security group	Assigned

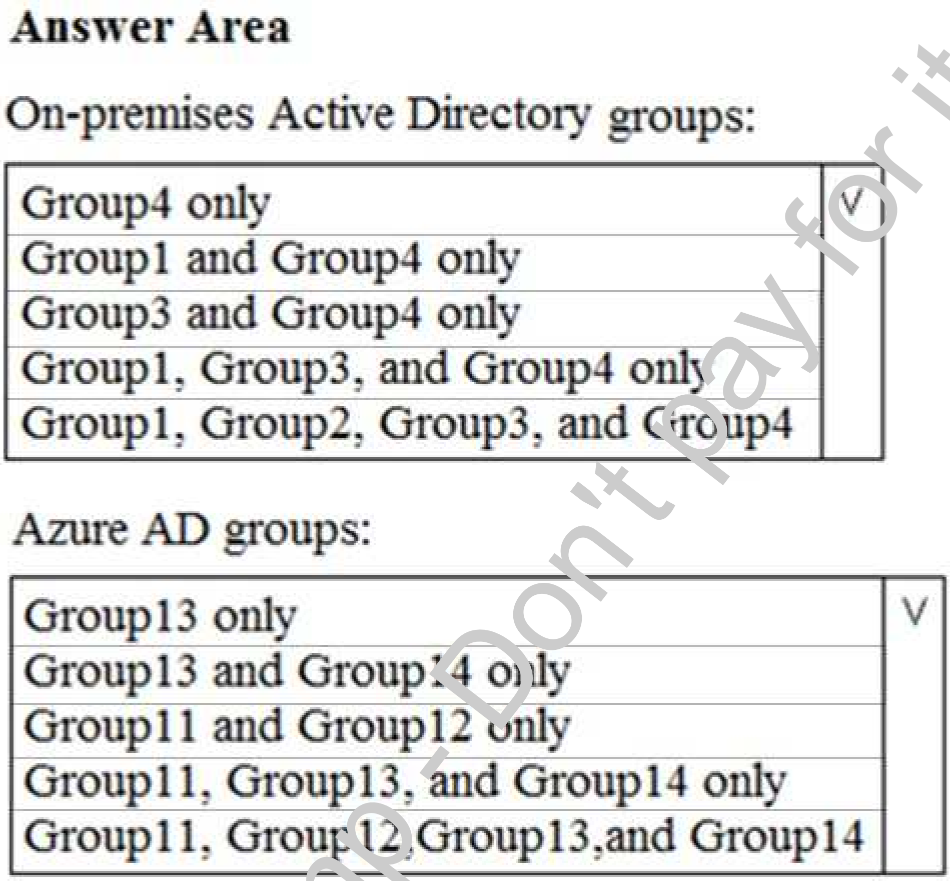
You create an Azure Information Protection policy named Policy1.

You need to apply Policy1.

To which groups can you apply Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

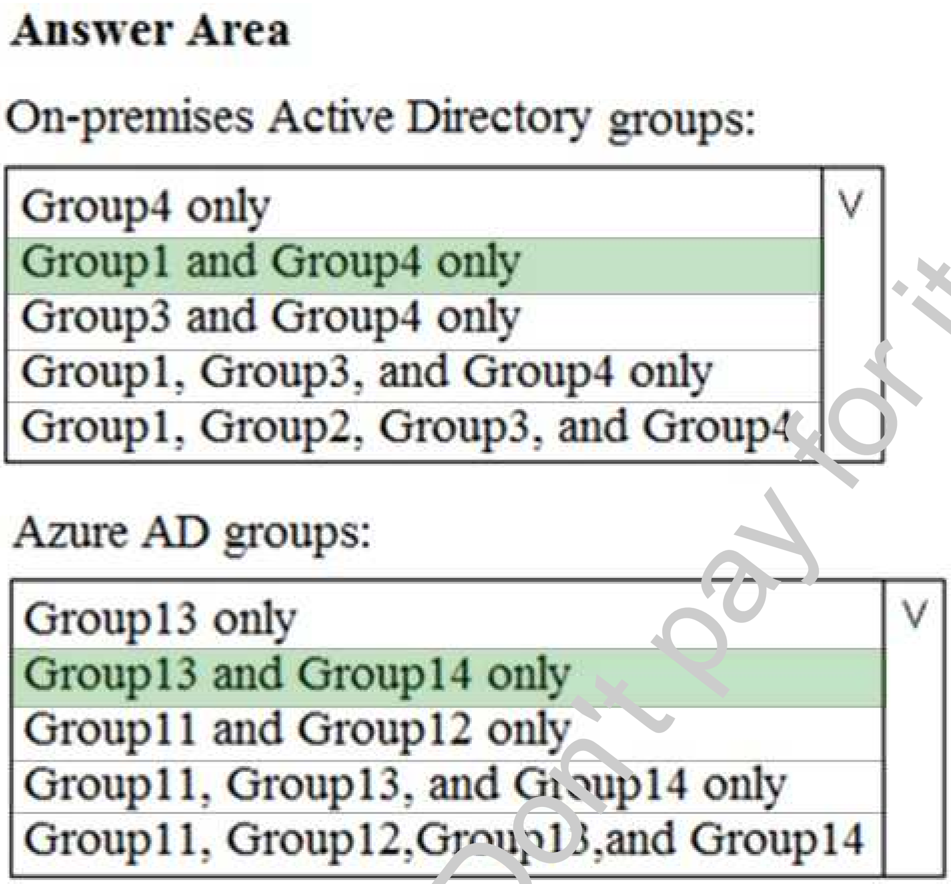
On-premises Active Directory groups:

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

Azure AD groups:

- Group13 only
- Group13 and Group14 only
- Group11 and Group12 only
- Group11, Group13, and Group14 only
- Group11, Group12,Group13,and Group14

Correct Answer:



Answer Area

On-premises Active Directory groups:

Group4 only
[✓ Group1 and Group4 only]
Group3 and Group4 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

Azure AD groups:

Group13 only
[✓ Group13 and Group14 only]
Group11 and Group12 only
Group11, Group13, and Group14 only
Group11, Group12,Group13,and Group14

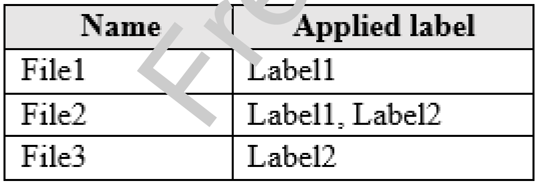
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/prepare

QUESTION 13
HOTSPOT

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

OneDrive stores files that are shared with external users. The files are configured as shown in the following table.



Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:

- Rule1:
- Conditions: Label1, Detect content that's shared with people outside my organization

- Actions: Restrict access to the content for external users
- User notifications: Notify the user who last modified the content
- User overrides: On
- Priority: 0

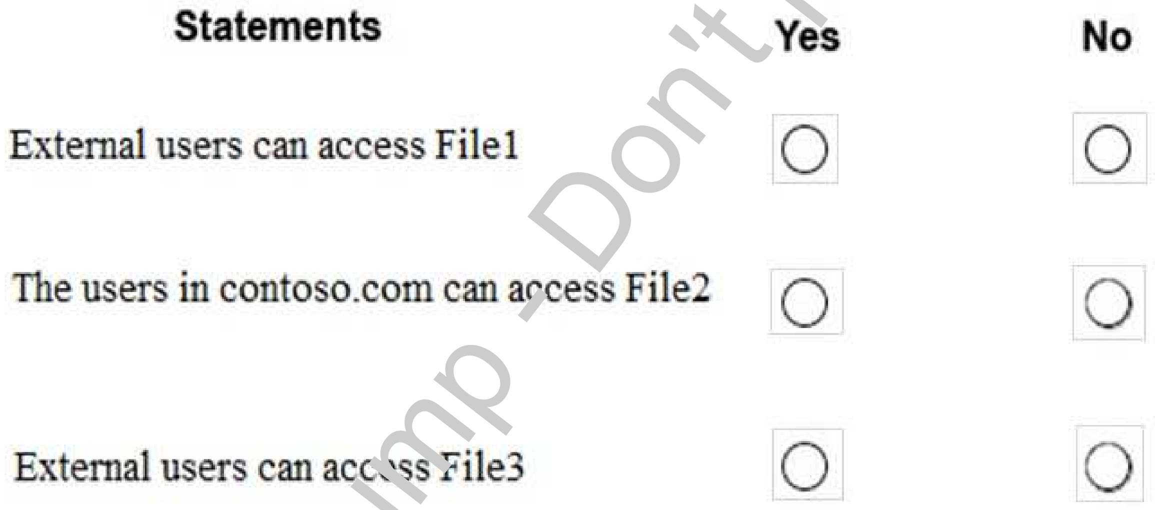
- Rule2:
- Conditions: Label1 or Label2
- Actions: Restrict access to the content
- Priority: 1

- Rule3:
- Conditions: Label2, Detect content that’s shared with people outside my organization
- Actions: Restrict access to the content for external users
- User notifications: Notify the user who last modified the content
- User overrides: On
- Priority: 2

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

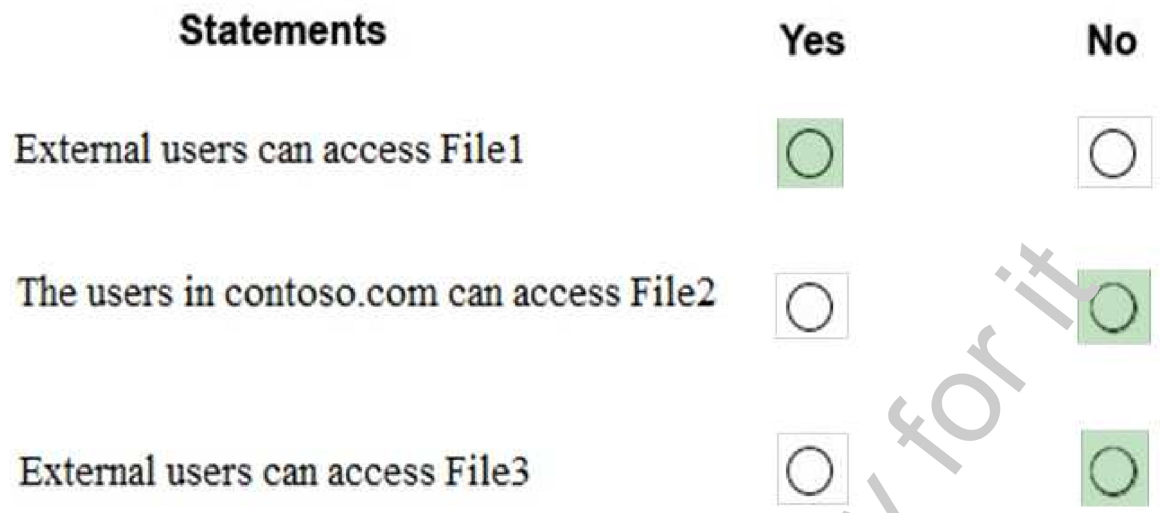
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
External users can access File1	○	○
The users in contoso.com can access File2	○	○
External users can access File3	○	○

Correct Answer:



Statements	Yes	No
External users can access File1	[✓ ○]	○
The users in contoso.com can access File2	○	[✓ ○]
External users can access File3	○	[✓ ○]

Section: [none]
Explanation

Explanation/Reference:

QUESTION 14
You have a Microsoft 365 subscription for a company named Contoso, Ltd. All data is in Microsoft 365.

Contoso works with a partner company named Litware, Inc. Litware has a Microsoft 365 subscription.

You need to allow users at Contoso to share files from Microsoft OneDrive to specific users at Litware.

Which two actions should you perform from the OneDrive admin center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Increase the permission level for OneDrive External sharing
B. Modify the Links settings
C. Change the permissions for OneDrive External sharing to the least permissive level
D. Decrease the permission level for OneDrive External sharing
E. Modify the Device access settings
F. Modify the Sync settings

Correct Answer: BD
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

QUESTION 15
You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

You need to prevent the users from downloading, printing, and syncing files.

What should you do?

A. Run the `Set-SPOTenant` cmdlet and specify the `-ConditionalAccessPolicy` parameter.
B. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps

https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

Testlet 1

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.

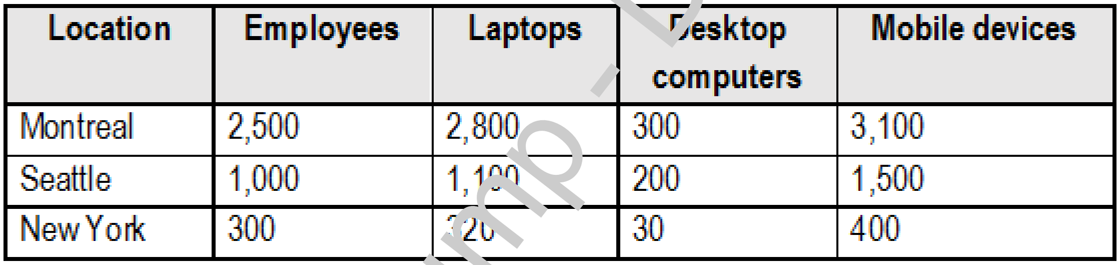
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

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

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

The company has the offices shown in the following table.



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

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment

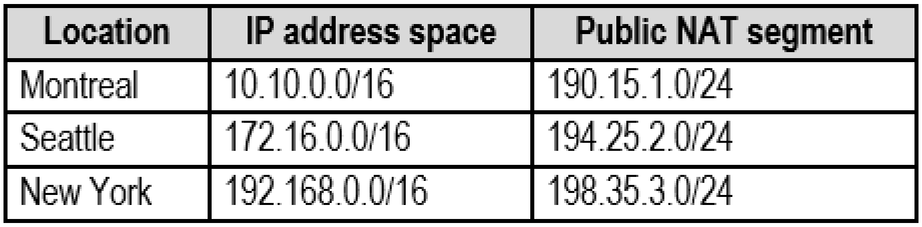
Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

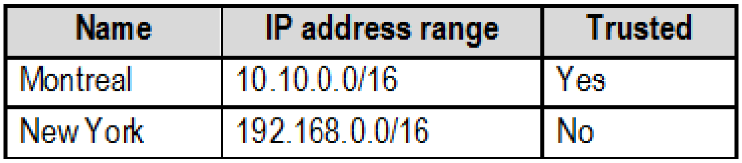
Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.



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

Named locations are defined in Azure AD as shown in the following table.

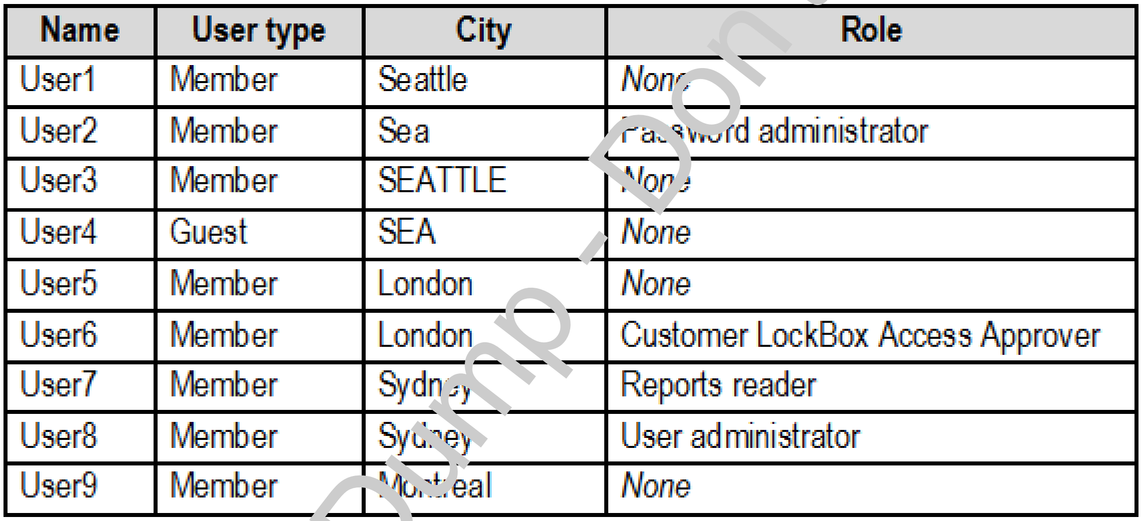


Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

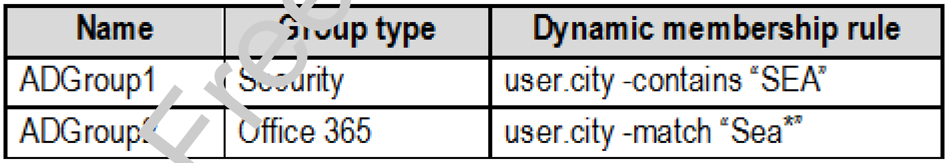
Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.



Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

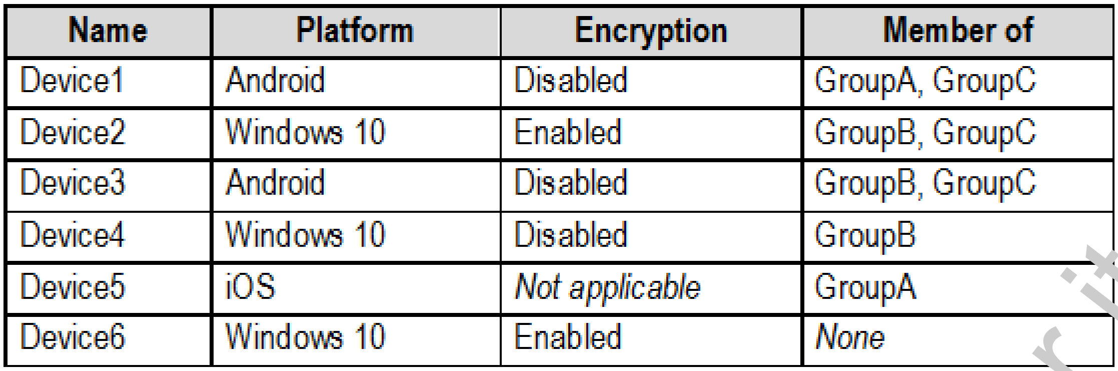


Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

Customer Lockbox is enabled in Microsoft 365.

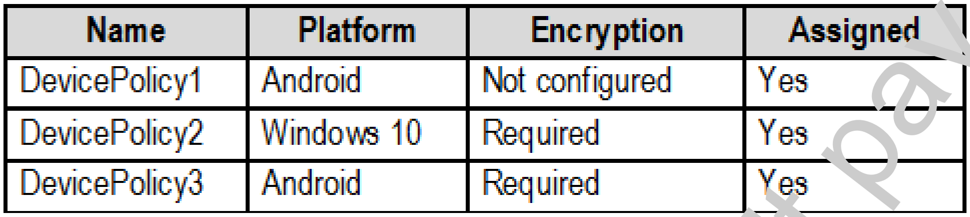
Microsoft Intune Configuration

The devices enrolled in Intune are configured as shown in the following table.



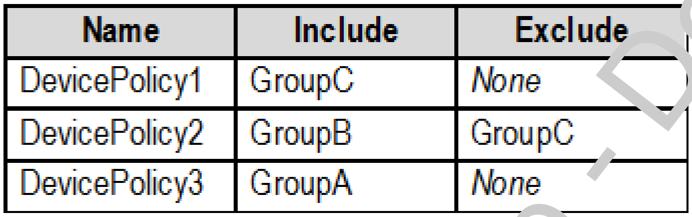
Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

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



Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

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



Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to **Compliant**.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

- Use the principle of least privilege
- Enable User1 to assign the Reports reader role to users
- Ensure that User6 approves Customer Lockbox requests as quickly as possible
- Ensure that User9 can enable and configure Azure AD Privileged Identity Management

QUESTION 1
What should User6 use to meet the technical requirements?

A. Supervision in the Security & Compliance admin center
B. Service requests in the Microsoft 365 admin center
C. Security & privacy in the Microsoft 365 admin center
D. Data subject requests in the Security & Compliance admin center

Correct Answer: B
Section: [none]

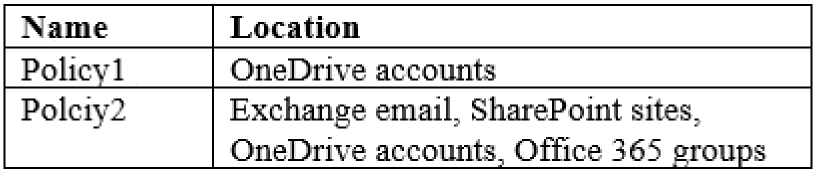
Explanation

Explanation/Reference:

Question Set 2

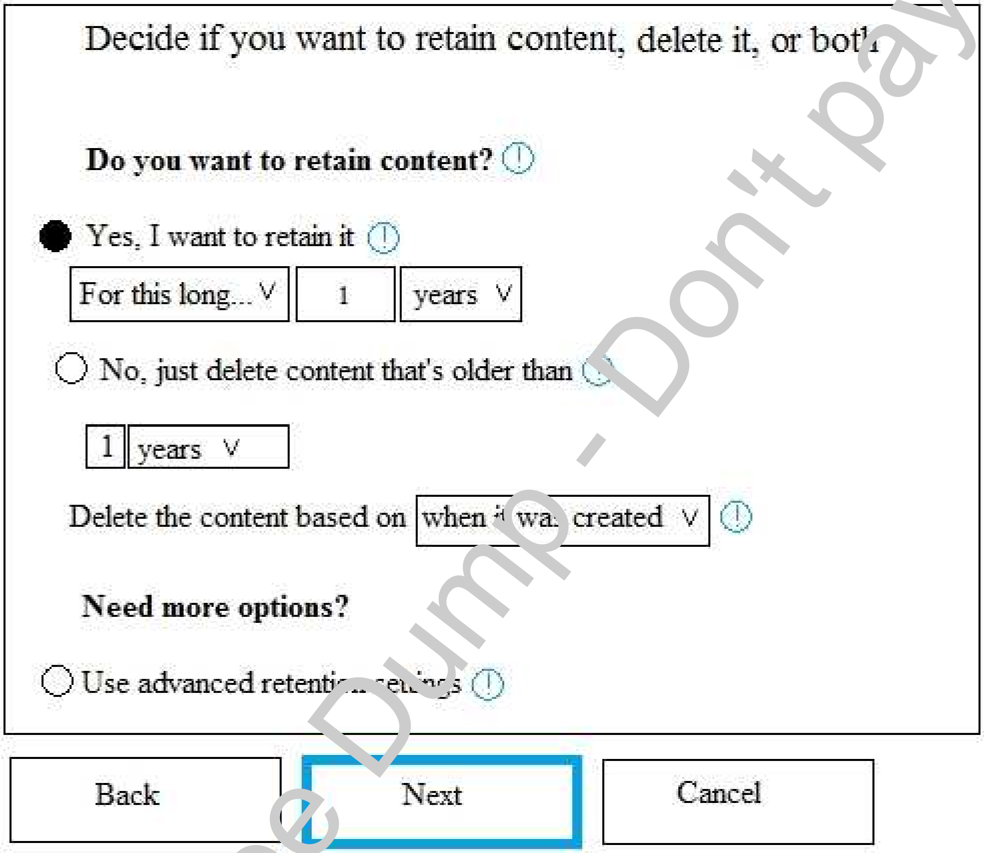
QUESTION 1
HOTSPOT

You have a Microsoft 365 subscription. From the Security & Compliance admin center, you create the retention policies shown in the following table.



Name	Location
Policy1	OneDrive accounts
Polciy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

Policy1 if configured as showing in the following exhibit.



Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

● Yes, I want to retain it ⓘ

For this long... ∨ | 1 | years ∨

○ No, just delete content that's older than ⓘ

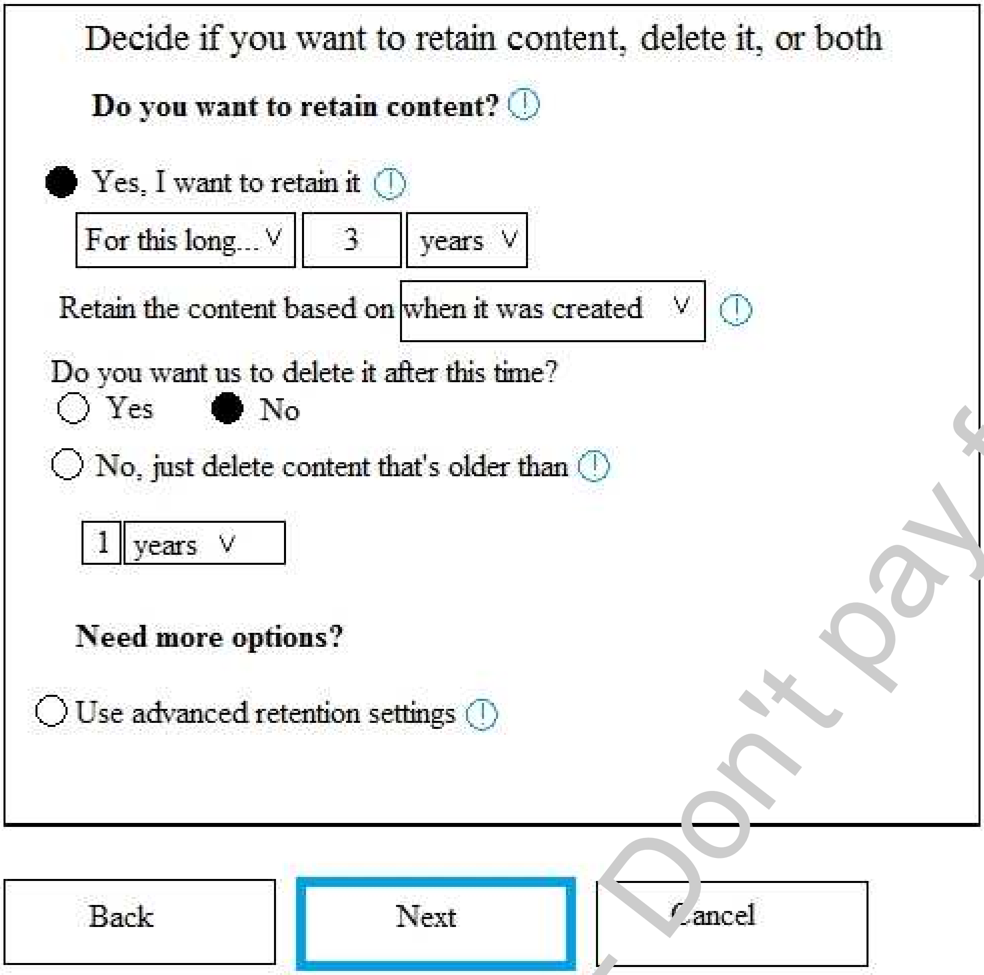
1 | years ∨

Delete the content based on: when it was created ∨ ⓘ

Need more options?

○ Use advanced retention settings ⓘ

Policy2 is configured as shown in the following exhibit.



Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

● Yes, I want to retain it ⓘ

3

Retain the content based on when it was created ∨ ⓘ

Do you want us to delete it after this time?
○ Yes ● No

○ No, just delete content that's older than ⓘ

1 years ∨

Need more options?

○ Use advanced retention settings ⓘ

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

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the-principles-of-retention-or-what-takes-precedence

QUESTION 2
You have a Microsoft 365 subscription.

You need to enable auditing for all Microsoft Exchange Online users.

What should you do?

A. From the Exchange admin center, create a journal rule
B. Run the `Set-MailboxDatabase` cmdlet

C. Run the `Set-Mailbox` cmdlet

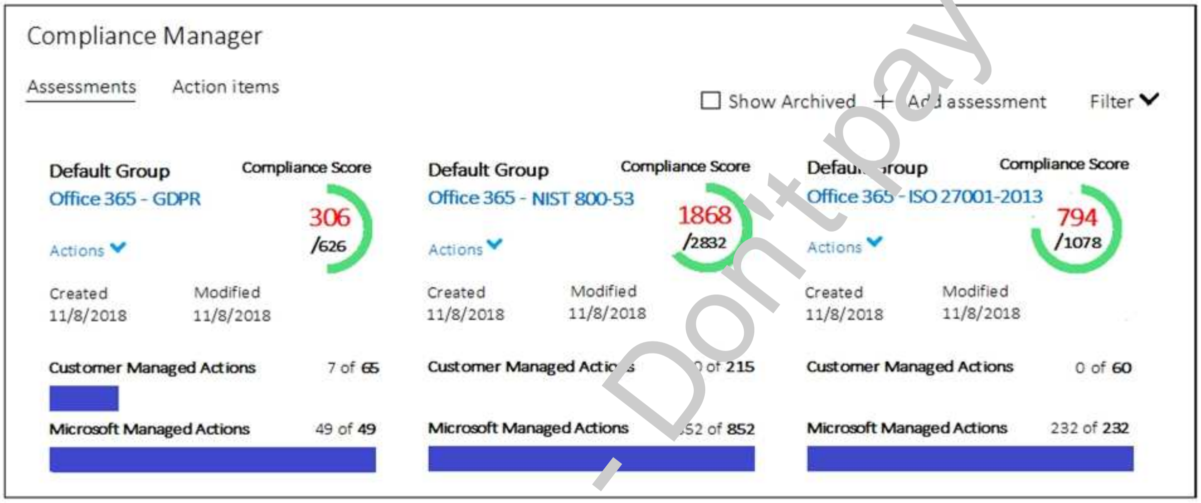
D. From the Exchange admin center, create a mail flow message trace rule.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing

QUESTION 3
HOTSPOT

You view Compliance Manager as shown in the following exhibit.



Default Group
Office 365 - GDPR
Compliance Score 306 /626
Actions
Created 11/8/2018
Modified 11/8/2018
Customer Managed Actions 7 of 65
Microsoft Managed Actions 49 of 49

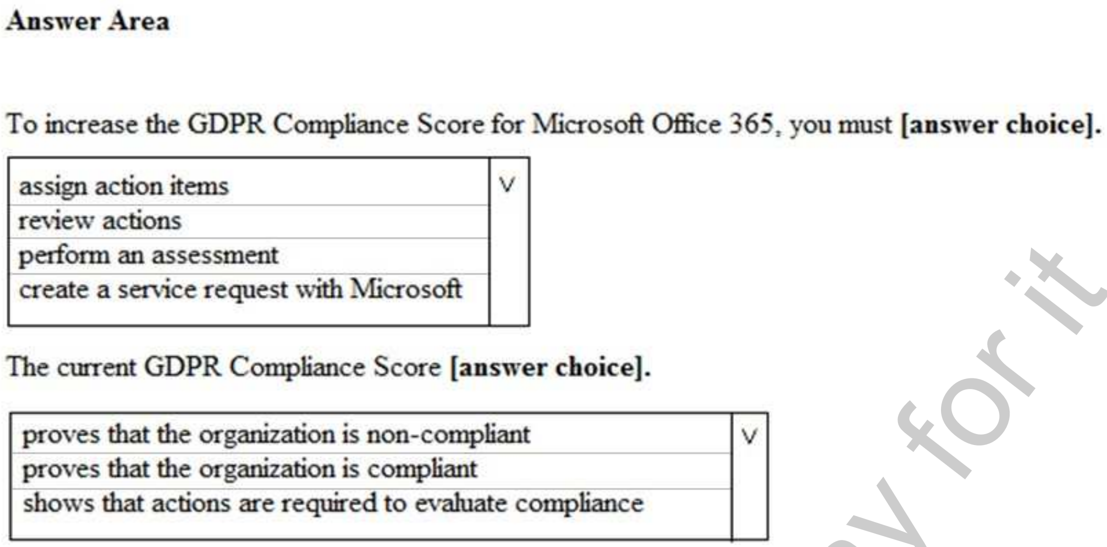
Default Group
Office 365 - NIST 800-53
Compliance Score 1868 /2832
Actions
Created 11/8/2018
Modified 11/8/2018
Customer Managed Actions 0 of 215
Microsoft Managed Actions 852 of 852

Default Group
Office 365 - ISO 27001-2013
Compliance Score 794 /1078
Actions
Created 11/8/2018
Modified 11/8/2018
Customer Managed Actions 0 of 60
Microsoft Managed Actions 232 of 232

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.

Hot Area:



Answer Area

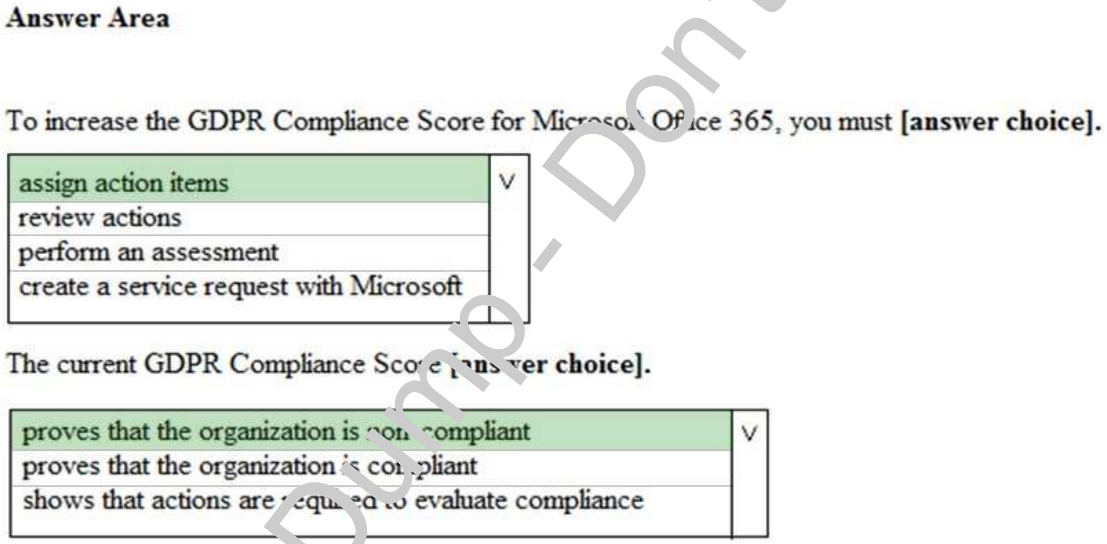
To increase the GDPR Compliance Score for Microsoft Office 365, you must **[answer choice].**

- assign action items
- review actions
- perform an assessment
- create a service request with Microsoft

The current GDPR Compliance Score **[answer choice].**

- proves that the organization is non-compliant
- proves that the organization is compliant
- shows that actions are required to evaluate compliance

Correct Answer:



Answer Area

To increase the GDPR Compliance Score for Microsoft Office 365, you must **[answer choice].**

- [✓ assign action items]
- review actions
- perform an assessment
- create a service request with Microsoft

The current GDPR Compliance Score **[answer choice].**

- [✓ proves that the organization is non-compliant]
- proves that the organization is compliant
- shows that actions are required to evaluate compliance

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud

QUESTION 4
You have a Microsoft 365 subscription.

All computers run Windows 10 Enterprise and are managed by using Microsoft Intune.

You plan to view only security-related Windows telemetry data.

You need to ensure that only Windows security data is sent to Microsoft.

What should you create from the Intune admin center?

A. a device configuration profile that has device restrictions configured
B. a device configuration profile that has the Endpoint Protection settings configured
C. a device compliance policy that has the System Security settings configured
D. a device compliance policy that has the Device Health settings configured

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10#reporting-and-telemetry

QUESTION 5
You create a label that encrypts email data. Users report that they cannot use the label in Outlook on the web to protect the email messages they send.

You need to ensure that the users can use the new label to protect their email.

What should you do?

A. Modify the priority order of label policies
B. Wait six hours and ask the users to try again
C. Create a label policy
D. Create a new sensitive information type

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 6
You have a Microsoft 365 subscription that includes a user named Admin1.

You need to ensure that Admin1 can preserve all the mailbox content of users, including their deleted items.

The solution must use the principle of least privilege.

What should you do?

A. From the Microsoft 365 admin center, assign the Exchange administrator role to Admin1.
B. From the Exchange admin center, assign the Discovery Management admin role to Admin1.
C. From the Azure Active Directory admin center, assign the Service administrator role to Admin1.
D. From the Exchange admin center, assign the Recipient Management admin role to Admin1.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 7
You have a hybrid Microsoft 365 environment.

All computers run Windows 10 Enterprise and have Microsoft Office 365 ProPlus installed. All the computers are joined to Active Directory.

You have a server named Server1 that runs Windows Server 2016. Server1 hosts the telemetry database. You need to prevent private details in the telemetry data from being transmitted to Microsoft.

What should you do?

A. On Server1, run `readinessreportcreator.exe`
B. Configure a registry entry on Server1
C. Configure a registry entry on the computers
D. On the computers, run `tdadm.exe`

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 8
Your company has a Microsoft 365 subscription that includes a user named User1.

You suspect that User1 sent email messages to a competitor detailing company secrets.

You need to recommend a solution to ensure that you can review any email messages sent by User1 to the competitor, including sent items that were deleted.

What should you include in the recommendation?

A. Enable In-Place Archiving for the mailbox of User1
B. From the Security & Compliance, perform a content search of the mailbox of User1
C. Place a Litigation Hold on the mailbox of User1
D. Configure message delivery restrictions for the mailbox of User1

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 9
You have a Microsoft 365 subscription.

Yesterday, you created retention labels and published the labels to Microsoft Exchange Online mailboxes.

You need to ensure that the labels will be available for manual assignment as soon as possible.

What should you do?

A. From the Security & Compliance admin center, create a label policy
B. From Exchange Online PowerShell, run `Start-RetentionAutoTagLearning`
C. From Exchange Online PowerShell, run `Start-ManagedFolderAssistant`
D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 10
DRAG DROP

You have a Microsoft 365 subscription.

You have a site collection named SiteCollection1 that contains a site named Site2. Site2 contains a document library named Customers.

Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.

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.

Select and Place:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 11
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 questions 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 have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the `Set-Maibox -Identity "User1" -AuditEnabled $true` command.

Does that meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps

QUESTION 12
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 questions 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 have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the `Set-AuditConfig -Workload Exchange` command.

Does that meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps

QUESTION 13
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 questions 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 have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the `Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets *Mailbox*` command.

Does that meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-adminauditlogconfig?view=exchange-ps

QUESTION 14
You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. The files in Site1 are protected by using Microsoft Azure Information Protection.

From the Security & Compliance admin center, you create a label that designates personal data.

You need to auto-apply the new label to all the content in Site1.

What should you do first?

A. From PowerShell, run `Set-ManagedContentSettings`.
B. From PowerShell, run `Set-ComplianceTag`.
C. From the Security & Compliance admin center, create a Data Subject Request (DSR).
D. Remove Azure Information Protection from the Site1 files.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/apply-labels-to-personal-data-in-office-365

QUESTION 15
You have a Microsoft 365 subscription.

You need to be notified by email whenever an administrator starts an eDiscovery search.

What should you do from the Security & Compliance admin center?

A. From Search & investigation, create a guided search.

B. From Events, create an event.
C. From Alerts, create an alert policy.
D. From Search & investigation, create an eDiscovery case.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

QUESTION 16
You have a Microsoft 365 subscription.

A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.

You need to limit alert notifications to actionable DLP events.

What should you do?

A. From the Security & Compliance admin center, modify the Policy Tips of a DLP policy.
B. From the Cloud App Security admin center, apply a filter to the alerts.
C. From the Security & Compliance admin center, modify the User overrides settings of a DLP policy.
D. From the Security & Compliance admin center, modify the matched activities threshold of an alert policy.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

QUESTION 17
HOTSPOT

You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1.

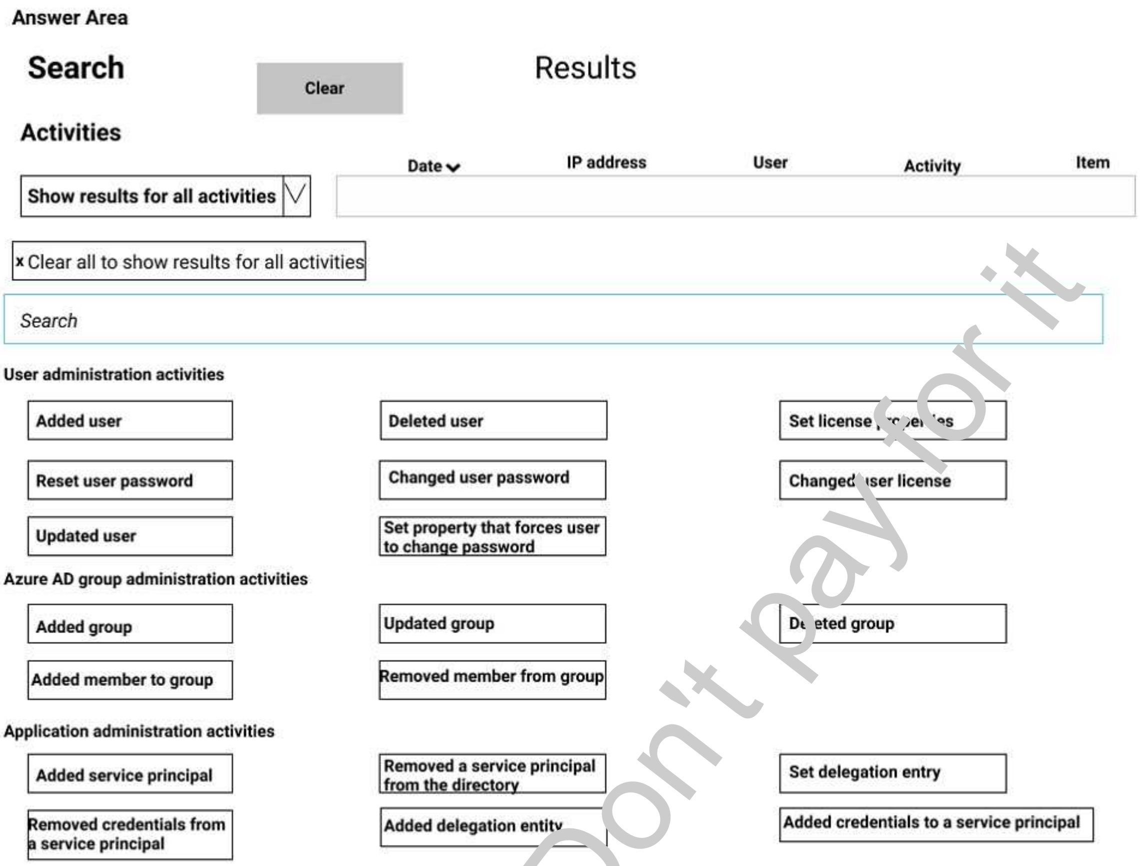
You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two activities should you use in the search? To answer, select the appropriate activities in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Search

Clear

Results

Activities

Show results for all activities ▽

Date ⌄	IP address	User	Activity	Item

× Clear all to show results for all activities

Search

User administration activities

Added user

Deleted user

Set license properties

Reset user password

Changed user password

Changed user license

Updated user

Set property that forces user to change password

Azure AD group administration activities

Added group

Updated group

Deleted group

Added member to group

Removed member from group

Application administration activities

Added service principal

Removed a service principal from the directory

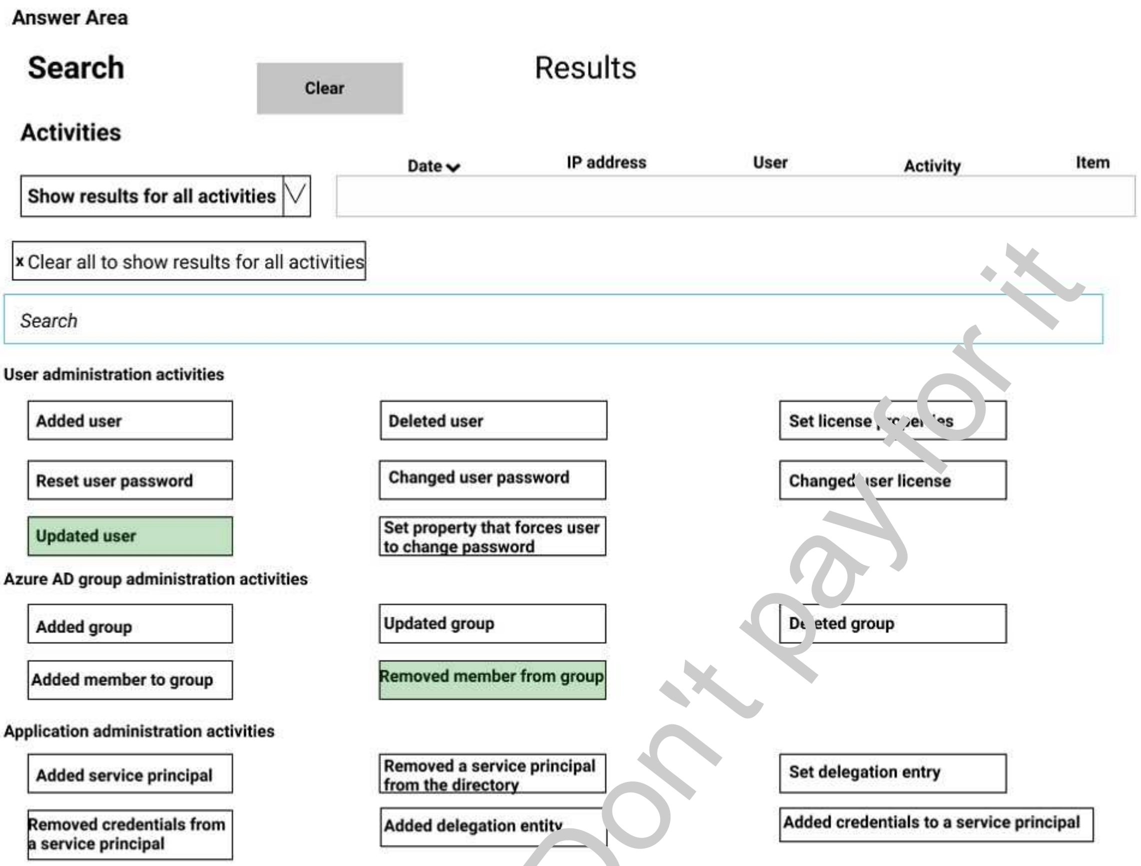
Set delegation entry

Removed credentials from a service principal

Added delegation entity

Added credentials to a service principal

Correct Answer:



Answer Area

Search

Clear

Results

Activities

Date ⌄ IP address User Activity Item

Show results for all activities ⌄

× Clear all to show results for all activities

Search

User administration activities

Added user

Deleted user

Set license properties

Reset user password

Changed user password

Changed user license

[✓ Updated user]

Set property that forces user to change password

Azure AD group administration activities

Added group

Updated group

Deleted group

Added member to group

[✓ Removed member from group]

Application administration activities

Added service principal

Removed a service principal from the directory

Set delegation entry

Removed credentials from a service principal

Added delegation entity

Added credentials to a service principal

Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

QUESTION 18
You have a Microsoft 365 subscription.

You create and run a content search from the Security & Compliance admin center.

You need to download the results of the content search.

What should you obtain first?

A. an export key
B. a password
C. a certificate
D. a pin

Correct Answer: A
Section: [none]
Explanation

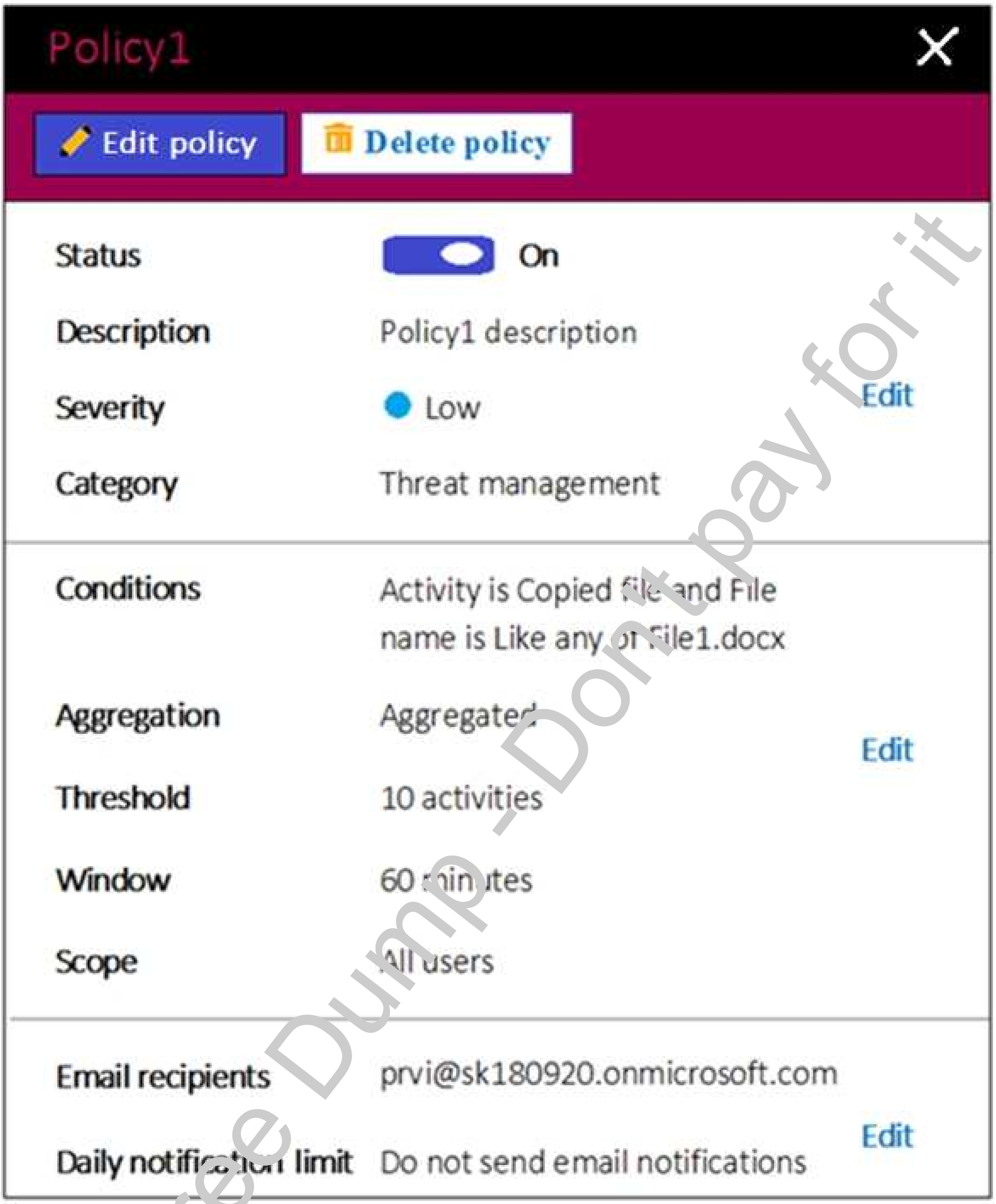
Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results

QUESTION 19
HOTSPOT

You have a Microsoft 365 subscription that include three users named User1, User2, and User3.

A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute.

You create an alert policy named Policy1 as shown in the following exhibit.



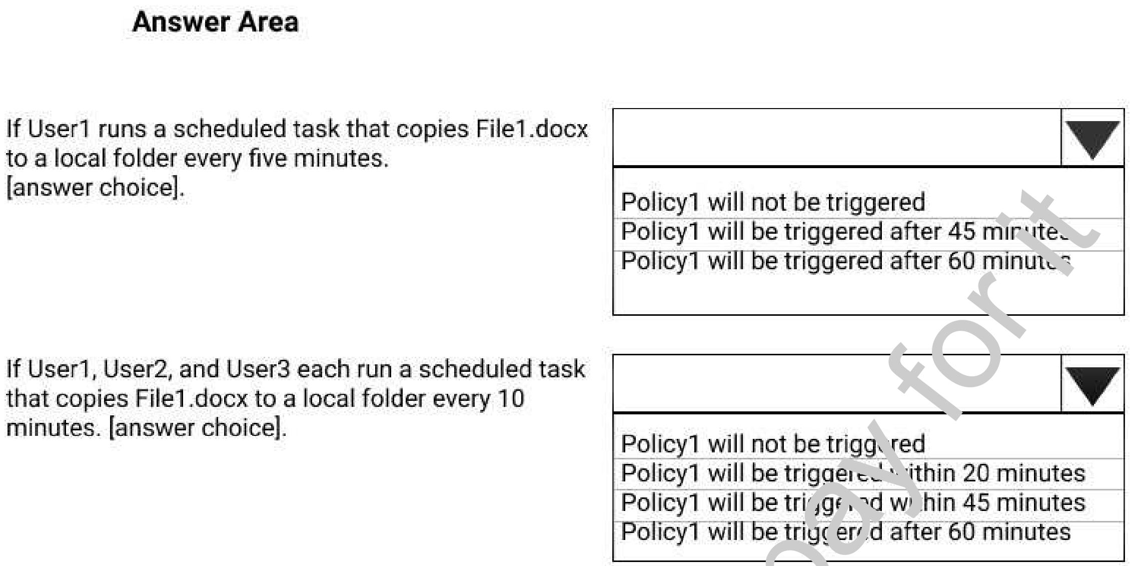
Policy1

Status	On
Description	Policy1 description
Severity	● Low
Category	Threat management
Conditions	Activity is Copied file and File name is Like any of File1.docx
Aggregation	Aggregated
Threshold	10 activities
Window	60 minutes
Scope	All users
Email recipients	prvi@sk180920.onmicrosoft.com
Daily notification limit	Do not send email notifications

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.

Hot Area:



Answer Area

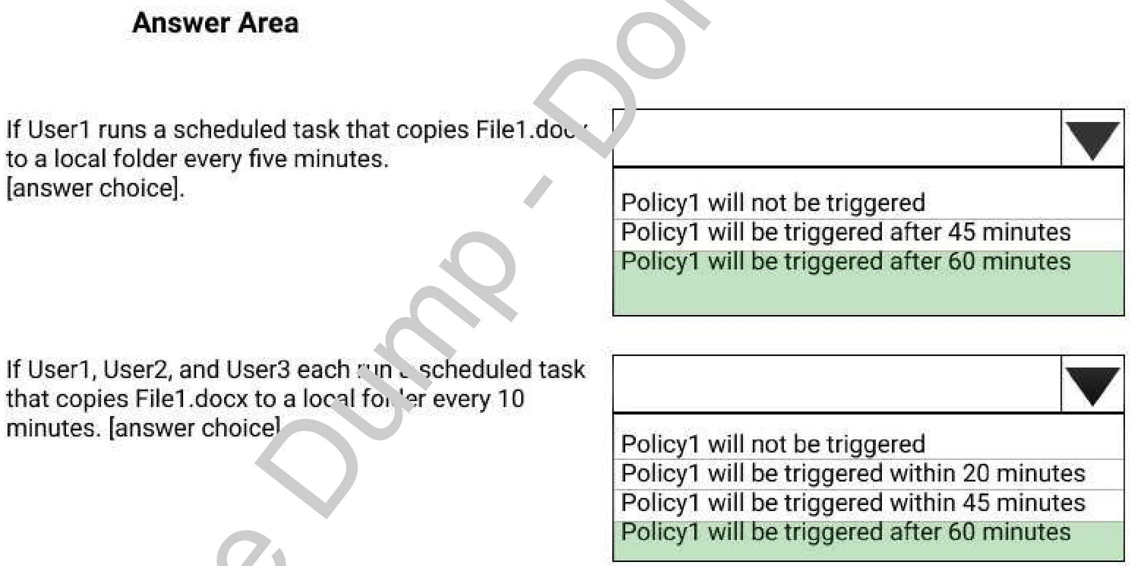
If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered after 45 minutes
- Policy1 will be triggered after 60 minutes

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered within 20 minutes
- Policy1 will be triggered within 45 minutes
- Policy1 will be triggered after 60 minutes

Correct Answer:



Answer Area

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered after 45 minutes
- [✓ Policy1 will be triggered after 60 minutes]

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered within 20 minutes
- Policy1 will be triggered within 45 minutes
- [✓ Policy1 will be triggered after 60 minutes]

Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

QUESTION 20
You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E5 license.

How long will auditing data be retained?

A. 30 days
B. 90 days
C. 365 days
D. 5 years

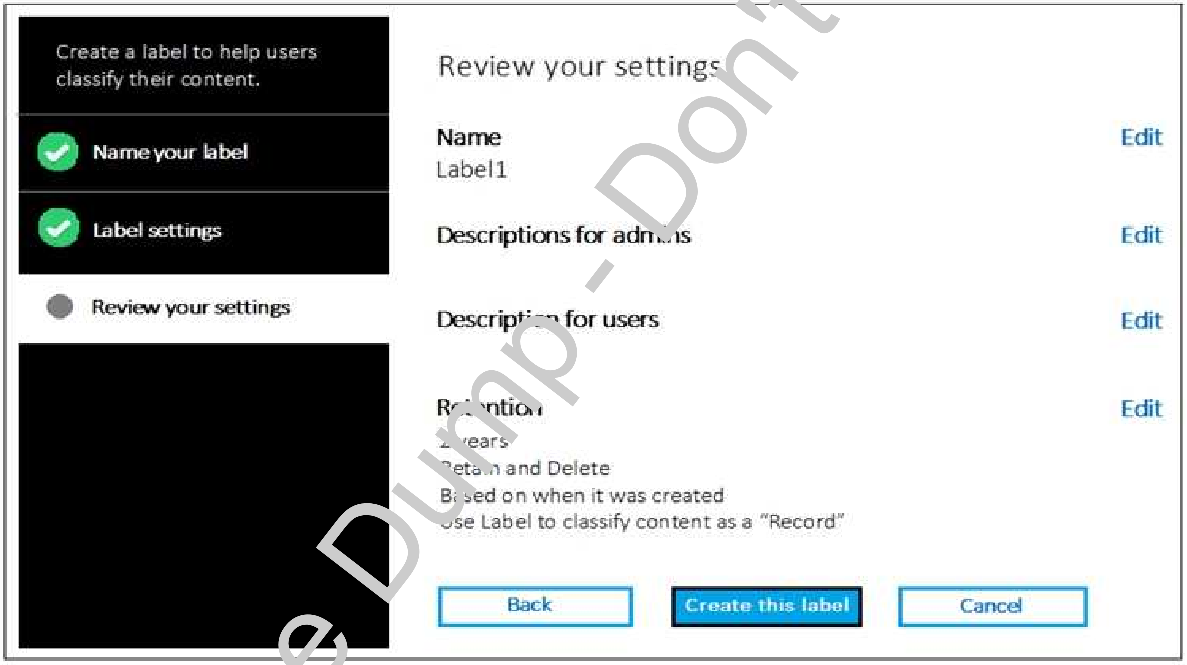
Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

QUESTION 21
HOTSPOT

You have a Microsoft 365 subscription.

You create a retention label named Label1 as shown in the following exhibit.



Create a label to help users classify their content.

✓ Name your label

✓ Label settings

● Review your settings

Review your settings

Name
Label1

Descriptions for admins

Description for users

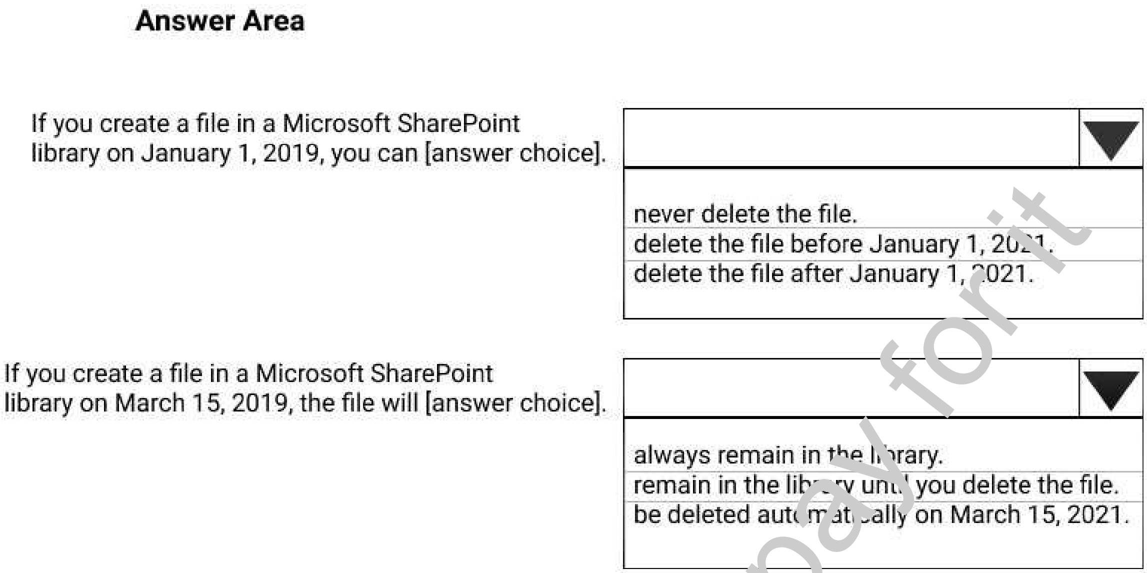
Retention
2 years
Retain and Delete
Based on when it was created
Use Label to classify content as a "Record"

You publish Label1 to SharePoint sites.

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.

Hot Area:



Answer Area

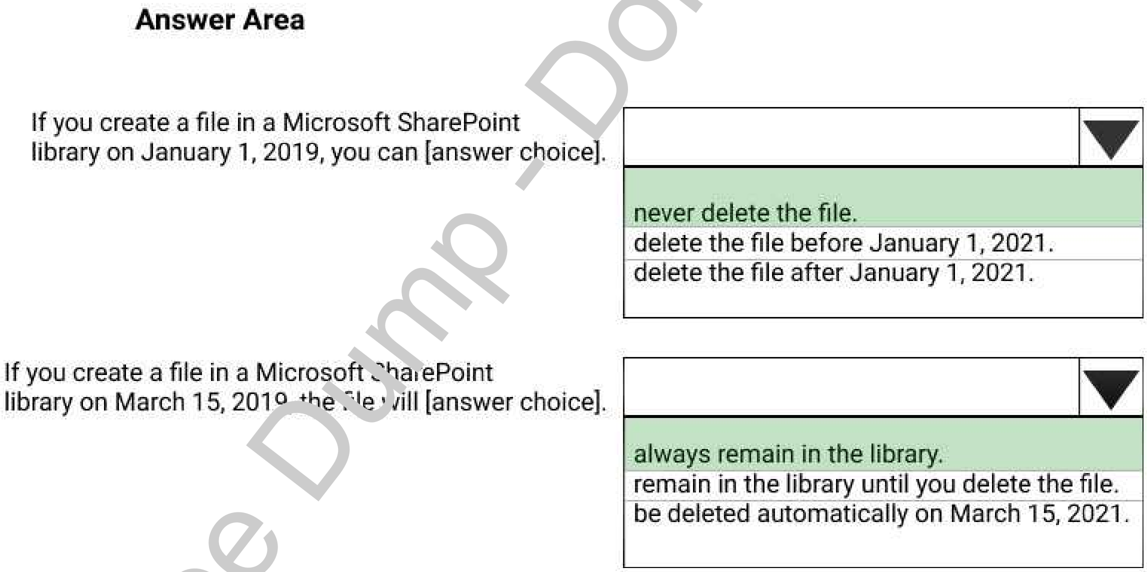
If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

- never delete the file.
- delete the file before January 1, 2021.
- delete the file after January 1, 2021.

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

- always remain in the library.
- remain in the library until you delete the file.
- be deleted automatically on March 15, 2021.

Correct Answer:



Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

- [✓ never delete the file.]
- delete the file before January 1, 2021.
- delete the file after January 1, 2021.

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

- [✓ always remain in the library.]
- remain in the library until you delete the file.
- be deleted automatically on March 15, 2021.

Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/labels

QUESTION 22
You have a Microsoft 365 subscription.

You create a retention policy and apply the policy to Exchange Online mailboxes.

You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible.

What should you do?

A. From Exchange Online PowerShell, run `Start-RetentionAutoTagLearning`
B. From Exchange Online PowerShell, run `Start-ManagedFolderAssistant`
C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy
D. From the Security & Compliance admin center, create a label policy

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/labels

QUESTION 23
You have a Microsoft 365 subscription.

You need to ensure that users can manually designate which content will be subject to data loss prevention (DLP) policies.

What should you create first?

A. A retention label in Microsoft Office 365
B. A custom sensitive information type
C. A Data Subject Request (DSR)
D. A safe attachments policy in Microsoft Office 365

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool#more-information-about-using-the-dsr-case-tool

QUESTION 24
You have a Microsoft 365 subscription.

A user reports that changes were made to several files in Microsoft OneDrive.

You need to identify which files were modified by which users in the user's OneDrive.

What should you do?

A. From the Azure Active Directory admin center, open the audit log
B. From the OneDrive admin center, select **Device access**
C. From Security & Compliance, perform an eDiscovery search
D. From Microsoft Cloud App Security, open the activity log

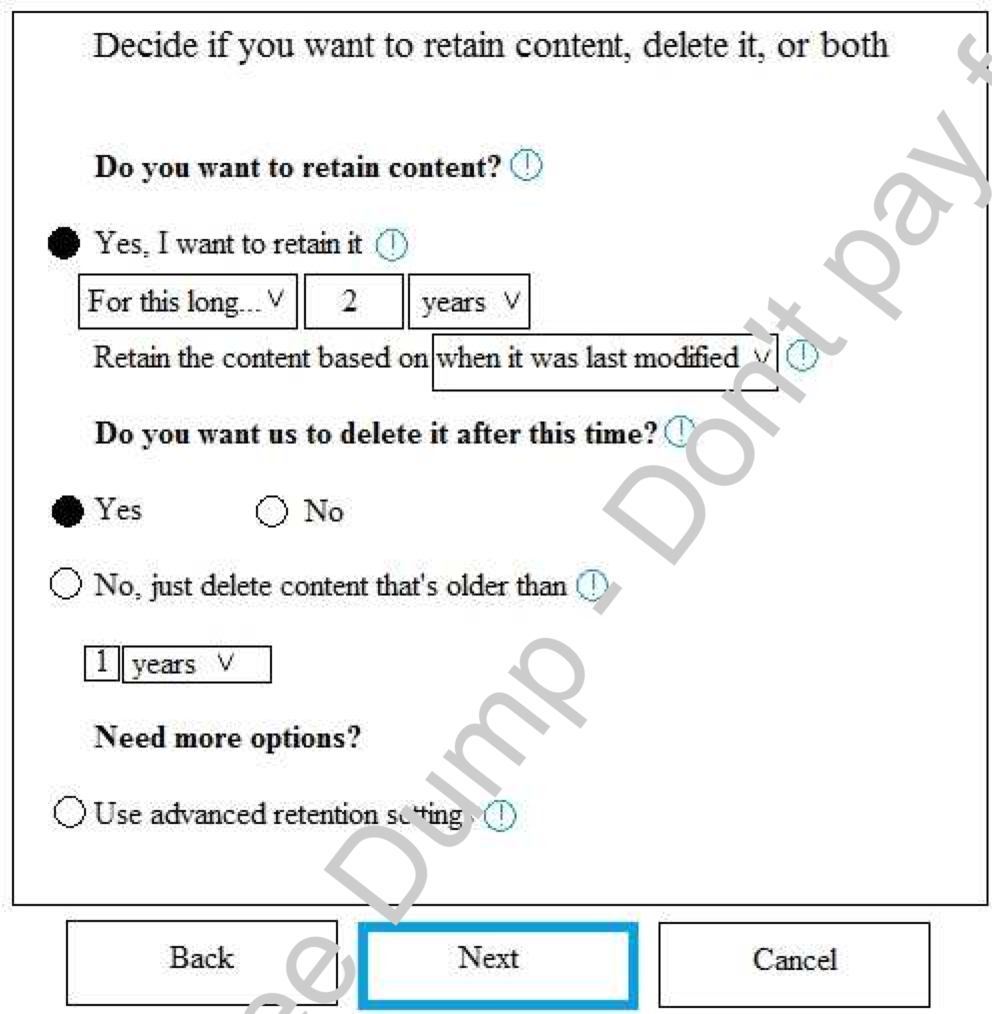
Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/activity-filters

QUESTION 25
HOTSPOT

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 as shown in the following exhibit.



Decide if you want to retain content, delete it, or both

Do you want to retain content?

● Yes, I want to retain it

For this long... | 2 | years

Retain the content based on: when it was last modified

Do you want us to delete it after this time?

● Yes ○ No

○ No, just delete content that's older than

1 years

Need more options?

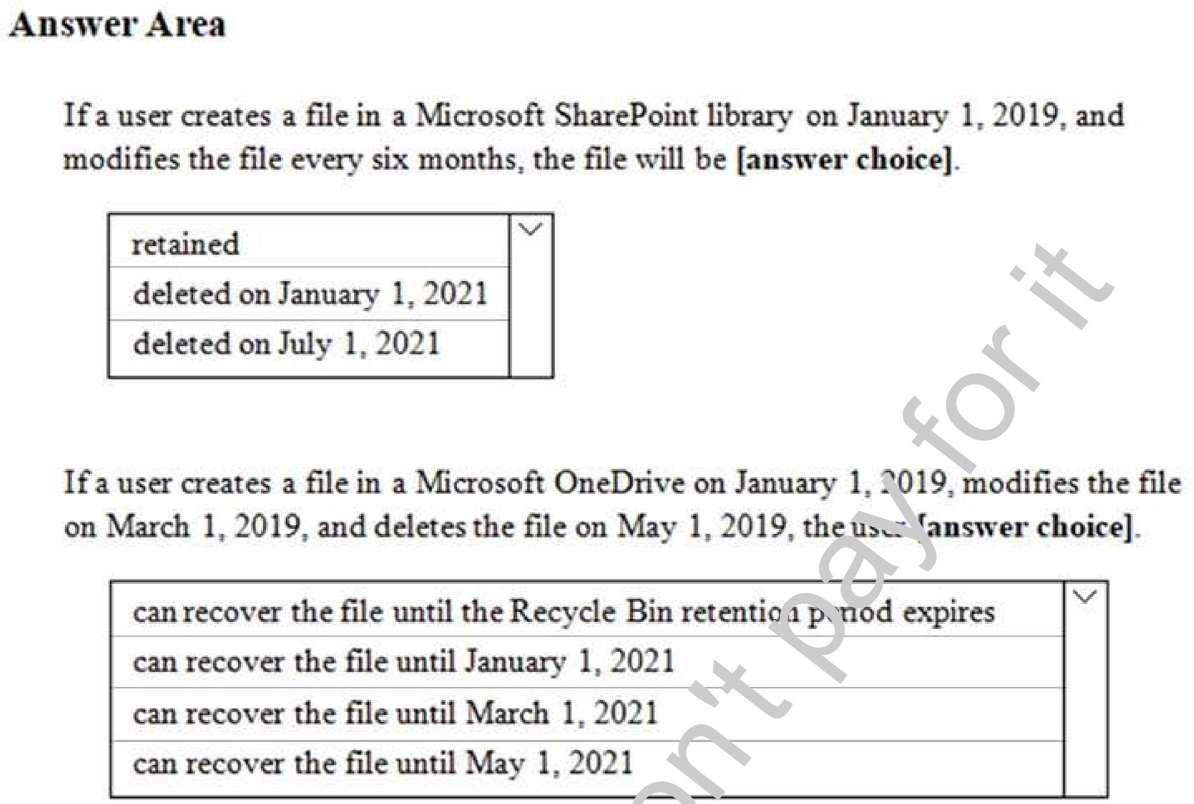
○ Use advanced retention settings

You apply Retention1 to SharePoint sites and OneDrive accounts.

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.

Hot Area:



Answer Area

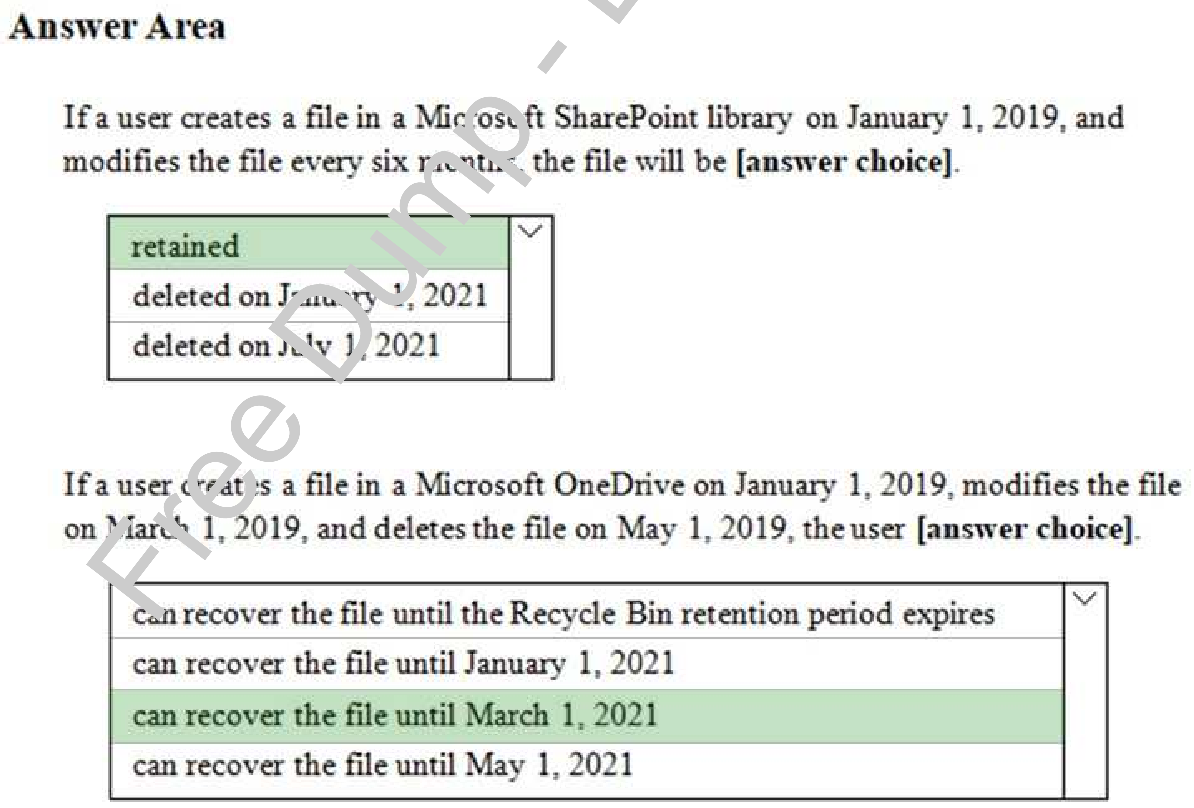
If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be **[answer choice]**.

- retained
- deleted on January 1, 2021
- deleted on July 1, 2021

If a user creates a file in a Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice]**.

- can recover the file until the Recycle Bin retention period expires
- can recover the file until January 1, 2021
- can recover the file until March 1, 2021
- can recover the file until May 1, 2021

Correct Answer:



Answer Area

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be **[answer choice]**.

- [✓ retained]
- deleted on January 1, 2021
- deleted on July 1, 2021

If a user creates a file in a Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice]**.

- can recover the file until the Recycle Bin retention period expires
- can recover the file until January 1, 2021
- [✓ can recover the file until March 1, 2021]
- can recover the file until May 1, 2021

Section: [none]
Explanation

Explanation/Reference:

QUESTION 26
DRAG DROP

You have a Microsoft 365 subscription.

A customer requests that you provide her with all documents that reference her by name.

You need to provide the customer with a copy of the content.

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

Select and Place:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365

QUESTION 27
You have a Microsoft 365 subscription. You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the Cloud App Security admin center, create a file policy.
B. From the SharePoint admin center, modify the Site Settings.
C. From the SharePoint admin center, create a label.
D. From the SharePoint admin center, modify the records management settings.
E. From the Security admin center, publish a label.

Correct Answer: CE
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-office-365-labels-and-dlp

QUESTION 28
You recently created and published several labels policies in a Microsoft 365 subscription.

You need to view which labels were applied by users manually and which labels were applied automatically.

What should you do from the Security & Compliance admin center?

A. From Search & investigation, select **Content search**
B. From Data governance, select **Events**
C. From Search & investigation, select **eDiscovery**
D. From Reports, select **Dashboard**

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 29
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions 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 have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the `Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner` command.

Does that meet the goal?

A. Yes
B. No

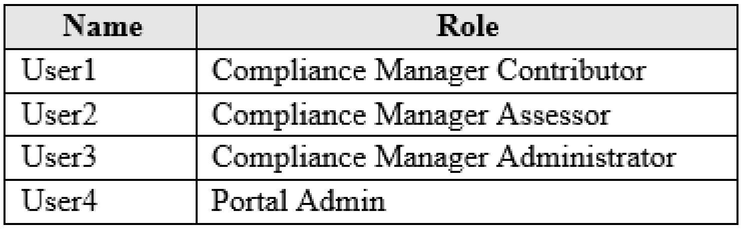
Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps

QUESTION 30
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions 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 that contains the users shown in the following table.



Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend assigning the Compliance Manager Reader role to User1.

Does this meet the goal?

A. Yes
B. No

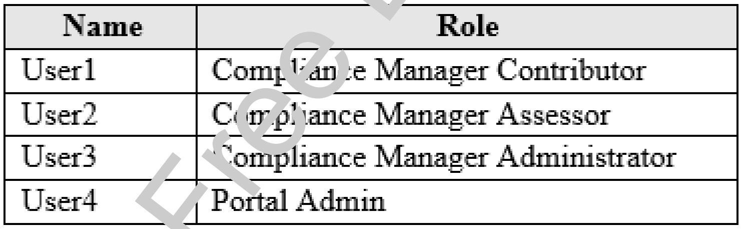
Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager

QUESTION 31
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 questions 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 that contains the users shown in the following table.



Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend modifying the licenses assigned to User5.

Does this meet the goal?

A. Yes
B. No

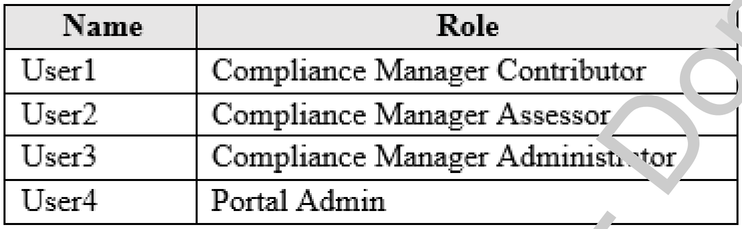
Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager

QUESTION 32
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 questions 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 that contains the users shown in the following table.



Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend assigning the Compliance Manager Reader role to User5.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager

QUESTION 33
You have a Microsoft 365 subscription.

You enable auditing for the subscription.

You plan to provide a user named Auditor with the ability to review audit logs.

You add Auditor to the Global administrator role group.

Several days later, you discover that Auditor disabled auditing.

You remove Auditor from the Global administrator role group and enable auditing.

You need to modify Auditor to meet the following requirements:

- Be prevented from disabling auditing
- Use the principle of least privilege
- Be able to review the audit log

To which role group should you add Auditor?

A. Security reader
B. Compliance administrator
C. Security operator
D. Security administrator

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center

QUESTION 34
You have a Microsoft 365 subscription.

You have a team named Team1 in Microsoft Teams.

You plan to place all the content in Team1 on hold.

You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.

Which cmdlet should you use?

A. `Get-UnifiedGroup`
B. `Get-MailUser`
C. `Get-TeamMessagingSettings`
D. `Get-TeamChannel`

Correct Answer: A
Section: [none]
Explanation

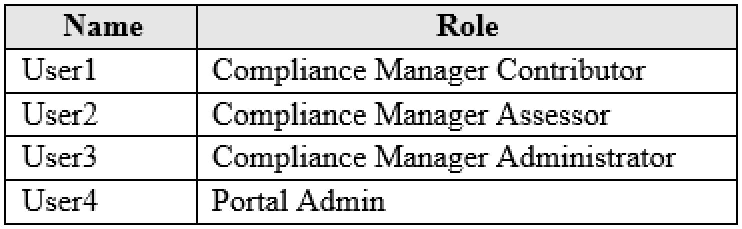
Explanation/Reference:

QUESTION 35
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 questions 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 that contains the users shown in the following table.



Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend removing User1 from the Compliance Manager Contributor role.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager

QUESTION 36
You have a Microsoft 365 subscription.

The Global administrator role is assigned to your user account. You have a user named Admin1.

You create an eDiscovery case named Case1.

You need to ensure that Admin1 can view the results of Case1.

What should you do first?

A. From the Azure Active Directory admin center, assign a role group to Admin1.
B. From the Microsoft 365 admin center, assign a role to Admin1.
C. From Security & Compliance admin center, assign a role group to Admin1.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions