MS-500.41q

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

MS-500

Microsoft 365 Security Administration (beta)

Testlet 1

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 range 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
Group 1	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
- Integrate Windows Defender and Windows Defender ATP on domain-joined servers
- 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 want 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 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:

Testlet 2

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	Desktops 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 implement Azure AD Privileged Identity Management

QUESTION 1
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 2
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 3
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 3

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 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 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 Source Anchor settings.

Does that meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 3
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 4
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 5
Your company has a Microsoft 365 subscription.

The company forbids 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 Set 1

QUESTION 1
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 2
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 address that you intend to spoof belongs to the Executive group members.

What should you do first?

A. From Azure ATP admin center, configure the primary workspace settings
B. From the Microsoft Azure portal, configure the user risk 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 3
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 4
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 5
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 6
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 7
You have a Microsoft 365 subscription.

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

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

Which type of threat management policy should you create from the Security&Compliance admin center?

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

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 8
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 9
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 10
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 Set 1

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 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 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 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 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 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 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 synching files.

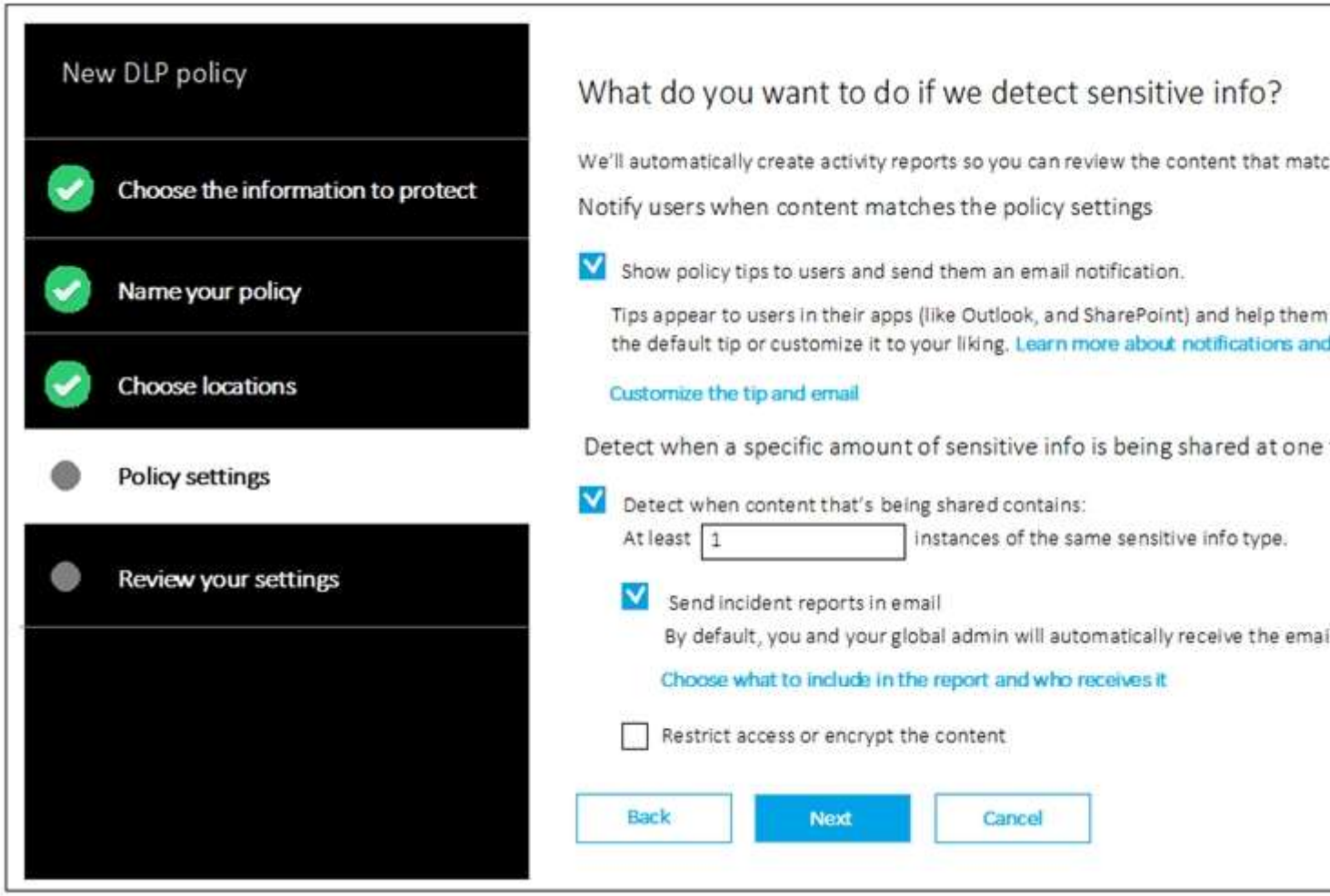
What should you do?

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:

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



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. Compliance Policy Center
C. eDiscovery Center
D. Enterprise Search Center
E. Document Center

Correct Answer: C
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 Set 1

QUESTION 1
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 2
You have a Microsoft 365 subscription.

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

What should you do?

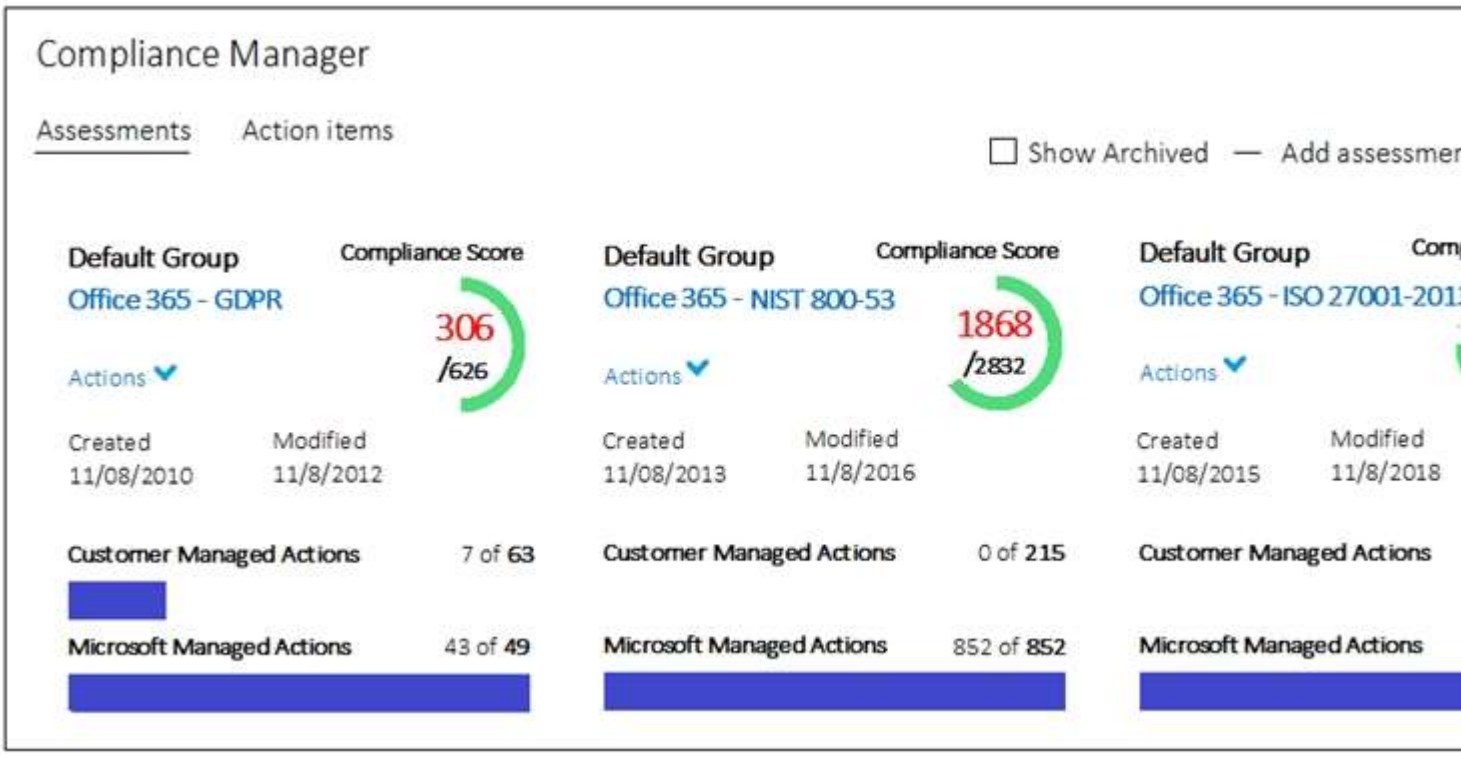
A. From the Exchange admin center, create a journal rule
B. Run the `Set-MailboxDatabase` cmdlet
C. Run the `Set-Mailbox` cmdlet
D. From the Exchange admin center, create a mail flow message trace rule.

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.



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	v
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	v
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	v
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	v
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 configuration 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 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 on Server1
C. Configure a registry on the computers
D. On the computers, run `tdadm.exe`

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 7
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 8
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 9
DRAG DROP

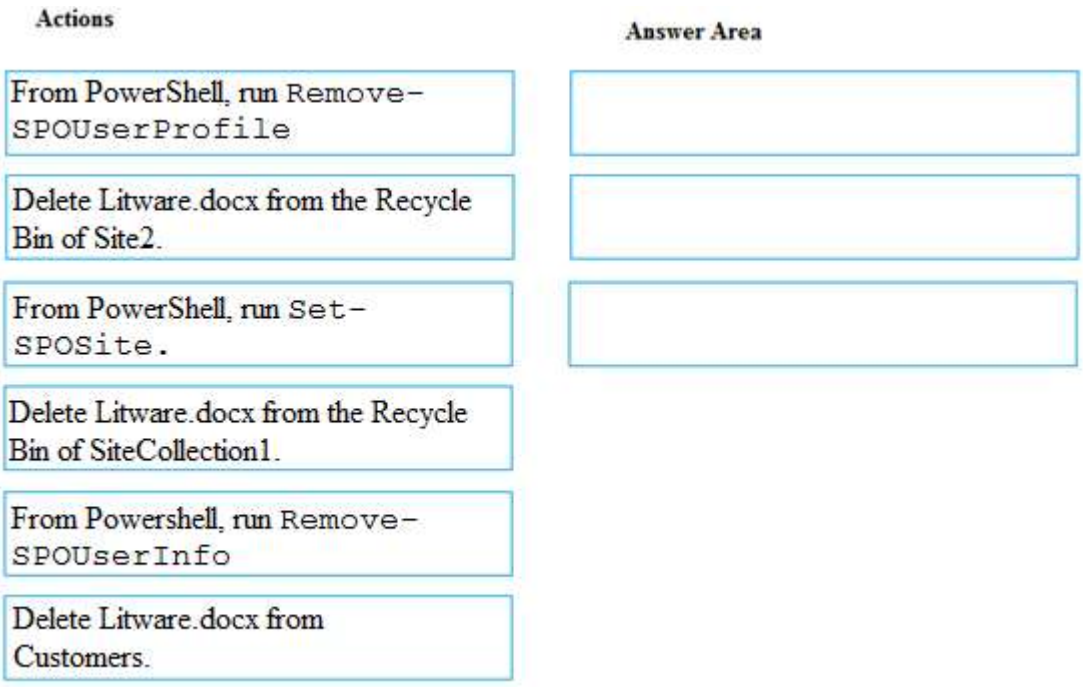
You have a Microsoft 365 subscription.

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

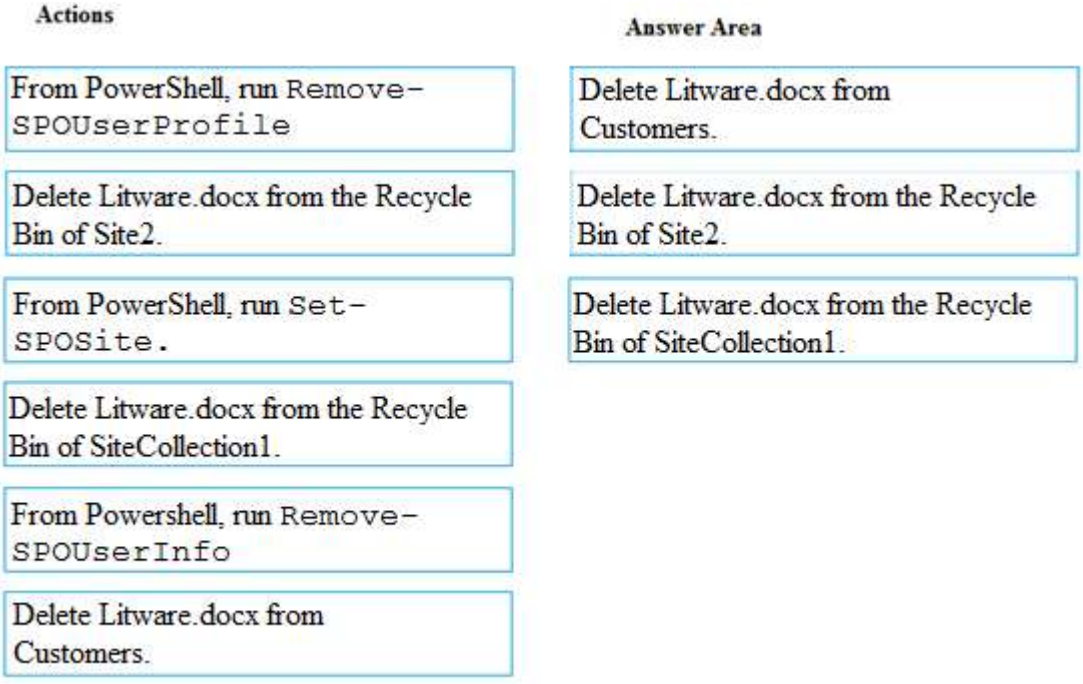
Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.

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 10
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 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-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 12
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 13
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 14

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

Testlet 2

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	Desktops 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 implement 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: