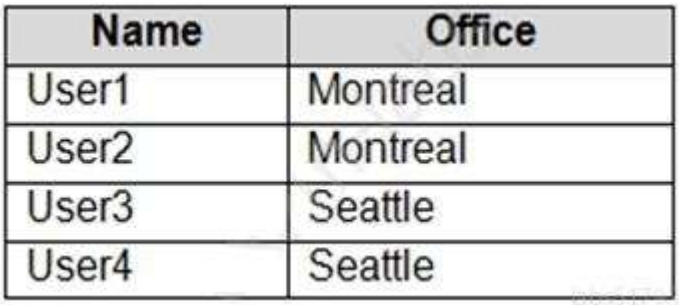
- **Vendor:** Microsoft
- **Exam Code:** MS-101
- **Exam Name:** Microsoft 365 Mobility and Security
- **New Updated Questions from Braindump2go**
- **(Updated in November/2021)**

QUESTION 352
Case Study 3 - Litware, Inc
Overview
General Overviews

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

Environment
Existing Environment

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

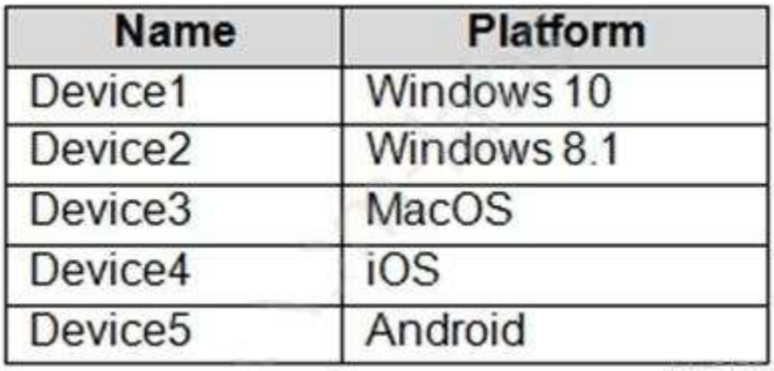


Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

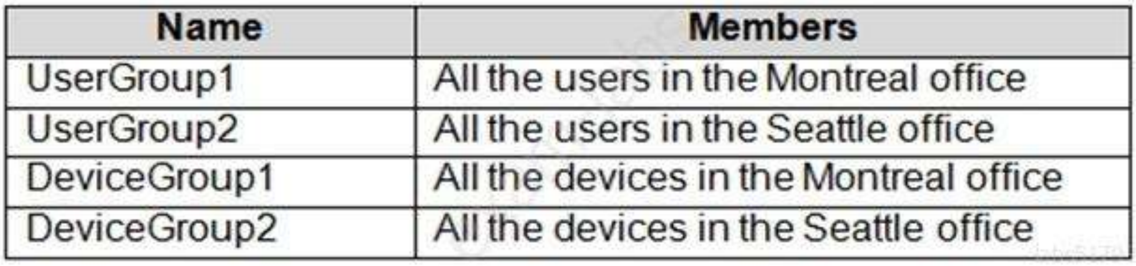
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

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



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

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



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

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

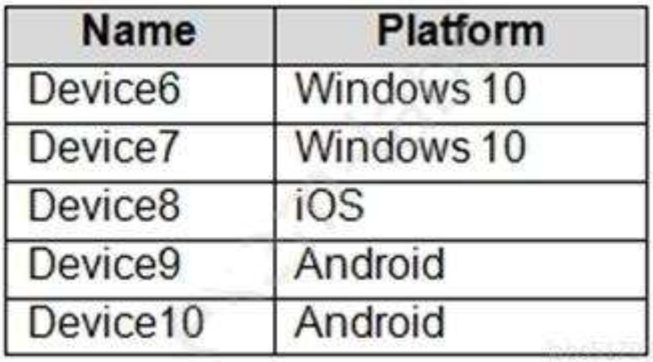
Problem Statements

Litware identifies the following issues:
- Users open email attachments that contain malicious content.
- Devices without an assigned compliance policy show a status of Compliant.
- User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
- Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

Requirements

Planned Changes

Litware plans to implement the following changes:
- Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
- Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
- Implement data loss prevention (DLP) policies to protect confidential information.
- Grant User2 permissions to review the audit logs of he litware.com tenant.
- Deploy new devices to the Seattle office as shown in the following table.



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

- Implement a notification system for when DLP policies are triggered.
- Configure a Safe Attachments policy for the litware.com tenant.

Technical Requirements

Litware identifies the following technical requirements:
- Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
- Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
- All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Azure AD.
- Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
- A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
- User2 must be granted the permissions to review audit logs for the following activities:
  - Admin activities in Microsoft Exchange Online
  - Admin activities in SharePoint Online
  - Admin activities in Azure AD
- Users must be able to apply sensitivity labels to documents by using Office for the web.
- Windows Autopilot must be used for device provisioning, whenever possible.

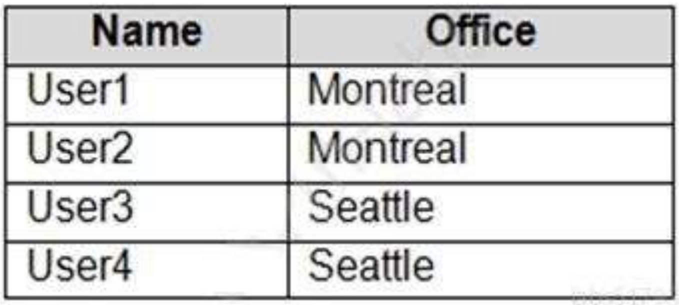
- A DLP policy must be created to meet the following requirements:
  - Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
  - Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
- The principle of least privilege must be used.

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

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

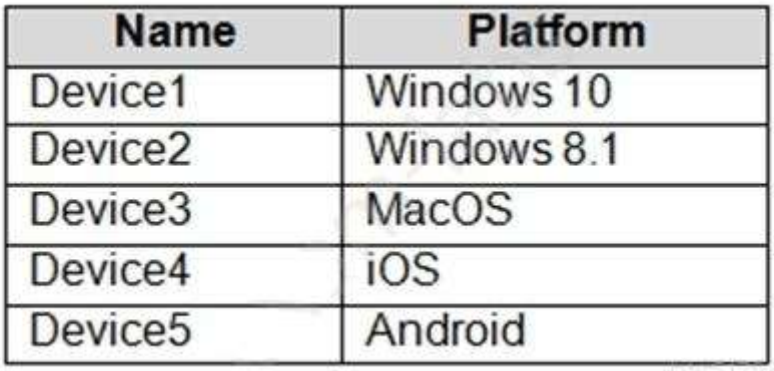
Answer: D
Explanation:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/safe-attachments.md

QUESTION 353
Case Study 3 - Litware, Inc
Overview
General Overviews
Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.
Environment
Existing Environment
The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.



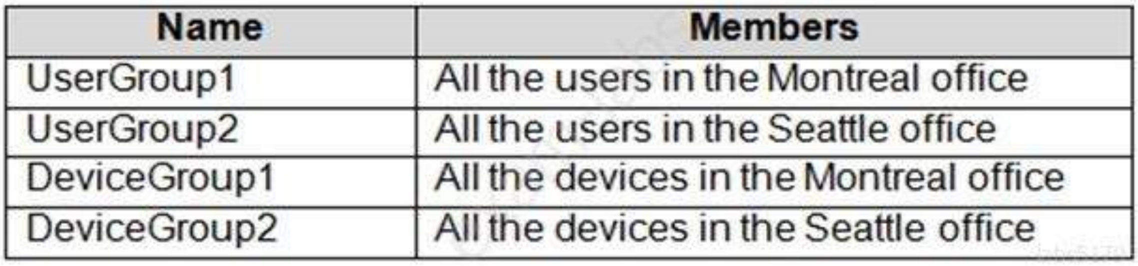
Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.
Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.



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

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



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

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

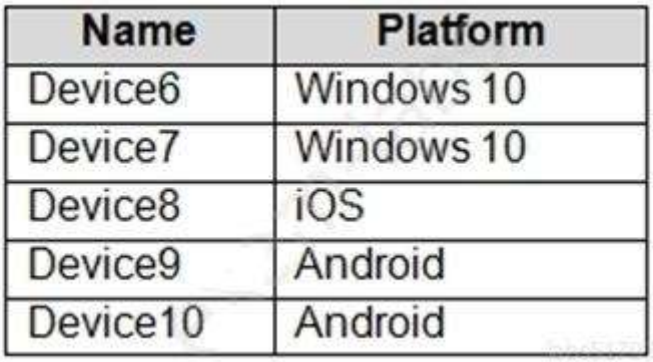
Problem Statements

Litware identifies the following issues:
- Users open email attachments that contain malicious content.
- Devices without an assigned compliance policy show a status of Compliant.
- User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
- Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

Requirements

Planned Changes

Litware plans to implement the following changes:
- Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
- Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
- Implement data loss prevention (DLP) policies to protect confidential information.
- Grant User2 permissions to review the audit logs of he litware.com tenant.
- Deploy new devices to the Seattle office as shown in the following table.



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

- Implement a notification system for when DLP policies are triggered.
- Configure a Safe Attachments policy for the litware.com tenant.

Technical Requirements

Litware identifies the following technical requirements:
- Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
- Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
- All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Azure AD.
- Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
- A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
- User2 must be granted the permissions to review audit logs for the following activities:
  - Admin activities in Microsoft Exchange Online
  - Admin activities in SharePoint Online
  - Admin activities in Azure AD
- Users must be able to apply sensitivity labels to documents by using Office for the web.
- Windows Autopilot must be used for device provisioning, whenever possible.

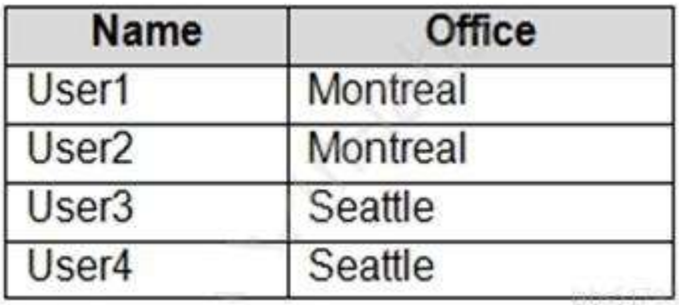
- A DLP policy must be created to meet the following requirements:
    - Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
    - Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
- The principle of least privilege must be used.

You need to configure Office on the web to meet the technical requirements.
What should you do?

A. Assign the Global reader role to User1.
B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.
C. Configure an auto-labeling policy to apply the sensitivity labels.
D. Assign the Office apps admin role to User1.

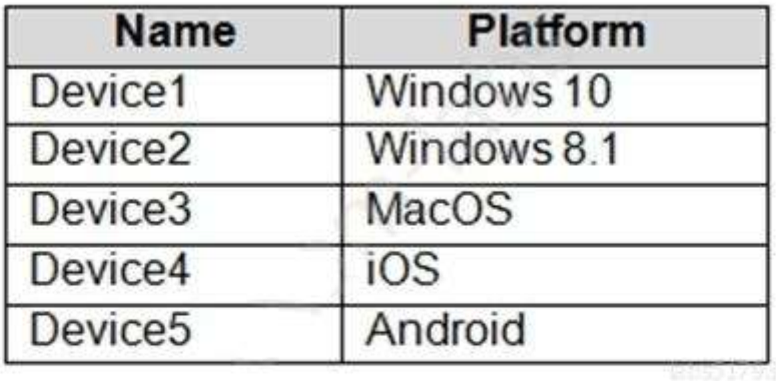
Answer: B
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files? view=o365-worldwide

QUESTION 354
Case Study 3 - Litware, Inc
Overview
General Overviews
Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.
Environment
Existing Environment
The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.



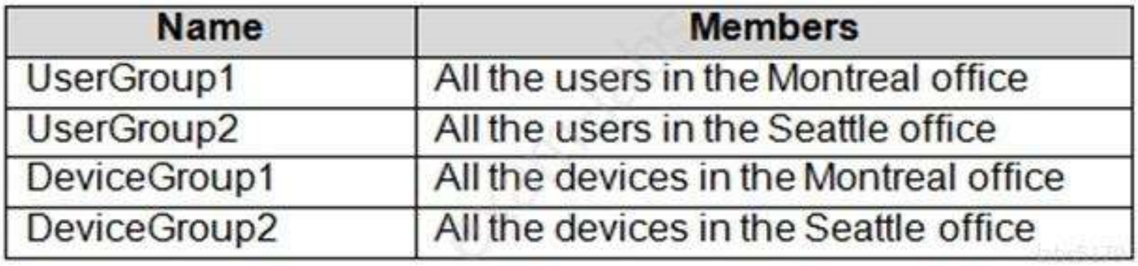
Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.
Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.



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

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



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

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

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

Problem Statements

Litware identifies the following issues:

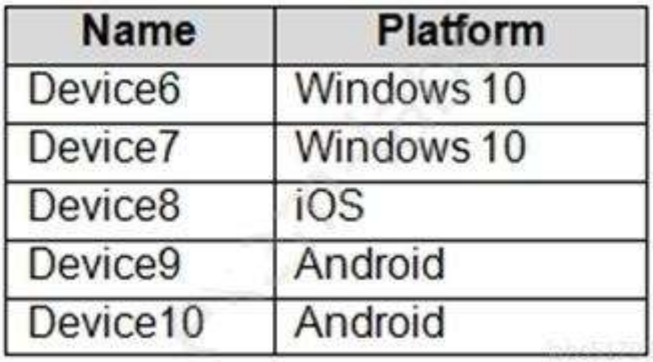
- Users open email attachments that contain malicious content.
- Devices without an assigned compliance policy show a status of Compliant.
- User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
- Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

Requirements

Planned Changes

Litware plans to implement the following changes:

- Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
- Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
- Implement data loss prevention (DLP) policies to protect confidential information.
- Grant User2 permissions to review the audit logs of he litware.com tenant.
- Deploy new devices to the Seattle office as shown in the following table.



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

- Implement a notification system for when DLP policies are triggered.
- Configure a Safe Attachments policy for the litware.com tenant.

Technical Requirements

Litware identifies the following technical requirements:

- Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
- Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
- All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Azure AD.
- Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
- A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
- User2 must be granted the permissions to review audit logs for the following activities:
  - Admin activities in Microsoft Exchange Online
  - Admin activities in SharePoint Online
  - Admin activities in Azure AD
- Users must be able to apply sensitivity labels to documents by using Office for the web.
- Windows Autopilot must be used for device provisioning, whenever possible.

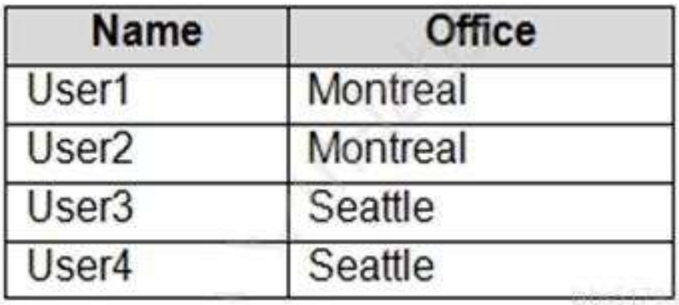
- A DLP policy must be created to meet the following requirements:
    - Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
    - Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
- The principle of least privilege must be used.

You create the planned DLP policies.
You need to configure notifications to meet the technical requirements.
What should you do?

A. From the Microsoft 365 security center, configure an alert policy.
B. From the Microsoft Endpoint Manager admin center, configure a custom notification.
C. From the Microsoft 365 admin center, configure a Briefing email.
D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

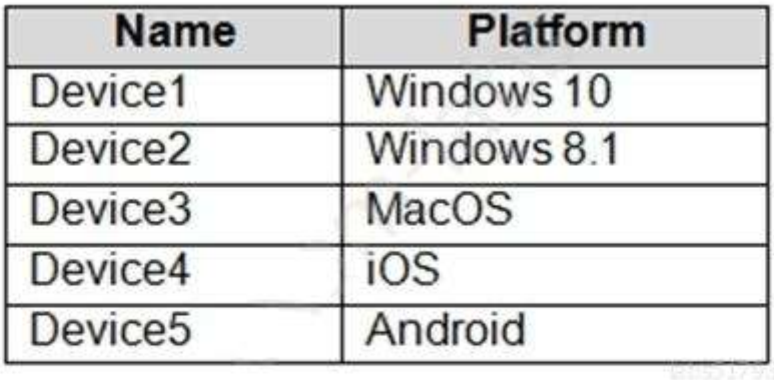
Answer: D
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide

QUESTION 355
Case Study 3 - Litware, Inc
Overview
General Overviews
Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.
Environment
Existing Environment
The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.



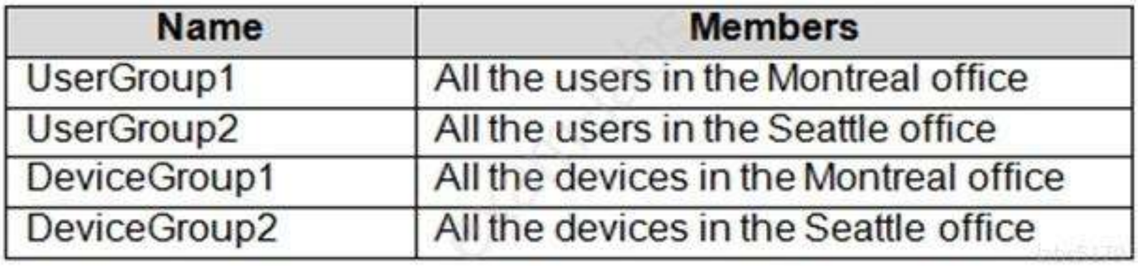
Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.
Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.



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

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



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

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

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

Problem Statements

Litware identifies the following issues:

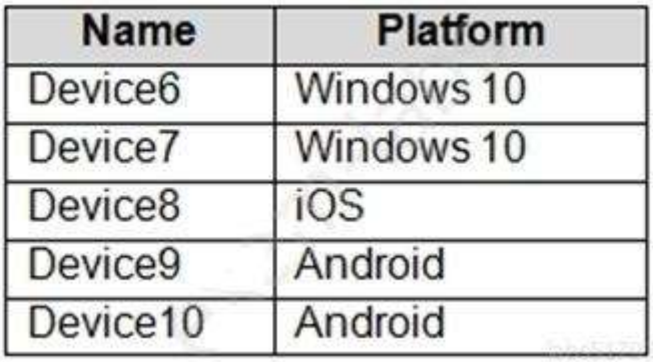
- Users open email attachments that contain malicious content.
- Devices without an assigned compliance policy show a status of Compliant.
- User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
- Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

Requirements

Planned Changes

Litware plans to implement the following changes:

- Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
- Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
- Implement data loss prevention (DLP) policies to protect confidential information.
- Grant User2 permissions to review the audit logs of he litware.com tenant.
- Deploy new devices to the Seattle office as shown in the following table.



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

- Implement a notification system for when DLP policies are triggered.
- Configure a Safe Attachments policy for the litware.com tenant.

Technical Requirements

Litware identifies the following technical requirements:

- Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
- Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
- All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Azure AD.
- Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
- A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
- User2 must be granted the permissions to review audit logs for the following activities:
    - Admin activities in Microsoft Exchange Online
    - Admin activities in SharePoint Online
    - Admin activities in Azure AD
- Users must be able to apply sensitivity labels to documents by using Office for the web.
- Windows Autopilot must be used for device provisioning, whenever possible.

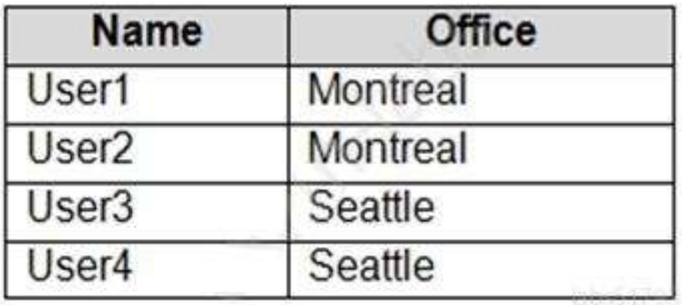
- A DLP policy must be created to meet the following requirements:
    - Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
    - Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
- The principle of least privilege must be used.

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

A. From Compliance policies, modify the Notifications settings.
B. From Locations, create a new location for noncompliant devices.
C. From Retire Noncompliant Devices, select Clear All Devices Retire State.
D. Modify the Compliance policy settings.

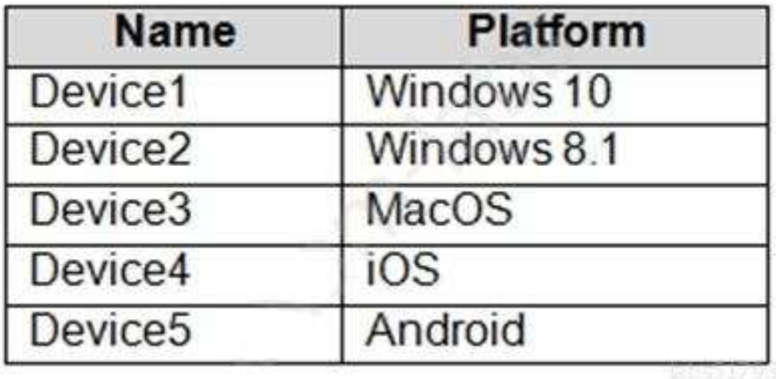
Answer: D
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

QUESTION 356
Case Study 3 - Litware, Inc
Overview
General Overviews
Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.
Environment
Existing Environment
The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.



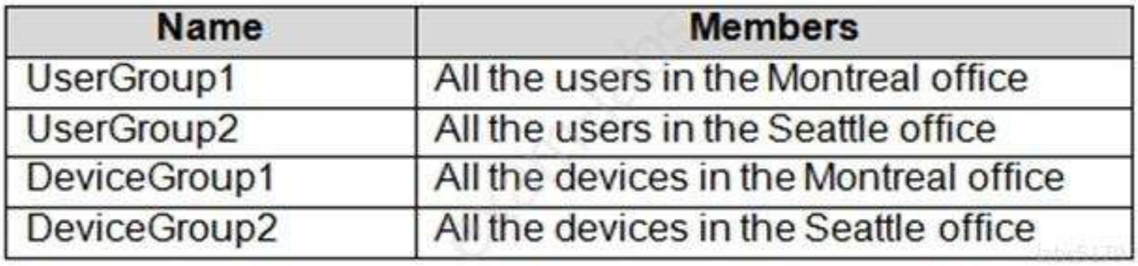
Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.
Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.



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

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



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

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

Problem Statements

Litware identifies the following issues:

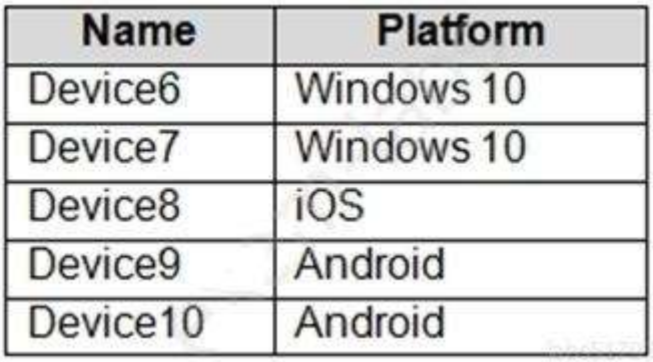
- Users open email attachments that contain malicious content.
- Devices without an assigned compliance policy show a status of Compliant.
- User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
- Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

Requirements

Planned Changes

Litware plans to implement the following changes:

- Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
- Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
- Implement data loss prevention (DLP) policies to protect confidential information.
- Grant User2 permissions to review the audit logs of he litware.com tenant.
- Deploy new devices to the Seattle office as shown in the following table.



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

- Implement a notification system for when DLP policies are triggered.
- Configure a Safe Attachments policy for the litware.com tenant.

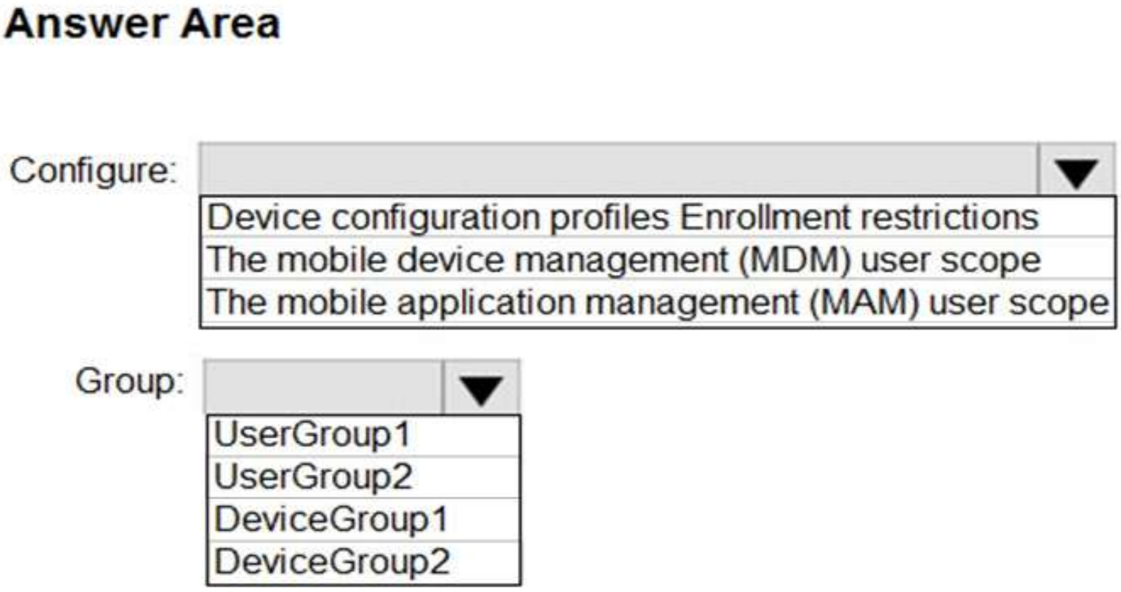
Technical Requirements

Litware identifies the following technical requirements:

- Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
- Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
- All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Azure AD.
- Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
- A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
- User2 must be granted the permissions to review audit logs for the following activities:
  - Admin activities in Microsoft Exchange Online
  - Admin activities in SharePoint Online
  - Admin activities in Azure AD
- Users must be able to apply sensitivity labels to documents by using Office for the web.
- Windows Autopilot must be used for device provisioning, whenever possible.

- A DLP policy must be created to meet the following requirements:
    - Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
    - Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
- The principle of least privilege must be used.

Hotspot Question
You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.
What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

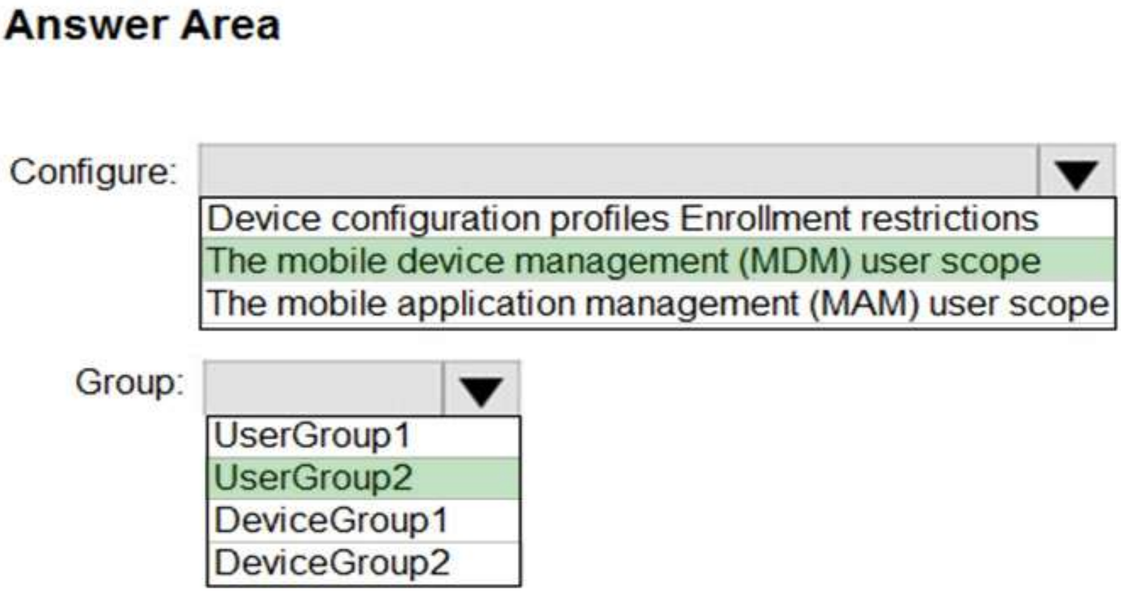


Answer Area

Configure:
Device configuration profiles Enrollment restrictions
The mobile device management (MDM) user scope
The mobile application management (MAM) user scope

Group:
UserGroup1
UserGroup2
DeviceGroup1
DeviceGroup2

Answer:



Answer Area

Configure:
Device configuration profiles Enrollment restrictions
[✓ The mobile device management (MDM) user scope]
The mobile application management (MAM) user scope

Group:
UserGroup1
[✓ UserGroup2]
DeviceGroup1
DeviceGroup2

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

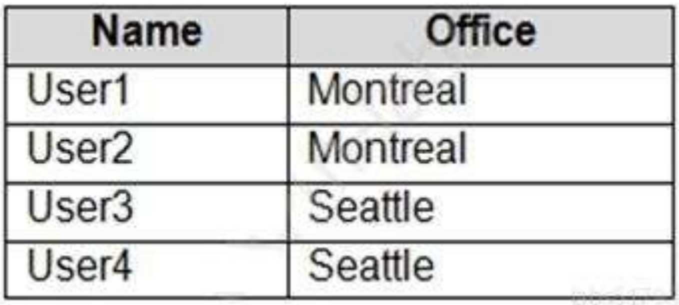
QUESTION 357
Case Study 3 - Litware, Inc
Overview
General Overviews

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

Environment

Existing Environment

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

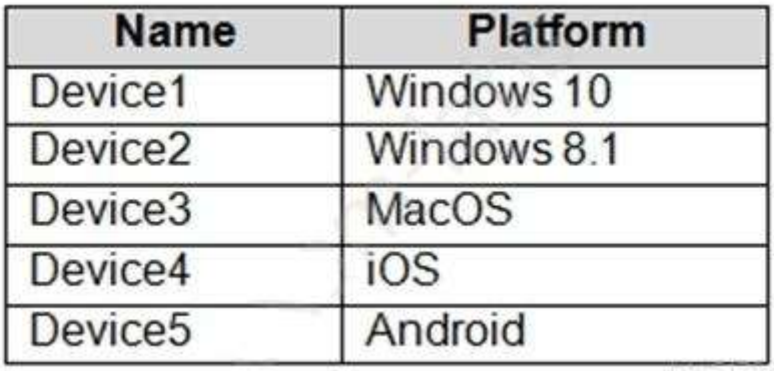


Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

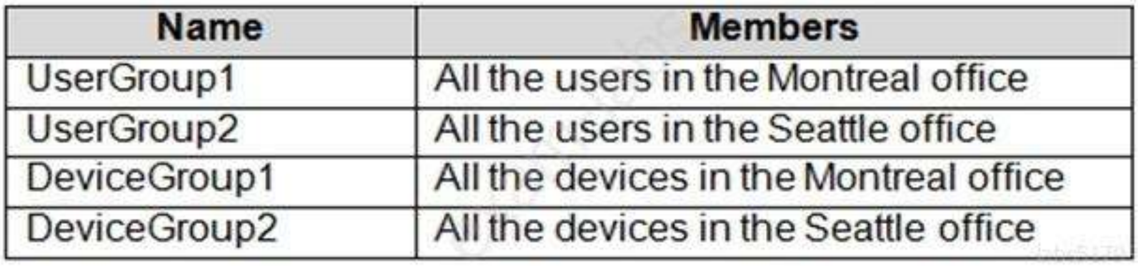
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

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



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

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



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

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

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

Problem Statements

Litware identifies the following issues:

- Users open email attachments that contain malicious content.
- Devices without an assigned compliance policy show a status of Compliant.
- User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
- Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

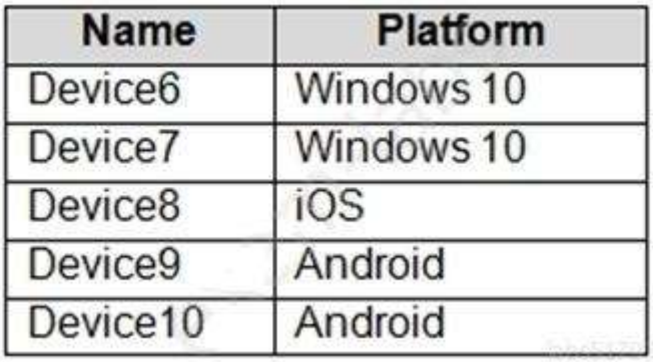
Requirements

Planned Changes

Litware plans to implement the following changes:

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

- Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
- Implement data loss prevention (DLP) policies to protect confidential information.
- Grant User2 permissions to review the audit logs of he litware.com tenant.
- Deploy new devices to the Seattle office as shown in the following table.



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

- Implement a notification system for when DLP policies are triggered.
- Configure a Safe Attachments policy for the litware.com tenant.

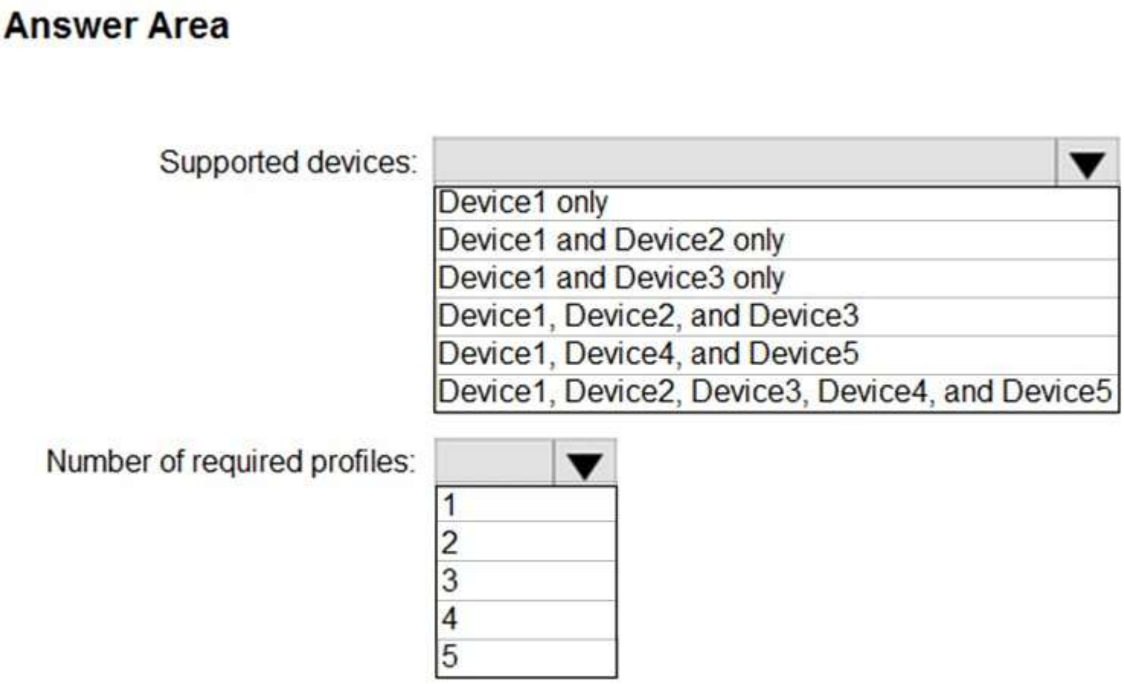
Technical Requirements

Litware identifies the following technical requirements:

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

Hotspot Question

You plan to implement the endpoint protection device configuration profiles to support the planned changes.
You need to identify which devices will be supported, and how many profiles you should implement.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

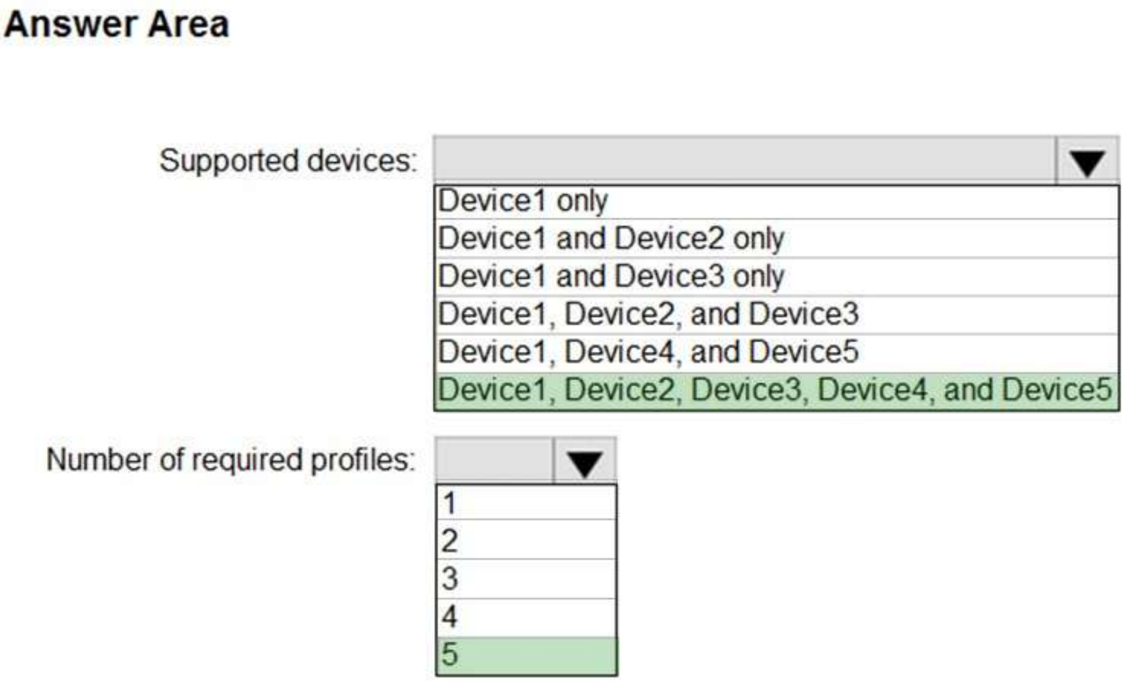
Supported devices:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2, and Device3
- Device1, Device4, and Device5
- Device1, Device2, Device3, Device4, and Device5

Number of required profiles:

- 1
- 2
- 3
- 4
- 5

Answer:



Answer Area

Supported devices:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2, and Device3
- Device1, Device4, and Device5
- [✓ Device1, Device2, Device3, Device4, and Device5]

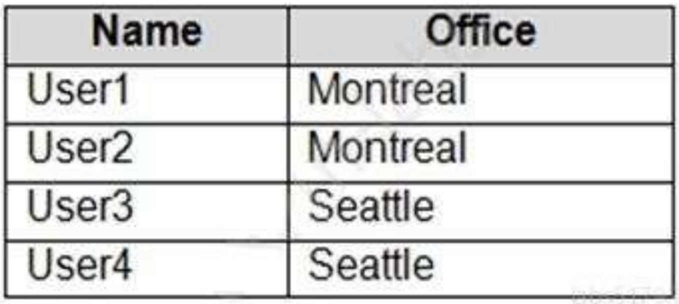
Number of required profiles:

- 1
- 2
- 3
- 4
- [✓ 5]

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

QUESTION 358
Case Study 3 - Litware, Inc
Overview
General Overviews
Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.
Environment
Existing Environment

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

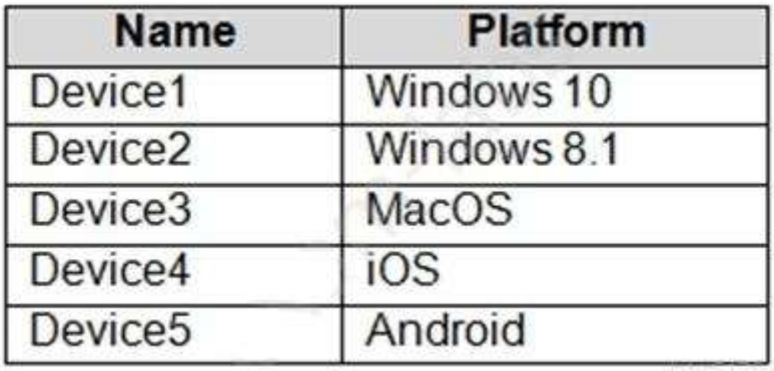


Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

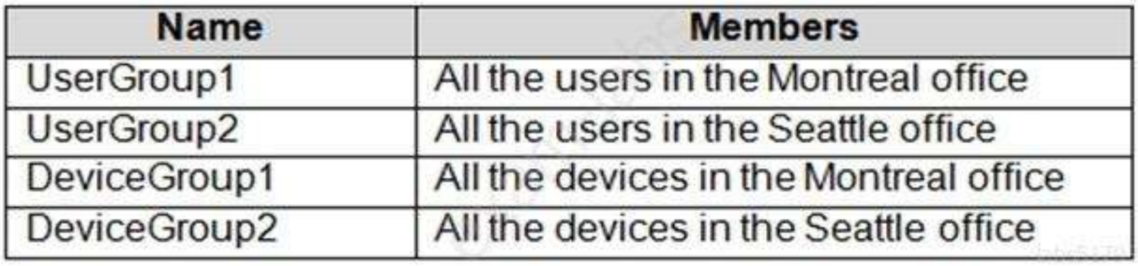
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

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



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

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



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

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

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

Problem Statements

Litware identifies the following issues:

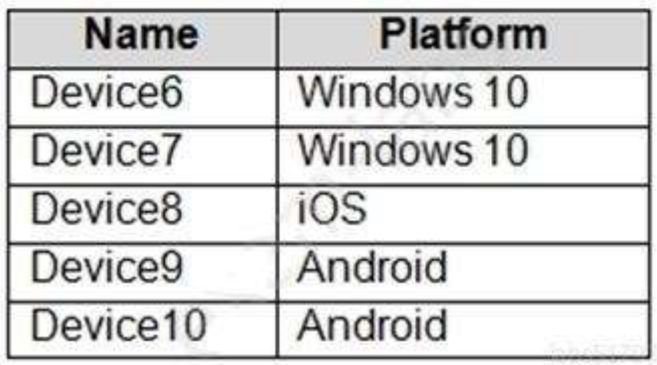
- Users open email attachments that contain malicious content.
- Devices without an assigned compliance policy show a status of Compliant.
- User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
- Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

Requirements

Planned Changes

Litware plans to implement the following changes:

- Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
- Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
- Implement data loss prevention (DLP) policies to protect confidential information.
- Grant User2 permissions to review the audit logs of he litware.com tenant.
- Deploy new devices to the Seattle office as shown in the following table.



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

- Implement a notification system for when DLP policies are triggered.
- Configure a Safe Attachments policy for the litware.com tenant.

Technical Requirements

Litware identifies the following technical requirements:

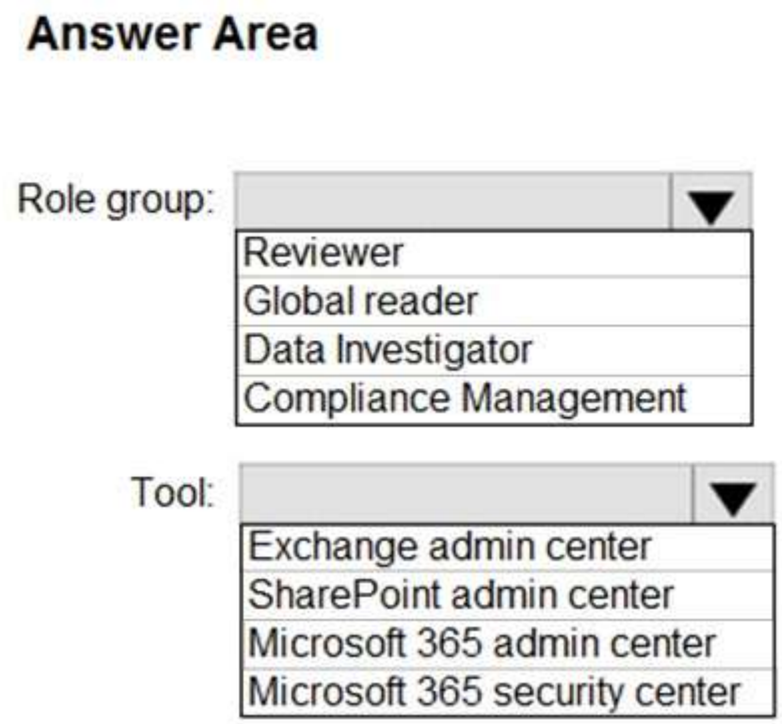
- Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
- Emails messages that contain attachments must be delivered immediately, and placeholder must be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

Hotspot Question

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

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

NOTE: Each correct selection is worth one point.



Answer Area

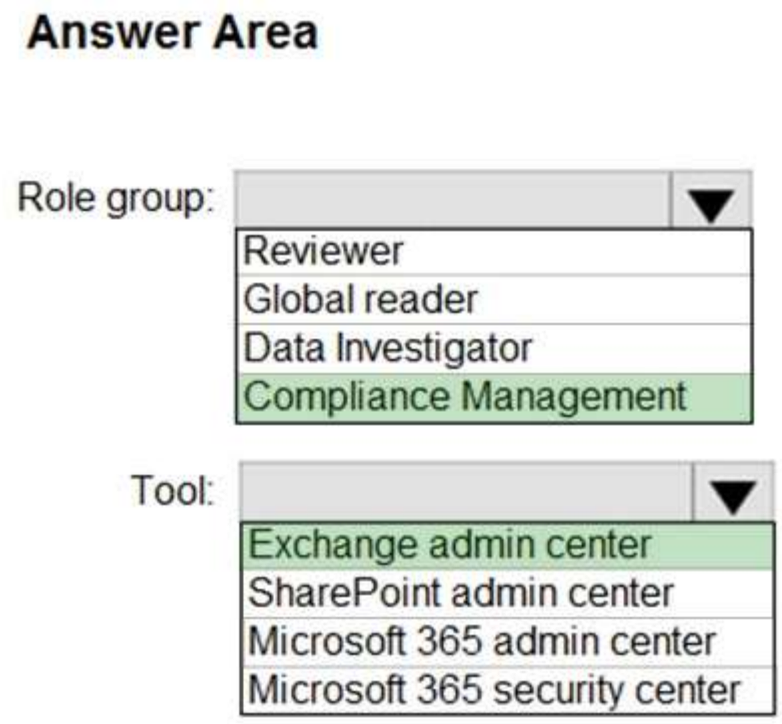
Role group:

- Reviewer
- Global reader
- Data Investigator
- Compliance Management

Tool:

- Exchange admin center
- SharePoint admin center
- Microsoft 365 admin center
- Microsoft 365 security center

Answer:



Answer Area

Role group:

- Reviewer
- Global reader
- Data Investigator
- [✓ Compliance Management]

Tool:

- [✓ Exchange admin center]
- SharePoint admin center
- Microsoft 365 admin center
- Microsoft 365 security center

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

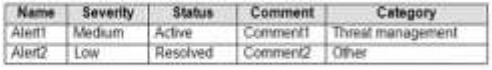
QUESTION 359
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions

will not appear in the review screen.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select System, and then you select About to view information about the system.
Does this meet the goal?

A. Yes
B. No

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

QUESTION 360
You have a Microsoft 365 subscription that contains the alerts shown in the following table.



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

Which properties of the alerts can you modify?

A. Status only
B. Status and Comment only
C. Status and Severity only
D. Status, Severity, and Comment only
E. Status, Severity, Comment and Category

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

QUESTION 361
You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.
Devices are onboarded by using Microsoft Defender for Endpoint.
You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.
What should you create first?

A. a device configuration policy
B. a device compliance policy
C. a conditional access policy
D. an endpoint detection and response policy

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

QUESTION 362
You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.
From Microsoft Defender Security Center, you perform a security investigation.
You need to run a PowerShell script on the device to collect forensic information.
Which action should you select on the device page?

A. Initiate Live Response Session
B. Initiate Automated Investigation

C. Collect investigation package
D. Go hunt

Answer: A
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

QUESTION 363
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft 365 compliance policies to meet the following requirements:
- Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
- Report on shared documents that contain PII.
What should you create?

A. an alert policy
B. a data loss prevention (DLP) policy
C. a retention policy
D. a Microsoft Cloud App Security policy

Answer: B
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide