

 Custom View Settings

Topic 1 - Question Set 1

Question #1

Topic 1

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 are deploying Microsoft Endpoint Manager.

You successfully enroll Windows 10 devices in Endpoint Manager.

When you try to enroll an iOS device in Endpoint Manager, you get an error.

You need to ensure that you can enroll the iOS device in Endpoint Manager.

Solution: You add your user account as a device enrollment manager.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (100%)

Question #2

Topic 1

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 are deploying Microsoft Endpoint Manager.

You successfully enroll Windows 10 devices in Endpoint Manager.

When you try to enroll an iOS device in Endpoint Manager, you get an error.

You need to ensure that you can enroll the iOS device in Endpoint Manager.

Solution: You configure the Apple MDM Push certificate.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

References:

<https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get>

Community vote distribution

A (100%)

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

You are deploying Microsoft Endpoint Manager.

You successfully enroll Windows 10 devices in Endpoint Manager.

When you try to enroll an iOS device in Endpoint Manager, you get an error.

You need to ensure that you can enroll the iOS device in Endpoint Manager.

Solution: You create an Apple Configurator enrollment profile.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You create a device configuration profile from the Device Management admin center.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD). You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch). You configure pilot co-management. You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1. You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You add Device1 to an Active Directory group.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients>

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

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD). You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch). You configure pilot co-management. You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1. You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You unjoin Device1 from the Active Directory domain.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

HOTSPOT -

Your network contains an Active Directory forest named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You use Microsoft Endpoint Configuration Manager for device management.

You have the Windows 10 devices shown in the following table.

Name	Collection
Device1	Collection1
Device2	Collection2

You configure Endpoint Configuration Manager co-management as follows:

⇒ Automatic enrollment in Intune: Pilot

⇒ Pilot collection for all workloads: Collection2

You configure co-management workloads as shown in the following exhibit.

Properties

Tenant onboarding | Enablement | **Workloads** | Staging

For Windows 10 devices that are in a co-management state, you can have Microsoft Intune start managing different workloads. Choose Pilot Intune to have Intune manage the workloads for only clients in the Pilot group (specified later in this wizard). If you are not ready to move workloads to Intune, select Configuration Manager.

[Learn more](#)

	Configuration Manager	Pilot Intune	Intune
Compliance policies:		<input checked="" type="radio"/>	
Device Configuration:	<input checked="" type="radio"/>		
Endpoint Protection:		<input checked="" type="radio"/>	
Resource access policies:	<input checked="" type="radio"/>		
Office Click-to-Run apps:	<input checked="" type="radio"/>		
Windows Update policies:			<input checked="" type="radio"/>

OK Cancel Apply

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
Microsoft Intune manages the compliance policies for Device1.	<input type="radio"/>	<input type="radio"/>
Configuration Manager manages the Windows Update policies for Device1.	<input type="radio"/>	<input type="radio"/>
Microsoft Intune manages Endpoint Protection for Device2.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	<input type="radio"/>	<input checked="" type="radio"/>
Configuration Manager manages the Windows Update policies for Device1.	<input type="radio"/>	<input checked="" type="radio"/>
Microsoft Intune manages Endpoint Protection for Device2.	<input checked="" type="radio"/>	<input type="radio"/>

Correct Answer:

HOTSPOT -

You have three devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Member of
Device1	Windows 10	Group1
Device2	Android	Group2, Group3
Device3	Windows 10	Group2, Group3

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

Name	Platform	Assigned
Policy1	Windows 10 and later	Yes
Policy2	Android	No
Policy3	Windows 10 and later	Yes

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

Name	Include	Exclude
Policy1	Group3	None
Policy2	Group2	Group3

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Policy1 applies to Device3.	<input type="radio"/>	<input type="radio"/>
Policy2 applies to Device2.	<input type="radio"/>	<input type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
Policy1 applies to Device3.	<input checked="" type="radio"/>	<input type="radio"/>
Policy2 applies to Device2.	<input checked="" type="radio"/>	<input type="radio"/>

You have Windows 10 Pro devices that are joined to an Active Directory domain.

You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise.

You are evaluating whether to deploy Windows Hello for Business.

What are two prerequisites of the deployment? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Microsoft Endpoint Manager enrollment
- B. Microsoft Azure Active Directory (Azure AD)
- C. smartcards
- D. TPM-enabled devices

Correct Answer: AB

Reference:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-sso-base>

You have a Microsoft 365 tenant.

All users are assigned the Enterprise Mobility + Security license.

You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the device is enrolled in Microsoft Endpoint Manager automatically.

What should you configure?

- A. Enrollment restrictions from the Endpoint Manager admin center
- B. device enrollment managers from the Endpoint Manager admin center
- C. MAM User scope from the Azure Active Directory admin center
- D. MDM User scope from the Azure Active Directory admin center

Correct Answer: *D*

References:

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

HOTSPOT -

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

The device type restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

You add User3 as a device enrollment manager in Endpoint Manager.

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 enroll Windows devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Android devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll iOS devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll Android devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll iOS devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1:

No. User1 is in Group1. The two device type policies that apply to Group1 are Policy3 and the Default (All Users) policy. However, Policy3 has a higher priority than the default policy so Policy3 is the only effective policy. Policy3 allows the enrolment of Android and iOS devices only, not Windows.

Box 2:

No. User2 is in Group1 and Group2. The device type policies that apply to Group1 and Group2 are Policy2, Policy3 and the Default (All Users) policy. However, Policy2 has a higher priority than Policy 3 and the default policy so Policy2 is the only effective policy. Policy2 allows the enrolment of Windows devices only, not Android.

Box 3:

Yes. User3 is a device enrollment manager. Device restrictions do not apply to a device enrollment manager.

Reference:

<https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set>

HOTSPOT -

You create two device compliance policies for Android devices as shown in the following table.

Policy	Configuration	Action	Assigned to
Policy1	Require encryption of the data storage on the device.	Mark as noncompliant immediately.	Group1
Policy2	Require Google Play services.	Mark as noncompliant immediately.	Group2

You have the Android devices shown in the following table.

Name	User	Configuration
Android1	User1	Not encrypted
Android2	User2	Google Play services not configured
Android3	User3	Not encrypted Google Play services configured

The users belong to the groups shown in the following table.

User	Group
User1	Group1
User2	Group1, Group2
User3	Group2

The users enroll their device in Microsoft Endpoint Manager.

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
The device of User1 is compliant.	<input type="radio"/>	<input type="radio"/>
The device of User2 is compliant.	<input type="radio"/>	<input type="radio"/>
The device of User3 is compliant.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	The device of User1 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
	The device of User2 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
	The device of User3 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

References:

<https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-android>

HOTSPOT -

Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.

You update the Windows 10 devices by using Windows Update for Business.

What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Quality updates:

▼
14 days
30 days
60 days
120 days

Feature updates:

▼
60 days
180 days
365 days
540 days

Answer Area

Correct Answer:

Quality updates:

▼
14 days
30 days
60 days
120 days

Feature updates:

▼
60 days
180 days
365 days
540 days

References:

<https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb>

Your company uses Microsoft Endpoint Configuration Manager and Microsoft Endpoint Manager to co-manage devices. Which two actions can be performed only from Endpoint Manager? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Deploy applications to Windows 10 devices.
- B. Deploy VPN profiles to iOS devices.
- C. Deploy VPN profiles to Windows 10 devices.
- D. Publish applications to Android devices.

Correct Answer: BD

References:

<https://docs.microsoft.com/en-us/sccm/comanage/overview>

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/create-vpn-profiles>

Community vote distribution

BD (100%)

HOTSPOT -

Your network contains an Active Directory domain named contoso.com that uses Microsoft System Center Configuration Manager (Current Branch).

You have Windows 10 and Windows 8.1 devices.

You need to ensure that you can analyze the upgrade readiness of all the Windows 8.1 devices and analyze the update compliance of all the Windows 10 devices.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

First action to perform:

	▼
Enroll the devices in Microsoft Intune.	
Configure device compliance in Microsoft Intune.	
Create a Microsoft Azure Log Analytics workspace.	
Add an alias (CNAME) record to the DNS zone of contoso.com.	

Second action to perform:

	▼
Configure all the devices to have a commercial ID.	
Configure software inventory in Configuration Manager.	
Configure all the devices to join the Windows Insider Program.	
Configure and restart the Windows Update service on all the devices.	

Answer Area

First action to perform:

	▼
Enroll the devices in Microsoft Intune.	
Configure device compliance in Microsoft Intune.	
Create a Microsoft Azure Log Analytics workspace.	
Add an alias (CNAME) record to the DNS zone of contoso.com.	

Correct Answer:

Second action to perform:

	▼
Configure all the devices to have a commercial ID.	
Configure software inventory in Configuration Manager.	
Configure all the devices to join the Windows Insider Program.	
Configure and restart the Windows Update service on all the devices.	

References:

<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-get-started> <https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started>

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

You have a Microsoft 365 subscription.

You need to ensure that administrators can manage the configuration settings for all the Windows 10 devices in your organization.

What should you configure?

- A. the Enrollment restrictions
- B. the mobile device management (MDM) authority
- C. the Exchange on-premises access settings
- D. the Windows enrollment settings

Correct Answer: B

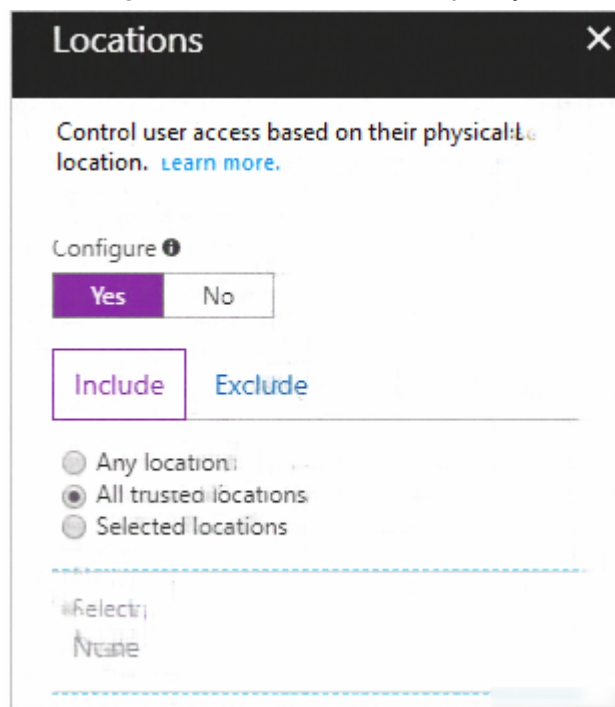
References:

<https://docs.microsoft.com/en-us/intune/mdm-authority-set>

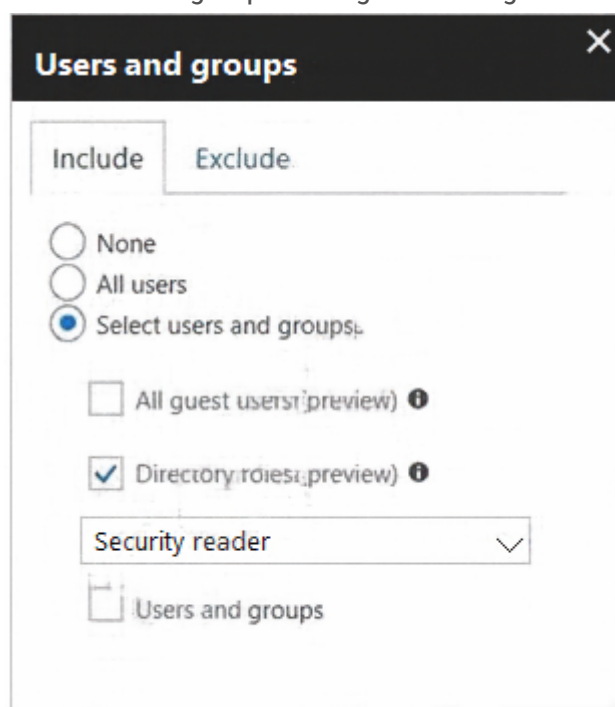
Community vote distribution

B (100%)

You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the Locations tab.)



The users and groups settings are configured as shown in the Users and Groups exhibit. (Click Users and Groups tab.)



Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office.

You need to ensure that the members of the Security reader group can sign in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege.

What should you do?

- A. From the conditional access policy, configure the device state.
- B. From the Azure Active Directory admin center, create a custom control.
- C. From the Endpoint Manager admin center, create a device compliance policy.
- D. From the Azure Active Directory admin center, create a named location.

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

Community vote distribution

D (100%)

You have computers that run Windows 10 Enterprise and are joined to the domain.
You plan to delay the installation of new Windows builds so that the IT department can test application compatibility.
You need to prevent Windows from being updated for the next 30 days.
Which two Group Policy settings should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Select when Quality Updates are received
- B. Select when Preview Builds and Feature Updates are received
- C. Turn off auto-restart for updates during active hours
- D. Manage preview builds
- E. Automatic updates detection frequency

Correct Answer: *BD*

References:
<https://insider.windows.com/en-us/for-business-organization-admin/>

Community vote distribution

AB (80%)	BD (20%)
----------	----------

HOTSPOT -

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

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

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Non configured	15	Yes

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

Name	Assigned to
Policy2	Group2
Policy3	Group3

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as noncompliant after 10 days.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as noncompliant after 15 days.	<input type="radio"/>	<input type="radio"/>

Answer Area**Correct Answer:**

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 is marked as noncompliant after 10 days.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 is marked as noncompliant after 15 days.	<input type="radio"/>	<input checked="" type="radio"/>

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

You need to provide a user with the ability to sign up for Microsoft Store for Business for contoso.com. The solution must use the principle of least privilege.

Which role should you assign to the user?

- A. Cloud application administrator
- B. Application administrator
- C. Global administrator
- D. Service administrator

Correct Answer: C

References:

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

Community vote distribution

C (100%)

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

You are deploying Microsoft Endpoint Manager.

You successfully enroll Windows 10 devices in Endpoint Manager.

When you try to enroll an iOS device in Endpoint Manager, you get an error.

You need to ensure that you can enroll the iOS device in Endpoint Manager.

Solution: You create the Mobility (MDM and MAM) settings.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You add Device1 to a Configuration Manager device collection.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients>

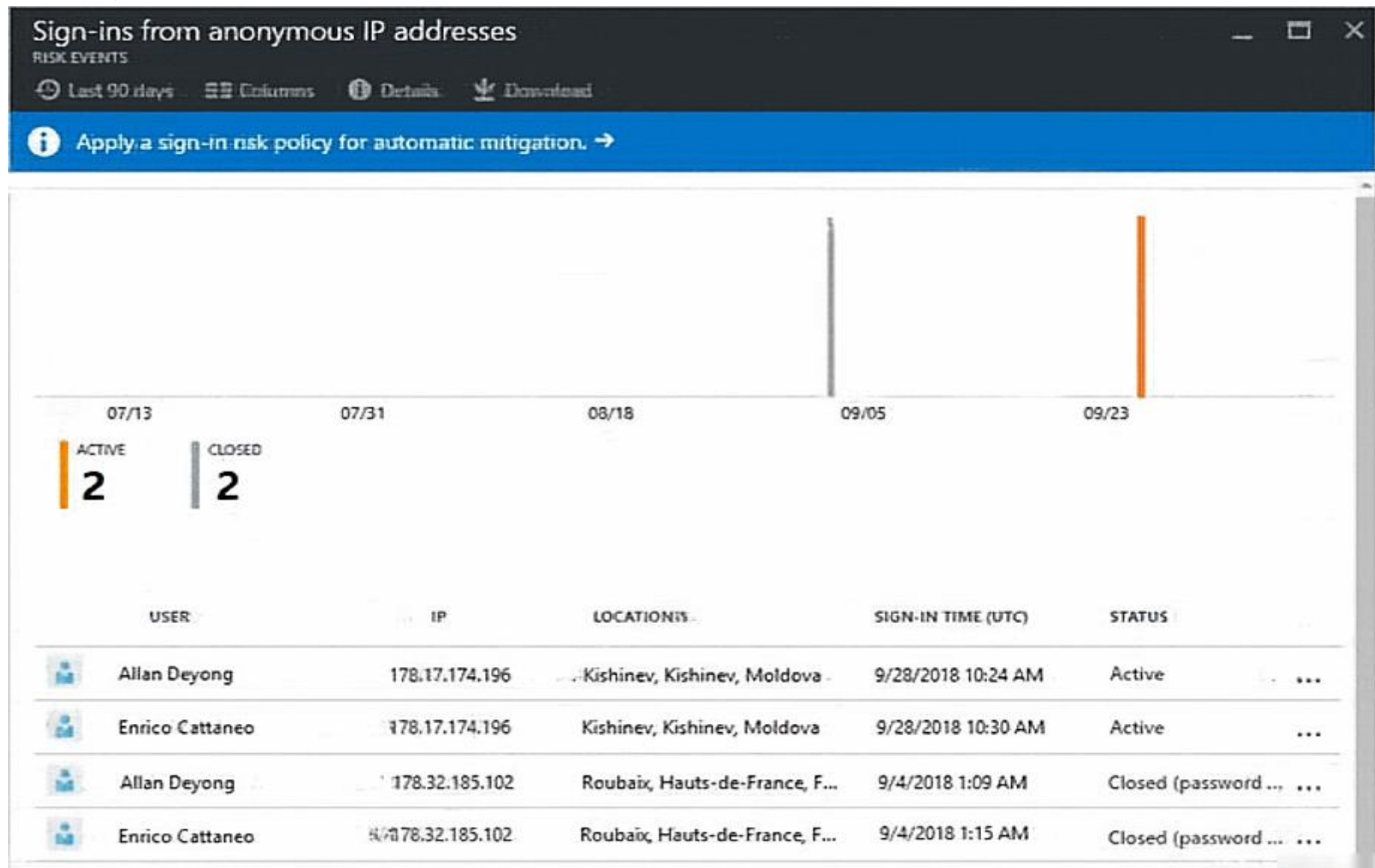
Community vote distribution

B (58%)

A (33%)

8%

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit. (Click the Exhibit tab.)



You need to reduce the likelihood that the sign-ins are identified as risky.

What should you do?

- A. From the Security & Compliance admin center, create a classification label.
- B. From the Security & Compliance admin center, add the users to the Security Readers role group.
- C. From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.
- D. From the Conditional access blade in the Azure Active Directory admin center, create named locations.

Correct Answer: D

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

Community vote distribution

D (100%)

Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents.

Users in other departments must not be restricted.

What should you do?

- A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
- B. Modify the default safe links policy.
- C. Create a data loss prevention (DLP) policy that has a Content contains condition.
- D. Create a new safe links policy.

Correct Answer: D

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients>

Community vote distribution

D (100%)

You have a Microsoft 365 tenant.

You have a line-of-business application named App1 that users access by using the My Apps portal.

After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control.

You need to be alerted by email if impossible travel is detected for a user of App1. The solution must ensure that alerts are generated for App1 only.

What should you do?

- A. From Microsoft Cloud App Security, create a Cloud Discovery anomaly detection policy.
- B. From Microsoft Cloud App Security, modify the impossible travel alert policy.
- C. From Microsoft Cloud App Security, create an app discovery policy.
- D. From the Azure Active Directory admin center, modify the conditional access policy.

Correct Answer: A

References:

<https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-anomaly-detection-policy>

Community vote distribution

A (75%)

B (25%)

A user receives the following message when attempting to sign in to <https://myapps.microsoft.com>:

⌘Your sign-in was blocked. We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity. Please contact your admin.⌘

Which configuration prevents the users from signing in?

- A. Microsoft Azure Active Directory (Azure AD) Identity Protection policies
- B. Microsoft Azure Active Directory (Azure AD) conditional access policies
- C. Endpoint Manager compliance policies
- D. Security & Compliance data loss prevention (DLP) policies

Correct Answer: *B*

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview> <https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

Community vote distribution

A (100%)

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group2

Your company uses Microsoft Intune.

Several devices are enrolled in Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

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

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

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

☞ The Assignments settings are configured as follows:

- 1. Users and groups: Group1
- 2. Cloud apps: Microsoft Office 365 Exchange Online
- 3. Conditions: Include All device state, exclude Device marked as compliant

☞ Access controls is set to Block access.

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
User1 can access Microsoft Exchange Online from Device1.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes.

User1 is in Group1. The Conditional Access Policy applies to Group1. The Conditional Access Policy blocks access unless the device is marked as compliant.

BitLocker is disabled for Device1. Device1 is in Group3 which is assigned device Policy1. The BitLocker policy in Policy1 is not configured so BitLocker is not required.

Therefore, Device1 is compliant so User1 can access Exchange online from Device1.

Box 2: No.

User1 is in Group1. The Conditional Access Policy applies to Group1. The Conditional Access Policy blocks access unless the device is marked as compliant.

BitLocker is disabled for Device2. Device2 is in Group4 which is assigned device Policy2. The BitLocker policy in Policy2 is Required so BitLocker is required.

Therefore, Device2 is not compliant so User1 cannot access Exchange online from Device2.

Box3: Yes.

User2 is in Group2. The Conditional Access Policy applies to Group1. The Conditional Access Policy does not apply to Group2. So even though Device2 is non-compliant, User2 can access Exchange Online using Device2 because there is no Conditional Access Policy preventing him/her from doing so.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions>

Question #28

Topic 1

HOTSPOT -

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	None	None

The device limit restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All Users

You add User3 as a device enrollment manager in Endpoint Manager.

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 enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/intune/device-enrollment-manager-enroll>

HOTSPOT -

Your company has a Microsoft 365 tenant.

You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM).

The device type restrictions are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

The device limit restrictions are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

What is the effective configuration for the members of the Engineering group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Device limit:

5

10

15

Allowed platform:

Android only

iOS only

All platforms

Answer Area

Device limit:

5

10

15

Correct Answer:

Allowed platform:

Android only

iOS only

All platforms

Your network contains an Active Directory domain named contoso.com. The domain contains 100 Windows 8.1 devices. You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices. You need to recommend a Windows 10 deployment method. What should you recommend?

- A. a provisioning package
- B. an in-place upgrade
- C. wipe and load refresh
- D. Windows Autopilot

Correct Answer: B

References:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure>

Community vote distribution

C (100%)

You use Microsoft System Center Configuration Manager (Current Branch) to manage devices. Your company uses the following types of devices:

- ☞ Windows 10
- ☞ Windows 8.1
- ☞ Android
- ☞ iOS

Which devices can be managed by using co-management?

- A. Windows 10 and Windows 8.1 only
- B. Windows 10, Android, and iOS only
- C. Windows 10 only
- D. Windows 10, Windows 8.1, Android, and iOS

Correct Answer: C

You can manage only Windows 10 devices by using co-management.

When you concurrently manage Windows 10 devices with both Configuration Manager and Microsoft Intune, this configuration is called co-management. When you manage devices with Configuration Manager and enroll to a third-party MDM service, this configuration is called coexistence.

Reference:

<https://docs.microsoft.com/en-us/configmgr/comanage/overview>

HOTSPOT -

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

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

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

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

Name	Assigned to
Policy1	Group3
Policy2	Group2

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is compliant.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	Device1 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
	Device2 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
	Device3 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Your company has a Microsoft 365 E3 subscription.

All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).

You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution must minimize downtime for the users.

What should you use?

- A. Windows Autopilot
- B. Windows Update
- C. Subscription Activation
- D. an in-place upgrade

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation>

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

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

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients>

Community vote distribution

A (100%)

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

You are deploying Microsoft Endpoint Manager.

You successfully enroll Windows 10 devices in Endpoint Manager.

When you try to enroll an iOS device in Endpoint Manager, you get an error.

You need to ensure that you can enroll the iOS device in Endpoint Manager.

Solution: You configure the Mobility (MDM and MAM) settings.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Your company has 10 offices.

The network contains an Active Directory domain named contoso.com. The domain contains 500 client computers. Each office is configured as a separate subnet.

You discover that one of the offices has the following:

- ☞ Computers that have several preinstalled applications
- ☞ Computers that use nonstandard computer names
- ☞ Computers that have Windows 10 preinstalled
- ☞ Computers that are in a workgroup

You must configure all computers in the office to meet the following corporate requirements:

All computers in the office must be joined to the domain.

-
- ☞ All computers in the office must have computer names that use a prefix of CONTOSO.
- ☞ All computers in the office must only have approved corporate applications installed.

You need to recommend a solution to redeploy the computers. The solution must minimize the deployment time.

Which deployment method should you recommend?

A. a provisioning package

B. wipe and load refresh

C. Windows Autopilot

D. an in-place upgrade

Correct Answer: A

By using a Provisioning, IT administrators can create a self-contained package that contains all of the configuration, settings, and apps that need to be applied to a device.

Incorrect Answers:

C: With Windows Autopilot the user can set up pre-configure devices without the need consult their IT administrator.

D: Use the In-Place Upgrade option when you want to keep all (or at least most) existing applications.

References:

<https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios> <https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot>

Community vote distribution

A (100%)

Your company has a Microsoft 365 subscription. The subscription contains 500 devices that run Windows 10 and 100 devices that run iOS. You need to create Microsoft Endpoint Manager device configuration profiles to meet the following requirements:

- ⇒ Configure Wi-Fi connectivity to a secured network named ContosoNet.
- ⇒ Require passwords of at least six characters to lock the devices.

What is the minimum number of device configuration profiles that you should create?

- A. 4
- B. 2
- C. 1

Correct Answer: B

Community vote distribution

B (50%)

A (50%)

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription. The company recently hired four new users who have the devices shown in the following table.

Name	Operating system
User1	Windows 8
User2	Windows 10
User3	Android 8.0
User4	iOS 11

You configure the Microsoft 365 subscription to ensure that the new devices enroll in Microsoft Endpoint Manager automatically. Which users have a device that can enroll in Microsoft Endpoint Manager automatically?

- A. User1, User2, User3, and User4
- B. User2 only
- C. User1 and User2 only
- D. User1, User2, and User3 only

Correct Answer: B

Community vote distribution

B (100%)

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

Name	Can enroll devices to Microsoft Endpoint Manager by using auto-discovery
Contoso.com	Yes
Contoso.onmicrosoft.com	Yes

The company plans to add a custom domain named fabrikam.com to the subscription, and then to enable enrollment of devices to Endpoint Manager by using auto-discovery for fabrikam.com.

You need to add a DNS record to the fabrikam.com domain to enable device enrollment by using auto-discovery.

Which record type should you use for the new record?

- A. PTR
- B. SRV
- C. CNAME
- D. TXT

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium>

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

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

Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the ReadyForWindows status of App2 to Highly adopted.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

App1 has a low install count (20 or less) so will be Ready to upgrade. We just need to change the setting for App2.

References:

<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps>

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the Importance status of App1 to Business critical.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Business Critical will prevent the app having a status of Ready to upgrade.

References:

<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps>

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the ReadyForWindows status of App1 to Highly adopted.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

App1 has a low install count (20 or less) so will be Ready to upgrade. We need to change the setting for App2.

References:

<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps>

Community vote distribution

B (100%)

HOTSPOT -

You have 100 computers that run Windows 8.1 and are enrolled in Upgrade Readiness.

Two of the computers are configured as shown in the following table.

Name	Architecture	Memory	Applications installed
Computer1	64-bit	1 GB	App1
Computer2	32-bit	2 GB	App2

From Upgrade Readiness, you view the applications shown in the following table.

Name	UpgradeDecision
App1	Ready to upgrade
App2	Review in progress

You enroll a computer named Computer3 in Upgrade Readiness. Computer3 has the following configurations:

- ⇒ 8 GB of memory
- ⇒ 64-bit architecture
- ⇒ An application named App3 installed

App3 is installed on Computer3 only.

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
Computer1 has an UpgradeDecision status of Ready to upgrade.	<input type="radio"/>	<input type="radio"/>
Computer2 has an UpgradeDecision status of Ready to upgrade.	<input type="radio"/>	<input type="radio"/>
Computer3 has an UpgradeDecision status of Ready to upgrade.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	Computer1 has an UpgradeDecision status of Ready to upgrade.	<input type="radio"/>	<input checked="" type="radio"/>
	Computer2 has an UpgradeDecision status of Ready to upgrade.	<input type="radio"/>	<input checked="" type="radio"/>
	Computer3 has an UpgradeDecision status of Ready to upgrade.	<input checked="" type="radio"/>	<input type="radio"/>

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD).

The domain contains two servers named Server1 and Server2 that run Windows Server 2016. Server1 has the File Server Resource Manager role service installed.

You need to configure Server1 to use the Azure Rights Management (Azure RMS) connector.

You install the Microsoft Management connector on Server1.

What should you do next on Server1?

- A. Run the GenConnectorConfig.ps1 script.
- B. Configure the URL of the AIPMigrated group.
- C. Enable BitLocker Drive Encryption (BitLocker).
- D. Install a certification authority (CA).

Correct Answer: A

If you want to use the server configuration tool for the RMS connector, to automate the configuration of registry settings on your on-premises servers, download and run the GenConnectorConfig.ps1 script.

References:

<https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector#installing-the-rms-connector>

Community vote distribution

A (100%)

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You sign up for Microsoft Store for Business.

The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	None
User2	Basic Purchaser	None
User3	None	Application administrator
User4	None	Cloud application administrator

Microsoft Store for Business has the following Shopping behavior settings:

☞ Make everyone a Basic Purchaser is set to Off.

☞ Allow app requests is set to On.

You need to identify which users can add apps to the Microsoft Store for Business private store.

Which users should you identify?

- A. User1 and User2 only
- B. User3 only
- C. User1 only
- D. User3 and User4 only

Correct Answer: A

Community vote distribution

C (79%)

A (21%)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.
You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.
Solution: You set the importance status of App2 to Low install count.
Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

If an app is installed on less than 2% of the targeted devices, it's marked Low install count. Two percent is the default value. You can adjust the threshold in the readiness settings from 0% to 10%. Desktop Analytics automatically marks these apps as Ready to upgrade.

Reference:
<https://docs.microsoft.com/en-us/configmgr/desktop-analytics/about-deployment-plans>

Community vote distribution

A (100%)

You have two conditional access policies named Policy1 and Policy2.

Policy1 has the following settings:

☞ Assignments:

- Users and groups: User1
- Cloud apps or actions: Office 365 Exchange Online
- Conditions: 0 conditions selected

☞ Access controls:

- Grant: Grant access
- Session: 0 controls selected

☞ Enable policy: On

Policy2 has the following settings:

☞ Assignments:

- Users and groups: User1
- Cloud apps or actions: Office 365 Exchange Online
- Conditions: 0 conditions selected

☞ Access controls:

- Grant: Block access
- Session: 0 controls selected

☞ Enable policy: On

You need to ensure that User1 can access Microsoft Exchange Online only from devices that are marked as compliant.

What should you do?

- A. Modify the Grant settings of Policy2.
- B. Disable Policy2.
- C. Modify the Conditions settings of Policy2.
- D. Modify the Grant settings of Policy1.

Correct Answer: C

Community vote distribution

C (100%)

You have a Microsoft 365 E5 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to ensure that users can enroll devices in Microsoft Endpoint Manager without manually entering the address of Microsoft Endpoint Manager.

Which two DNS records should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a CNAME record for AutoDiscover.contoso.com
- B. a CNAME record for EnterpriseEnrollment.contoso.com
- C. a TXT record for EnterpriseRegistration.contoso.com
- D. an SRV record for _SIP._TLS.contoso.com
- E. an SRV record for _SIPfederationTLS.contoso.com
- F. a CNAME record for EnterpriseRegistration.contoso.com
- G. a TXT record for EnterpriseEnrollment.contoso.com

Correct Answer: *BF*

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium>

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

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

Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You raise the forest functional level to Windows Server 2016. You copy the Group Policy Administrative Templates from a Windows 10 computer to the

Netlogon share on all the domain controllers.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: *B*

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

Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You copy the Group Policy Administrative Templates from a Windows 10 computer to Server1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Community vote distribution

B (57%)

A (43%)

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

Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You upgrade Server1 to Windows Server 2019.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Community vote distribution

B (100%)

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

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

You plan to enable co-management. You need to identify which devices support co-management without requiring the installation of additional software. Which devices should you identify?

- A. Device1 only
- B. Device2 only
- C. Device3 only
- D. Device2 and Device3 only
- E. Device1, Device2, and Device3

Correct Answer: D

Community vote distribution

C (100%)

HOTSPOT -

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

Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.

Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress.	<input checked="" type="radio"/> Yes <input type="radio"/> No
Show time limit error when installation takes longer than specified number of minutes.	<input type="text" value="60"/>
Show custom message when time limit error occurs.	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow users to collect logs about installation errors.	<input type="radio"/> Yes <input checked="" type="radio"/> No
Only show page to devices provisioned by out-of-box experience (OOBE)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Block device use until all apps and profiles are installed	<input type="radio"/> Yes <input checked="" type="radio"/> No

You assign the policy to Group1.

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input checked="" type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status>




HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

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

Configure
Microsoft Intune

 Save  Discard  Delete

MDM user scope ⓘ

None

Some

All

Groups

Select groups
Group1

>

MDM terms of use URL ⓘ

https://portal.manage.microsoft.com/TermsOfUse.aspx

MDM discovery URL ⓘ

https://enrollment.manage.microsoft.com/enrollmentserver/discov ...

MDM compliance URL ⓘ

https://portal.manage.microsoft.com/?portalAction=Compliance

[Restore default MDM URLs](#)

MAM User scope ⓘ

None

Some

All

Groups

Select groups
Group2

>

MAM Terms of use URL ⓘ

MAM Discovery URL ⓘ

https://wip.mam.manage.microsoft.com/Enroll

MAM Compliance URL ⓘ

[Restore default MAM URLs](#)

You purchase a Windows 10 device named Device1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>

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

HOTSPOT -

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

In Azure:

	▼
Add and configure the Diagnostics settings for the Azure Activity Log.	
Add and configure an Azure Log Analytics workspace.	
Add an Azure Storage account and Azure Cognitive Search	
Add an Azure Storage account and a file share.	

On the computers:

	▼
Create an event subscription.	
Modify the membership of the Event Log Readers group.	
Enroll in Microsoft Endpoint Manager.	
Install the Microsoft Monitoring Agent.	

Correct Answer:

Answer Area

In Azure:

	▼
Add and configure the Diagnostics settings for the Azure Activity Log.	
Add and configure an Azure Log Analytics workspace.	
Add an Azure Storage account and Azure Cognitive Search	
Add an Azure Storage account and a file share.	

On the computers:

	▼
Create an event subscription.	
Modify the membership of the Event Log Readers group.	
Enroll in Microsoft Endpoint Manager.	
Install the Microsoft Monitoring Agent.	

Reference:

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

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>

DRAG DROP -

You have a Microsoft 365 E5 subscription.

Several users have iOS devices.

You plan to enroll the iOS devices in Microsoft Endpoint Manager.

You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.

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

Select and Place:

Actions

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Create a certificate from the Apple Push Certificates Portal.

From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

Answer Area

Correct Answer:

Actions

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.

From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

Answer Area

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Create a certificate from the Apple Push Certificates Portal.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.



Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get>

HOTSPOT -

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

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

You have the apps shown in the following table.

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
App1 can be assigned as a required install for User3.	<input type="radio"/>	<input type="radio"/>
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
App3 can be installed automatically for UserGroup1.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
App1 can be assigned as a required install for User3.	<input type="radio"/>	<input checked="" type="radio"/>
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
App3 can be installed automatically for UserGroup1.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

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

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

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

Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You raise the domain functional level to Windows Server 2019. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

You have a Microsoft 365 E5 subscription.

You plan to deploy 100 new Windows 10 devices.

You need to identify the appropriate version of Windows 10 for the new devices. The version must meet the following requirements:

- ☞ Be serviced for a minimum of 24 months.

Support Microsoft Application Virtualization (App-V).

Which version should you identify?

- A. Windows 10 Pro, version 1909
- B. Windows 10 Pro, version 2004
- C. Windows 10 Enterprise, version 1909
- D. Windows 10 Enterprise, version 2004

Correct Answer: D

Reference:

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

Community vote distribution

C (100%)

HOTSPOT -

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

Name	Members
Group1	User1
Group2	User2, Group1

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

⇒ MDM user scope: Some

- Groups: Group1

⇒ MAM user scope: Some

- Groups: Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	<input checked="" type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

HOTSPOT -

You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:

Deploy a VPN connection by using a VPN device configuration profile.

-
- ⇒ Configure security settings by using an Endpoint Protection device configuration profile.

You need to identify which devices will support the management tasks.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

VPN device configuration profile:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2 and Device3	

Endpoint Protection device configuration profile:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2 and Device3	

Correct Answer:

Answer Area

VPN device configuration profile:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2 and Device3	

Endpoint Protection device configuration profile:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2 and Device3	

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure> <https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos>

DRAG DROP -

You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune.

You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices.

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:

Actions

Create an app configuration policy

Link the account to Intune

Create a Microsoft account

Configure a mobile device management (MDM) push certificate

Add the app

Create a Google account

Assign the app

Answer Area**Correct Answer:****Actions**

Create an app configuration policy

Link the account to Intune

Create a Microsoft account

Configure a mobile device management (MDM) push certificate

Add the app

Create a Google account

Assign the app

Answer Area

Create a Google account

Link the account to Intune

Add the app

Assign the app

**Reference:**

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work#assign-a-managed-google-play-app-to-android-enterprise-fully-managed-devices>

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

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager.
To which devices can you deploy Microsoft 365 Apps for enterprise?

- A. Device1 only
- B. Device1 and Device3 only
- C. Device2 and Device4 only
- D. Device1, Device2, and Device3 only
- E. Device1, Device2, Device3, and Device4

Correct Answer: B

Reference:

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

Community vote distribution

B (60%)

E (40%)

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

Name	Platform	Azure Active Directory (Azure AD)
Device1	Windows 10	Joined
Device2	Windows 10	Registered
Device3	Windows 10	Not joined or registered
Device4	Android	Registered

You plan to review device startup performance issues by using Endpoint analytics.
Which devices can you monitor by using Endpoint analytics?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1, Device2, and Device3 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/mem/analytics/overview>

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

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

What should you configure in the profile?

- A. Microsoft Defender Credential Guard
- B. BitLocker Drive Encryption (BitLocker)
- C. Microsoft Defender
- D. Microsoft Defender Exploit Guard

Correct Answer: A

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 Device Manager, you view the computer properties.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Reference:

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

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

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

You have a computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: At a command prompt, you run the winver.exe command.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Reference:

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

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

You have a computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select Update & Security to view the update history.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference:

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

Community vote distribution

B (100%)

You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management.

You need to add the phone number of the help desk to the Company Portal app.

What should you do?

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

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

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

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

Correct Answer: C

Reference:

<https://systemcenterdudes.com/intune-company-portal-customization/>

Community vote distribution

C (100%)

You have a Microsoft 365 E5 tenant.

You plan to deploy 1,000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.

You need to recommend a Microsoft Intune enrollment option that meets the following requirements:

- ☞ Minimizes user interaction
- ☞ Minimizes administrative effort
- ☞ Automatically installs corporate apps

What should you recommend?

- A. Apple Configurator enrollment
- B. Automated Device Enrollment (ADE)
- C. bring your own device (BYOD) user and device enrollment.

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll>


HOTSPOT -

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

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

All users have Windows 10 Enterprise devices.

The Products & services settings in Microsoft Store for Business are shown in the following exhibit.

**Microsoft Remote Desktop**
Free • Online • [Product Details](#)[Install](#)

Licenses


Unlimited licenses
0 used

Billing

\$0.00 (Free app)

Settings & Actions

Not in private store
[More actions available on details page](#)

**Excel Mobile**
Free • Online • [Product Details](#)[Install](#)

Licenses

Unlimited licenses
0 used

Billing

\$0.00 (Free app)

Settings & Actions

In private store
[More actions available on details page](#)

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
User2 can install the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	<input type="radio"/>	<input type="radio"/>
User4 can manage the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	<input checked="" type="radio"/>	<input type="radio"/>
User4 can manage the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

Your company has offices in five cities.

The company has a Microsoft 365 tenant.

Each office is managed by a local administrator.

You plan to deploy Microsoft Intune.

You need to recommend a solution to manage resources in Intune that meets the following requirements:

- ☞ Local administrators must be able to manage only the resources in their respective office.
- ☞ Local administrators must be prevented from managing resources in other offices.
- ☞ Administrative effort must be minimized.

What should you include in the recommendation?

- A. scope tags
- B. device categories
- C. configuration profiles
- D. conditional access policies

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags>

HOTSPOT -

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

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	None

Users are assigned Microsoft Store for Business roles as shown in the following table.

User	Role
User1	None
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Add apps to the private store:

▼

User3 only

User2 and User3 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Install apps from the private store:

▼

User3 only

User2 and User3 only

User1 and User3 only

User2, User3 and User4 only

User1, User2, User3, and User4

Answer Area

Add apps to the private store:

▼

User3 only

User2 and User3 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Correct Answer:

Install apps from the private store:

▼

User3 only

User2 and User3 only

User1 and User3 only

User2, User3 and User4 only

User1, User2, User3, and User4

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business> <https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store>

Question #75

Topic 1

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

Correct Answer: A

Reference:

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

Question #76

Topic 1

You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune.

You plan to purchase volume-purchased apps and deploy the apps to the devices.

You need to track used licenses and manage the apps by using Intune.

What should you use to purchase the apps?

A. Microsoft Store for Business

B. Apple Configurator

C. Apple Business Manager

D. Apple iTunes Store

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios>

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

Name	Windows 10 edition	Azure Active Directory (Azure AD)	Mobile device management (MDM) enrollment
Device1	Windows 10 Pro	Registered	Microsoft Intune
Device2	Windows 10 Enterprise	Joined	Microsoft Intune
Device3	Windows 10 Pro	Joined	Not enrolled
Device4	Windows 10 Enterprise	Registered	Microsoft Intune
Device5	Windows 10 Enterprise	Joined	Not enrolled

You add custom apps to the private store in Microsoft Store Business.

You plan to create a policy to show only the private store in Microsoft Store for Business.

To which devices can the policy be applied?

- A. Device2 only
- B. Device1 and Device3 only
- C. Device2 and Device4 only
- D. Device2, Device3, and Device5 only
- E. Device1, Device2, Device3, Device4, and Device5

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/manage-access-to-private-store#show-private-store-only-using-mdm-policy>

HOTSPOT -

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

You have devices enrolled in Intune as shown in the following table.

Name	Platform	Member of	Scope (Tags)
Device1	Windows 10	Group1 Group3	Tag1
Device2	Android	Group2	Tag2

You create the device configuration profiles shown in the following table.

Name	Platform	Assignments: Included groups	Assignments: Excluded groups	Scope tags
Profile1	Windows 10 and later	Group1	Group3	Tag1, Tag2
Profile2	Android Enterprise	All devices	Group2	Tag1, Tag2
Profile3	Android Enterprise	Group2, Group3	Group3	Tag1
Profile4	Windows 10 and later	Group3	None	Default

Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Device1:

No profiles

Profile1 only

Profile4 only

Profile1 and Profile4 only

Profile1, Profile1, and Profile4 only

Device2:

No profiles

Profile1 only

Profile2 only

Profile3 only

Profile1 and Profile2 only

Profile2 and Profile3 only

Answer Area

Correct Answer:

Device1:

No profiles

Profile1 only

Profile4 only

Profile1 and Profile4 only

Profile1, Profile1, and Profile4 only

Device2:

No profiles

Profile1 only

Profile2 only

Profile3 only

Profile1 and Profile2 only

Profile2 and Profile3 only

Question #79

Topic 1

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

You need to ensure that users can select a department when they enroll their device in Intune.

What should you create?

- A. scope tags
- B. device configuration profiles
- C. device categories
- D. device compliance policies

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>

HOTSPOT -

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

Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	None	Purchaser	Group2
User3	None	Basic Purchaser	Group3

You perform the following actions:

- ⇒ Provision the private store in Microsoft Store for Business.
- ⇒ Add an app named App1 to the private store.
- ⇒ Set Private store availability for App1 to Specific groups, and then select Group3.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>
User2 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>
User3 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
User1 can install App1 from the private store.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can install App1 from the private store.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can install App1 from the private store.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store-for-business#private-store-availability>

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1.

You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:

- ⇒ Assign licenses to users.
- ⇒ Procure apps from Microsoft Store.
- ⇒ Manage private store availability for all items.

The solution must use the principle of least privilege.

Which Microsoft Store for Business role should you assign to User1?

- A. Admin
- B. Device Guard signer
- C. Basic Purchaser
- D. Purchaser

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview>

Community vote distribution

A (100%)

Your company has multiple offices.

You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.

You need to ensure that the local administrators can manage only the devices in their respective office.

What should you use?

- A. scope tags
- B. configuration profiles
- C. device categories
- D. conditional access policies

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags>

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:

- ☞ Show app and profile configuration progress: Yes
- ☞ Allow users to collect logs about installation errors: Yes
- ☞ Only show page to devices provisioned by out-of-box experience (OOBE): No
- ☞ Assignments: 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
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>

Correct Answer:**Answer Area**

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status>

DRAG DROP -

You have a Microsoft 365 E5 tenant.

You need to implement compliance solutions that meet the following requirements:

- ☞ Use a file plan to manage retention labels.
- ☞ Identify, monitor, and automatically protect sensitive information.

Capture employee communications for examination by designated reviewers.

▪

Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Solutions

Data loss prevention

Information governance

Insider risk management

Records management

Answer Area

Identify, monitor, and automatically protect sensitive information:

Solution

Capture employee communications for examination by designated reviewers:

Solution

Use a file plan to manage retention labels:

Solution

Correct Answer:**Solutions**

Data loss prevention

Information governance

Insider risk management

Records management

Answer Area

Identify, monitor, and automatically protect sensitive information:

Data loss prevention

Capture employee communications for examination by designated reviewers:

Insider risk management

Use a file plan to manage retention labels:

Information governance

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide> <https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance?view=o365-worldwide> <https://docs.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide>

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the Security & Compliance admin center, you create a threat management policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: *B*

From the Security & Compliance admin center, Alerts, you create a new alert policy.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies>

Community vote distribution

B (50%)

A (50%)

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Security & Compliance admin center, create a safe attachments policy.
- C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- D. From the Security & Compliance admin center, create an alert policy.

Correct Answer: *D*

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies>

You have a Microsoft Azure Active Directory (Azure AD) tenant.
The organization needs to sign up for Microsoft Store for Business. The solution must use the principle of least privilege.
Which role should you assign to the user?

- A. Global administrator
- B. Cloud application administrator
- C. Application administrator
- D. Service administrator

Correct Answer: *A*

References:

<https://docs.microsoft.com/en-us/microsoft-store/sign-up-microsoft-store-for-business>

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

You have a Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint site, you create an alert.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: *B*

Community vote distribution

B (100%)

You have a Microsoft 365 subscription and an on-premises Active Directory domain named contoso.com. All client computers run Windows 10 Enterprise and are joined to the domain.

You need to enable Windows Defender Credential Guard on all the computers.

What should you do?

- A. From the Microsoft 365 Defender, configure the DKIM signatures for the domain.
- B. From a domain controller, create a Group Policy object (GPO) that enables the Restrict delegation of credentials to remote servers setting.
- C. From the Security & Compliance admin center, create a device security policy.
- D. From a domain controller, create a Group Policy object (GPO) that enabled the Turn On Virtualization Based Security setting.

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage>

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

The company purchases a cloud app named App1 that supports Microsoft Cloud App Security monitoring.

You configure App1 to be available from the My Apps portal.

You need to ensure that you can monitor App1 from Cloud App Security.

What should you do?

- A. From the Azure Active Directory admin center, create a conditional access policy.
- B. From the Azure Active Directory admin center, create an app registration.
- C. From the Endpoint Management admin center, create an app protection policy.
- D. From the Endpoint Management admin center, create an app configuration policy.

Correct Answer: A

HOTSPOT -

You use Microsoft Defender for Endpoint.

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

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

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

Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

To which machine group will each computer be added? To answer, select the appropriate options in the answer are.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Computer1-London:

	▼
Group1	
Group2	
Group3	
Ungrouped machines	

Server1-London:

	▼
Group1	
Group2	
Group3	
Ungrouped machines	

Answer Area

Correct Answer:

Computer1-London:

	▼
Group1	
Group2	
Group3	
Ungrouped machines	

Server1-London:

	▼
Group1	
Group2	
Group3	
Ungrouped machines	

Question #8

Topic 2

Your company has 5,000 Windows 10 devices. All the devices are protected by using Microsoft Defender Advanced Threat Protection (ATP). You need to create a filtered view that displays which Microsoft Defender ATP alert events have a high severity and occurred during the last seven days.

What should you use in Microsoft Defender ATP?

- A. the threat intelligence API
- B. Automated investigations
- C. Threat analytics
- D. Advanced hunting

Correct Answer: B

References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/investigate-alerts-windows-defender-advanced-threat-protection> <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automated-investigations-windows-defender-advanced-threat-protection>

Community vote distribution

D (100%)

Question #9

Topic 2

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

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

You have a Microsoft 365 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Device Management admin center, you create a device configuration profile.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (100%)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Security & Compliance admin center, you assign the Security Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Security Administrator has the required permissions, but it is not assigned from the Security and Compliance Center.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/manage-admins>

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 an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Security administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

The Security administrator has Full access with full permissions in Cloud App Security.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/manage-admins>

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 an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

The Compliance administrator has read-only permissions and can manage alerts, can create and modify file policies, allow file governance actions, and view all the built-in reports under Data Management, but cannot access Security recommendations for cloud platforms.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/manage-admins>

HOTSPOT -

Your company purchases a cloud app named App1.

You plan to publish App1 by using a conditional access policy named Policy1.

You need to ensure that you can control access to App1 by using a Microsoft Cloud App Security session policy.

Which two settings should you modify in Policy1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Policy1

Conditional access policy

 Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Policy1

Assignments

Users and groups ⓘ

All users



Cloud apps or actions ⓘ

No cloud apps or actions selected



Conditions ⓘ

0 conditions selected



Access control

Answer Area

Policy1

Conditional access policy

 Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Policy1

Correct Answer:

Assignments

Users and groups ⓘ All users	>
Cloud apps or actions ⓘ No cloud apps or actions selected	>
Conditions ⓘ 0 conditions selected	>

Access control

Reference:
<https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-aad>

HOTSPOT -

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP includes the machine groups shown in the following table.

Rank	Machine group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped machines (default)	<i>Not applicable</i>

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

Machines > computer1



computer1

Domain

adatum.com

OS

Windows 10 x64

Version 1903

Build 18362

Risk level ⓘ

■ ■ ■ ■ No known risks

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Computer1 will be a member of [answer choice].

▼
Group3 only
Group4 only
Group3 and Group4 only
Ungrouped machines

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

▼
Group1 only
Group1 and Group2 only
Group1, Group2, Group3, and Group4
Ungrouped machines

Answer Area

Computer1 will be a member of [answer choice].

▼
Group3 only
Group4 only
Group3 and Group4 only
Ungrouped machines

Correct Answer:

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

▼
Group1 only
Group1 and Group2 only
Group1, Group2, Group3, and Group4
Ungrouped machines

HOTSPOT -

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

You need to minimize the likelihood that users will be affected by the following threats:

- ☞ Opening files in Microsoft SharePoint that contain malicious content
- ☞ Impersonation and spoofing attacks in email messages

Which policies should you create in the Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Opening files in SharePoint that contain malicious content:

▼
Anti-spam
anti-phishing
safe attachments
Safe Links

Impersonation and spoofing attacks in email messages:

▼
Anti-spam
anti-phishing
safe attachments
Safe Links

Correct Answer:

Answer Area

Opening files in SharePoint that contain malicious content:

▼
Anti-spam
anti-phishing
safe attachments
Safe Links

Impersonation and spoofing attacks in email messages:

▼
Anti-spam
anti-phishing
safe attachments
Safe Links

Box 1: ATP Safe Attachments -

ATP Safe Attachments provides zero-day protection to safeguard your messaging system, by checking email attachments for malicious content. It routes all messages and attachments that do not have a virus/malware signature to a special environment, and then uses machine learning and analysis techniques to detect malicious intent. If no suspicious activity is found, the message is forwarded to the mailbox.

Box 2: ATP anti-phishing -

ATP anti-phishing protection detects attempts to impersonate your users and custom domains. It applies machine learning models and advanced impersonation- detection algorithms to avert phishing attacks.

ATP Safe Links provides time-of-click verification of URLs, for example, in emails messages and Office files. Protection is ongoing and applies across your messaging and Office environment. Links are scanned for each click: safe links remain accessible and malicious links are dynamically blocked.

References:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp#configure-atp-policies>

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do first?

- A. From Microsoft Cloud App Security, create an access policy.
- B. From the Security & Compliance admin center, create an eDiscovery case.
- C. From Microsoft Cloud App Security, create an activity policy.
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

Correct Answer: D

A DLP policy contains a few basic things:

Where to protect the content: locations such as Exchange Online, SharePoint Online, and OneDrive for Business sites, as well as Microsoft Teams chat and channel messages.

When and how to protect the content by enforcing rules comprised of:

Conditions the content must match before the rule is enforced. For example, a rule might be configured to look only for content containing Social Security numbers that's been shared with people outside your organization.

Actions that you want the rule to take automatically when content matching the conditions is found. For example, a rule might be configured to block access to a document and send both the user and compliance officer an email notification.

References:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies>

Community vote distribution

B (100%)

You have a Microsoft 365 subscription.

From the subscription, you perform an audit log search, and you download all the results.

You plan to review the audit log data by using Microsoft Excel.

You need to ensure that each audited property appears in a separate Excel column.

What should you do first?

- A. From Power Query Editor, transform the JSON data.
- B. Format the Operations column by using conditional formatting.
- C. Format the AuditData column by using conditional formatting.
- D. From Power Query Editor, transform the XML data.

Correct Answer: A

After you search the Office 365 audit log and download the search results to a CSV file, the file contains a column named AuditData, which contains additional information about each event. The data in this column is formatted as a JSON object, which contains multiple properties that are configured as property:value pairs separated by commas. You can use the JSON transform feature in the Power Query Editor in Excel to split each property in the JSON object in the AuditData column into multiple columns so that each property has its own column. This lets you sort and filter on one or more of these properties

References:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records>

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

- A. From the Exchange admin center, create a spam filter policy.
- B. From the Security & Compliance admin center, create a data governance event.
- C. From the Security & Compliance admin center, create an alert policy.
- D. From the Exchange admin center, create a mail flow rule.

Correct Answer: C

You can create alert policies to track malware activity and data loss incidents. We've also included several default alert policies that help you monitor activities such as assigning admin privileges in Exchange Online, malware attacks, phishing campaigns, and unusual levels of file deletions and external sharing.

The Email messages containing malware removed after delivery default alert generates an alert when any messages containing malware are delivered to mailboxes in your organization.

Incorrect answers:

A: A spam filter policy includes selecting the action to take on messages that are identified as spam. Spam filter policy settings are applied to inbound messages.

B: A data governance event commences when an administrator creates it, following which background processes look for content relating to the event and take the retention action defined in the label. The retention action can be to keep or remove items, or to mark them for manual disposition.

D: You can inspect email attachments in your Exchange Online organization by setting up mail flow rules. Exchange Online offers mail flow rules that provide the ability to examine email attachments as a part of your messaging security and compliance needs. However, mail flow rules are not used to detect malware in emails.

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies>

DRAG DROP -

You have the Microsoft Azure Advanced Threat Protection (ATP) workspace shown in the Workspace exhibit. (Click the Workspace tab.)

Workspace ?[Manage Azure ATP user roles](#) ?

NAME	TYPE	INTEGRATION	GEOLOCATION
testworkspace	Primary	Windows Defender ATP	Europe

The sensors settings for the workspace are configured as shown in the Sensors exhibit. (Click the Sensors tab.)

Sensors ?

Configure [Directory Services](#) to install the first Sensor or Standalone Sensor.

NAME	TYPE	DOMAIN CO...	VERSION	SERVICE STATUS	HEALTH
No Sensors registered					

You need to ensure that Azure ATP stores data in Asia.

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

- Modify the integration setting for the workspace.
- Delete the workspace.
- Regenerate the access keys.
- Create a new workspace.
- Modify the Azure ATP user roles.

Answer Area**Correct Answer:****Actions**

- Modify the integration setting for the workspace.
- Delete the workspace.
- Regenerate the access keys.
- Create a new workspace.
- Modify the Azure ATP user roles.

Answer Area

- Delete the workspace.
- Create a new workspace.
- Regenerate the access keys.

Your company has five security information and event management (SIEM) appliances. The traffic logs from each appliance are saved to a file share named Logs.

You need to analyze the traffic logs.

What should you do from Microsoft Cloud App Security?

- A. Click Investigate, and then click Activity log.
- B. Click Control, and then click Policies. Create a file policy.
- C. Click Discover, and then click Create snapshot report.
- D. Click Investigate, and then click Files.

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports>

Community vote distribution

C (100%)

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

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

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Cloud App Security admin center, you assign the App/instance admin role for all Microsoft Online Services to User1.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

App/instance admin: Has full or read-only permissions to all of the data in Microsoft Cloud App Security that deals exclusively with the specific app or instance of an app selected.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/manage-admins>

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant is configured to use Azure AD Identity Protection. You plan to use an application named App1 that creates reports of Azure AD Identity Protection usage. You register App1 in the tenant. You need to ensure that App1 can read the risk event information of contoso.com. To which API should you delegate permissions?

- A. Windows Azure Service Management API
- B. Windows Azure Active Directory
- C. Microsoft Graph
- D. Office 365 Management

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/graph/api/resources/identityprotection-root?view=graph-rest-beta>

Community vote distribution

C (100%)

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains computers that run Windows 10 Enterprise and are managed by using Microsoft Endpoint Manager. The computers are configured as shown in the following table.

Name	CPU	Cores	RAM	TPM
Computer1	64-bit	2	12 GB	Enabled
Computer2	64-bit	4	12 GB	Enabled
Computer3	64-bit	8	16 GB	Disabled
Computer4	32-bit	4	4 GB	Disabled

You plan to implement Windows Defender Application Guard for contoso.com. You need to identify on which two Windows 10 computers Windows Defender Application Guard can be installed. Which two computers should you identify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Computer1
- B. Computer3
- C. Computer2
- D. Computer4

Correct Answer: BC

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard>

Community vote distribution

BC (100%)

HOTSPOT -

Your company uses Microsoft Defender for Endpoint.

The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Machine group
Device1	ATP1
Device2	ATP1
Device3	ATP2

The alerts visible in the Microsoft Defender for Endpoint alerts queue are shown in the following table.

Name	Machine
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

⇒ Triggering IOC: Any IOC

⇒ Action: Hide alert

⇒ Suppression scope: Alerts on ATP1 machine group

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
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input checked="" type="radio"/>

A suppression rule will not affect alerts that are already in the alerts queue. Only new alerts will be suppressed.

HOTSPOT -

Your company has a Microsoft 365 subscription.

You need to configure Microsoft 365 to meet the following requirements:







- ☞ Malware found in email attachments must be quarantined for 20 days.
- ☞ The email address of senders to your company must be verified.

Which two options should you configure in the Security & Compliance admin center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.







Hot Area:

Answer Area

ATP anti-phishing  Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.	ATP safe attachments  Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.	ATP Safe Links  Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.
Anti-spam  Protect your organization's email from spam, including what actions to take if spam is detected.	DKIM  Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.	Anti-malware  Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

Correct Answer:

Answer Area

ATP anti-phishing  Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.	ATP safe attachments  Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.	ATP Safe Links  Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.
Anti-spam  Protect your organization's email from spam, including what actions to take if spam is detected.	DKIM  Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.	Anti-malware  Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

You have a Microsoft 365 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP). All the devices in your organization are onboarded to Microsoft Defender ATP. You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours. What should you do?

- A. From Alerts queue, create a suppression rule and assign an alert
- B. From the Security & Compliance admin center, create an audit log search
- C. From Advanced hunting, create a query and a detection rule
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules>

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

Name	Role
User1	Security administrator
User2	Security operator
User3	Security reader
User4	Compliance administrator

You plan to implement Microsoft Defender for Endpoint.

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

You need to identify which user can view security incidents from the Microsoft Defender Security Center.

Which user should you identify?

- A. User1
- B. User2
- C. User3
- D. User4

Correct Answer: A

Community vote distribution

A (80%)

C (20%)

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.

You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for 10 test devices. During the onboarding process, you configure Microsoft

Defender for Endpoint-related data to be stored in the United States.

You plan to onboard all the devices to Microsoft Defender for Endpoint.

You need to store the Microsoft Defender for Endpoint data in Europe.

What should you do first?

- A. Create a workspace.
- B. Onboard a new device.
- C. Delete the workspace.
- D. Offboard the test devices.

Correct Answer: *D*

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- C. From the Exchange admin center, create an anti-malware policy.
- D. From the Exchange admin center, create a mail flow rule.

Correct Answer: *C*

Reference:

<https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection>

You have a Microsoft 365 subscription that contains 500 users.

You have several hundred computers that run the 64-bit version of Windows 10 Enterprise and have the following configurations:

- ☞ Two volumes that contain data
- ☞ A CPU that has two cores
- ☞ TPM disabled
- ☞ 4 GB of RAM

All the computers are managed by using Microsoft Endpoint Manager.

You need to ensure that you can turn on Windows Defender Application Guard on the computers.

What should you do first?

- A. Modify the edition of Windows 10.
- B. Create an additional volume.
- C. Replace the CPU and enable TPM.
- D. Replace the CPU and increase the RAM.

Correct Answer: *D*

The computers need 4 CPU cores and 8GB of RAM.

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard>

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

From Microsoft Defender for Endpoint, you turn on the Allow or block file advanced feature.

You need to block users from downloading a file named File1.exe.

What should you use?

- A. a suppression rule
- B. an indicator
- C. a device configuration profile

Correct Answer: *B*

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/respond-file-alerts#allow-or-block-file>

Community vote distribution

B (100%)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.



You need to enable user access to the partner company's portal.

Which Microsoft Defender for Endpoint setting should you modify?

- A. Custom detections
- B. Advanced hunting
- C. Alert notifications
- D. Indicators
- E. Alert suppression

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-indicators?view=o365-worldwide>

HOTSPOT -

You have a Microsoft 365 subscription.

You create a Microsoft Cloud App Security policy named Risk1 based on the Logon from a risky IP address template as shown in the following exhibit.

Create activity policy

Policy template *

Logon from a risky IP address

Policy name *

Risk1

Description

Alert when a user logs on from a risky IP address to your sanctioned services. 'Risky' IP category contains by default anonymous proxies and TOR exits point. You can add more IP addresses to this category through the 'IP addresses range' settings page.

Policy severity *

High

Category *

Threat detection

Create filters for the policy

Act on:

☒ **Single activity**
Every activity that matches the filters

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

ACTIVITIES MATCHING ALL OF THE FOLLOWING

☒ IP address Category equals Risky

☒ Activity type equals Log on

[+ Add filter](#)

[Edit and preview results](#)

Alerts

☒ Create an alert for each matching event with the policy's severity [Use your organization's default settings](#)

Daily alert limit

☒ Send alert as email [?](#)

☒ Admin1@contoso.com

☐ Send alert as text message [?](#)

[Save these alert settings as the default for your organization](#)

☐ Send alerts to Flow [PREVIEW](#)
[Create a playbook in Flow](#)

Governance

☐ All apps [Notify user](#)

☒ **Notify user** [?](#)

☐ CC additional users

☐ Notify additional users [?](#)

☐ Suspend user [?](#)
For Azure Active Directory users

☐ Require user to sign in again [?](#)
For Azure Active Directory users

You have two users named User1 and User2. Each user signs in to Microsoft SharePoint Online from a risky IP address 10 times within 24 hours.

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

Admin1 will receive [answer choice].

▼

one notification

five notifications

ten notifications

no notifications

User1 will receive [answer choice].

▼

one notification

five notifications

ten notifications

no notifications

Answer Area

Admin1 will receive [answer choice].

▼

one notification

five notifications

ten notifications

no notifications

User1 will receive [answer choice].

▼

one notification

five notifications

ten notifications

no notifications

Correct Answer:

HOTSPOT -

You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 is a member of Group1.

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	None
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	None

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 view Device1 in Microsoft Defender Security Center.	<input type="radio"/>	<input type="radio"/>
User2 can sign in to Microsoft Defender Security Center.	<input type="radio"/>	<input type="radio"/>
User3 can view Device1 in Microsoft Defender Security Center.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
User1 can view Device1 in Microsoft Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in to Microsoft Defender Security Center.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can view Device1 in Microsoft Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>

HOTSPOT -

Your company uses Microsoft Cloud App Security.

You plan to integrate Cloud App Security and security information and event management (SIEM).

You need to deploy a SIEM agent on a server that runs Windows Server 2016.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

First action to perform:

	▼
Install Java 8.	
Install Microsoft .NET Framework 3.5.	
Add the Windows Internal Database feature.	
Add the Setup and Boot Event Collection feature.	

Second action to perform:

	▼
Run the Set-MMagent cmdlet.	
Add the Setup and Boot Event Collection feature.	
Run the java command and specify the -jar parameter.	
Run the Install-WindowsFeature cmdlet and specify the -source parameter.	

Answer Area

First action to perform:

	▼
Install Java 8.	
Install Microsoft .NET Framework 3.5.	
Add the Windows Internal Database feature.	
Add the Setup and Boot Event Collection feature.	

Correct Answer:

Second action to perform:

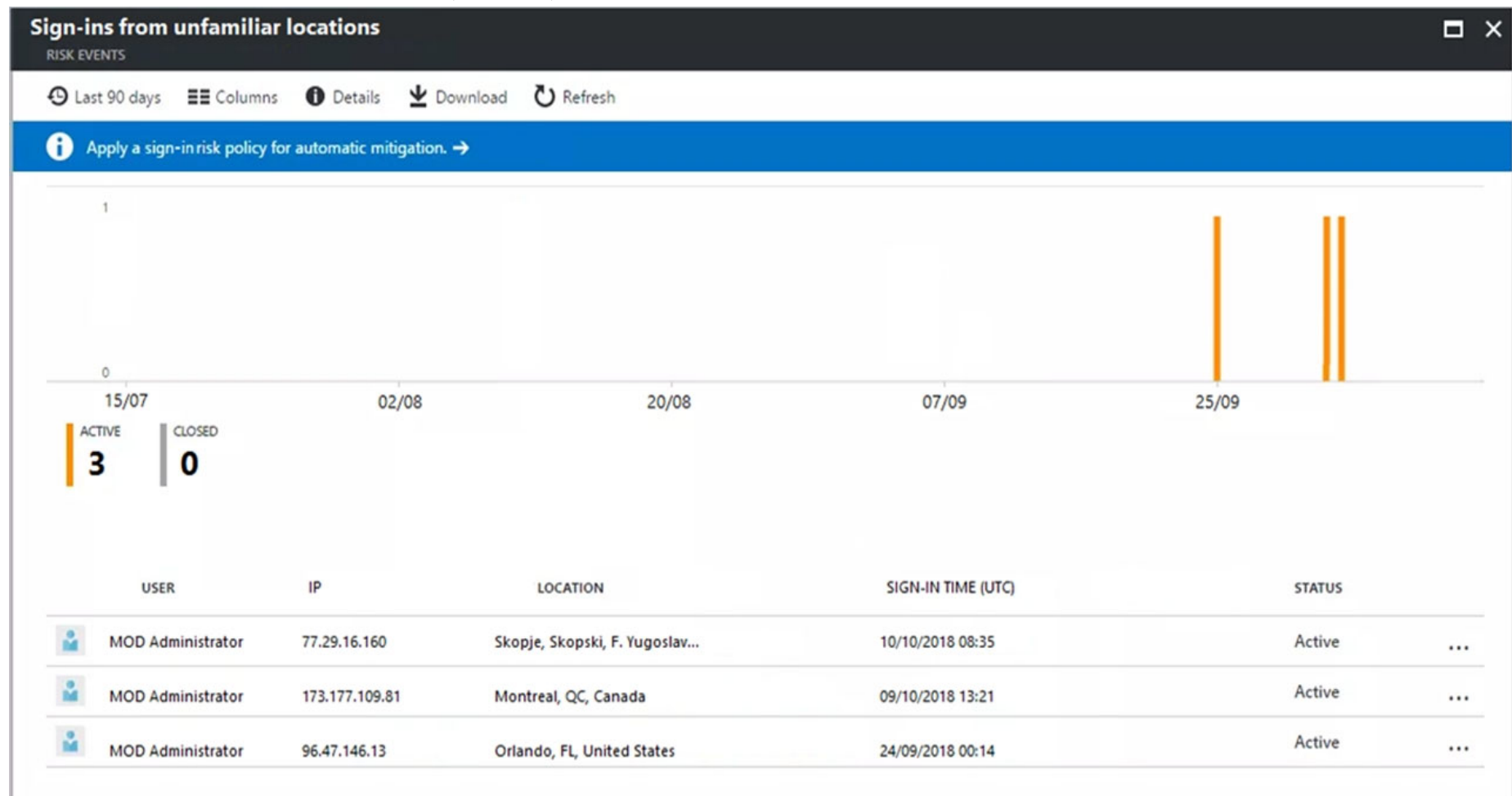
	▼
Run the Set-MMagent cmdlet.	
Add the Setup and Boot Event Collection feature.	
Run the java command and specify the -jar parameter.	
Run the Install-WindowsFeature cmdlet and specify the -source parameter.	

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-your-siem-server-with-office-365-cas>

HOTSPOT -

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events 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 require multi-factor authentication when signing in to unfamiliar locations, you must create a [answer choice].

▼

☐ named location in Azure AD
 ☒ sign-in risk policy
 ☐ user risk policy

To avoid generating alerts when signing in to the Montreal location, create [answer choice].

▼

☐ a named location in Azure AD
 ☒ a sign-in risk policy
 ☐ a user risk policy

Answer Area

To require multi-factor authentication when signing in to unfamiliar locations, you must create a [answer choice].

▼

☐ named location in Azure AD
 ☒ sign-in risk policy
 ☐ user risk policy

Correct Answer:

To avoid generating alerts when signing in to the Montreal location, create [answer choice].

▼

☒ a named location in Azure AD
 ☐ a sign-in risk policy
 ☐ a user risk policy

References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy> <https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations>

Question #37

Topic 2

Your company uses Microsoft Defender for Identity and Microsoft 365 Defender.
You need to integrate Microsoft Defender for Identity and Microsoft 365 Defender.
What should you do?

- A. From Microsoft Defender for Identity, configure the notifications and reports.
- B. From Microsoft Defender for Identity, configure the data sources.
- C. From Microsoft Defender Security Center, configure the Machine management settings.
- D. From Microsoft Defender Security Center, configure the General settings.

Correct Answer: *B*

Reference:

<https://blog.ahasayen.com/azure-atp-and-windows-defender-atp-integration/>

HOTSPOT -

You have a Microsoft Azure Activity Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

Rank	Machine group	Machine	User access
1	ATP1	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 Device2.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	User1 can run an antivirus scan on Device2.	<input type="radio"/>	<input checked="" type="radio"/>
	User2 can collect an investigation package from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
	User3 can isolate Device1.	<input checked="" type="radio"/>	<input type="radio"/>

References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/user-roles-windows-defender-advanced-threat-protection>

HOTSPOT -

You have a Microsoft 365 subscription. All client devices are managed by Microsoft Endpoint Manager.

You need to implement Microsoft Defender Advanced Threat Protection (ATP) for all the supported devices enrolled in mobile device management (MDM).

What should you include in the device configuration profile? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Platform:

▼
Android
iOS
Windows 10 and later
Windows 8.1 and later

Settings:

▼
Offboard package
Onboard package
Windows Defender Applicaion Guard
Windows Defender Firewall

Answer Area

Platform:

▼
Android
iOS
Windows 10 and later
Windows 8.1 and later

Correct Answer:

Settings:

▼
Offboard package
Onboard package
Windows Defender Applicaion Guard
Windows Defender Firewall

Reference:

<https://docs.microsoft.com/en-us/intune/advanced-threat-protection>

You have a Microsoft 365 subscription.

Your company purchases a new financial application named App1.

From Cloud Discovery in Microsoft Cloud App Security, you view the Discovered apps page and discover that many applications have a low score because they are missing information about domain registration and consumer popularity.

You need to prevent the missing information from affecting the App1 score.

What should you configure from the Cloud Discover settings?

- A. Organization details
- B. Default behavior
- C. Score metrics
- D. App tags

Correct Answer: C

Reference:

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

You have a Microsoft 365 E5 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Exchange admin center, create a spam filter policy.
- C. From the Exchange admin center, create an anti-malware policy.
- D. From the Exchange admin center, create a mail flow rule.

Correct Answer: C
Reference:
<https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection>

HOTSPOT -
You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
A user named User1 stores documents in Microsoft OneDrive.
You need to place the contents of User1's OneDrive account on an eDiscovery hold.
Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

https://

	▼
onedrive.live.com/	
contoso.onmicrosoft.com/	
contoso.sharepoint.com/	
contoso-my.sharepoint.com/	

	▼
User1	
Sites/User1	
contoso_onmicrosoft_com/User1	
personal/User1_contoso_onmicrosoft_com	

Correct Answer:
Answer Area

https://

	▼
onedrive.live.com/	
contoso.onmicrosoft.com/	
contoso.sharepoint.com/	
contoso-my.sharepoint.com/	

	▼
User1	
Sites/User1	
contoso_onmicrosoft_com/User1	
personal/User1_contoso_onmicrosoft_com	

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

HOTSPOT -

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

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

The tenant has a conditional access policy that has the following configurations:

- ☞ Name: Policy1
- ☞ Assignments:
 - Users and groups: Group1
 - Cloud apps or actions: All cloud apps
- ☞ Access controls:
 - ☞ Grant, require multi-factor authentication
 - ☞ Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to On .	<input type="radio"/>	<input type="radio"/>
Admin2 can set Enable policy for Policy1 to Off .	<input type="radio"/>	<input type="radio"/>
Admin3 can set Users and groups for Policy1 to All users .	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to On .	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can set Enable policy for Policy1 to Off .	<input checked="" type="radio"/>	<input type="radio"/>
Admin3 can set Users and groups for Policy1 to All users .	<input checked="" type="radio"/>	<input type="radio"/>

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

- ☞ Conditional Access policies can be enabled in report-only mode.
- ☞ During sign-in, policies in report-only mode are evaluated but not enforced.
- ☞ Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
- ☞ Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:

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

Your network contains an on-premises Active Directory domain.

Your company has a security policy that prevents additional software from being installed on domain controllers.

You need to monitor a domain controller by using Microsoft Defender for Identity.

What should you do? More than one answer choice may achieve the goal. Choose the BEST answer.

- A. Deploy a Microsoft Defender for identity sensor, and then configure port mirroring.
- B. Deploy a Microsoft Defender for identity sensor, and then configure detections.
- C. Deploy a Microsoft Defender for Identity standalone sensor, and then configure detections.
- D. Deploy a Microsoft Defender for Identity standalone sensor, and then configure port mirroring.

Correct Answer: D

We cannot install additional software on the domain controllers. Azure ATP Standalone Sensor is a full agent installed on a dedicated server that can monitor traffic from multiple domain controllers. This is an alternative to those that do not wish to install an agent directly on a domain controller.

Incorrect Answers:

A, B: Azure ATP Sensor is a lightweight agent installed directly on a domain controller to monitor and report traffic. However, we cannot install additional software on the domain controllers

Reference:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5> <https://docs.microsoft.com/en-us/defender-for-identity/configure-port-mirroring> <https://blog.enablingtechcorp.com/secure-and-monitor-domain-controllers-with-azure-atp>

Community vote distribution

D (100%)

Your company has digitally signed applications.

You need to ensure that Microsoft Defender for Endpoint considers the digitally signed applications safe and never analyzes them.

What should you create in the Microsoft Defender Security Center?

- A. a custom detection rule
- B. an allowed/blocked list rule
- C. an alert suppression rule
- D. an indicator

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators>

DRAG DROP -

You create a Microsoft 365 subscription.

You need to create a deployment plan for Microsoft Defender for Identity.

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:

Actions

Answer Area

Configure the sensor settings.

Download the Defender for Identity
sensor setup package.

Create a Threat policy.

Install sensors.

Create a Defender for Identity
instance.

Create an Azure Active Directory
(Azure AD) conditional access policy.



Correct Answer:

Actions

Answer Area

Create a Defender for Identity
instance.

Download the Defender for Identity
sensor setup package.

Create a Threat policy.

Install sensors.

Configure the sensor settings.



Create an Azure Active Directory
(Azure AD) conditional access policy.

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/install-step1> <https://docs.microsoft.com/en-us/defender-for-identity/install-step3>

<https://docs.microsoft.com/en-us/defender-for-identity/install-step4>

Question #47

Topic 2

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

A. the Security & Compliance admin center

B. Microsoft Defender Security Center

C. the Microsoft 365 admin center

D. the Azure Advanced Threat Protection portal

E. the Cloud App Security portal

Correct Answer: *D*

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

Community vote distribution

B (100%)

Question #48

Topic 2

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

You have a Microsoft 365 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Endpoint Management admin center, you create a device configuration profile.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

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

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Security administrator role.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide>

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

You need to assign the Security Administrator role.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide>

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

You need to assign the Security Administrator role.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide>

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

A. From the Exchange admin center, create an in-place eDiscovery & hold.

B. From the Security & Compliance admin center, create a data governance event.

C. From the Exchange admin center, create an anti-malware policy.

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

Correct Answer: *C*


Reference:

<https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection>

You implement Microsoft Defender for Identity.

You have a Defender for Identity sensor configured as shown in the following exhibit.

Updates

Domain Controller restart during updates   OFF

NAME	↑	Type	VERSION	AUTOMATIC RESTART	DELAYED UPDATE	STATUS
LON-DC1		Sensor	2.48.5521	 ON	 ON	Up to date

Save

How long after the Azure ATP cloud service is updated will the sensor update?

- A. 72 hours
- B. 12 hours
- C. 48 hours
- D. 7 days
- E. 20 hours

Correct Answer: A

Sensors set to Delayed update are updated on a delay of 72 hours.

References:

<https://docs.microsoft.com/en-us/defender-for-identity/sensor-update>

HOTSPOT -

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Member
1	Group1	Name starts with COMP
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped machines (default)	Not applicable

You onboard computers to Microsoft Defender ATP as shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer1 and Computer2 members? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Computer1:

Group1 only

Group2 only

Group1 and Group2

Ungrouped machines

Computer2:

Group1 only

Group3 only

Group1 and Group3

Answer Area

Correct Answer:

Computer1:

Group1 only

Group2 only

Group1 and Group2

Ungrouped machines

Computer2:

Group1 only

Group3 only

Group1 and Group3

When a device is matched to more than one group, it is added only to the highest ranked group.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide>

You have Windows 10 devices that are managed by using Microsoft Endpoint Manager.
You need to configure the security settings in Microsoft Edge.
What should you create in Microsoft Endpoint Manager?

- A. an app configuration policy
- B. an app
- C. a device configuration profile
- D. a device compliance policy

Correct Answer: C

Reference:

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

HOTSPOT -

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

Name	Role
User1	Global admin
User2	<i>None</i>
User3	<i>None</i>

You provision the private store in Microsoft Store for Business.

You assign Microsoft Store for Business roles to the users as shown in the following table.

Name	Role
User1	<i>None</i>
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Can add apps to the private store:

	▼
User2 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, and User3	

Can assign apps from Microsoft Store for Business:

	▼
User2 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, and User3	

Answer Area

Can add apps to the private store:

Correct Answer:

	▼
User2 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, and User3	

Can assign apps from Microsoft Store for Business:

	▼
User2 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, and User3	

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business> <https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-role>

DRAG DROP -

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

Operating system	Quantity
Windows 8.1	5
Windows 10	5
Windows Server 2016	5

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must avoid installing software on the devices whenever possible.

Which onboarding method should you use for each operating system? To answer, drag the appropriate methods to the correct operating systems.

Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Methods

Answer Area

A local script

A Microsoft Defender for identity sensor

Microsoft Monitoring Agent

Windows 8.1:

Windows 10:

Windows Server 2016:

Correct Answer:

Methods

Answer Area

A local script

A Microsoft Defender for identity sensor

Microsoft Monitoring Agent

Windows 8.1:

Windows 10:

Windows Server 2016:

Microsoft Monitoring Agent

A local script

Microsoft Monitoring Agent

Reference:

- <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-downlevel?view=o365-worldwide>
- <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide>
- <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide>

The users at your company use Dropbox Business to store documents. The users access Dropbox Business by using the MyApps portal. You need to ensure that user access to Dropbox Business is authenticated by using a Microsoft 365 identity. The documents must be protected if the data is downloaded to a device that is not trusted. What should you do?

- A. From the Azure Active Directory admin center, configure conditional access settings.
- B. From the Azure Active Directory admin center, configure the device settings.
- C. From the Azure Active Directory admin center, configure organizational relationships settings.
- D. From the Endpoint Manager admin center, configure device enrollment settings.

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/campaigns/m365-campaigns-conditional-access?view=o365-worldwide>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions>

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 subscription. You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization. You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the SharePoint admin center, you modify the sharing settings. Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 subscription. You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network. Solution: From the Device Management admin center, you create a trusted location and a compliance policy. Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678>

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Microsoft 365 admin center, you configure the Organization profile settings.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678A>

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Azure Active Directory admin center, you create a trusted location and a conditional access policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678>

HOTSPOT -

You have Microsoft 365 subscription.

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

Policy1

Edit policy

Delete policy

Status	<input checked="" type="checkbox"/> On
Description	Description
Severity	<input checked="" type="radio"/> Low Edit
Category	Threat management
Conditions	Activity is Detected malware in file
Aggregation	Aggregated
Threshold	20 activities Edit
Window	120 minutes
Scope	All users

Email recipients	User1@sk190107outlook.onmicrosoft.com
Daily notification limit	100 Edit

Close

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

Policy1 will trigger an alert if malware is detected in

Exchange Online only

SharePoint Online only

SharePoint Online or OneDrive only

Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is

5

12

20

100

Correct Answer:

Answer Area

Policy1 will trigger an alert if malware is detected in

Exchange Online only

SharePoint Online only

SharePoint Online or OneDrive only

Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is

5

12

20

100

Note: The Aggregation settings has a 120 minute window

Question #64

Topic 2

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

- A. From the Security & Compliance admin center, create a label and a label policy.
- B. From the Exchange admin center, create a mail flow rule.
- C. From the Security & Compliance admin center, start a message trace.
- D. From Exchange admin center, start a mail flow message trace.

Correct Answer: A

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

HOTSPOT -

You have a new Microsoft 365 subscription.

A user named User1 has a mailbox in Microsoft Exchange Online.

You need to log any changes to the mailbox folder permissions of User1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

<div><div></div><div>▼</div></div> User1	<div><div></div><div>▼</div></div> \$true
Set-AdminAuditLogConfig	-AdminAuditLogEnabled
Set-Mailbox	-AuditEnabled
Set-UnifiedAuditSetting	-UnifiedAuditLogIngestionEnabled

Correct Answer:

Answer Area

<div><div></div><div>▼</div></div> User1	<div><div></div><div>▼</div></div> \$true
Set-AdminAuditLogConfig	-AdminAuditLogEnabled
Set-Mailbox	-AuditEnabled
Set-UnifiedAuditSetting	-UnifiedAuditLogIngestionEnabled

To enable auditing for a single mailbox (in this example, belonging to Holly Sharp), use this PowerShell command: Set-Mailbox username -AuditEnabled \$true

References:

<https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins> <https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps>

You have a Microsoft 365 subscription.

You recently configured a Microsoft SharePoint Online tenant in the subscription.

You plan to create an alert policy.

You need to ensure that an alert is generated only when malware is detected in more than five documents stored in SharePoint Online during a period of 10 minutes.

What should you do first?

- A. Enable Microsoft Office 365 Cloud App Security.
- B. Deploy Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP)
- C. Enable Microsoft Office 365 Analytics.

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/use-case-admin-quarantine>

DRAG DROP -

Your company has a Microsoft 365 E5 tenant.

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

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

What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Solutions

An app configuration policy

An app protection policy

A compliance policy

A configuration profile

Answer Area

Company-owned devices:

Solution

Personal devices:

Solution

Correct Answer:

Solutions

An app configuration policy

A configuration profile

Answer Area

Company-owned devices:

A compliance policy

Personal devices:

An app protection policy

HOTSPOT -

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

Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? 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 in Microsoft Endpoint Manager:

	▼
An app configuration policy	
An app protection policy	
A conditional access policy	
A device compliance policy	

Minimum number of required policies:

	▼
1	
2	
3	
5	

Answer Area

Policy to create in Microsoft Endpoint Manager:

	▼
An app configuration policy	
An app protection policy	
A conditional access policy	
A device compliance policy	

Correct Answer:

Minimum number of required policies:

	▼
1	
2	
3	
5	

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy>

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 Defender.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 Defender?

- A. Microsoft Cloud App Security
- B. Azure Sentinel
- C. Azure Web Application Firewall
- D. Azure Information Protection

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide>

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 Defender.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 Defender?

- A. Azure Sentinel
- B. Azure Information Protection
- C. Azure Security Center
- D. Microsoft Defender for Identity

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide>

You have a Microsoft 365 E5 subscription.

All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender Advanced Threat Protection

(Microsoft Defender ATP).

You need to configure Microsoft Defender ATP on the computers.

What should you create from the Endpoint Management admin center?

- A. a Microsoft Defender ATP baseline profile
- B. a device configuration profile
- C. an update policy for iOS
- D. a mobile device management (MDM) security baseline profile

Correct Answer: B

Reference:

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

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

Correct Answer: *B*

Reference:

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

DRAG DROP -

Your company purchases a cloud app named App1.

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

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

Select and Place:

Actions**Answer Area**

Deploy Azure Active Directory
(Azure AD) Application Proxy.

From the Cloud App Security admin
center, add an app connector.

Sign in to App1.

Create a conditional access policy.

From the Azure Active Directory admin
center, configure the Diagnostic settings.

From the Azure Active Directory admin
center, add an app registration for App1.



Correct Answer:

Actions**Answer Area**

Deploy Azure Active Directory
(Azure AD) Application Proxy.

From the Cloud App Security admin
center, add an app connector.

Create a conditional access policy.

Sign in to App1.



From the Azure Active Directory admin
center, configure the Diagnostic settings.

From the Azure Active Directory admin
center, add an app registration for App1.

Reference:

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

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

Correct Answer: B

Reference:

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

HOTSPOT -

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

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

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

Home / Policy Management		Notifications
Policy configurations		
+ Create Copy Reorder priority Remove		Total policy configurations: 3
Name	Priority ↑	Recommendation status
Office Users Policy	0	
Sales Team Policy	1	
All users	2	

The policies use the settings shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The default shared folder location for User1 is:

▼

https://sharepoint.contoso.com/addins_all_users

https://sharepoint.contoso.com/addins_office_users

https://sharepoint.contoso.com/addins_sales_team_users_

The default Office theme for User 2 is:

▼

Colorful

Dark Gray

White

Correct Answer:

Answer Area

The default shared folder location for User1 is:

▼

https://sharepoint.contoso.com/addins_all_users

https://sharepoint.contoso.com/addins_office_users

https://sharepoint.contoso.com/addins_sales_team_users_

The default Office theme for User 2 is:

▼

Colorful

Question #76

Topic 2

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

Correct Answer: A

Reference:

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

Question #77

Topic 2

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

Correct Answer: B

Reference:

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

HOTSPOT -

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

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

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

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

The policies use the settings shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 has their cache cleared on close.	<input type="radio"/>	<input type="radio"/>
User2 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>
User3 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	User1 has their cache cleared on close.	<input type="radio"/>	<input checked="" type="radio"/>
	User2 has Cursor movement set to Visual.	<input type="radio"/>	<input checked="" type="radio"/>
	User3 has Cursor movement set to Visual.	<input type="radio"/>	<input checked="" type="radio"/>

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

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

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro
Device3	Windows 10 Enterprise
Device4	Ubuntu 18.04 LTS

You plan to implement attack surface reduction (ASR) rules.

Which devices will support the ASR rules?

- A. Device1, Device2, Device3, and Device4
- B. Device1, Device2, and Device3 only
- C. Device2 and Device3 only
- D. Device3 only

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements>

You have a Microsoft 365 tenant.

You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.

What should you use?

- A. an attack surface reduction (ASR) policy
- B. an app configuration policy
- C. a device compliance policy
- D. a device configuration profile

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices>

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles.

Which platform can you manage by using the profiles?

- A. Android Enterprise
- B. Windows 10
- C. Windows 8.1
- D. Android

Correct Answer: B

Intune device configuration profiles can be applied to Windows 10 devices and macOS devices

Note:

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

1. Windows 10
2. macOS

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

1. Ubuntu Linux
2. iOS

Reference:

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

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

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

Which policy type should you configure?

- A. conditional access
- B. account protection
- C. attack surface reduction (ASR)
- D. Endpoint detection and response

Correct Answer: A

Reference:

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

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

The policies are assigned to Device1.

Which policy settings will be applied to Device1?

- A. only the settings of Policy1
- B. only the settings of Policy2
- C. only the settings of Policy3
- D. no settings

Correct Answer: C

HOTSPOT -

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

You plan to attack surface reduction (ASR) rules for the Windows 10 devices.

You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.

You need to find the ASR rules that match the activities on the devices.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

▼

AlertInfo
DeviceEvents
DeviceInfo

|

▼

 ActionType startswith 'ASR'

lookup
project
render
where

Answer Area

Correct Answer:

▼

AlertInfo
DeviceEvents
DeviceInfo

|

▼

 ActionType startswith 'ASR'

lookup
project
render
where

Reference:

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction-rules-part-3/ba-p/1360968>

HOTSPOT -

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.

You have devices enrolled in Microsoft Intune as shown in the following table.

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

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Devices that can onboarded to Microsoft Defender for Endpoint:

Device 1 only
Device 1 and Device 2 only
Device 1 and Device 3 only
Device 1 and Device 4 only
Device 1, Device 2, and Device 4 only
Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

A conditional access policy only
A device compliance policy only
A device configuration profile only
A device configuration profile and a conditional access policy only
Device configuration profile, device compliance policy, and conditional access policy

Correct Answer:

Answer Area

Devices that can onboarded to Microsoft Defender for Endpoint:

Device 1 only
Device 1 and Device 2 only
Device 1 and Device 3 only
Device 1 and Device 4 only
Device 1, Device 2, and Device 4 only
Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

A conditional access policy only
A device compliance policy only
A device configuration profile only
A device configuration profile and a conditional access policy only
Device configuration profile, device compliance policy, and conditional access policy

Reference:

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

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

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

You plan to create a new Windows 10 Security Baseline profile.
To which groups can you assign to the profile?

- A. Group3 only
- B. Group1 and Group3 only
- C. Group2 and Group3 only
- D. Group1, Group2, and Group3

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile> <https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

You have a Microsoft 365 E5 subscription that contains a user named User1.
The subscription has a single anti-malware policy as shown in the following exhibit.

Default

general

► settings

Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be released only by an admin.

Do you want to notify recipients if their messages are quarantined?

☐ No

☐ Yes and use the default notification text

☒ Yes and use custom notification text

*Custom notification text:

Malware was removed.

Common Attachment Types Filter

Turn on this feature to block attachment types that may harm your computer.

☒ Off

☐ On - Emails with attachments of filtered file types will trigger the Malware Detection Response (recommended)

FILE TYPES

.ace

Save Cancel

An email message that contains text and two attachments is sent to User1. One attachment is infected with malware.
How will the email message and the attachments be processed?

- A. Both attachments will be removed. The email message will be quarantined, and User1 will receive an email message without any attachments and an email message that includes the following text: "Malware was removed."
- B. The email message will be quarantined, and the message will remain undelivered.
- C. Both attachments will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: "Malware was removed."
- D. The malware-infected attachment will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

Correct Answer: C

Reference:

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

HOTSPOT -

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

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

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

Name	Modified	Modified By
File1.docx	About a minute ago	Prvi
File2.docx	A few seconds ago	Prvi
File3.docx	A few seconds ago	Prvi

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

User2:

Answer Area

Correct Answer:

User1:

	▼
File1.docx only	
File1.docx and File2.docx only	
File1.docx, File2.docx, and File3.docx	

User2:

	▼
File1.docx only	
File1.docx and File2.docx only	
File1.docx, File2.docx, and File3.docx	

Reference:

<https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/> <https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/>

You have a Microsoft 365 E5 tenant.

The Microsoft Secure Score for the tenant is shown in the following exhibit.

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

↓ Export

12 items

🔍 Search

🔼 Filter

{≡} Group by ▾

Applied filters:

Rank ⓘ	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	+16.95%	0/10
2	Ensure all users can complete multi-factor authentication for...	+15.25%	0/9
3	Enable policy to block legacy authentication	+13.56%	0/8
4	Turn on user risk policy	+11.86%	0/7
5	Turn on sign-in risk policy	+11.86%	0/7
6	Do not allow users to grant consent to unmanaged applicatio...	+6.78%	0/4
7	Enable self-service password reset	+1.69%	0/1
8	Turn on customer Lockbox feature	+1.69%	0/1
9	Use limited administrative roles	+1.69%	0/1
10	Designate more than one global admin	+1.69%	0/1

You plan to enable Security defaults for Azure Active Directory (Azure AD).

Which three improvement actions will this affect?

- A. Require MFA for administrative roles.
- B. Ensure all users can complete multi-factor authentication for secure access
- C. Enable policy to block legacy authentication
- D. Enable self-service password reset
- E. Use limited administrative roles

Correct Answer: ABC

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

You have a Microsoft 365 E5 subscription.

You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.

What should you do?

- A. From the Cloud App Security admin center, select Users and accounts.
- B. From the Microsoft 365 Defender, view the Threat tracker.
- C. From the Microsoft 365 admin center, view the Security & compliance report.
- D. From the Azure Active Directory admin center, view the Risky sign-ins report.

Correct Answer: A

HOTSPOT -

You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager. You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard.

ASR2 will be used to configure Microsoft Defender SmartScreen.

Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

ASR1:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

ASR2:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

Answer Area

Correct Answer:

ASR1:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

ASR2:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

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

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles.

Which platform can you manage by using the profiles?

- A. Ubuntu Linux
- B. macOS
- C. iOS
- D. Android

Correct Answer: B

Intune device configuration profiles can be applied to Windows 10 devices and macOS devices

Note:

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

1. Windows 10
2. macOS

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

1. Android Enterprise
2. Windows 8.1

Reference:

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

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

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

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

You need to enable User1 to create Compliance Manager assessments.

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

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md>

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

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

You need to enable User1 to create Compliance Manager assessments.

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

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md>

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

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

You need to enable User1 to create Compliance Manager assessments.

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

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md>

HOTSPOT -

You have a Microsoft 365 E5 subscription.

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

How do you want the alert to be triggered?

- ☐ Every time an activity matches the rule
- ☐ When the volume of matched activities reaches a threshold

More than or equal to activities

During the last minutes

On

- ☒ When the volume of matched activities becomes unusual

On

You need to identify the following:

- ☞ How many days it will take to establish a baseline for unusual activity.
- ☞ Whether alerts will be triggered during the establishment of the baseline.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

How many days it will take to establish the baseline:

<input type="text"/>	▼
1	
5	
7	
10	

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

<input type="text"/>	▼
Alerts will be triggered.	
Alerts will not be triggered.	
Alerts will be triggered only after the process to establish the baseline has been running for one day.	

Correct Answer:

Answer Area

How many days it will take to establish the baseline:

1
5
7
10

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

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

Reference:

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

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

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert occurs only on a Windows 10 device. The solution must minimize administrative effort.

What should you do first?

- A. From the Microsoft 365 admin center, create a mail-enabled security group.
- B. From the Microsoft 365 Defender portal, create a device group.
- C. From the Microsoft Endpoint Manager admin center, create a device category.
- D. From the Azure Active Directory admin center, create a dynamic device group.

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide>

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide>

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

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange admin role.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

You need to assign the Security Administrator role.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide>

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

- A. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- B. From the Security & Compliance admin center, create a label and a label policy.
- C. From the Security & Compliance admin center, start a message trace.
- D. From Microsoft Cloud App Security, create an activity policy.

Correct Answer: B

You have a Microsoft 365 tenant.

You discover that administrative tasks are unavailable in the Microsoft 365 audit logs of the tenant.

You run the Get-AdminAuditLogConfig cmdlet and receive the following output:

```
RunspaceId           : 4cb214a3 -c11d-4dbf-a59a-3c055d010576
AdminAuditLogEnabled  : True
LogLevel             : Verbose
TestCmdletLoggingEnabled : False
AdminAuditLogCmdlets  : {}
AdminAuditLogParameters : {}
AdminAuditLogExcludedCmdlets : {}
AdminAuditLogAgeLimit : 90.00:00:00
LoadBalancerCount     : 3
RefreshInterval       : 10
PartitionInfo         : {}
UnifiedAuditLogIngestionEnabled : False
UnifiedAuditLogFirstOptInDate :
AdminDisplayName      :
ExchangeVersion       : 0.10 (14.0.100.0)
Name                  : Default
DistinguishedName     : CN=Default,CN=Configuration,CN=Contoso.onmicrosoft.com;OU=Microsoft Exchange
                        Hosted Organizations,DC=FF0,DC=extest,DC=microsoft,DC=com
Identity              : FF0.extest.microsoft.com/Microsoft Exchange Hosted Organizations/Contoso.onmicrosoft.com/Configuration/Default
ObjectCategory        :
ObjectClass            : {msExchAdminAuditLogConfig}
WhenChanged           :
WhenCreated           :
WhenChangedUTC         :
WhenCreatedUTC        :
ExchangeObjectId      : 00075a1f-b49e-4769-983d-be2587651f3b
OrganizationId        : FF0.extest.microsoft.com/Microsoft Exchange Hosted Organizations/Contoso.onmicrosoft.com - FF0.extest.microsoft.com/Microsoft Exchange Hosted
                        Organizations/Contoso.onmicrosoft.com/Configuration
Id                    : FF0.extest.microsoft.com/Microsoft Exchange Hosted Organizations/Contoso.onmicrosoft.com/Configuration/Default
Guid                  : 00075a1f-b49e-4769-983d-be2587651f3b
OriginatingServer     :
IsValid               : True
ObjectState           : New
```

You need to ensure that administrative tasks are logged in the Microsoft 365 audit logs.

Which attribute should you modify?

- A. TestCmdletLoggingEnabled
- B. UnifiedAuditLogIngestionEnabled
- C. AdminAuditLogEnabled

Correct Answer: B

References:

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

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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Microsoft 365 compliance center, you create a data loss prevention (DLP) policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

In Microsoft 365, you can create a data loss prevention (DLP) policy in two different admin centers:

☞ In the Security & Compliance admin center (now known as the Microsoft 365 Compliance Center), you can create a single DLP policy to help protect content in

SharePoint, OneDrive, Exchange, Teams, and now Endpoint Devices.

☞ In the Exchange admin center, you can create a DLP policy to help protect content only in Exchange.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers?view=o365-worldwide>

Your company has a Microsoft 365 tenant.

The company sells products online and processes credit card information.

You need to be notified if a file stored in Microsoft SharePoint Online contains credit card information. The file must be removed automatically from its current location until an administrator can review its contents.

What should you use?

A. a Microsoft 365 compliance center data loss prevention (DLP) policy

B. a Microsoft Cloud App Security access policy

C. a Microsoft 365 compliance center retention policy

D. a Microsoft Cloud App Security file policy

Correct Answer: A

References:

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

HOTSPOT -

You configure an anti-phishing policy as shown in the following exhibit.

Policy setting	Policy name Description Applied to		
		Managers	
		If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.OnMicrosoft.com	Edit
Impersonation	Users to protect Protect all domains I own Protect specific domains Action > User impersonation Action > Domain impersonation Safety tips > User impersonation Safety tips > Domain impersonation Safety tips > Unusual characters Mailbox intelligence	On - 3 User(s) specified On On - 2 Domain(s) specified Move message to the recipients' Junk Email folders Delete the message before it's delivered Off Off Off Off	Edit
Spoof	Enable antispoofting protection Action	On Quarantine the message	Edit
Advanced settings	Advanced phishing thresholds	3 - More Aggressive	Edit

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 message is identified as a domain impersonation, **[answer choice]**.

the message is delivered to the Inbox folder

the message is moved to the Deleted Items folder

the message is moved to the Junk Email folder

the message is NOT delivered

To reduce the likelihood of the impersonation policy generating false positives, configure **[answer choice]**.

Domain impersonation

Enable antispoofting protection

Mailbox intelligence

Correct Answer:

Answer Area

If a message is identified as a domain impersonation, **[answer choice]**.

the message is delivered to the Inbox folder

the message is moved to the Deleted Items folder

the message is moved to the Junk Email folder

the message is NOT delivered

To reduce the likelihood of the impersonation policy generating false positives, configure **[answer choice]**.

Domain impersonation

Enable antispoofting protection

Mailbox intelligence

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies#learn-about-atp-anti-phishing-policy-options>

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint Online site. What should you do?

- A. From the Security & Compliance admin center, create an alert policy.
- B. From the SharePoint Online site, create an alert.
- C. From the SharePoint Online admin center, modify the sharing settings.
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

Correct Answer: A

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/create-activity-alerts>

HOTSPOT -

You have a Microsoft 365 subscription.

You are configuring permissions for Security & Compliance.

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

Name	Task
User1	Download all Security & Compliance reports
User2	Create and manage Security & Compliance alerts.

The solution must use the principle of least privilege.

To which role should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

Records Management
Security Administrator
Security Reader
Supervisory Review

User2:

Compliance Administrator
Organization Management
Security Administrator
Security Reader
Supervisory Review

Answer Area

Correct Answer:

User1:

Records Management
Security Administrator
Security Reader
Supervisory Review

User2:

Compliance Administrator
Organization Management
Security Administrator
Security Reader
Supervisory Review

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles>

HOTSPOT -

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

Your company implements Windows Information Protection (WIP).

You need to modify which users and applications are affected by WIP.

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

To modify which users are affected by WIP, configure:

The Azure AD app registration
The Azure AD device settings
The MAM User scope
The mobile device management (MDM) authority

To modify which applications are affected by WIP, configure:

App configuration policies
App protection policies
Compliance policies
Device configuration profiles

Answer Area

To modify which users are affected by WIP, configure:

The Azure AD app registration
The Azure AD device settings
The MAM User scope
The mobile device management (MDM) authority

Correct Answer:

To modify which applications are affected by WIP, configure:

App configuration policies
App protection policies
Compliance policies
Device configuration profiles

References:

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure>

HOTSPOT -

You have a Microsoft 365 subscription.

All users are assigned Microsoft Azure Active Directory Premium licenses.

From the Device Management admin center, you set Microsoft Intune as the MDM authority.

You need to ensure that when the members of a group named Marketing join a device to Azure Active Directory (Azure AD), the device is enrolled automatically in

Intune. The Marketing group members must be limited to five devices enrolled in Intune.

Which two options should you use to perform the configurations? To answer, select the appropriate blades in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Device enrollment

Microsoft Intune

 Search (Ctrl+/) 



Overview



Quick start

Manage



Apple enrollment



Android enrollment



Windows enrollment



Terms and conditions



Enrollment restrictions



Device categories



Corporate device identifiers



Device enrollment managers

Monitor



Enrollment failures



Audit logs



Incomplete user enrollments

Device enrollment

Microsoft Intune

 Search (Ctrl+/) 

 Overview

 Quick start


Manage

 Apple enrollment

 Android enrollment

 Windows enrollment

 Terms and conditions

 Enrollment restrictions

 Device categories

 Corporate device identifiers

 Device enrollment managers

Monitor

 Enrollment failures

 Audit logs

 Incomplete user enrollments

Correct Answer:

Device enrollment manager (DEM) is an Intune permission that can be applied to an Azure AD user account and lets the user enroll up to 1,000 devices

You can create and manage enrollment restrictions that define what devices can enroll into management with Intune, including the:

☞ Number of devices.

☞ Operating systems and versions.

The Marketing group members must be limited to five devices enrolled in Intune

References:

<https://docs.microsoft.com/en-us/intune/enrollment/device-enrollment-manager-enroll> <https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set>

Question #10

Topic 3

You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content.

What should you do?

- A. Run the Set-AadrmOnboardingControlPolicy cmdlet.
- B. Run the Add-AadrmRoleBasedAdministrator cmdlet.
- C. Create an Azure Information Protection policy.
- D. Configure the protection activation status for Azure Information Protection.

Correct Answer: C

Reference:

<https://blogs.technet.microsoft.com/kemckinn/2018/05/17/creating-labels-for-azure-information-protection/>

Question #11

Topic 3

Your company has a Microsoft 365 subscription.

You need to identify which users performed the following privileged administration tasks:

- ☞ Deleted a folder from the second-stage Recycle Bin of Microsoft SharePoint
- ☞ Opened a mailbox of which the user was not the owner
- ☞ Reset a user password

What should you use?

- A. Microsoft Azure Active Directory (Azure AD) audit logs
- B. Microsoft 365 compliance content search
- C. Microsoft Azure Active Directory (Azure AD) sign-ins
- D. Microsoft 365 compliance audit log search

Correct Answer: A

You can view the required information in the audit logs. The Azure AD audit logs provide records of system activities for compliance. To access the audit report, select Audit logs in the Activity section of Azure Active Directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs> <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-logs-overview>

You have a Microsoft 365 subscription. You have a user named User1.
You need to ensure that User1 can place a litigation hold on all mailbox content.
What permission should you assign to User1?

- A. the eDiscovery Manager role from the Microsoft 365 compliance center
- B. the Compliance Management role from the Exchange admin center
- C. the User management administrator role from Microsoft 365 admin center
- D. the Information Protection administrator role from the Azure Active Directory admin center

Correct Answer: A

References:

<https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions?view=exchserver-2019>

You have a Microsoft 365 subscription.
All users are assigned a Microsoft 365 E3 license.
You enable auditing for your organization.
What is the maximum amount of time data will be retained in the Microsoft 365 audit log?

- A. 2 years
- B. 1 year
- C. 30 days
- D. 90 days

Correct Answer: D

References:

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

HOTSPOT -

Your company is based in the United Kingdom (UK).

Users frequently handle data that contains Personally Identifiable Information (PII).

You create a data loss prevention (DLP) policy that applies to users inside and outside the company. The policy is configured as shown in the following exhibit.

New DLP policy

- ✓ Choose the information to protect
- ✓ Name your policy
- ✓ Choose locations
- ✓ Policy settings
- Review your settings

Review your settings

Template name [Edit](#)
U.K. Personally Identifiable Information (PII) Data

Policy name [Edit](#)
U.K. Personally Identifiable Information (PII) Data

Description [Edit](#)

Applies to content in these locations [Edit](#)
Exchange email
SharePoint sites
OneDrive accounts

Policy settings [Edit](#)
If the content contains these types of sensitive info: U.K., National Insurance Number (NINO)U.S. / U.K. Passport Number then notify people with a policy tip and email message.

If there are at least 10 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override.

Turn policy on after it's created? [Edit](#)
☐ Yes

[Back](#) [Create](#) [Cancel](#)

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 attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be **[answer choice]**.

	▼
allowed	
blocked without warning	
blocked, but the user can override the policy	

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be **[answer choice]**.

	▼
allowed	
blocked without warning	
blocked, but the user can override the policy	

Correct Answer:

Answer Area

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be **[answer choice]**.

	▼
allowed	
blocked without warning	
blocked, but the user can override the policy	

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be **[answer choice]**.

	▼
allowed	
blocked without warning	
blocked, but the user can override the policy	

References:

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

HOTSPOT -





You have a Microsoft 365 subscription that contains all the user data.

You plan to create the retention policy shown in the Choose Locations exhibit. (Click the Choose Locations tab.)

Choose locations

We'll publish the labels to the locations you choose.

- ☐ All locations. Includes content in Exchange email, Office 365 groups, OneDrive and SharePoint documents.
- ☒ Let me choose specific locations.

Status	Location	Include	Exclude
<input checked="" type="checkbox"/>	 Exchange email	1 recipient Choose recipients	- Exclude recipients
<input type="checkbox"/>	 SharePoint sites		
<input type="checkbox"/>	 OneDrive accounts		
<input checked="" type="checkbox"/>	 Office 365 groups	1 group Choose groups	- Exclude recipients

You configure the Advanced retention settings as shown in the Retention exhibit. (Click the Retention tab.)

Advanced retention

Keyword query editor

merger
acquisition
takeover

^ Actions

When content matches the conditions, perform the following actions.

Retention actions

☒ Retain the content ⓘ

For this long... ▾

5

years ▾

Do you want us to delete it after this time?

☒ Yes ☐ No

☐ Don't retain the content. Just delete it if it's older than ⓘ

1

years ▾

Retain or delete the content based on

when it was created ▾ ⓘ

The locations specified in the policy include the groups shown in the following table.

Location	Include
Exchange email	A distribution group named LegalDL
Office 365 groups	A security group named LegalSG

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
Any file stored in the Microsoft SharePoint Online group library by a user in the LegalSG group will be stored for five years, and then deleted.	<input type="radio"/>	<input type="radio"/>
An email message that contains the word takeover and is sent by a user in the LegalDL group will be deleted automatically after five years.	<input type="radio"/>	<input type="radio"/>
A user sends an email message that contains the word takeover. The following week, the user is added to the LegalDL group. The message will be deleted automatically after five years.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Any file stored in the Microsoft SharePoint Online group library by a user in the LegalSG group will be stored for five years, and then deleted.	<input type="radio"/>	<input checked="" type="radio"/>
An email message that contains the word takeover and is sent by a user in the LegalDL group will be deleted automatically after five years.	<input checked="" type="radio"/>	<input type="radio"/>
A user sends an email message that contains the word takeover. The following week, the user is added to the LegalDL group. The message will be deleted automatically after five years.	<input checked="" type="radio"/>	<input type="radio"/>

References:

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

HOTSPOT -

You have retention policies in Microsoft 365 as shown in the following table.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

Policy1 is configured as shown in the Policy1 exhibit. (Click the Policy1 tab.)

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... 7 years

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

2 years

Delete the content based on when it was created ⓘ

Need more options?

☐ Use advanced retention settings ⓘ

Back

Next

Cancel

Policy2 is configured as shown in the Policy2 exhibit. (Click the Policy2 tab.)

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... 4 years

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 ⓘ

2 years

Need more options?

☐ Use advanced retention settings ⓘ

Back

Next

Cancel

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 a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	<input checked="" type="radio"/>	<input type="radio"/>
	If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	<input checked="" type="radio"/>	<input type="radio"/>
	If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	<input checked="" type="radio"/>	<input type="radio"/>

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or-what-takes-precedence>

Question #17

Topic 3

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy.

What should you configure?

- A. incident reports
- B. actions
- C. exceptions
- D. user overrides

Correct Answer: D

References:

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

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

- A. From the Security & Compliance admin center, create an eDiscovery case.
- B. From the Exchange admin center, create a mail flow rule.
- C. From the Security & Compliance admin center, start a message trace.
- D. From Microsoft Cloud App Security, create an access policy.

Correct Answer: A

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/ediscovery-cases#step-2-create-a-new-case>

You have a Microsoft 365 E5 subscription.

You run an eDiscovery search that returns the following Azure Rights Management (Azure RMS) encrypted content:

- ☞ Microsoft Exchange emails
- ☞ Microsoft OneDrive documents
- ☞ Microsoft SharePoint documents

Which content can be decrypted when you export the eDiscovery search results?

- A. Exchange emails only
- B. SharePoint documents, OneDrive documents, and Exchange emails
- C. OneDrive documents only
- D. SharePoint documents and OneDrive documents only
- E. SharePoint documents only

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/export-search-results?view=o365-worldwide>

You have a Microsoft 365 subscription.

You plan to connect to Microsoft Exchange Online PowerShell and run the following cmdlets:

- Search-MailboxAuditLog
- Test-ClientAccessRule
- Set-GroupMailbox

Get-Mailbox -

▪

Which cmdlet will generate an entry in the Microsoft Office 365 audit log?

- A. Search-MailboxAuditLog
- B. Test-ClientAccessRule
- C. Set-GroupMailbox
- D. Get-Mailbox

Correct Answer: C

Reference:

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

HOTSPOT -

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Office 365 role group
User1	None	Compliance data administrator
User2	Global administrator	None

You create a retention label named Label1 that has the following configurations:

- Retains content for five years
- Automatically deletes all content that is older than five years

You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

- Applies to content that contains the word Merger
- Specifies the OneDrive accounts and SharePoint sites locations

You run the following command.

```
Set-RetentionCompliancePolicy Policy1 -RestrictiveRetention $true -Force
```

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	<input type="radio"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input type="radio"/>
User2 can add the word Acquisition to Policy1.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can add the word Acquisition to Policy1.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps>

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2.

On September 5, 2019, you create and enforce a terms of use (ToU) in the tenant. The ToU has the following settings:

- ☞ Name: Terms1
- ☞ Display name: Terms1 name
- ☞ Require users to expand the terms of use: Off
- ☞ Require users to consent on every device: Off
- ☞ Expire consents: On
- ☞ Expire starting on: October 10, 2019
- ☞ Frequency: Monthly

User1 accepts Terms1 on September 5, 2019. User2 accepts Terms1 on October 5, 2019.

When will Terms1 expire for the first time for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:	<div><div></div><div>▼</div></div> <div><div>October 5, 2019</div><div>October 10, 2019</div><div>November 5, 2019</div><div>November 10, 2019</div></div>
User2:	<div><div></div><div>▼</div></div> <div><div>October 5, 2019</div><div>October 10, 2019</div><div>November 5, 2019</div><div>November 10, 2019</div></div>

Answer Area

Correct Answer:

User1:	<div><div></div><div>▼</div></div> <div><div>October 5, 2019</div><div>October 10, 2019</div><div>November 5, 2019</div><div>November 10, 2019</div></div>
User2:	<div><div></div><div>▼</div></div> <div><div>October 5, 2019</div><div>October 10, 2019</div><div>November 5, 2019</div><div>November 10, 2019</div></div>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

Your company uses on-premises Windows Server File Classification Infrastructure (FCI). Some documents on the on-premises file servers are classified as

Confidential.

You migrate the files from the on-premises file servers to Microsoft SharePoint Online.

You need to ensure that you can implement data loss prevention (DLP) policies for the uploaded files based on the Confidential classification.

What should you do first?

- A. From the SharePoint admin center, configure hybrid search.
- B. From the SharePoint admin center, create a managed property.
- C. From the Security & Compliance Center PowerShell, run the New-DataClassification cmdlet.
- D. From the Security & Compliance Center PowerShell, run the New-DlpComplianceRule cmdlet.

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-dlp/new-dataclassification?view=exchange-ps>

You have a Microsoft 365 subscription.

From the Microsoft 365 compliance center, you create a content search of all the mailboxes that contain the word ProjectX.

You need to export the results of the content search.

What do you need to download the report?

- A. a certification authority (CA) certificate
- B. an export key
- C. a password
- D. a user certificate

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results>

HOTSPOT -

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

You have three applications named App1, App2, and App3. The apps use files that have the same file extensions.

Your company uses Windows Information Protection (WIP). WIP has the following configurations:

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

From App1, you create a file named File1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

You can open File1 from:

App1 only
App1 and App2 only
App1 and App3 only
App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

App1 only
App3 only
App1 and App2 only
App2 and App3 only
App1, App2, and App3

Answer Area

You can open File1 from:

App1 only
App1 and App2 only
App1 and App3 only
App1, App2 and App3

Correct Answer:

If you open File1 in App1, App2, and App3, an action will be logged for:

App1 only
App3 only
App1 and App2 only
App2 and App3 only
App1, App2, and App3

References:

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure>

HOTSPOT -

You have a Microsoft 365 subscription.

You have a group named Support. Users in the Support group frequently send email messages to external users.

The manager of the Support group wants to randomly review messages that contain attachments.

You need to provide the manager with the ability to review messages that contain attachments sent from the Support group users to external users. The manager must have access to only 10 percent of the messages.

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

To meet the goal for the manager, create:

	▼
A label policy	
A retention policy	
A supervision policy	
An alert policy	
MyAnalytics	

To review the messages, the manager must use:

	▼
A message trace	
An eDiscovery case	
MyAnalytics	
Outlook Web App	

Answer Area

Correct Answer:

To meet the goal for the manager, create:

	▼
A label policy	
A retention policy	
A supervision policy	
An alert policy	
MyAnalytics	

To review the messages, the manager must use:

	▼
A message trace	
An eDiscovery case	
MyAnalytics	
Outlook Web App	

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/supervision-policies>

Your company has a Microsoft 365 subscription.

You implement Microsoft Azure Information Protection.

You need to automatically protect email messages that contain the word Confidential in the subject line.

What should you create?

- A. a mail flow rule from the Exchange admin center
- B. a message trace from the Security & Compliance admin center
- C. a supervision policy from the Security & Compliance admin center
- D. a sharing policy from the Exchange admin center

Correct Answer: A

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-exo-rules>

You have a Microsoft 365 subscription.

You need to investigate user activity in Microsoft 365, including from where users signed in, which applications were used, and increases in activity during the past month. The solution must minimize administrative effort.

Which admin center should you use?

- A. Azure ATP
- B. Security & Compliance
- C. Cloud App Security
- D. Flow

Correct Answer: B

References:

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

HOTSPOT -

A user named User1 has files in Microsoft OneDrive as shown in the following table.

Name	Date created	Date last modified
File1	January 1, 2019	January 16, 2019
File2	January 15, 2019	January 20, 2019

On February 1, 2019, you apply a retention policy named Policy1 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... months

Retain the content based on ⓘ

Do you want us to delete it after this time? ⓘ

☒ Yes ☐ No

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

years

Need more options?

☐ Use advanced retention settings ⓘ

[Back](#)[Next](#)[Cancel](#)

On February 5, 2019, User1 edits File2.

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
On March 1, 2019, File 1 is deleted automatically.	<input type="radio"/>	<input type="radio"/>
On February 20, 2019, File 2 is available in OneDrive.	<input type="radio"/>	<input type="radio"/>
On March 5, 2019, File 2 is deleted automatically.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
On March 1, 2019, File 1 is deleted automatically.	<input checked="" type="radio"/>	<input type="radio"/>
On February 20, 2019, File 2 is available in OneDrive.	<input checked="" type="radio"/>	<input type="radio"/>
On March 5, 2019, File 2 is deleted automatically.	<input checked="" type="radio"/>	<input type="radio"/>

Question #30

Topic 3

You have a Microsoft 365 subscription that uses a default domain named contoso.com.
You have two users named User1 and User2.
From the Microsoft 365 compliance center, you add User1 to the eDiscovery Manager role group.
From the Microsoft 365 compliance center, User1 creates a case named Case1.
You need to ensure that User1 can add User2 as a case member. The solution must use the principle of least privilege.
To which role group should you add User2?

- A. eDiscovery Manager
- B. eDiscovery Administrator
- C. Security Administrator

Correct Answer: A

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/add-or-remove-members-from-a-case-in-advanced-ediscovery?view=o365-worldwide>

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You sign up for Microsoft Store for Business.
The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	None
User2	Basic Purchaser	None
User3	None	Application administrator
User4	None	Cloud application administrator
User5	None	None

Microsoft Store for Business has the following Shopping behavior settings:

- ☞ Allow users to shop is set to On.
- ☞ Make everyone a Basic Purchaser is set to Off.

You need to identify which users can install apps from the Microsoft Store for Business private store.
Which users should you identify?

- A. User1 and User2 only
- B. User1 only
- C. User1, User2, User3, and User4 only
- D. User3 and User4 only
- E. User1, User2, User3, User4, and User5

Correct Answer: A

Allow users to shop controls the shopping experience in Microsoft Store for Education. When this setting is on, Purchasers and Basic Purchasers can purchase products and services from Microsoft Store for Education.

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business>

You have a Microsoft 365 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

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

You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable

Information (PII) from being emailed to users outside your organization.

To which users can User1 send documents that contain PII?

- A. User2 only
- B. User2 and User3 only
- C. User2, User3, and User4 only
- D. User2, User3, User4, and User5

Correct Answer: B

Guest accounts are considered "outside your organization". Users who have non-guest accounts in a host organization's Active Directory or Azure Active

Directory tenant are considered as people inside the organization.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide>

HOTSPOT -

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

Name	Role
User1	Exchange administrator
User2	Security administrator
User3	None

You run the following cmdlet.

```
Set-MailboxAuditBypassAssociation -Mailbox User2
```

```
-AuditByPassEnabled $true
```

The users perform the following actions:

- ⇒ User1 accesses an item in the mailbox of User2.
- ⇒ User2 modifies a mailbox item in the mailbox of User3.
- ⇒ User3 signs in to her mailbox.

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
The action performed by User1 is audited.	<input type="radio"/>	<input type="radio"/>
The action performed by User2 is audited.	<input type="radio"/>	<input type="radio"/>
The action performed by User3 is audited.	<input type="radio"/>	<input type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
The action performed by User1 is audited.	<input checked="" type="radio"/>	<input type="radio"/>
The action performed by User2 is audited.	<input type="radio"/>	<input checked="" type="radio"/>
The action performed by User3 is audited.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/powershell/module/exchange/set-mailboxauditbypassassociation?view=exchange-ps>

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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Exchange admin center, you create a data loss prevention (DLP) policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

In Microsoft 365, you can create a data loss prevention (DLP) policy in two different admin centers:

🔗 In the Security & Compliance admin center (now known as the Microsoft 365 Compliance Center), you can create a single DLP policy to help protect content in

SharePoint, OneDrive, Exchange, Teams, and now Endpoint Devices.

🔗 In the Exchange admin center, you can create a DLP policy to help protect content only in Exchange.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers?view=o365-worldwide>

HOTSPOT -

You have a Microsoft 365 subscription.

Your network uses an IP address space of 51.40.15.0/24.

An Exchange Online administrator recently created a role named Role1 from a computer on the network.

You need to identify the name of the administrator by using an audit log search.

For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Activities to search for:

	▼
Exchange mailbox activities	
Site administration activities	
Show results for all activities	
Role administration activities	

Field to filter by:

	▼
Item	
User	
Detail	
IP address	

Answer Area

Correct Answer:

Activities to search for:

	▼
Exchange mailbox activities	
Site administration activities	
Show results for all activities	
Role administration activities	

Field to filter by:

	▼
Item	
User	
Detail	
IP address	

You have a Microsoft 365 subscription that uses Microsoft 365 compliance center retention policies.

You implement a preservation lock on a retention policy that is assigned to all executive users.

Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point?

- A. Add locations to the policy
- B. Reduce the duration of policy
- C. Remove locations from the policy
- D. Extend the duration of the policy
- E. Disable the policy

Correct Answer: AD

You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.

What should you create to ensure that the DLP policy can detect the customer IDs?

- A. a sensitive information type
- B. a sensitivity label
- C. a PowerShell script
- D. a retention label

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide>

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

You need to ensure that User1 can search the Microsoft 365 audit logs from the Security & Compliance admin center.

Which role should you assign to User1?

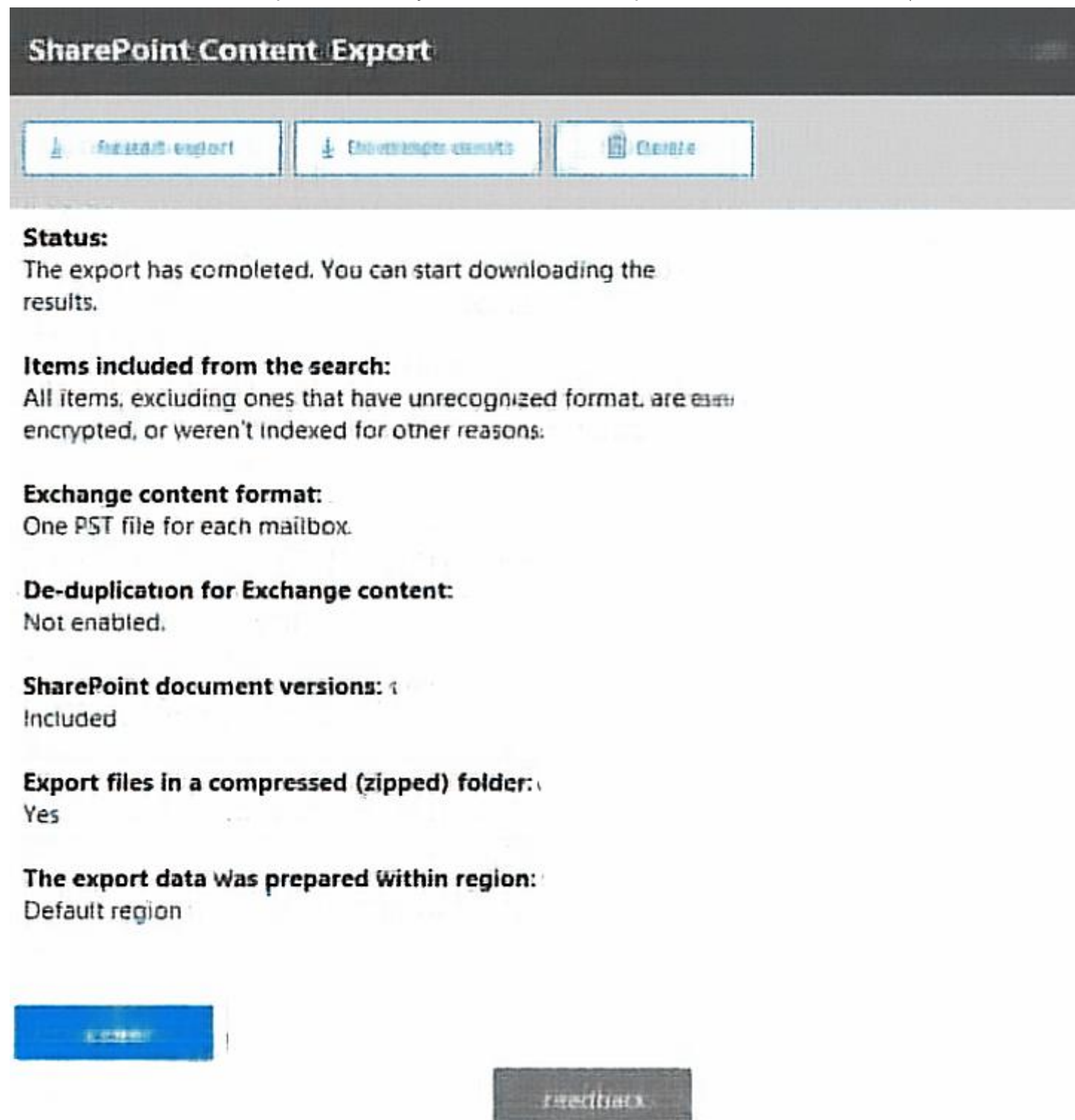
- A. View-Only Audit Logs in the Security & Compliance admin center
- B. View-Only Audit Logs in the Exchange admin center
- C. Security reader in the Azure Active Directory admin center
- D. Security Reader in the Security & Compliance admin center

Correct Answer: B

Reference:

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

From the Microsoft 365 compliance center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)



What will be excluded from the export?

- A. a 10-MB XLSX file
- B. a 5-MB MP3 file
- C. a 5-KB RTF file
- D. an 80-MB PPTX file

Correct Answer: B

Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.

Note:

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

1. a 5-MB MP3 file
2. a 12-MB BMP file

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

1. a 60-MB DOCX file
2. a 100-MB VSDX file
3. a 75-MB PDF file

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide>

<https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report>

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint Online.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

- A. the locations of the DLP policy
- B. the user overrides of the DLP policy rule
- C. the status of the DLP policy
- D. the conditions of the DLP policy rule

Correct Answer: A

References:

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

You have a Microsoft 365 subscription.

You need to view the IP address from which a user synced a Microsoft SharePoint Online library.

What should you do?

- A. From the SharePoint Online admin center, view the usage reports.
- B. From the Microsoft 365 compliance center, perform an audit log search.
- C. From the Microsoft 365 admin center, view the usage reports.
- D. From the Microsoft 365 admin center, view the properties of the user's user account.

Correct Answer: B

References:

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

HOTSPOT -

Your network contains an Active Directory domain named contoso.com. The domain contains the file servers shown in the following table.

Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

A file named File1.abc is stored on Server1. A file named File2.abc is stored on Server2. Three apps named App1, App2 and App3 are installed on a Windows 10 device named Device1. All three apps open files that have the .abc file extension.

You implement Windows Information Protection (WIP) by creating a policy named Policy1 that has the following configuration:

- Exempt apps: App2
- Protected apps: App1
- Windows Information Protection mode: Block
- Network boundary: IPv4 range of: 192.168.1.1-192.168.1.255

You ensure that Policy1 applies to Device1.

You need to identify the apps from which you can open File1.abc.

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
You can open File1.abc in App1.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App2.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App3.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	You can open File1.abc in App1.	<input checked="" type="radio"/>	<input type="radio"/>
	You can open File1.abc in App2.	<input checked="" type="radio"/>	<input type="radio"/>
	You can open File1.abc in App3.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure>

In Microsoft 365, you configure a data loss prevention (DLP) policy named Policy1. Policy1 detects the sharing of United States (US) bank account numbers in email messages and attachments.

Policy1 is configured as shown in the exhibit. (Click the Exhibit tab.)

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content

☒ Block people from sharing and restrict access to shared content

By default, users are blocked from sending email messages to people. You can choose who has access to shared SharePoint and OneDrive content. Block these people from accessing SharePoint and OneDrive content...

☐ Everyone. Only the content owner, the last modifier, and the site admin will continue to have access

☒ Only people outside your organization. People inside your organization will continue to have access.

☐ Encrypt email messages (applies only to content in Exchange)

You need to ensure that internal users can email documents that contain US bank account numbers to external users who have an email suffix of contoso.com.

What should you configure?

- A. an exception
- B. an action
- C. a condition
- D. a group

Correct Answer: A

You need to add an exception. In the Advanced Settings of the DLP policy, there is an 'Add Exception' button. This gives you several options that you can select as the exception. One of the options is 'except when recipient domain is'. Select that option and enter the domain name: contoso.com.

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies#how-dlp-policies-work>

HOTSPOT -

You have a document in Microsoft OneDrive that is encrypted by using Microsoft Azure Information Protection as shown in the following exhibit.

Protection settings ⓘ

Azure (cloud key)

HYOK (AD RMS)

Select the protection action type ⓘ

- ☒ Set permissions
- ☐ Set user-defined permissions (Preview)

USERS**PERMISSIONS**

M365x901434.onmicrosoft.com

Co-Owner

...

[+ Add permissions](#)**Content expiration**

Always

Never

By days

Number of days the content is valid

30

**Allow offline access**

Balance security requirements (includes access after revocation) with the flexibility to open protected content without an Internet connection. [More information and recommended settings](#)

Always

Never

By days

Number of days the content is available without an Internet connection

7



Protection template ID - template id is automatically generated after template is saved

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 copy the file from OneDrive to your internet connected computer, you [answer choice].

▼

cannot open the document
can open the document indefinitely
can open the document for up to 7 days
can open the document for up to 30 days

If you email the document to a user outside your organization, the user [answer choice].

▼

cannot open the document
can open the document indefinitely
can open the document for up to 7 days
can open the document for up to 30 days

Correct Answer:

Answer Area

If you copy the file from OneDrive to your internet connected computer, you [answer choice].

	▼
cannot open the document	
can open the document indefinitely	
can open the document for up to 7 days	
can open the document for up to 30 days	

If you email the document to a user outside your organization, the user [answer choice].

	▼
cannot open the document	
can open the document indefinitely	
can open the document for up to 7 days	
can open the document for up to 30 days	

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection>

HOTSPOT -

You have a Microsoft Office 365 subscription.

You need to delegate eDiscovery tasks as shown in the following table.

User	Task
User1	<ul style="list-style-type: none">• Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content.• View only the eDiscovery cases created by User1.• Configure case settings.• Place content on hold.
User2	<ul style="list-style-type: none">• View the eDiscovery cases created by both User1 and User2.• Export data from Advanced eDiscovery.

The solution must follow the principle of the least privilege.

To which role group should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

▼
eDiscovery Administrator
eDiscovery Manager
Records Management
Reviewer
Security Administrator

User2:

▼
eDiscovery Administrator
eDiscovery Manager
Records Management
Reviewer
Security Administrator

Answer Area

Correct Answer:

User1:

▼
eDiscovery Administrator
eDiscovery Manager
Records Management
Reviewer
Security Administrator

User2:

▼
eDiscovery Administrator
eDiscovery Manager
Records Management
Reviewer
Security Administrator

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions>

You have a Microsoft 365 subscription.

You need to identify which administrative users performed eDiscovery searches during the past week.

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

- A. Perform a content search
- B. Create a supervision policy
- C. Create an eDiscovery case
- D. Perform an audit log search

Correct Answer: *D*

HOTSPOT -

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

Choose the types of content to protect

This policy will protect that matches these requirements. You can choose sensitive info types and existing labels

Content contains

Any of these

Sensitive info type

Credit Card Number

Match accuracy

min

85

max

100

x

Retention labels

1 year

x

Add

+ Add group

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

DLP1 cannot be applied to [answer choice].

	▼
Exchange email	
SharePoint sites	
OneDrive accounts	

DLP1 will be applied only to documents that have [answer choice].

	▼
both a credit card number and the 1 year label applied	
either a credit card number or the 1 year label applied	
between 85 and 100 credit card numbers	

Correct Answer:

Answer Area

DLP1 cannot be applied to [answer choice].

	▼
Exchange email	
SharePoint sites	
OneDrive accounts	

DLP1 will be applied only to documents that have [answer choice].

	▼
both a credit card number and the 1 year label applied	
either a credit card number or the 1 year label applied	
between 85 and 100 credit card numbers	

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

Reference:

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

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

You have a Microsoft 365 subscription.

From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-ComplianceSecurityFilter cmdlet with the appropriate parameters.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-filtering-for-content-search> <https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-content-search/new-compliancesecurityfilter?view=exchange-ps>

HOTSPOT -

You have a Microsoft 365 subscription that uses a default domain named contoso.com. The domain contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2

The domain contains the devices shown in the following table.

Name	Compliance status
Device1	Compliant
Device2	Noncompliant

The domain contains conditional access policies that control access to a cloud app named App1. The policies are configured as shown in the following table.

Name	Includes	Excludes	Device state includes	Device state excludes	Grant
Policy1	Group1	None	All device states	Device marked as compliant	Block access
Policy2	Group1	Group2	None	None	Block Access
Policy3	Group1	None	All device states	None	Grant access

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 access App1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from Device2.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Correct Answer: User1 can access App1 from Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access App1 from Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access App1 from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

Note: Block access overrides Grant access

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access>

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.

To which location can the policy be applied?

- A. OneDrive accounts
- B. Exchange email
- C. Teams chat and channel messages
- D. SharePoint sites

Correct Answer: B

You enable the Azure AD Identity Protection weekly digest email.

You create the users shown in the following table.

Name	Role
Admin1	Security reader
Admin2	User administrator
Admin3	Security administrator
Admin4	Compliance administrator

Which users will receive the weekly digest email automatically?

- A. Admin2, Admin3, and Admin4 only
- B. Admin1, Admin2, Admin3, and Admin4
- C. Admin2 and Admin3 only
- D. Admin3 only
- E. Admin1 and Admin3 only

Correct Answer: E

By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or Security Administrators will automatically be added to the recipients list.

HOTSPOT -

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

A user named User1 has files on a Windows 10 device as shown in the following table.

Name	Text in file
File1.docx	Importing and exporting is easy. For import, you need a source, and for export, you need a destination.
File2.docx	You must declare what you want to import. Dangerous items cannot be imported. If you want to import valuables, you must pay customs.
File3.docx	IM are initials for instant messaging. You can use Microsoft Skype for IM, but there are also other IM programs.

In Azure Information Protection, you create a label named Label1 that is configured to apply automatically. Label1 is configured as shown in the following exhibit.

Condition: Condition1

Default Directory - Azure Information Protection

Save Discard Delete

Choose the type of condition ⓘ

Information Types Custom

* Name

Condition1 ✓

* Match exact phrase or pattern ⓘ

im ✓

Match as a regular expression

Off On

Match with case sensitivity

Off On

* Minimum number of occurrences

2

Count occurrences with unique values only

Off On

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Label1 applies to File1.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File2.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File3.docx.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	Label1 applies to File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
	Label1 applies to File2.docx.	<input checked="" type="radio"/>	<input type="radio"/>
	Label1 applies to File3.docx.	<input type="radio"/>	<input checked="" type="radio"/>

The phrase to match is "im" and it is case sensitive. The phrase must also appear at least twice.

Box 1: No -
File1.docx contain the word "import" once only

Box 2: Yes -
File2.docx contains two occurrences of the word "import" as well as the word "imported"

Box 3: No -
File3.docx contains "IM" but his is not the correct letter case.

References:
<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

HOTSPOT -

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

Three files were created on February 1, 2019, as shown in the following table.

Name	Stored in
File1	Microsoft OneDrive
File2	A Microsoft SharePoint library
File3	Microsoft Exchange Online email

On March 1, 2019, you create two retention labels named Label1 and Label2.

The settings for Label1 are configured as shown in the Label1 exhibit. (Click the Label1 tab.)

Label settings

Retention ⓘ



On

When this label is applied to content...

☒ Retain the content ⓘ

For this long... ▾ 2 years ▾

What do you want to do after this time?

☐ Delete the content automatically. ⓘ

☒ Trigger a disposition review. ⓘ

Notify these people when there are items ready to review

User1@sk180818.onmicrosoft.com ×

☐ Nothing. Leave the content as is. ⓘ

☐ Don't retain the content. Just delete it if it's older than ⓘ

1 years ▾

Retain or delete the content based on when it was created ▾ ⓘ

Label classification

☐ Use label to classify content as a "Record" ⓘ

The settings for Label2 are configured as shown in the Label2 exhibit. (Click the Label2 tab.)

Label settings

Retention ⓘ



On

When this label is applied to content...

☐ Retain the content ⓘ

For this long... ▾

2

years ▾

☒ Don't retain the content. Just delete it if it's older than ⓘ

1

years ▾

Retain or delete the content based on

when it was created ▾ ⓘ

You apply the retention labels to Exchange email, SharePoint sites, and OneDrive accounts.
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
File1 will be deleted automatically on February1, 2020.	<input type="radio"/>	<input type="radio"/>
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input type="radio"/>
File3 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	<input type="radio"/>	<input checked="" type="radio"/>
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input checked="" type="radio"/>
File3 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -
Retention overrides deletion.

Box 2: No -
Content in a document library will be moved to the first-stage Recycle Bin within 7 days of disposition, and then permanently deleted another 93 days after that.
Thus 100 days in total.

Box 3: No -
Items in an Exchange mailbox will be permanently deleted within 14 days of disposition.

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/labels> <https://docs.microsoft.com/en-us/office365/securitycompliance/disposition-reviews>

DRAG DROP -

You have a Microsoft 365 subscription.

In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:

- ☞ Block emails that contain financial data.
- ☞ Display the following policy tip text: Message blocked.

From the Microsoft 365 compliance center, you create a DLP policy named Policy2 that has the following configurations:

- ☞ Use the following location: Exchange email.
- ☞ Display the following policy tip text: Message contains sensitive data.
- ☞ When a user sends an email, notify the user if the email contains health records.

What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Results

The email will be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and the user will receive the policy tip: Message blocked.

The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records:

Result

When the user sends an email that contains only financial data:

Result

Correct Answer:

Results

The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and the user will receive the policy tip: Message blocked.

The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records:

The email will be blocked, and the user will receive the policy tip: Message blocked.

When the user sends an email that contains only financial data:

The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked.

If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the

Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.

Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers>

DRAG DROP -

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD). The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2016	File Server Resource Manager (FSRM)
Server2	Windows Server 2016	None

You use Azure Information Protection.

You need to ensure that you can apply Azure Information Protection labels to the file stores on Server1.

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

- Authorize Server1.
- Install the Microsoft Rights Management connector on Server2.
- Install a certificate on Server2.
- Install a certificate on Server1.
- Register a service principal name for Server1.
- Run GenConnectorConfig.ps1 on Server1.
- Run GenConnectorConfig.ps1 on Server2.

Answer Area

Correct Answer:

Actions

-
-
- Install a certificate on Server2.
- Install a certificate on Server1.
- Register a service principal name for Server1.
-
- Run GenConnectorConfig.ps1 on Server2.

Answer Area

- Install the Microsoft Rights Management connector on Server2.
- Authorize Server1.
- Run GenConnectorConfig.ps1 on Server1.

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector> <https://docs.microsoft.com/en-us/azure/information-protection/configure-servers-rms-connector>

You have a Microsoft 365 E5 subscription.

Users have the devices shown in the following table.

Name	Platform	Owner	Enrolled in Microsoft Endpoint Manager
Device1	Android	User1	Yes
Device2	Android	User1	No
Device3	iOS	User1	No
Device4	Windows 10	User2	Yes
Device5	Windows 10	User2	No
Device6	iOS	User2	Yes

On which devices can you manage apps by using app configuration policies in Microsoft Endpoint Manager?

- A. Device1, Device4, and Device6
- B. Device2, Device3, and Device5
- C. Device1, Device2, Device3, and Device6
- D. Device1, Device2, Device4, and Device5

Correct Answer: C

You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

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

You have a Microsoft 365 subscription.

From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group. You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-AzureRmRoleAssignment cmdlet with the appropriate parameters.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

References:

<https://docs.microsoft.com/en-us/powershell/module/azurerms.resources/new-azurermroleassignment?view=azurermps-6.13.0>

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

You have a Microsoft 365 subscription.

From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Security & Compliance admin center, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains two users named Admin1 and Admin2.

All users are assigned a Microsoft 365 Enterprise E5 license and auditing is turned on.

You create the audit retention policy shown in the exhibit. (Click the Exhibit tab.)

New audit retention policy



Name *:

Policy1

Description

Record Types

AzureActiveDirectory ▾

Activities

Added user, Deleted user, Reset user password, Changed user password, Changed user license, ...(7) ▾

Users:

Admin1 ×

Duration *:

☒ 90 Days

☐ 6 Months

☐ 1 Year

Priority *:

100

Save

Cancel

After Policy1 is created, the following actions are performed:

⇒ Admin1 creates a user named User1.

⇒ Admin2 creates a user named User2.

How long will the audit events for the creation of User1 and User2 be retained? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

▼

0 days

30 days

90 days

180 days

365 days

User2:

▼

0 days

30 days

90 days

180 days

365 days

Answer Area

Question #60

Topic 3

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. You sign for Microsoft Store for Business. The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	None
User2	Basic Purchaser	None
User3	None	Application administrator
User4	None	Cloud application administrator

Microsoft Store for Business has the following Shopping behavior settings:

- ☞ Allow users to shop is set to On
- ☞ Make everyone a Basic Purchaser is set to Off

You need to identify which users can install apps from the Microsoft for Business private store. Which users should you identify?

- A. User3 only
- B. User1 only
- C. User1 and User2 only
- D. User3 and User4 only

Correct Answer: C

Allow users to shop controls the shopping experience in Microsoft Store for Education. When this setting is on, Purchasers and Basic Purchasers can purchase products and services from Microsoft Store for Education.

References:

<https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business>

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

In the tenant, you create a user named User1.

You need to ensure that User1 can publish retention labels from the Microsoft 365 compliance center. The solution must use the principle of least privilege.

To which role group should you add User1?

- A. Security Administrator
- B. Records Management
- C. Compliance Administrator
- D. eDiscovery Manager

Correct Answer: B

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/file-plan-manager>

You plan to use the Security & Compliance admin center to import several PST files into Microsoft 365 mailboxes.

Which three actions should you perform before you import the data? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From the Exchange admin center, create a public folder.
- B. Copy the PST files by using AzCopy.
- C. From the Exchange admin center, assign admin roles.
- D. From the Microsoft Azure portal, create a storage account that has a blob container.
- E. From the Microsoft 365 admin center, deploy an add-in.
- F. Create a mapping file that uses the CSV file format.

Correct Answer: BCF

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/use-network-upload-to-import-pst-files>

HOTSPOT -

You have a Microsoft 365 tenant.

You plan to create a retention policy as shown in the following exhibit.

Create a policy to retain what you want and get rid of what you don't.

- ✓ Name your policy
- ✓ Settings
- ✓ Choose locations
- Review your settings

Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name: contoso [Edit](#)

Description: [Edit](#)

Applies to content in these locations [Edit](#)

- Exchange email
- OneDrive accounts
- SharePoint sites
- Office 365 groups

Settings [Edit](#)

Retention period: Don't retain content, but delete it if it's older than 7 years

⚠ Content that's currently older than this will be deleted after you turn on the policy

[Back](#) [Save for later](#) [Create this policy](#) [Cancel](#)

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

Microsoft SharePoint files that are affected by the policy will be [answer choice].

	▼
recoverable for up to seven years	
deleted seven years after they were created	
retained for only seven years from when they were created	

Once the policy is created, [answer choice].

	▼
some data may be deleted immediately	
data will be retained for a minimum of seven years	
users will be prevented from permanently deleting email messages for seven years	

Correct Answer:

Answer Area

Microsoft SharePoint files that are affected by the policy will be [answer choice].

	▼
recoverable for up to seven years	
deleted seven years after they were created	
retained for only seven years from when they were created	

Once the policy is created, [answer choice].

	▼
some data may be deleted immediately	
data will be retained for a minimum of seven years	
users will be prevented from permanently deleting email messages for seven years	

Question #64

Topic 3

You deploy Microsoft Azure Information Protection.

You need to ensure that a security administrator named SecAdmin1 can always read and inspect data protected by Azure Rights Management (Azure RMS).

What should you do?

- A. From the Security & Compliance admin center, add SecAdmin1 to the eDiscovery Manager role group.
- B. From the Azure Active Directory admin center, add SecAdmin1 to the Security Reader role group.
- C. From the Security & Compliance admin center, add SecAdmin1 to the Compliance Administrator role group.
- D. From Windows PowerShell, enable the super user feature and assign the role to SecAdmin1.

Correct Answer: D

The super user feature of the Azure Rights Management service from Azure Information Protection ensures that authorized people and services can always read and inspect the data that Azure Rights Management protects for your organization. However, the super user feature is not enabled by default. The PowerShell cmdlet Enable-AadrmSuperUserFeature is used to manually enable the super user feature.

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-super-users>

Question #65

Topic 3

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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Cloud App Security admin center, you create an access policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

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

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

You create a Microsoft Defender for Identity instance named Contoso.

The tenant contains the users shown in the following table.

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

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

Solution: You instruct User4 to modify the Defender for Identity sensor configuration.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Only Azure ATP administrators can modify the sensors.

Any global administrator or security administrator on the tenant's Azure Active Directory is automatically an Azure ATP administrator.

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-role-groups>

HOTSPOT -

You have a Microsoft 365 tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Azure AD role	Office 365 role group
User1	Application administrator	eDiscovery Administrator
User2	Application administrator	Organization Management
User3	Cloud application administrator	Global Administrator
User4	Compliance administrator	eDiscovery Manager

You have the eDiscovery cases shown in the following table.

Name	Created by
Case1	User1
Case2	User2
Case3	User3
Case4	User4

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 delete Case4.	<input type="radio"/>	<input type="radio"/>
User3 can add members to Case2.	<input type="radio"/>	<input type="radio"/>
User4 can close Case3.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	User1 can delete Case4.	<input checked="" type="radio"/>	<input type="radio"/>
	User3 can add members to Case2.	<input type="radio"/>	<input checked="" type="radio"/>
	User4 can close Case3.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions>

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

- A. From Microsoft Cloud App Security, create an activity policy.
- B. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- C. From the Exchange admin center, start a mail flow message trace.
- D. From the Security & Compliance admin center, create an eDiscovery case.

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds?view=o365-worldwide>

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

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

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

You create a Microsoft Defender for Identity instance named Contoso.

The tenant contains the users shown in the following table.

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

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

Solution: You instruct User3 to modify the Defender for Identity sensor configuration.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Only Azure ATP administrators can modify the sensors.

Any global administrator or security administrator on the tenant's Azure Active Directory is automatically an Azure ATP administrator.

Reference:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-role-groups>

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant named sk180818.onmicrosoft.com. The tenant contains the users shown in the following table.

Name	Username	Type
User1	User1@sk180818.onmicrosoft.com	Member
User2	User2@sk180818.onmicrosoft.com	Member
User3	User3@sk180818.onmicrosoft.com	Member
User4	User4@gmail.com	Guest

In Azure Information Protection, you create a label named Label1 as shown in the following exhibit.

Protection settings ⓘ

Azure (cloud key)

HYOK (AD RMS)

Select the protection action type ⓘ

☒ Set permissions

☐ Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
sk180818.onmicrosoft.com	Reviewer
User1@sk180818.onmicrosoft.com	Co-Owner
User2@sk180818.onmicrosoft.com	Co-Author

+ Add permissions

Label1 is applied to a file named File1.

You send File1 as an email attachment to User1, User2, User3, and User4.

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
User2 can modify File1.	<input type="radio"/>	<input type="radio"/>
User3 can print File1.	<input type="radio"/>	<input type="radio"/>
User4 can read File1.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements

Yes

No

Correct Answer:

User2 can modify File1.

☒☐

User3 can print File1.

☐☒

User4 can read File1.

☐☒

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#rights-included-in-permissions-levels>

HOTSPOT -

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The company stores 2 TBs of data in SharePoint Online document libraries. The tenant has the labels shown in the following table.

Name	Type
Label1	Sensitivity label
Label2	Retention label
Label3	Azure Information Protection label

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
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>
Label2 can now be used as a retention label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	<input checked="" type="radio"/>	<input type="radio"/>
Label2 can now be used as a retention label or an Azure Information Protection label.	<input type="radio"/>	<input checked="" type="radio"/>
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	<input checked="" type="radio"/>	<input type="radio"/>

HOTSPOT -

You create a Microsoft 365 subscription.

Your company's privacy policy states that user activities must NOT be audited.

You need to disable audit logging in Microsoft 365.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

	▼
Set-AdminAuditLogConfig	
Set-AuditConfig	
Set-AuditConfigurationRule	

	▼
-AdminAuditLogEnabled	
-AdminAuditLogParameters	
-LogLevel	
-UnifiedAuditLogIngestionEnabled	

\$false

Correct Answer:

Answer Area

	▼
Set-AdminAuditLogConfig	
Set-AuditConfig	
Set-AuditConfigurationRule	

	▼
-AdminAuditLogEnabled	
-AdminAuditLogParameters	
-LogLevel	
-UnifiedAuditLogIngestionEnabled	

\$false

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/turn-audit-log-search-on-or-off>

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

Name	Type
Mailbox1	Microsoft Exchange Online mailbox
Account1	Microsoft OneDrive account
Site1	Microsoft SharePoint Online site
Channel1	Microsoft Teams channel

To which resources can you apply a sensitivity label by using an auto-labeling policy?

- A. Mailbox1 and Site1 only
- B. Mailbox1, Account1, and Site1 only
- C. Account1 and Site1 only
- D. Mailbox1, Account1, Site1, and Channel1
- E. Account1, Site1, and Channel1 only

Correct Answer: E

Reference:

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

HOTSPOT -

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Users who can assign Retention1:

▼

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

Users who can assign Retention2:

▼

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

Answer Area

Users who can assign Retention1:

▼

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

Correct Answer:

Users who can assign Retention2:

▼

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

Reference:

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

You have a Microsoft 365 subscription.

You need to grant a user named User1 access to download compliance reports from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do?

- A. Add User1 to the Service Assurance User role group.
- B. Create a new role group that has the Preview role and add User1 to the role group.
- C. Add User1 to the Compliance Administrator role group.
- D. Add User1 to the Security Reader role group.

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/download-existing-reports?view=o365-worldwide>

You have a Microsoft 365 subscription.

Some users have iPads that are managed by your company.

You plan to prevent the iPad users from copying corporate data in Microsoft Word and pasting the data into other applications.

What should you create?

- A. A conditional access policy.
- B. A compliance policy.
- C. An app protection policy.
- D. An app configuration policy.

Correct Answer: C

References:

<https://docs.microsoft.com/en-us/intune/app-protection-policy>

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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Azure portal, you create a Microsoft Azure Information Protection label and an Azure Information Protection policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

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

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

You create a Microsoft Defender for Identity instance named Contoso.

The tenant contains the users shown in the following table.

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

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

Solution: You instruct User1 to modify the Defender for Identity sensor configuration.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Only Azure ATP administrators can modify the sensors.

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-role-groups>

HOTSPOT -

You have a data loss prevention (DLP) policy.

You need to increase the likelihood that the DLP policy will apply to data that contains medical terms from the International Classification of Diseases (ICD-9-CM).

The solution must minimize the number of false positives.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Content contains

Any of these ▼

PII Identifiers

Sensitive info type

U.S. Social Security Number (SSN)

Instance count

min
1

max
any

Match accuracy

min
50

max
100

Add ▼

and ▼

Any of these ▼

Medical Terms

Sensitive info type

International Classification of Diseases (ICD-9-CM)

Instance count

min
1

max
any

Match accuracy

min
50

max
100

Add ▼

Content contains

Any of these ▼

PII Identifiers

Sensitive info type

U.S. Social Security Number (SSN)

Instance count

min
1

max
any

Match accuracy

min
50

max
100

Add ▼

Correct Answer:

and ▼

Any of these ▼

Medical Terms

Sensitive info type

International Classification of Diseases (ICD-9-CM)

Instance count

min
1

max
any

Match accuracy

min
50

max
100

Add ▼

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies> <https://docs.microsoft.com/en-us/office365/securitycompliance/what-the-sensitive-information-types-look-for#international-classification-of-diseases-icd-9-cm>

HOTSPOT -

From the Microsoft 365 compliance center, you create a retention policy named Policy1.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

<div>▼</div>	-Identity "Policy1"	<div>▼</div> \$true
Set-ComplianceTag		-enabled
Set-HoldCompliancePolicy		-Force
Set-RetentionCompliancePolicy		-RestrictiveRetention
Set-RetentionPolicy		-RetentionPolicyTagLinks
Set-RetentionPolicyTag		-SystemTag

Answer Area

Correct Answer:

<div>▼</div>	-Identity "Policy1"	<div>▼</div> \$true
Set-ComplianceTag		-enabled
Set-HoldCompliancePolicy		-Force
Set-RetentionCompliancePolicy		-RestrictiveRetention
Set-RetentionPolicy		-RetentionPolicyTagLinks
Set-RetentionPolicyTag		-SystemTag

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps>

You create a new Microsoft 365 subscription and assign Microsoft 365 E3 licenses to 100 users.

From the Security & Compliance admin center, you enable auditing.

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. An administrator creates a new Microsoft SharePoint site collection.
- B. An administrator creates a new mail flow rule.
- C. A user shares a Microsoft SharePoint folder with an external user.
- D. A user delegates permissions to their mailbox.
- E. A user purges messages from their mailbox.

Correct Answer: ABC

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c>

HOTSPOT -

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

Create a label to help users classify their content.

- ✓ Name your label
- ✓ Label settings
- Review your settings

Review your settings

Name [Edit](#)
6Months

Description for admins [Edit](#)

Description for users [Edit](#)

Retention [Edit](#)
6 months
Retain and Delete
Based on when it was created

[Back](#) [Create this label](#) [Cancel](#)

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

Automatically apply a label to content

- ✓ Choose label to auto-apply
- ✓ Choose conditions
- ✓ Name your policy
- Locations
- Review your settings

Detect content that matches this query:

^ Conditions

We'll apply this policy to content that matches these conditions. ⓘ

Keyword query editor

ProjectX

[Back](#) [Next](#) [Cancel](#)

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the work ProjectX.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input checked="" type="radio"/>
	Any sent email message that contains the word ProjectX will be retained for six months.	<input checked="" type="radio"/>	<input type="radio"/>
	Users are required to manually apply a label to email messages that contain the work ProjectX.	<input type="radio"/>	<input checked="" type="radio"/>

References:

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

Question #83

Topic 3

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

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

You create a Microsoft Defender for Identity instance named Contoso.

The tenant contains the users shown in the following table.

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

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

Solution: You instruct User2 to modify the Defender for Identity sensor configuration.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

HOTSPOT -

You purchase a new Microsoft 365 subscription.

You create 100 users who are assigned Microsoft 365 E3 licenses.

A manager sends you an email message asking the following questions:

☞ Question1: Who created a team named Team1 14 days ago?

☞ Question2: Who signed in to the mailbox of User1 30 days ago?

☞ Question3: Who modified the list of site collection administrators of a site 60 days ago?

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
An audit log search from the Security & Compliance admin center will provide the answer to question 1.	<input type="radio"/>	<input type="radio"/>
An audit log search from the Security & Compliance admin center will provide the answer to question 2.	<input type="radio"/>	<input type="radio"/>
An audit log search from the Security & Compliance admin center will provide the answer to question 3.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	An audit log search from the Security & Compliance admin center will provide the answer to question 1.	<input checked="" type="radio"/>	<input type="radio"/>
	An audit log search from the Security & Compliance admin center will provide the answer to question 2.	<input type="radio"/>	<input checked="" type="radio"/>
	An audit log search from the Security & Compliance admin center will provide the answer to question 3.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c>
<https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing>

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

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

You have a Microsoft 365 subscription.

From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Azure Active Directory admin center, you create a conditional access policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

From the Microsoft 365 compliance center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)

SharePoint Content_Export

Restart export Download results Delete

Status:
The export has completed. You can start downloading the results.

Items included from the search:
All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

Exchange content format:
One PST file for each mailbox.

De-duplication for Exchange content:
Not enabled.

SharePoint document versions:
Included

Export files in a compressed (zipped) folder:
Yes

The export data was prepared within region:
Default region

Close Feedback

What will be excluded from the export?

- A. a 60-MB DOCX file
- B. a 12-MB BMP file
- C. a 5-KB RTF file
- D. an 80-MB PPTX file

Correct Answer: B

Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.

Incorrect Answers:

A: DOCX is a supported Microsoft PowerPoint file format.

C: RTF is a supported Rich Text File format.

D: PPTX is a supported Microsoft PowerPoint file format.

Note:

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

1. a 5-MB MP3 file
2. a 12-MB BMP file

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

1. a 10-MB XLSX file
2. a 100-MB VSDX file
3. a 75-MB PDF file

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide>

<https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report>

Question #87

Topic 3

You have a Microsoft 365 subscription.

From the Microsoft 365 compliance center, you create a content search of a mailbox.

You need to view the content of the mail messages found by the search as quickly as possible.

What should you select from the Content search settings?

- A. Export report
- B. Export results
- C. Re-run
- D. View results

Correct Answer: B

There is no 'View Results' option. You can preview results but that will only show up to 100 emails. To guarantee you're getting all results, you'll need to export them to a PST file.

References:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/limits-for-content-search>

HOTSPOT -

From the Security & Compliance admin center, you create a retention policy named Policy1.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

▼

Set-ComplianceTag

Set-HoldCompliancePolicy

Set-RetentionCompliancePolicy

Set-RetentionPolicy

Set-RetentionPolicyTag

-Identity "Policy1"

▼

-enabled

-Force

-RestrictiveRetention

-RetentionPolicyTagLinks

-System Tag

\$true

Correct Answer:

Answer Area

▼

Set-ComplianceTag

Set-HoldCompliancePolicy

Set-RetentionCompliancePolicy

Set-RetentionPolicy

Set-RetentionPolicyTag

-Identity "Policy1"

▼

-enabled

-Force

-RestrictiveRetention

-RetentionPolicyTagLinks

-System Tag

\$true

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps>

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

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

User1 reports that he cannot access documents shared to Group1.

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

You suspect that an administrator made a change that caused User1 to be removed from Group1.

You need to identify which administrator made the change.

Which audit log activity should you search in the Security & Compliance admin center?

- A. Azure AD group administration activities æ" Removed member from group
- B. User administration activities æ" Updated user
- C. Azure AD group administration activities æ" Updated group

Correct Answer: C

You have a Microsoft 365 E5 tenant.

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

What should you do in the Microsoft 365 compliance center?

- A. Create a Data Subject Request (DSR)
- B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data
- C. Create an assessment based on the EU GDPR assessment template
- D. Create an assessment based on the Data Protection Baseline assessment template

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr#data-protection-impact-assessment> <https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-list?view=o365-worldwide>

You have a Microsoft 365 E5 tenant.

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

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

NOTE: Each correct selection is worth one point.

- A. a data loss prevention (DLP) policy
- B. a sensitivity label policy
- C. a Microsoft Cloud App Security file policy
- D. a communication compliance policy
- E. a retention label policy

Correct Answer: AD

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide>
<https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance?view=o365-worldwide>

You have a Microsoft 365 E5 tenant.

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

You need to deploy the policy.

What should you do first?

- A. Review the sensitive information in Activity explorer
- B. Turn on the policy
- C. Run the policy in simulation mode
- D. Configure Azure Information Protection analytics

Correct Answer: C

Reference:

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

You have a Microsoft 365 tenant and a LinkedIn company page.

You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.

Where can you store data from the LinkedIn connector?

- A. a Microsoft OneDrive for Business folder
- B. a Microsoft SharePoint Online document library
- C. a Microsoft 365 mailbox
- D. Azure Files

Correct Answer: C

Reference:

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

HOTSPOT -

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area**Windows 10 compliance policy**

Windows 10 and later

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

Correct Answer:

Answer Area**Windows 10 compliance policy**

Windows 10 and later

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

Reference:

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

Correct Answer:

Answer Area

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	<input checked="" type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File2.txt.	<input checked="" type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File3.xlsx.	<input checked="" type="radio"/>	<input type="radio"/>

Question #96

Topic 3

You have a Microsoft 365 E5 tenant that contains a user named User1.
You plan to implement insider risk management.
You need to ensure that User1 can perform the following tasks:

- Review alerts.
- Manage cases.
- Create notice templates.
- Review user emails by using Content explorer.

The solution must use the principle of least privilege.
To which role group should you add User1?

- A. Insider Risk Management
- B. Insider Risk Management Analysts
- C. Insider Risk Management Investigators
- D. Insider Risk Management Admin

Correct Answer: C

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide>

Question #97

Topic 3

Your company has a Microsoft 365 E5 tenant that contains a user named User1.
You review the company's compliance score.
You need to assign the following improvement action to User1: Enable self-service password reset.
What should you do first?

- A. From Compliance Manager, turn off automated testing.
- B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
- C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
- D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

Correct Answer: D

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide>
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal>

Your company has a Microsoft 365 E5 tenant.

The company must meet the requirements of the ISO/IEC 27001:2013 standard.

You need to assess the company's current state of compliance.

What should you use?

- A. eDiscovery
- B. Information governance
- C. Compliance Manager
- D. Data Subject Requests (DSRs)

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001>

You have a Microsoft 365 E5 tenant.

Users store data in the following locations:

Microsoft Teams -

-
- ⇒ Microsoft OneDrive
- ⇒ Microsoft Exchange Online
- ⇒ Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.

What is the minimum number of retention policies that you should create?

- A. 1
- B. 2
- C. 3
- D. 4

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide>

HOTSPOT -

You have a Microsoft 365 E5 tenant.

You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)

Review your settings and finish

Name

Sensitivity1

Display name

Sensitivity1

Description for users

Sensitivity1

Scope

File.Email

Encryption

Content marking

Watermark: Watermark

Header: Header

Auto-labeling

Group settings

Site settings

Auto-labeling for database columns

None

You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)

Auto-labeling policy

 Edit Policy

 Delete Policy

Policy name

Auto-labeling policy

Description

Label in simulation

Sensitivity1

Info to label

IP Address

Apply to content in these locations

Exchange email All

Rules for auto-applying this label

Exchange email 1 rule

Mode

On

Comment

A user sends an email that contains the components shown in the following table.

Type	File	Includes IP address
Mail body	Not applicable	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

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
Sensitivity1 is applied to the email.	<input type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	Sensitivity1 is applied to the email.	<input checked="" type="radio"/>	<input type="radio"/>
	A watermark is added to File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
	A header is added to File2.xml.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

You have a Microsoft 365 E5 tenant.

You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.

You need to export the existing template.

Which file format should you use for the exported template?

- A. CSV
- B. XLSX
- C. JSON
- D. XML

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldwide#export-a-template>

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

Company policy requires that the devices have the following configurations:

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

You need to configure the devices to meet the requirements.

What should you use?

- A. an app configuration policy
- B. a compliance policy
- C. a security baseline profile
- D. a conditional access policy

Correct Answer: B

Reference:

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

HOTSPOT -

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

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

You plan to create a compliance policy named Compliance1.

You need to identify the groups that meet the following requirements:

- Can be added to Compliance1 as recipients of noncompliance notifications
- Can be assigned to Compliance1

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Can be added to Compliance1 as recipients of noncompliance notifications:

	▼
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group2 and Group3 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Can be assigned to Compliance1:

	▼
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group2 and Group3 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Answer Area

Can be added to Compliance1 as recipients of noncompliance notifications:

Correct Answer:

Can be assigned to Compliance1:

	▼
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group2 and Group3 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

	▼
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group2 and Group3 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Reference:

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

HOTSPOT -

You have a Microsoft 365 E5 tenant.

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

Compliance settings [Edit](#)**Microsoft Defender ATP**

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

Device Health

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

System Security

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

Actions for noncompliance [Edit](#)

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

▼

be locked remotely

display a notification

marked as compliant

marked as noncompliant

removed from the database

Rooted devices will be

▼

allowed to access company resources

marked as compliant

prevented from accessing company resources

reported with a low device threat

Correct Answer:

Answer Area

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

▼

be locked remotely

display a notification

marked as compliant

marked as noncompliant

removed from the database

Rooted devices will be

▼

allowed to access company resources

marked as compliant

prevented from accessing company resources

reported with a low device threat

Reference:

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

Question #105

Topic 3

You have a Microsoft 365 E5 tenant.
You create a retention label named Retention1 as shown in the following exhibit.

Review your settings

Name

Retention1

Edit

Description for admins

Edit

Description for users

Edit

File plan descriptors

Reference Id:1
Business function/department Legal
Category: Compliance
Authority type: Legal

Edit

Retention

7 years
Retain only
Based on when it was created

Edit

Back

Create this label

Cancel

When users attempt to apply Retention1, the label is unavailable.
You need to ensure that Retention1 is available to all the users.
What should you do?

- A. Create a new label policy

B. Modify the Authority type setting for Retention1.

C. Modify the Business function/department setting for Retention1.

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

Correct Answer: A

Reference:

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

You have the sensitivity labels shown in the following exhibit.

[Home](#) > sensitivity

Labels

Label policies

Auto-labeling(preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content onsite is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish labels Refresh

Name ↑	Order	Created by	Last modified
Label1	0-highest	Prvi	04/24/2020
- Label2	1	Prvi	04/24/2020
Label3	0-highest	Prvi	04/24/2020
Label4	0-highest	Prvi	04/24/2020
- Label5	5	Prvi	04/24/2020
Label6	0-highest	Prvi	04/24/2020

Which labels can users apply to content?

- A. Label3, Label4, and Label6 only
- B. Label1, Label2, Label3, Label4, Label5, and Label6
- C. Label1, Label2, and Label5 only
- D. Label1, Label3, Label4, and Label6 only

Correct Answer: D

Reference:

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

HOTSPOT -

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has the files shown in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	2
File4.bmp	3
File5.doc	5

For Site1, users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Visitor

You create a data loss prevention (DLP) policy named Policy1 as shown in the following exhibit.

New DLP policy

Choose the information to protect

Name your policy

Choose locations

Policy settings

Review your settings

Review your settings

Template name

Custom policy

Edit

Policy name

Policy1

Edit

Description

Edit

Applies to content in these locations

SharePoint sites

Edit

Policy settings

If the content contains these types of sensitive info: IP Address then notify people with a policy tip and email message.

If there are at least 2 instances of the same type of sensitive info, block access to the content.

Turn policy on after it's created?

Yes

Edit

How many files will be visible to User1 and User2 after Policy1 is applied? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

1

2

3

4

5

User2:

1

2

3

4

5

Answer Area

Correct Answer:

User1:

1

2

3

4

5

User2:

1

2

3

4

5

Reference:

<https://docs.microsoft.com/en-gb/exchange/security-and-compliance/mail-flow-rules/inspect-message-attachments>

HOTSPOT -

You have a Microsoft 365 tenant.

You need to create a custom Compliance Manager assessment template.

Which application should you use to create the template, and in which file format should the template be saved? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Application:

Microsoft Excel
Microsoft Forms
Microsoft Word
Visual Studio Code

File format:

csv
dbx
docx
dotx
json
xlsx
xltx

Answer Area

Application:

Microsoft Excel
Microsoft Forms
Microsoft Word
Visual Studio Code

File format:

csv
dbx
docx
dotx
json
xlsx
xltx

Correct Answer:

Reference:

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

HOTSPOT -

You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).

The tenant has two Compliance Manager assessments as shown in the following table.

Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Regulations
Enable multi-factor authentication for admins	Failed high risk	+27 points	0/27	NIST 800-53 Data Protection Baseline
Enable multi-factor authentication for non-admins	Failed high risk	+27 points	0/27	NIST 800-53, Data Protection Baseline

The Data Protection Baseline assessment has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Regulations
Establish a threat intelligence program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline
Establish and document a configuration management program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline

You perform the following actions:

- ☞ For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.
- ☞ Enable multi-factor authentication (MFA) for all users.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input checked="" type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input checked="" type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-assessments?view=o365-worldwide#create-assessments>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide#action-types-and-points>

You have a Microsoft 365 tenant.

Company policy requires that all Windows 10 devices meet the following minimum requirements:

- ☞ Require complex passwords.
- ☞ Require the encryption of data storage devices.

Have Microsoft Defender Antivirus real-time protection enabled.

▪

You need to prevent devices that do not meet the requirements from accessing resources in the tenant.

Which two components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a configuration policy
- B. a compliance policy
- C. a security baseline profile
- D. a conditional access policy
- E. a configuration profile

Correct Answer: *BD*

Reference:

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

You have a Microsoft 365 E5 tenant.

You need to ensure that when a document containing a credit card number is added to the tenant, the document is encrypted.

Which policy should you use?

- A. a retention policy
- B. a retention label policy
- C. an auto-labeling policy
- D. an insider risk policy

Correct Answer: *C*

Reference:

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

DRAG DROP -

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

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

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

Select and Place:

Actions

Create a sensitivity label.

Create an auto-labeling policy.

Create a sensitive information type.

Wait 24 hours, and then turn on the policy.

Publish the label.

Create a retention label.

Wait eight hours, and then turn on the policy.

Answer Area

Correct Answer:

Actions

Create a sensitive information type.

Wait 24 hours, and then turn on the policy.

Create a retention label.

Wait eight hours, and then turn on the policy.

Answer Area

Create a sensitivity label.

Publish the label.

Create an auto-labeling policy.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-label-policies-can-do>

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

HOTSPOT -

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

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

The tenant contains the devices shown in the following table.

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

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

Hot Area:

Answer Area**Statements****Yes****No**

Device1 is marked as compliant.

☐☐

Device2 is marked as compliant.

☐☐

Device3 is marked as compliant.

☐☐**Answer Area****Statements****Yes****No**

Correct Answer:

Device1 is marked as compliant.

☒☐

Device2 is marked as compliant.

☒☐

Device3 is marked as compliant.

☐☒

You have a Microsoft 365 E5 subscription.

You plan to implement records management and enable users to designate documents as regulatory records.

You need to ensure that the option to mark content as a regulatory record is visible when you create retention labels.

What should you do first?

- A. Configure custom detection rules.
- B. Create an Exact Data Match (EDM) schema.
- C. Run the Set-RegulatoryComplianceUI cmdlet.
- D. Run the Set-LabelPolicy cmdlet.

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide>

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

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

You have a Microsoft 365 subscription.

From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

HOTSPOT -

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

You need to configure Intune to meet the following requirements:

- ☞ Prevent users from enrolling personal devices.
- ☞ Ensure that users can enroll a maximum of 10 devices.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Prevent users from enrolling
personal devices:

	▼
Conditional access policies	
Device categories	
Device limit restrictions	
Device type restrictions	

Ensure that users can enroll a
maximum of 10 devices:

	▼
Conditional access policies	
Device categories	
Device limit restrictions	
Device type restrictions	

Correct Answer:

Answer Area

Prevent users from enrolling
personal devices:

	▼
Conditional access policies	
Device categories	
Device limit restrictions	
Device type restrictions	

Ensure that users can enroll a
maximum of 10 devices:

	▼
Conditional access policies	
Device categories	
Device limit restrictions	
Device type restrictions	

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#blocking-personal-windows-devices>

HOTSPOT -

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

Name: Case1 -

-
- ☞ Included content: Group1, User1, Site1
- ☞ Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders

The investigation for Case1 completes, and you close the case.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Holds are turned off for:

	▼
User1 only	
All locations	
Site1 and Group1 only	

Holds are placed on a delay hold for:

	▼
30 days	
90 days	
120 days	

Correct Answer:

Answer Area

Holds are turned off for:

User1 only

All locations

Site1 and Group1 only

Topic 4 - Testlet 1

Holds are placed on a delay hold for:

30 days

90 days

120 days

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

Introductory Info**Case Study -**

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

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

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	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 recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements -**Planned Changes -**

Contoso plans to implement the following changes:

Implement Microsoft 365.

- Manage devices by using Endpoint Manager.

Implement Microsoft Defender for Identity.

Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.

Update computers in the New York office with the spring Semi-Annual Channel feature update.

Technical Requirements -

Contoso identifies the following technical requirements:

When a Windows 10 device is joined to Azure AD, the device must enroll to Endpoint Manager automatically.

Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.

Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.

User1 must be able to enroll all the New York office mobile devices in Endpoint Manager.

Microsoft Defender for Identity sensors must be installed and must NOT use port mirroring.

Whenever possible, the principle of least privilege must be used.

A Microsoft Store for Business must be created.

Compliance Requirements -

Contoso identifies the following compliance requirements:

Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Endpoint Manager and configured in accordance with the corporate policy.

Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question

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

What is the minimum of dedicated support technicians required?

A. 1

B. 4

C. 7

D. 31

Correct Answer: B

Contoso identifies the following technical requirements:

☞ Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.

☞ Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.

You can enroll up to 1,000 mobile devices with a single Azure Active Directory account by using a device enrollment manager (DEM) account.

We have 3,100 devices; hence we will need 4 DEMs at a minimum.

Reference:

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

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

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	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 recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Implement Microsoft 365.

- Manage devices by using Endpoint Manager.

Implement Microsoft Defender for Identity.

Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.

Update computers in the New York office with the spring Semi-Annual Channel feature update.

Technical Requirements -

Contoso identifies the following technical requirements:

When a Windows 10 device is joined to Azure AD, the device must enroll to Endpoint Manager automatically.

Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.

Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.

User1 must be able to enroll all the New York office mobile devices in Endpoint Manager.

Microsoft Defender for Identity sensors must be installed and must NOT use port mirroring.

Whenever possible, the principle of least privilege must be used.

A Microsoft Store for Business must be created.

Compliance Requirements -

Contoso identifies the following compliance requirements:

Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Endpoint Manager and configured in accordance with the corporate policy.

Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question

You need to create the Microsoft Store for Business.

Which user can create the store?

A. User2

B. User3

C. User4

D. User5

Correct Answer: *C*

References:

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

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

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	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 recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Implement Microsoft 365.

- Manage devices by using Endpoint Manager.

Implement Microsoft Defender for Identity.
Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.
Update computers in the New York office with the spring Semi-Annual Channel feature update.

Technical Requirements -

Contoso identifies the following technical requirements:
When a Windows 10 device is joined to Azure AD, the device must enroll to Endpoint Manager automatically.
Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.
Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.
User1 must be able to enroll all the New York office mobile devices in Endpoint Manager.
Microsoft Defender for Identity sensors must be installed and must NOT use port mirroring.
Whenever possible, the principle of least privilege must be used.
A Microsoft Store for Business must be created.

Compliance Requirements -

Contoso identifies the following compliance requirements:
Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Endpoint Manager and configured in accordance with the corporate policy.
Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question

HOTSPOT -
You need to meet the Intune requirements for the Windows 10 devices.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Settings to configure in Azure AD:

Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

Correct Answer:

Answer Area

Settings to configure in Azure AD:

Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

References:

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

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

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	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 recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Implement Microsoft 365.

-

Manage devices by using Endpoint Manager.

Implement Microsoft Defender for Identity.

Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.

Update computers in the New York office with the spring Semi-Annual Channel feature update.

Technical Requirements -

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll to Endpoint Manager automatically.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.
- Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.
- User1 must be able to enroll all the New York office mobile devices in Endpoint Manager.
- Microsoft Defender for Identity sensors must be installed and must NOT use port mirroring.
- Whenever possible, the principle of least privilege must be used.
- A Microsoft Store for Business must be created.

Compliance Requirements -

Contoso identifies the following compliance requirements:

- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Endpoint Manager and configured in accordance with the corporate policy.
- Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question

HOTSPOT -

You need to configure a conditional access policy to meet the compliance requirements.

You add Exchange Online as a cloud app.

Which two additional settings should you configure in Policy1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

New	Conditions	Device state (preview)
<div><div>Info</div><div><div>Name</div><div>Policy1</div></div><div><div>Assignments</div><div><div>Users and groups</div><div>0 users and groups selected</div></div><div><div>Cloud apps or actions</div><div>1 app included</div></div><div><div>Conditions</div><div>0 conditions selected</div></div></div><div><div>Access controls</div><div><div>Grant</div><div>Block access</div></div><div><div>Session</div><div>0 controls selected</div></div></div><div><div>Enable policy</div><div>OnOff</div></div></div>	<div><div>Info</div><div><div>Sign-in risk</div><div>Not configured</div></div><div><div>Device platforms</div><div>Not configured</div></div><div><div>Locations</div><div>Not configured</div></div><div><div>Client apps (preview)</div><div>Not configured</div></div><div><div>Device state (preview)</div><div>Not configured</div></div></div>	<div><div>Info</div><div><div>Configure</div><div>YesNo</div></div><div><div>IncludeExclude</div></div><div><div>Select the device state condition used to exclude devices from policy.</div><div><div>Device Hybrid Azure AD joined</div></div><div><div>Device marked as compliant</div></div></div></div>

Correct Answer:

New	Conditions	Device state (preview)
<div>Info</div> <div>Name Policy1 ✓</div> <div>Assignments <div>Users and groups 0 users and groups selected</div><div>Cloud apps or actions 1 app included</div><div>Conditions 0 conditions selected</div></div> <div>Access controls <div>Grant Block access</div><div>Session 0 controls selected</div></div> <div>Enable policy On Off</div>	<div>Info</div> <div>Sign-in risk Not configured</div> <div>Device platforms Not configured</div> <div>Locations Not configured</div> <div>Client apps (preview) Not configured</div> <div>Device state (preview) Not configured</div>	<div>Info</div> <div>Configure Yes No</div> <div>Include Exclude</div> <div>Select the device state condition used to exclude devices from policy. <input type="checkbox"/> Device Hybrid Azure AD joined <input type="checkbox"/> Device marked as compliant</div>

References:

<https://docs.microsoft.com/en-us/intune/create-conditional-access-intune>

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

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

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	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 recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Implement Microsoft 365.

- Manage devices by using Endpoint Manager.

Implement Microsoft Defender for Identity.
Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.
Update computers in the New York office with the spring Semi-Annual Channel feature update.

Technical Requirements -

Contoso identifies the following technical requirements:
When a Windows 10 device is joined to Azure AD, the device must enroll to Endpoint Manager automatically.
Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.
Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.
User1 must be able to enroll all the New York office mobile devices in Endpoint Manager.
Microsoft Defender for Identity sensors must be installed and must NOT use port mirroring.
Whenever possible, the principle of least privilege must be used.
A Microsoft Store for Business must be created.

Compliance Requirements -

Contoso identifies the following compliance requirements:
Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Endpoint Manager and configured in accordance with the corporate policy.
Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question

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

Answer Area

Seattle:

6 months
18 months
24 months
30 months
5 years

New York:

6 months
18 months
24 months
30 months
5 years

Answer Area

Seattle:

	▼
6 months	
18 months	
24 months	
30 months	
5 years	

Correct Answer:

New York:

	▼
6 months	
18 months	
24 months	
30 months	
5 years	

Contoso plans to implement the following changes:

- ☞ Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.
- ☞ Update computers in the New York office with the spring Semi-Annual Channel feature update.

Box 1: 24 months -

September Feature Updates (fall Semi-Annual Channel feature updates) are serviced for 30 months from release date but by March, 6 of those 30 months have lapsed; hence, 24 months remains

Box 2: 18 months -

March Feature Updates (spring Semi-Annual Channel feature updates) are serviced for 18 months from release date

Reference:

<https://docs.microsoft.com/en-us/lifecycle/announcements/windows-10-servicing-support-updates>

Introductory Info**Case Study -**

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

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

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	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 recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements -**Planned Changes -**

Contoso plans to implement the following changes:

Implement Microsoft 365.

- Manage devices by using Endpoint Manager.

Implement Microsoft Defender for Identity.

Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.

Update computers in the New York office with the spring Semi-Annual Channel feature update.

Technical Requirements -

Contoso identifies the following technical requirements:

When a Windows 10 device is joined to Azure AD, the device must enroll to Endpoint Manager automatically.

Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.

Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.

User1 must be able to enroll all the New York office mobile devices in Endpoint Manager.

Microsoft Defender for Identity sensors must be installed and must NOT use port mirroring.

Whenever possible, the principle of least privilege must be used.

A Microsoft Store for Business must be created.

Compliance Requirements -

Contoso identifies the following compliance requirements:

Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Endpoint Manager and configured in accordance with the corporate policy.

Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question

You need to ensure that User1 can enroll the devices to meet the technical requirements.

What should you do?

- A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator role.
- B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
- C. From the Endpoint Manager admin center, add User1 as a device enrollment manager.
- D. From the Endpoint Manager admin center, configure the Enrollment restrictions.

Correct Answer: C

References:

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

Introductory Info**Case Study -**

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

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

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	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 recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements -**Planned Changes -**

Contoso plans to implement the following changes:

Implement Microsoft 365.

- Manage devices by using Endpoint Manager.

Implement Microsoft Defender for Identity.
Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.
Update computers in the New York office with the spring Semi-Annual Channel feature update.

Technical Requirements -

Contoso identifies the following technical requirements:

When a Windows 10 device is joined to Azure AD, the device must enroll to Endpoint Manager automatically.

Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.

Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.

User1 must be able to enroll all the New York office mobile devices in Endpoint Manager.

Microsoft Defender for Identity sensors must be installed and must NOT use port mirroring.

Whenever possible, the principle of least privilege must be used.

A Microsoft Store for Business must be created.

Compliance Requirements -

Contoso identifies the following compliance requirements:

Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Endpoint Manager and configured in accordance with the corporate policy.

Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question

HOTSPOT -

You need to meet the technical requirements and planned changes for Intune.

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

Settings to configure in Azure AD:

Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

Correct Answer:

Answer Area

Settings to configure in Azure AD:

Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

Reference:

Topic 5 - Testlet 2

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -

ADatum recently purchased a Microsoft 365 E5 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements -

ADatum enters into litigation. The legal department must be able to place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements -

Business Goals -

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -

ADatum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 365 users signed in. Based on that report, the security administrator must be able to create a policy to require multi-factor authentication when a sign-in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question

You need to recommend a solution for the security administrator. The solution must meet the technical requirements. What should you include in the recommendation?

- A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- B. Microsoft Azure Active Directory (Azure AD) Identity Protection
- C. Microsoft Azure Active Directory (Azure AD) conditional access policies
- D. Microsoft Azure Active Directory (Azure AD) authentication methods

Correct Answer: *C*

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/untrusted-networks>

Topic 6 - Testlet 3

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

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 the 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.

Email messages that contain attachments must be delivered immediately, and placeholders 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.

Question

HOTSPOT -

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.

Hot Area:

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 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	

Reference:

Topic 7 - Testlet 4

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

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

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	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 recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Implement Microsoft 365.

- Manage devices by using Endpoint Manager.

Implement Microsoft Defender for Identity.

Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.

Update computers in the New York office with the spring Semi-Annual Channel feature update.

Technical Requirements -

Contoso identifies the following technical requirements:

When a Windows 10 device is joined to Azure AD, the device must enroll to Endpoint Manager automatically.

Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.

Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.

User1 must be able to enroll all the New York office mobile devices in Endpoint Manager.

Microsoft Defender for Identity sensors must be installed and must NOT use port mirroring.

Whenever possible, the principle of least privilege must be used.

A Microsoft Store for Business must be created.

Compliance Requirements -

Contoso identifies the following compliance requirements:

Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Endpoint Manager and configured in accordance with the corporate policy.

Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question

On which server should you install the Defender for Identity sensor?

A. Server1

B. Server2

C. Server3

D. Server4

E. Server5

Correct Answer: A

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning>

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -

ADatum recently purchased a Microsoft 365 E5 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements -

ADatum enters into litigation. The legal department must be able to place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements -

Business Goals -

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -

ADatum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 365 users signed in. Based on that report, the security administrator must be able to create a policy to require multi-factor authentication when a sign-in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question

You need to meet the technical requirement for large-volume document retrieval.

What should you create?

- A. an activity policy from Microsoft Cloud App Security
- B. a data loss prevention (DLP) policy from the Microsoft 365 compliance center
- C. a file policy from Microsoft Cloud App Security
- D. an alert policy from the Microsoft 365 compliance center

Correct Answer: A

Reference:

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

Topic 9 - Testlet 6

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

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 the 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.

Email messages that contain attachments must be delivered immediately, and placeholders 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.

Question

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

Correct Answer: *D*

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/safe-attachments.md>

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

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 the 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.

Email messages that contain attachments must be delivered immediately, and placeholders 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.

Question

HOTSPOT -

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.

Hot Area:

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 Area

Correct Answer:

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

Reference:

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

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 the 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.

Email messages that contain attachments must be delivered immediately, and placeholders 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.

Question

You need to create the DLP policy to meet the technical requirements.

What should you configure first?

- A. sensitive info types
- B. the Insider risk management settings
- C. the event types
- D. the sensitivity labels

Correct Answer: *A*

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide>

Topic 10 - Testlet 7

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

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

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	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 recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Implement Microsoft 365.

-

Manage devices by using Endpoint Manager.

Implement Microsoft Defender for Identity.

Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.

Update computers in the New York office with the spring Semi-Annual Channel feature update.

Technical Requirements -

Contoso identifies the following technical requirements:

When a Windows 10 device is joined to Azure AD, the device must enroll to Endpoint Manager automatically.

Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.

Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.

User1 must be able to enroll all the New York office mobile devices in Endpoint Manager.

Microsoft Defender for Identity sensors must be installed and must NOT use port mirroring.

Whenever possible, the principle of least privilege must be used.

A Microsoft Store for Business must be created.

Compliance Requirements -

Contoso identifies the following compliance requirements:

Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Endpoint Manager and configured in accordance with the corporate policy.

Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question

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

What should you create from the Endpoint Management admin center?

- A. a device compliance policy
- B. a device configuration profile
- C. an app protection policy
- D. an app configuration policy

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure>

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -

ADatum recently purchased a Microsoft 365 E5 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements -

ADatum enters into litigation. The legal department must be able to place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements -

Business Goals -

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -

ADatum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 365 users signed in. Based on that report, the security administrator must be able to create a policy to require multi-factor authentication when a sign-in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question

Which report should the New York office auditors view?

- A. DLP incidents
- B. Top Senders and Recipients
- C. DLP false positives and overrides
- D. DLP policy matches

Correct Answer: A

References:

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -

ADatum recently purchased a Microsoft 365 E5 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements -

ADatum enters into litigation. The legal department must be able to place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements -

Business Goals -

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -

ADatum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 365 users signed in. Based on that report, the security administrator must be able to create a policy to require multi-factor authentication when a sign-in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question

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

What should you create?

- A. a data loss prevention (DLP) policy from the Microsoft 365 compliance center
- B. a data loss prevention (DLP) policy from the Exchange admin center
- C. a retention policy from the Exchange admin center
- D. a retention policy from the Microsoft 365 compliance center

Correct Answer: *D*

References:

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -

ADatum recently purchased a Microsoft 365 E5 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements -

ADatum enters into litigation. The legal department must be able to place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements -

Business Goals -

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -

ADatum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 365 users signed in. Based on that report, the security administrator must be able to create a policy to require multi-factor authentication when a sign-in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question

You need to protect the U.S. PII data to meet the technical requirements.

What should you create?

- A. a data loss prevention (DLP) policy that contains a domain exception
- B. a Security & Compliance retention policy that detects content containing sensitive data
- C. a Security & Compliance alert policy that contains an activity
- D. a data loss prevention (DLP) policy that contains a user override

Correct Answer: *C*

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/create-activity-alerts>

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -

ADatum recently purchased a Microsoft 365 E5 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements -

ADatum enters into litigation. The legal department must be able to place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements -

Business Goals -

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -

ADatum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 365 users signed in. Based on that report, the security administrator must be able to create a policy to require multi-factor authentication when a sign-in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question

DRAG DROP -

You need to meet the requirement for the legal department.

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

Select and Place:

Actions	Answer Area
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Correct Answer:

Actions

Create a data loss prevention (DLP) policy.

Create an eDiscovery case.

Create a label.

Run a content search.

Create a label policy.

Create a hold.

Assign eDiscovery permissions.

Publish a label.

Answer Area

Assign eDiscovery permissions.

Create an eDiscovery case.

Create a hold.

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -

ADatum recently purchased a Microsoft 365 E5 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements -

ADatum enters into litigation. The legal department must be able to place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements -

Business Goals -

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -

ADatum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 365 users signed in. Based on that report, the security administrator must be able to create a policy to require multi-factor authentication when a sign-in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question

HOTSPOT -

You need to meet the technical requirement for log analysis.

What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Minimum number of data sources:

1

3

6

Minimum number of log collectors:

1

3

6

Answer Area

Minimum number of data sources:

1

3

6

Correct Answer:

Minimum number of log collectors:

1

3

6

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -

ADatum recently purchased a Microsoft 365 E5 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements -

ADatum enters into litigation. The legal department must be able to place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements -

Business Goals -

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -

ADatum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 365 users signed in. Based on that report, the security administrator must be able to create a policy to require multi-factor authentication when a sign-in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question

HOTSPOT -

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

Hot Area:

Answer Area

From the Microsoft 365 compliance center, perform a search by using:

	▼
Audit log	
Data governance events	
DLP policy matches	
eDiscovery	

Filter by:

	▼
Activity	
Detail	
Item	
User agent	

Correct Answer:

Answer Area

From the Microsoft 365 compliance center, perform a search by using:

	▼
Audit log	
Data governance events	
DLP policy matches	
eDiscovery	

Filter by:

	▼
Activity	
Detail	
Item	
User agent	

References:

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

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 the 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.

Email messages that contain attachments must be delivered immediately, and placeholders 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.

Question

HOTSPOT -

You need to ensure that User2 can review the audit logs. The solution 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.

Hot Area:

Answer Area

Role group:

	▼
Reviewer	
Global reader	
Data Investigator	
Compliance Management	

Tool:

	▼
Exchange admin center	
SharePoint admin center	
Microsoft 365 admin center	
Microsoft 365 Defender	

Answer Area

Correct Answer:

Role group:

	▼
Reviewer	
Global reader	
Data Investigator	
Compliance Management	

Tool:

	▼
Exchange admin center	
SharePoint admin center	
Microsoft 365 admin center	
Microsoft 365 Defender	

Reference:

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

Introductory Info

Case Study -

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

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

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

To start the case study -

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

Overview -

General Overview -

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 the 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.

Email messages that contain attachments must be delivered immediately, and placeholders 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.

Question

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.

Correct Answer: *B*

Reference:

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

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 the 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.

Email messages that contain attachments must be delivered immediately, and placeholders 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.

Question

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 Defender, 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.

Correct Answer: *D*

Reference:

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

Introductory Info

Case Study -

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

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

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

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

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 the 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.

Email messages that contain attachments must be delivered immediately, and placeholders 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.

Question

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.

Correct Answer: *D*

Reference:

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