

Exam Questions MS-101

Microsoft 365 Mobility and Security (beta)

<https://www.2passeasy.com/dumps/MS-101/>



NEW QUESTION 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 Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intune. Solution: You configure the Mobility (MDM and MAM) settings. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 2

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

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

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

Answer: B

NEW QUESTION 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 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

Answer: B

NEW QUESTION 4

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 Device 1 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

Answer: B

NEW QUESTION 5

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 Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP contains the roles shown in the following table.

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

Windows 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	<i>None</i>

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

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 6

Your network contains an on premises Active Directory domain.

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

You need to monitor a domain controller by using Microsoft Azure Advanced Threat Protection (ATP). What should you do? More than one answer choice may achieve the goal. Select the BEST answer.

- A. Deploy an Azure ATP sensor, and then configure port mirroring.
 B. Deploy an Azure ATP sensor, and then configure detections.
 C. Deploy an Azure ATP standalone sensor, and then configure detections.
 D. Deploy an Azure ATP standalone sensor, and then configure port mirroring.

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5>all-atp-step5

NEW QUESTION 7

HOTSPOT

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows 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)	<i>Not applicable</i>

You onboard computers to Windows 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.

Computer1:

▼
Group1 only
Group2 only
Group1 and Group2
Ungrouped machines

Computer2:

▼
Group1 only
Group3 only
Group1 and Group3

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Computer1:

▼
Group1 only
Group2 only
Group1 and Group2
Ungrouped machines

Computer2:

▼
Group1 only
Group3 only
Group1 and Group3

NEW QUESTION 8

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 Windows Defender Advanced Threat Protection (ATP). 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.

Methods	Answer Area
A Microsoft Azure ATP sensor	Windows 8.1: <div></div>
A local script	Windows 10: <div></div>
Microsoft Monitoring Agent	Windows Server 2016: <div></div>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

References:

[hHYPERLINK "https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-threat-protection"](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-threat-protection)
[tps://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-threat-protection](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-threat-protection)
<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-endpoints-windows-defender-advanced-threat-protection>
[https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection"](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection)
[HYPERLINK "https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection"](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection)

defender-advanced-threat-protection

NEW QUESTION 9

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. Security & Compliance content search
- C. Microsoft Azure Active Directory (Azure AD) sign-ins
- D. Security & Compliance audit tag search

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-logs-overview>

NEW QUESTION 10

You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that User1 can place a hold on all mailbox content. Which role should you assign to User1?

- A. e Discovery Manager from the Security & Compliance admin center
- B. compliance management from the Exchange admin center
- C. User management administrator from the Microsoft 365 admin center
- D. Information Protection administrator from the Azure Active Directory admin center

Answer: A

Explanation:

References:

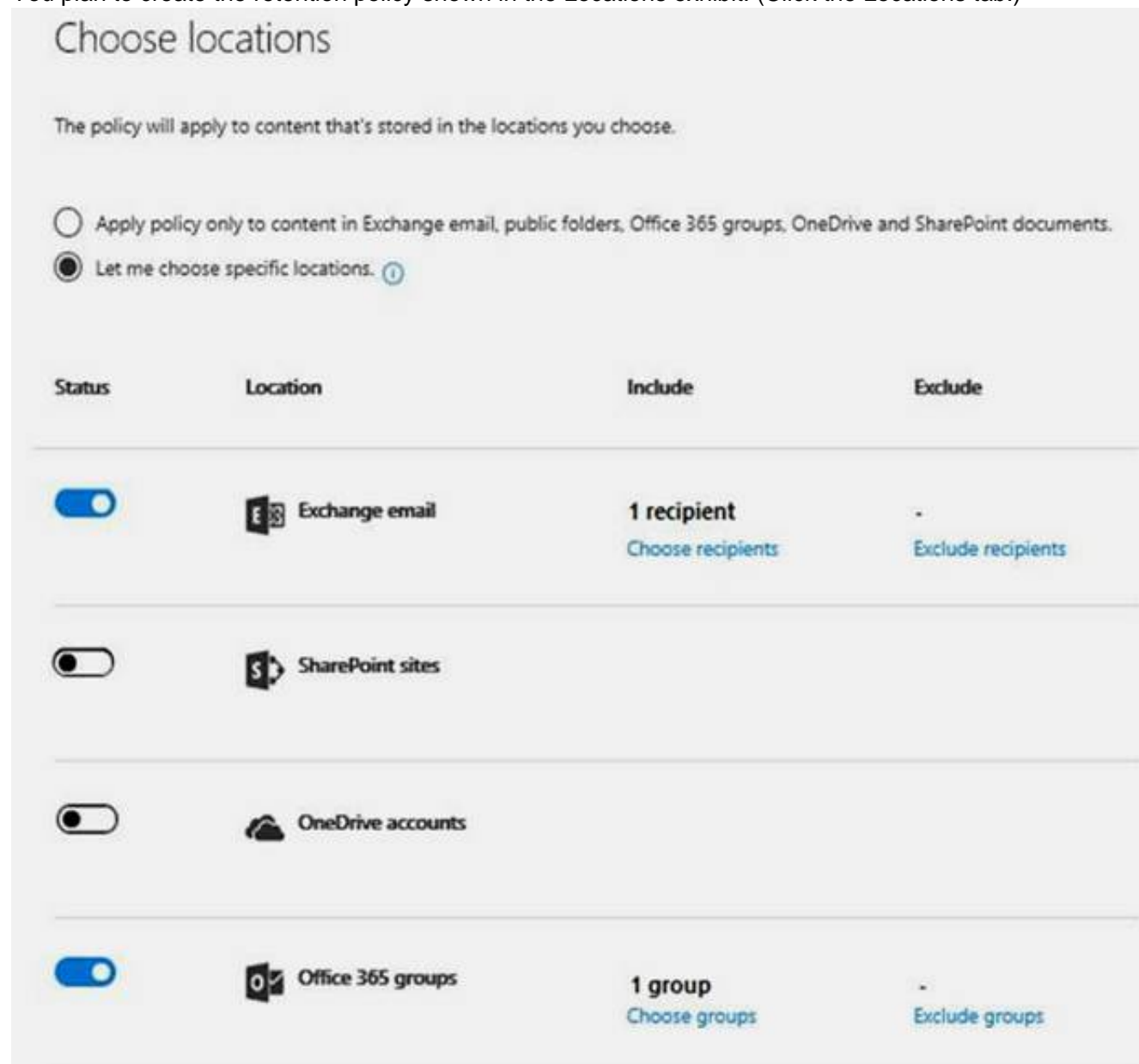
<https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions?view=exchserver-2019>

NEW QUESTION 10

HOTSPOT

You have a Microsoft 365 subscription that contains all the user data.

You plan to create the retention policy shown in the Locations exhibit. (Click the Locations tab.)



Choose locations

The policy will apply to content that's stored in the locations you choose.

☐ Apply policy only to content in Exchange email, public folders, 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 groups

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 LegalTeam
Office 365 groups	A security group named Legal365

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

Statements	Yes	No
Any file stored in Microsoft SharePoint group library by a user in the Legal365 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 LegalTeam group will be deleted automatically after five years.	<input type="radio"/>	<input type="radio"/>
If a new user is added to the LegalTeam group next week, and the user sends an email message that contains the word takeover, the message will be deleted automatically after five years.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 12

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.

If you copy the file to your local 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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection>

NEW QUESTION 14

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 action
 B. a group
 C. an exception
 D. a condition

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies#how-dlp-policies-work>

NEW QUESTION 15

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.

<div><div></div><div>User1</div></div> <div><div>Set-AdminAuditLogConfig</div><div>Set-Mailbox</div><div>Set-UnifiedAuditSetting</div></div>	<div><div></div><div>\$true</div></div> <div><div>-AdminAuditLogEnabled</div><div>-AuditEnabled</div><div>-UnifiedAuditLogIngestionEnabled</div></div>
--	--

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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>

NEW QUESTION 17

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.

Content contains

Any of these

PII Identifiers

Sensitive info type

U.S. Social Security Number (SSN)

min

max

1

any

min

max

50

100

Add

and

Any of these

Medical Terms

Sensitive info type

International Classification of Diseases (ICD-9-CM)

min

max

1

any

min

max

50

100

Add

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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>

NEW QUESTION 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.

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intune. Solution: You configure the Apple MDM Push certificate.
Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

References:

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

NEW QUESTION 23

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

Answer: A

Explanation:

References:

<https://www.sccconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/>

NEW QUESTION 25

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

Answer: A

Explanation:

References:

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

NEW QUESTION 30

You have a Microsoft 365 subscription.

You need to view the IP address from which a user synced a Microsoft SharePoint library.

What should you do?

- A. From the SharePoint admin center, view the usage reports.
- B. From the Security & Compliance admin 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.

Answer: B

Explanation:

References:

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

NEW QUESTION 34

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 User1 to the eDiscovery Manager role group.
- B. From the Azure Active Directory admin center, add User1 to the Security Reader role group.
- C. From the Security & Compliance admin center, add User1 to the Compliance Administrator role group.
- D. From Windows PowerShell, enable the super user feature and assign the role to SecAdmin1.

Answer: D

Explanation:
References:
<https://docs.microsoft.com/en-us/azure/information-protection/configure-super-users>

NEW QUESTION 36

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.

Answer: ABC

Explanation:
References:
[https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%25HYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%2farticle%2f0d4d0f35-390b-4518-800e-0c7ec95e946c"2farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c](https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%25HYPERLINK%20https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%2farticle%2f0d4d0f35-390b-4518-800e-0c7ec95e946c%2farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c)

NEW QUESTION 37

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 policy to retain what you want and get rid of what you don't.

- Name your label
- Label settings
- Review your settings

Review your settings

It will take up to 1 day to apply the retention policy to the locations you chose.

Name: 6Months [Edit]

Description for admins [Edit]

Description for users [Edit]

Retention: 6 months [Edit]
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.

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 40

HOTSPOT

You purchase a new Microsoft 365 subscription.

You create 100 users who are assigned Microsoft 365 E3 licenses. From the Security & Compliance admin center, you enable auditing.

Six months later, 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 changed the 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.

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%2farticle%2f0d4d0f35-390b-4518-800e-0c7ec95e946c>

<https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing>

NEW QUESTION 43

Your company has 5,000 Windows 10 devices. All the devices are protected by using Windows Defender

Advanced Threat Protection (ATP).

You need to view which Windows Defender ATP alert events have a high severity and occurred during the last seven days.

What should you use in Windows Defender ATP?

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

Answer: B

Explanation:

References:

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

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

NEW QUESTION 47

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 ?
Create Workspace				
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 ?					
① 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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Delete the workspace.

Create a new workspace.

Regenerate the access keys.

NEW QUESTION 51

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 Policie
- C. Create a file policy.
- D. Click Discover, and then click Create snapshot report.
- E. Click Investigate, and then click Files.

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/investigate-an-activity-in-office-365-cas>

NEW QUESTION 55

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 Security & Compliance admin center, create a safe attachments policy.

Answer: C

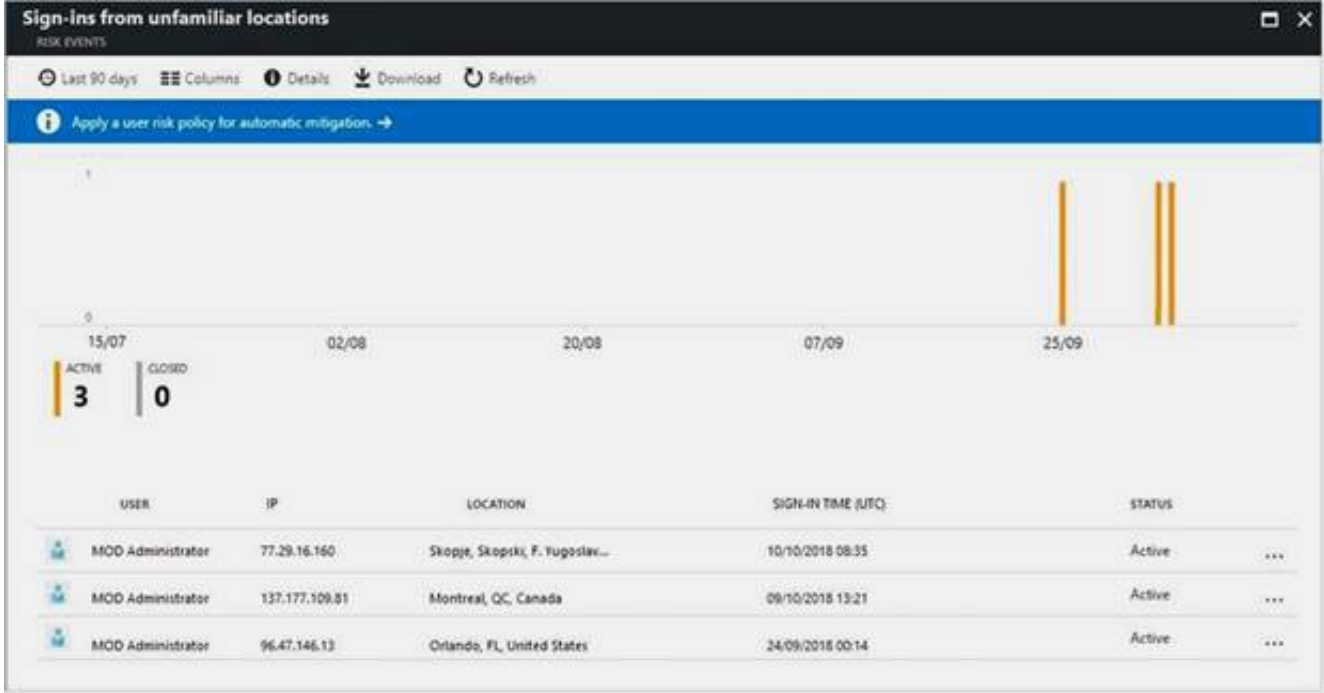
Explanation:

References:

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

NEW QUESTION 56
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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

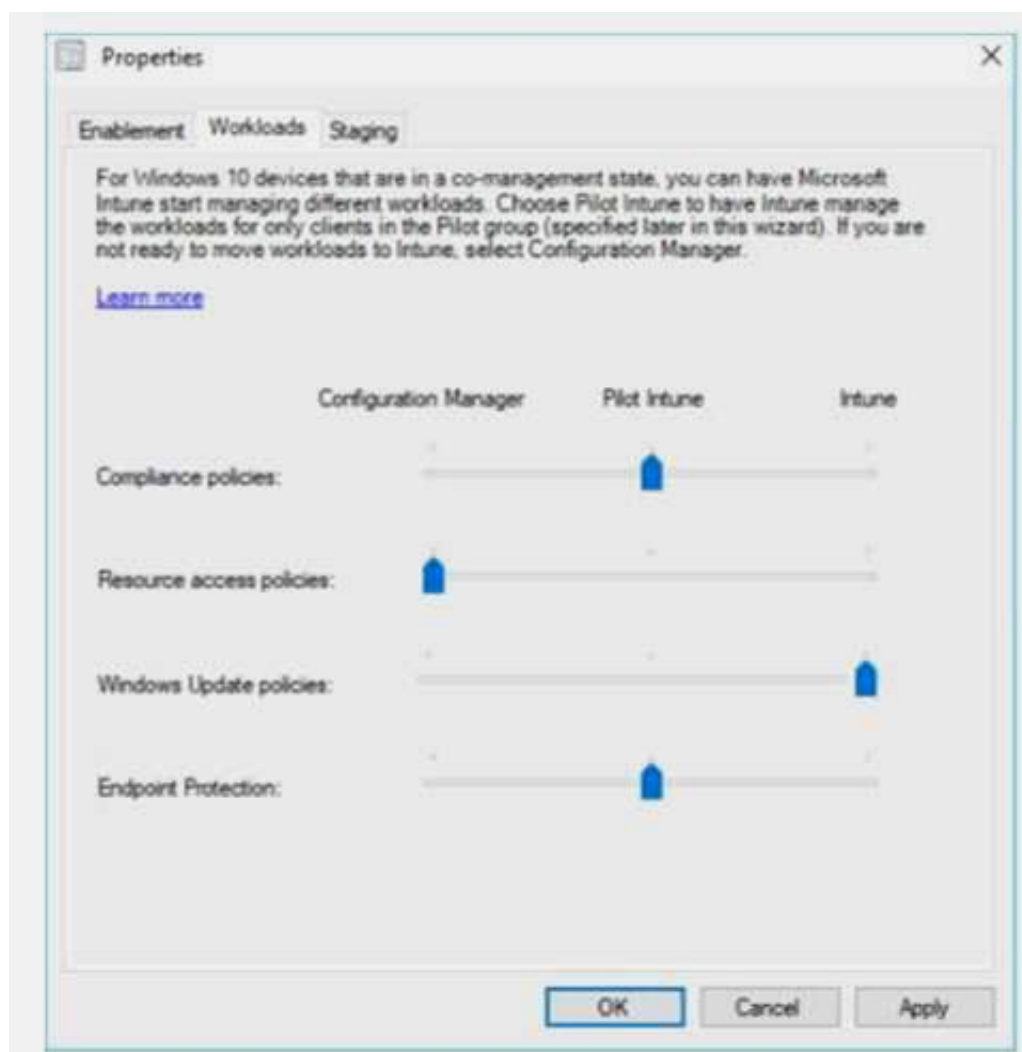
References:
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy>
<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations>

NEW QUESTION 60
HOTSPOT

Your network contains an Active Directory forest named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD). You use Microsoft System Center Configuration Manager (Current Branch) for device management. You have the Windows 10 devices shown in the following table.

Name	Collection
Device1	Collection1
Device2	Collection2

You configure Configuration Manager co-management as follows: Automatic enrollment in Intune: Pilot
Pilot collection: Collection2
You configure co-management workloads as shown in the following exhibit.



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

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"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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"/>

NEW QUESTION 64

HOTSPOT

You have three devices enrolled in Microsoft Intune 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 Intune 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.

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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"/>

NEW QUESTION 68

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 file 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.

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-dlp/newdataclassification?view=exchange-ps>

NEW QUESTION 71

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 Security & Compliance admin center, 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

Answer: A

Explanation:

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/newcompliancesecurityfilter?view=exchange-ps>

NEW QUESTION 74

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 Security & Compliance admin 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

Answer: B

Explanation:
References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/file-plan-manager>

NEW QUESTION 79

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

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	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area	Statements	Yes	No
	Label1 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input checked="" 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	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 80

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.

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.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://www.sherweb.com/blog/edis>[HYPERLINK "https://www.sherweb.com/blog/ediscovery-office-365/"](https://www.sherweb.com/blog/ediscovery-office-365/)covery-office-365/

NEW QUESTION 82

Which report should the New York office auditors view?

- A. DLP policy matches
- B. DLP false positives and overrides
- C. DLP incidents
- D. Top Senders and Recipients

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/SHYPERLINK> "https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies"ecuritycompliance/data-loss- prevention-policies

NEW QUESTION 83

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MS-101 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MS-101 Product From:

<https://www.2passeasy.com/dumps/MS-101/>

Money Back Guarantee

MS-101 Practice Exam Features:

- * MS-101 Questions and Answers Updated Frequently
- * MS-101 Practice Questions Verified by Expert Senior Certified Staff
- * MS-101 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * MS-101 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year