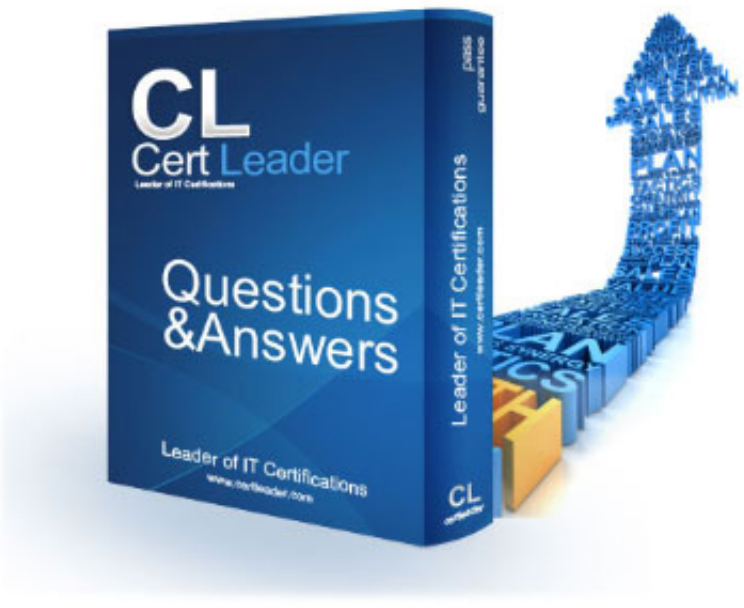
MS-101 Dumps

Microsoft 365 Mobility and Security (beta)

https://www.certleader.com/MS-101-dumps.html

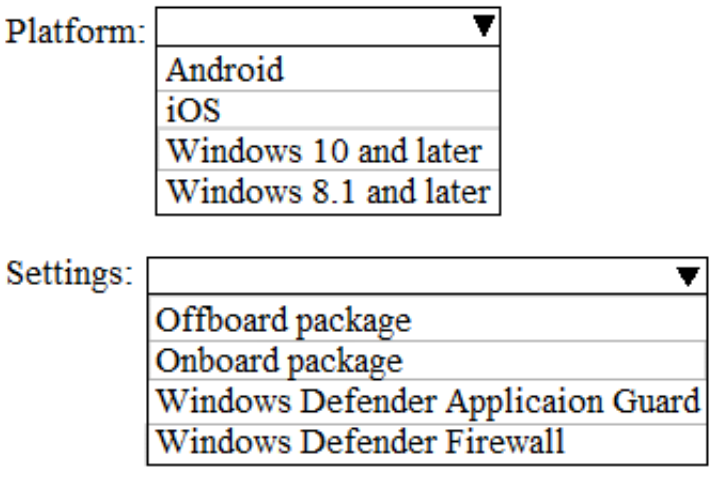


NEW QUESTION 1
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals- Some question sets might have more than one correct solution, while others might not have a correct solution.
After 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 Intuen. Solution: You configure the Mobility (MDM and MAM) settings. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 2
HOTSPOT
You have a Microsoft 365 subscription.
You need to implement Windows 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.



A. Mastered
B. Not Mastered

Answer: A

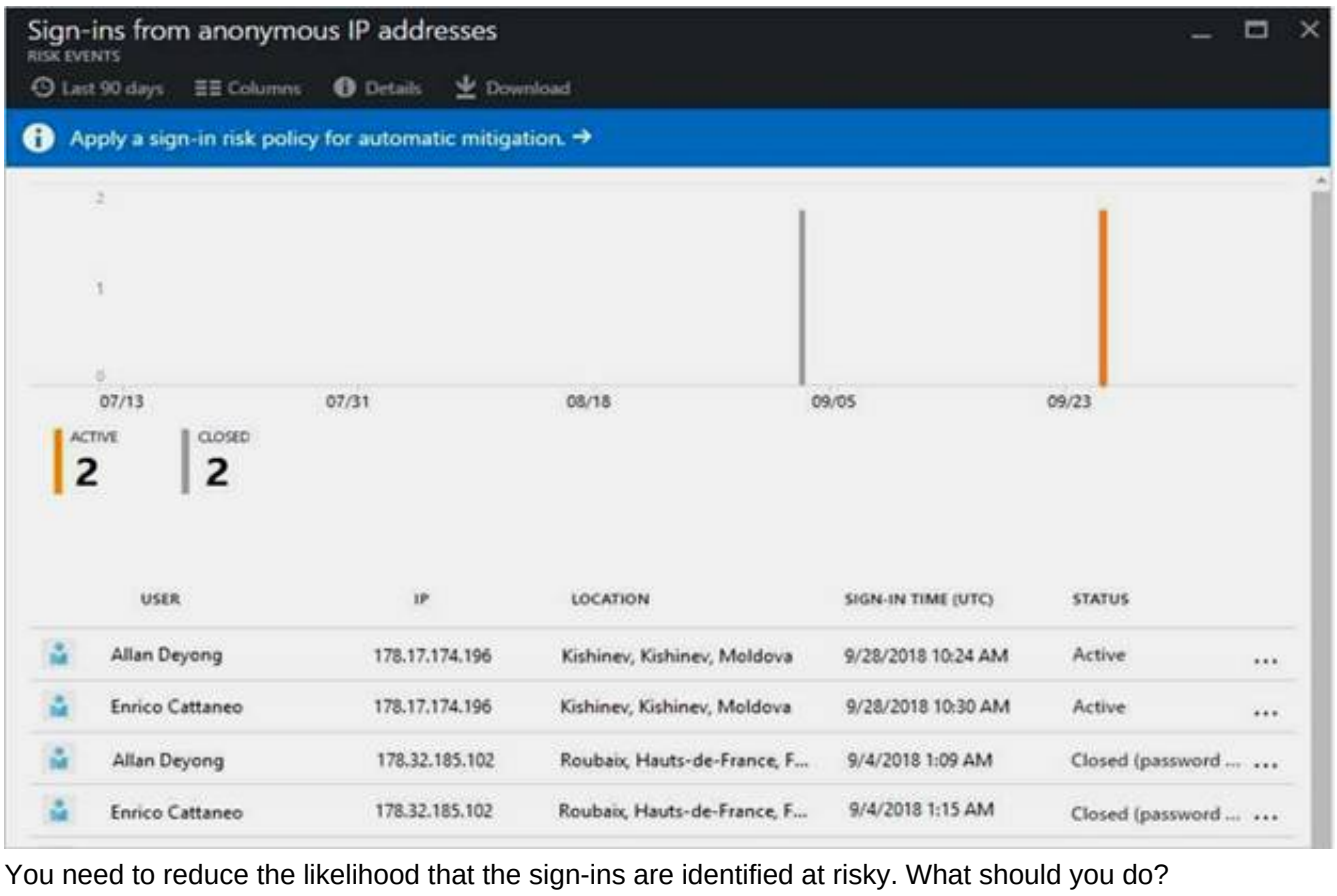
Explanation:
References:
https://docs.microsoft.com/en-us/intune/advanced-threat-protection

NEW QUESTION 3
You have a Microsoft 36S 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 score. What should you configure from the Cloud Discover settings?
A. Organization details
B. Default behavior
C. Score metrics
D. App tags

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/cloud-app-security/discovered-app-queries

NEW QUESTION 4
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 at 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.

Answer: D

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

NEW QUESTION 5
DRAG DROP
You create a Microsoft 36S subscription.
You need to create a deployment plan for Microsoft Azure Advanced Threat Protection (ATP).
Which five 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	Answer Area
Download the Azure ATP sensor setup package.	
Create a Security & Compliance threat management policy.	
Create an Azure Active Directory (Azure AD) conditional access policy.	
Install sensors.	
Create a workspace.	
Enter credentials.	
Configure the sensor settings.	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://blog.ahasayen.com/azure-advanced-threat-protection-deployment/

NEW QUESTION 6
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 from the Security & Compliance admin center?

A. Create a data toss 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.

Answer: D

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

NEW QUESTION 7
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 Appl. 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.

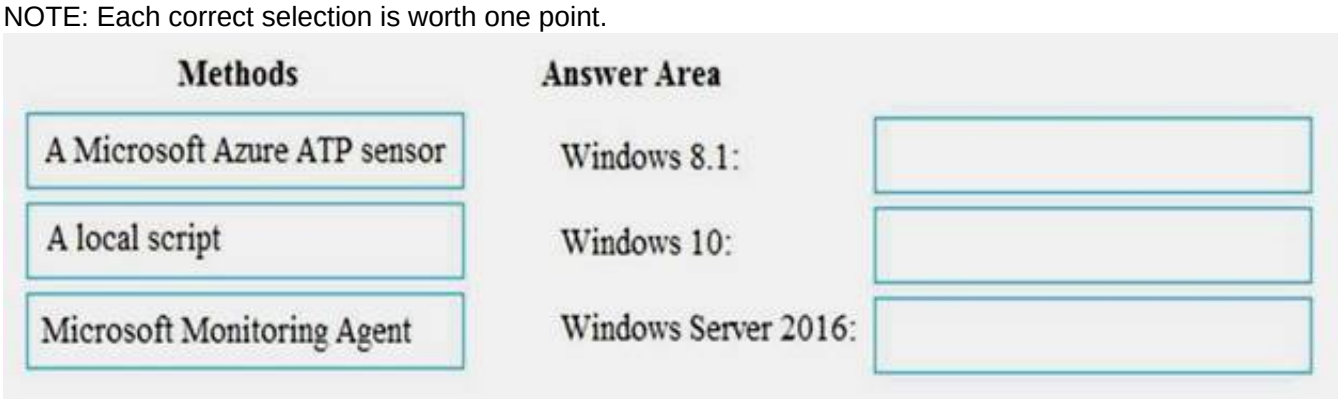
Answer: A

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

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.



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"ttps://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-HYPERLINK "https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection"windows-defender-advanced-threat-protection

NEW QUESTION 9
HOTSPOT
You have the Microsoft Azure Active Director (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:
• Users and groups: Group1
• Cloud apps: Microsoft Office 365 Exchange Online
• 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.

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	○	○
User1 can access Microsoft Exchange Online from Device2.	○	○
User2 can access Microsoft Exchange Online from Device2.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	◉	○
User1 can access Microsoft Exchange Online from Device2.	○	◉
User2 can access Microsoft Exchange Online from Device2.	◉	○

NEW QUESTION 10
HOTSPOT
You have several devices enrolled in Microsoft Intune.
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 Intune are configured as shown in the following table.

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

Statements	Yes	No
User1 can enroll Windows devices in Intune.	○	○
User2 can enroll Android devices in Intune.	○	○
User3 can enroll iOS devices in Intune.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Windows devices in Intune.	○	◯
User2 can enroll Android devices in Intune.	◯	○
User3 can enroll iOS devices in Intune.	◯	○

NEW QUESTION 10
The users at your company use Dropbox to store documents. The users access Dropbox by using the MyApps portal.
You need to ensure that user access to Dropbox is authenticated by using a Microsoft 365 identify. The documents must be protected if the data is downloaded to an untrusted device.
What should you do?

A. From the Intune admin center, configure the Conditional access settings.
B. From the Azure Active Directory admin center, configure the Organizational relationships settings
C. From the Azure Active Directory admin center, configure the Application proxy settings.
D. From the Azure Active Directory admin center, configure the Devices settings.

Answer: B

NEW QUESTION 12
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 provisiong package
B. an in place upgrade
C. wipe and load refresh
D. Windows Autopilot

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/windHYPERLINK "https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure"ows10- infrastructure

NEW QUESTION 17
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

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/sccm/core/plan-design/choose-a-device-management-solution#bkmk_intune

NEW QUESTION 19
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?

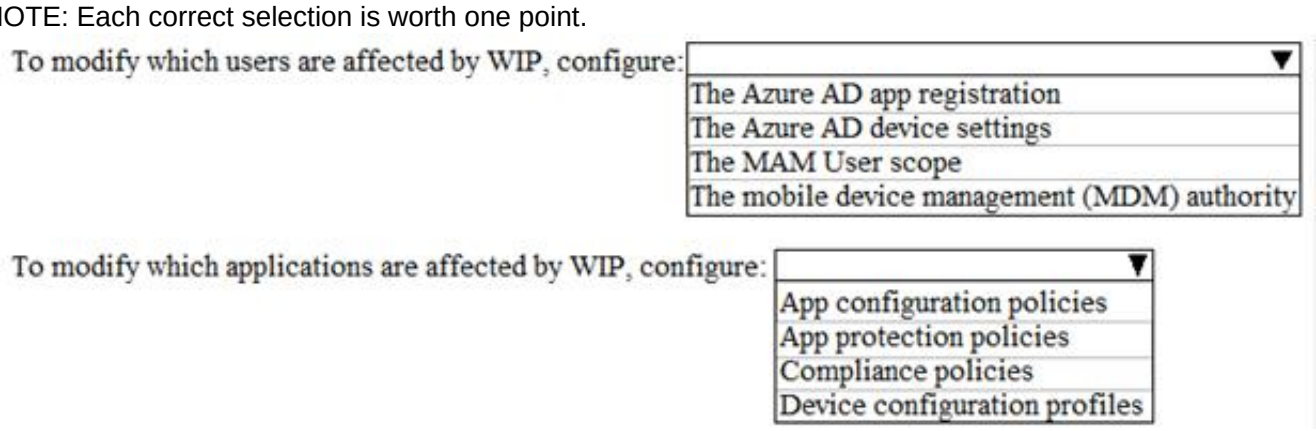
A. Windows Autopilot
B. Windows Update
C. Subscription Activation
D. an in-place upgrade

Answer: A

Explanation:

References:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

NEW QUESTION 20
HOTSPOT
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. 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 m the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protectHYPERLINK "https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure"ion/create-wip- policy-using-intune-azure

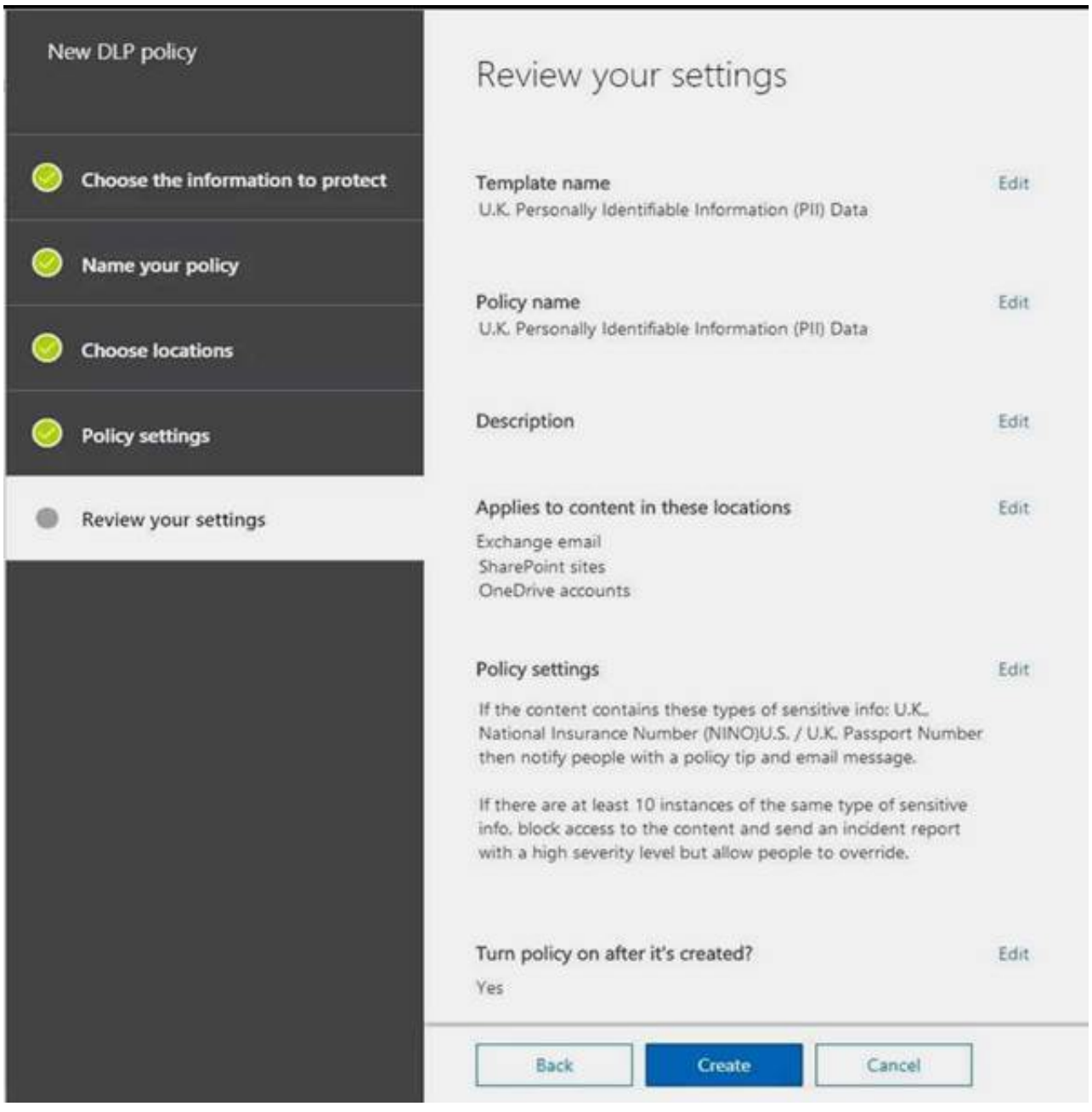
NEW QUESTION 21
You have a Microsoft 365 subscription
All users are assigned a Microsoft 365 E3 License. You enable auditing for your organization.
What is the maximum amount of time data will be retained in the Microsoft 365 audit log?

A. 2 years
B. 1 year
C. 30 days
D. 90 days

Answer: D

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

NEW QUESTION 26
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.



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 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**].

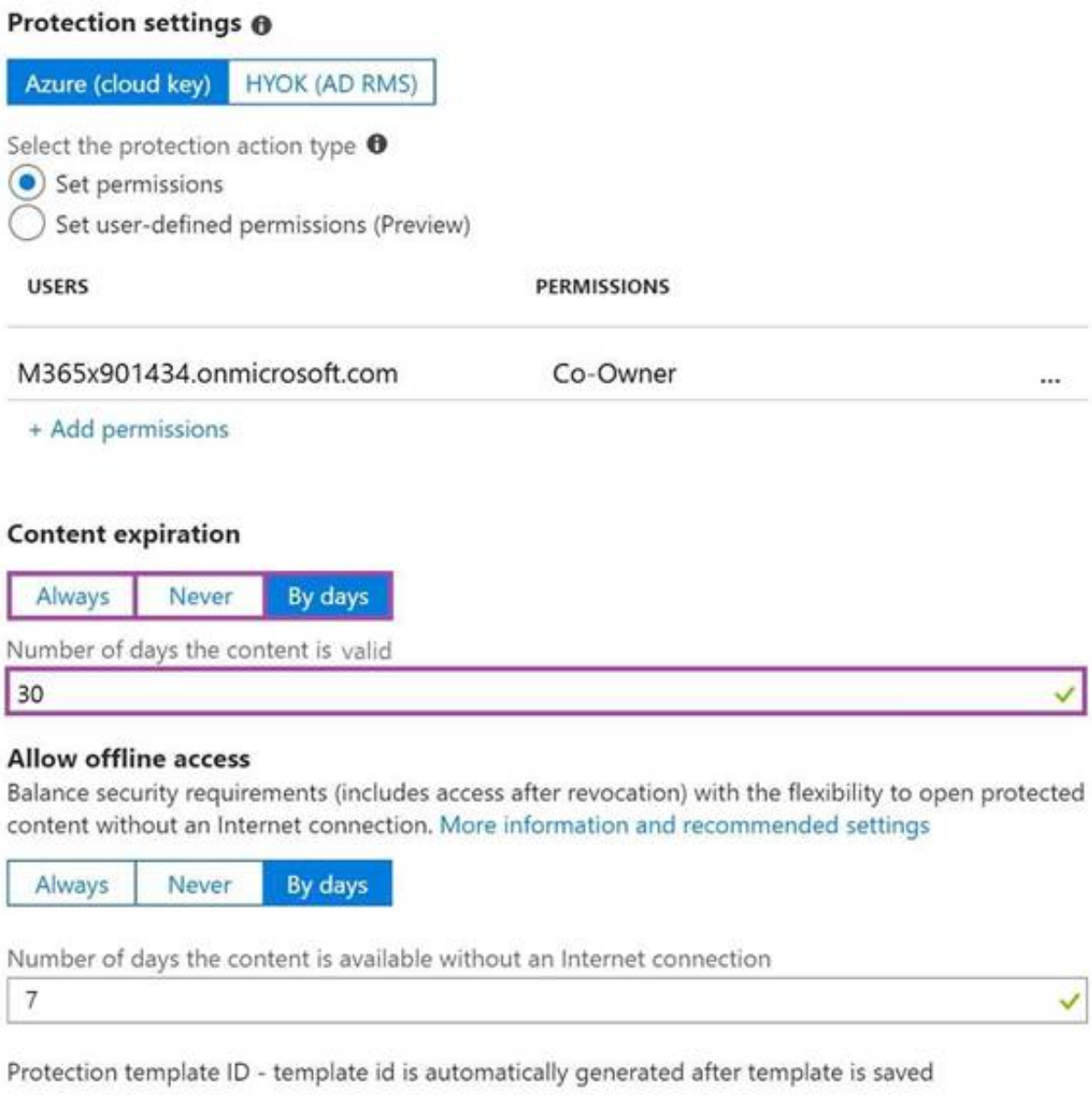
- allowed
- blocked without warning
- blocked, but the user can override the policy

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 27
HOTSPOT
You have a document in Microsoft OneDrive that is encrypted by using Microsoft Azure Information Protection as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

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

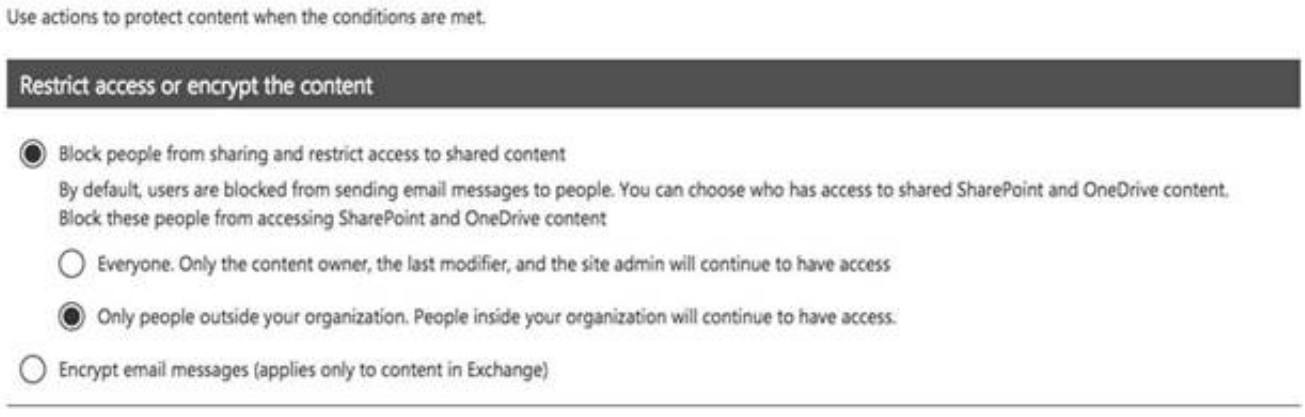
NEW QUESTION 31
You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User 1. You need to preserve a copy of all the email messages that contain the word Project X.
WDM should you do?

A. From the Security & Compliance admin center, create an eDiscovery case.
B. From the Exchange admin center, create a mail now rule.
C. From the Security fit Compliance adman center, start a message trace.
D. From Microsoft Cloud App Security, create an access policy.

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/ediscovery-cases#step-2-create-a-new-case

NEW QUESTION 36
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.)



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

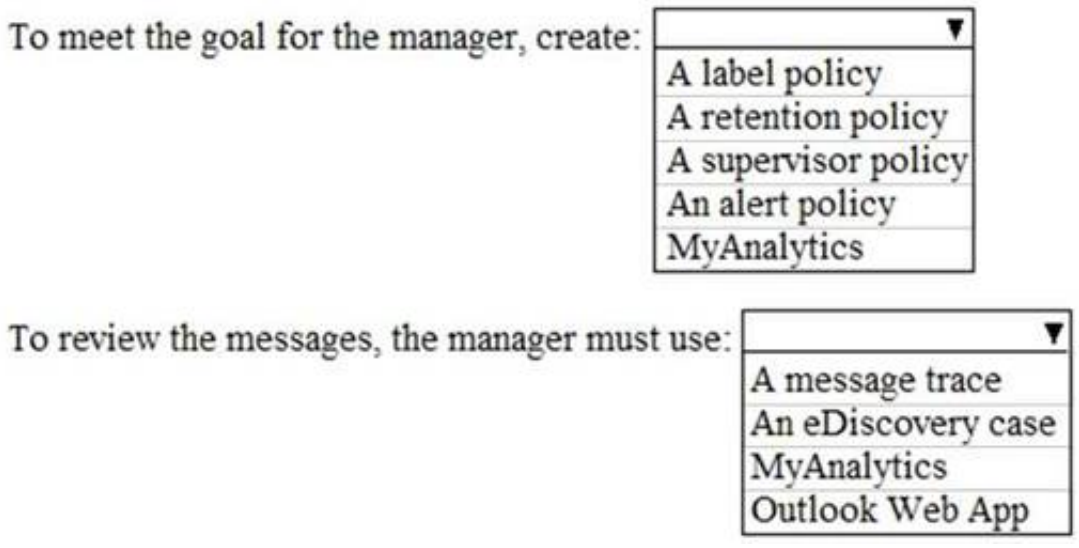
NEW QUESTION 41
You have a Microsoft 365 subscription.
From the Security & Compliance admin center, you create a content search of all the mailboxes that contain the word Project X.
You need to export the results of the content search. What do you need to download the report?

A. a certification authority (CA) certificate
B. an export key
C. a password
D. a user certificate

Answer: B

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

NEW QUESTION 42
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.



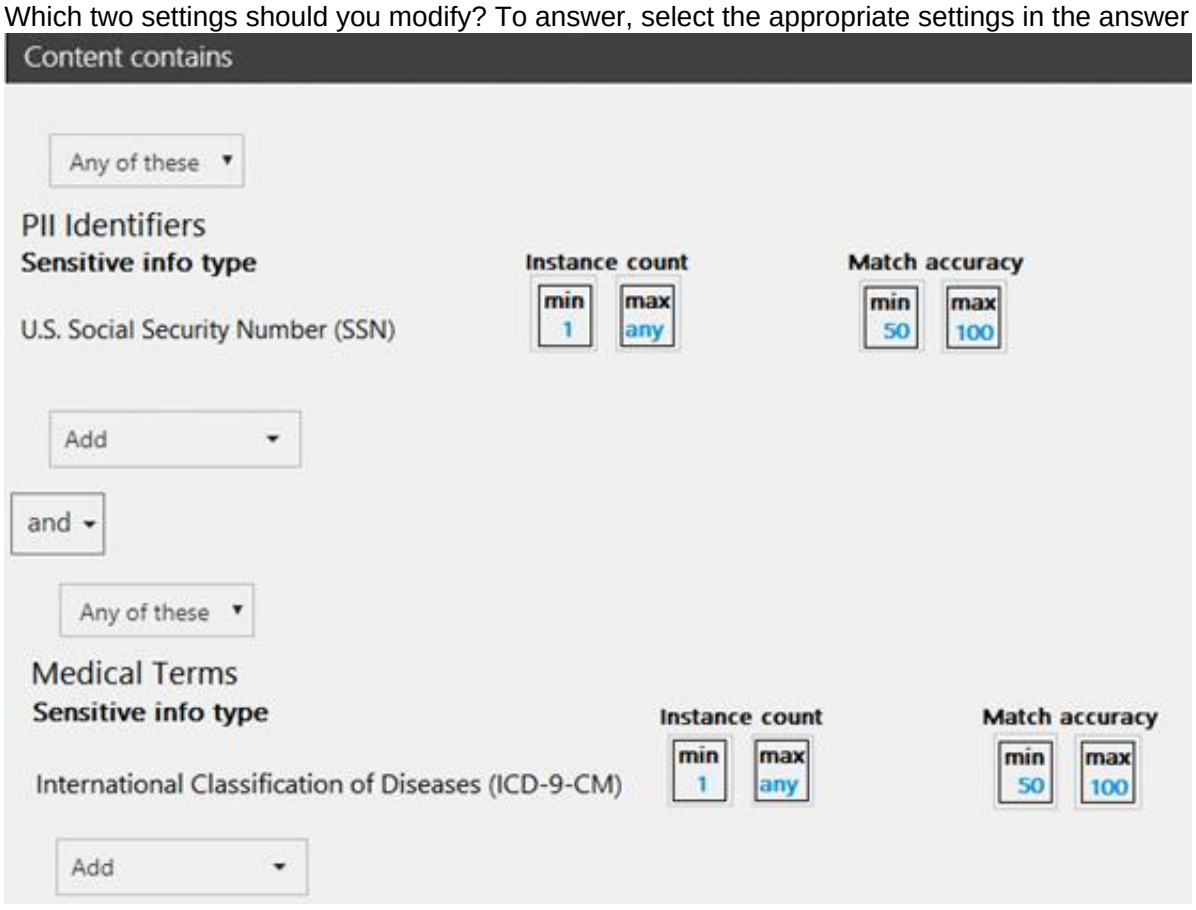
A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 47
HOTSPOT
You have a data loss prevention (DIP) 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.



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-inHYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/what-the-sensitive-information-types-look-for#international-classification-of-diseases-icd-9-cm"formation-types-look-for#international-classification-of-diseases-icd-9-cm

NEW QUESTION 50
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

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/information-protection/configure-exo-rules

NEW QUESTION 54
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

Answer: B

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

NEW QUESTION 58
HOTSPOT
You have a Microsoft Office 365 subscription.
You need to delegate eDiscovery tasks as shown in the following table.

User	Task
User1	• Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content. • View the eDiscovery cases created by User1. • Configure case settings. • Place content on hold.
User2	• View the eDiscovery cases created by User1. • 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.

User1: ▼
- eDiscovery Administrator
- eDiscovery Manager
- Records Management
- Reviewer
- Security Administrator

User2: ▼
- eDiscovery Administrator
- eDiscovery Manager
- Records Management
- Reviewer
- Security Administrator

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/office3HYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions"65/securitycompliance/assign- ediscovery-permissions

NEW QUESTION 61
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.

Answer: BCF

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/use-network-upload-to-import-pst- files

NEW QUESTION 64
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 69
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

NEW QUESTION 74
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 79
HOTSPOT
Your company uses Windows Defender Advanced Threat Protection (ATP). Windows 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)	*Not applicable*

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

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Computer1 will be a member of [**answer choice**].

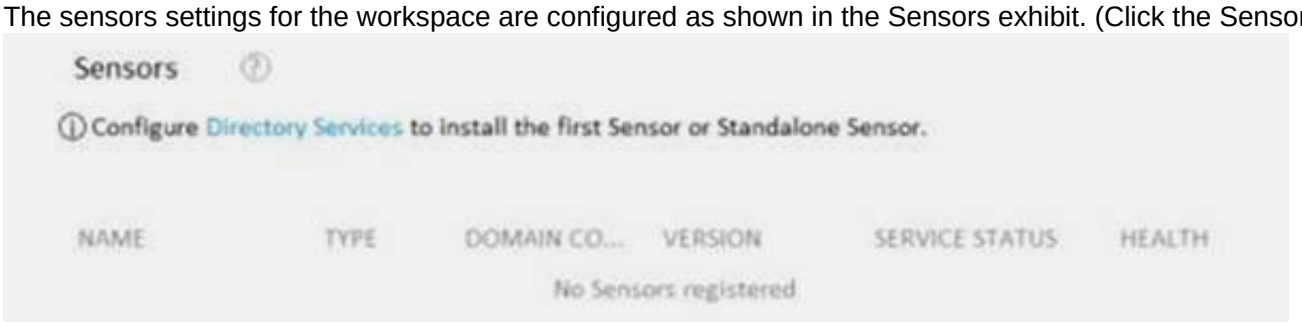
- Group3 only
- Group4 only
- **Group3 and Group4 only**
- Ungrouped machines

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

NEW QUESTION 83
DRAG DROP
You have the Microsoft Azure Advanced Threat Protection (ATP) workspace shown in the Workspace exhibit. (Click the Workspace tab.)

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



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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

1. Delete the workspace.
2. Create a new workspace.
3. Regenerate the access keys.

NEW QUESTION 88
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 90
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 Windows Defender Advanced Threat Protection (ATP) for 10 test devices. During the onboarding process, you configure Windows Defender ATP- related data to be stored in the United States.
You plan to onboard all the devices to Windows Defender ATP. You need to store the Windows Defender ATP data in Europe. What should you first?

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

Answer: D

NEW QUESTION 91
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 95
HOTSPOT
You configure an anti-phishing policy as shown in the following exhibit.

Policy setting	**Policy name**	Managers	
	Description		
	Applied to	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**	On - 3 User(s) specified	
	Protect all domains I own	On	
	Protect specific domains	On - 2 Domain(s) specified	
	Action > User impersonation	Move message to the recipients' Junk Email folders	
	Action > Domain impersonation	Delete the message before it's delivered	Edit
	Safety tips > User impersonation	Off	
	Safety tips > Domain impersonation	Off	
	Safety tips > Unusual characters	Off	
	Mailbox intelligence	Off	
Spoof	**Enable antispoofing protection**	On	
	Action	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.

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 messages are moved to the Junk Email folder

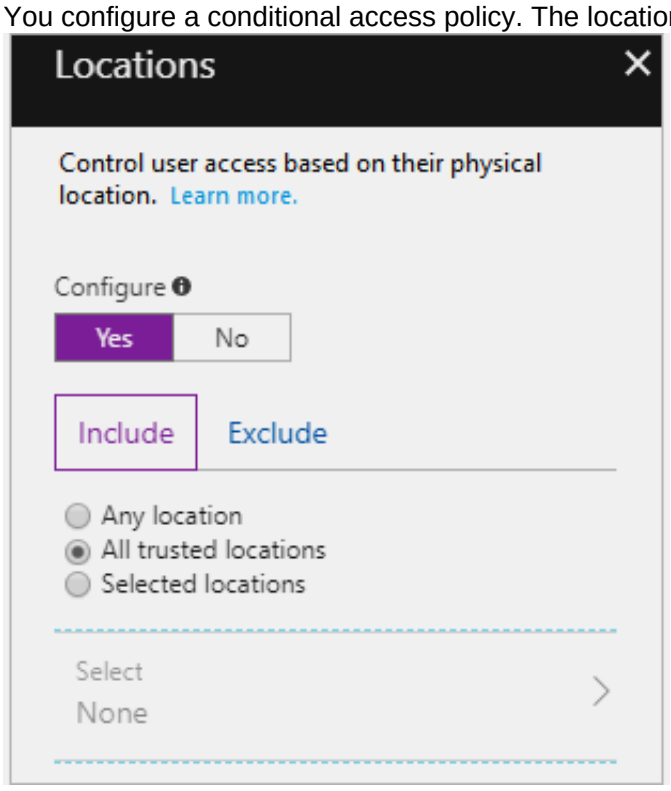
To reduce the likelihood of the impersonation policy generating false positives, configure [**answer choice**].
- Advanced phishing thresholds
- Domain impersonation
- Enable antispoofing protection
- Mailbox intelligence

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies#learn-about-HYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies#learn-about-atp-anti-phishing-policy-options"atp-anti-phishing-policy-options

NEW QUESTION 96
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 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 Intune admin center, create a device compliance policy.
D. From the Azure Active Directory admin center, create a named location.

Answer: D

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

NEW QUESTION 97
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

Answer: BD

NEW QUESTION 99
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.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

NEW QUESTION 101
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

Answer: C

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

NEW QUESTION 102
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 create the Mobility (MDM and MAM) settings. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 106
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	*None*
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	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.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-HYPERLINK "https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/user-roles-windows-defender-advanced-threat-protection"defender-atp/user-roles-windows-defender-advanced-threat-protection

NEW QUESTION 110
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:
Users and groups: Group1
Cloud apps: Microsoft Office 365 Exchange Online
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.

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	○	○
User1 can access Microsoft Exchange Online from Device2.	○	○
User2 can access Microsoft Exchange Online from Device2.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	○	○
User1 can access Microsoft Exchange Online from Device2.	○	○
User2 can access Microsoft Exchange Online from Device2.	○	○

NEW QUESTION 115
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 120
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

Answer: B

Explanation:
References:
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Onlineand-OneDrive-for/ba-p/46678A

NEW QUESTION 122
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-AzureRmRoleAssignment cmdlet with the appropriate parameters.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.resources/new- azurermroleassignment?view=azurermps-6.13.0

NEW QUESTION 124
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 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

Answer: B

NEW QUESTION 127
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 an Azure Advanced Threat Protection (ATP) workspace named Workspace1. The tenant contains users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	*None*
User2	Azure ATP Workspace1 Users	*None*
User3	*None*	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.
Solution: You instruct User1 to modify the Azure ATP sensor configuration. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 132
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 Intune automatically.

A. User1 and User2 only
B. User 1, User2, and User only
C. User1, User2.User3, and User4
D. User2only

Answer: C

NEW QUESTION 135
You have a Microsoft 365 subscription that uses a default domain named contoso.com.
You have two users named User 1 and User2.
From the Security & Compliance admin center, you add User1 to the ediscovery Manager role group. From the Security & Compliance admin 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

Answer: C

Explanation:
Case Study: 1 Contoso, Ltd 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 ES subscription.
Existing Environment Requirement
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 are 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.
Planned Changes
Contoso plans to implement the following changes:
•Implement Microsoft 365.
•Manage devices by using Microsoft Intune.
•Implement Azure Advanced Threat Protection (ATP).
•Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.
Technical Requirements
Contoso identifies the following technical requirements:
•When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automaticaiy.
•Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
•User1 must be able to enroll all the New York office mobile devices in Intune.
•Azure ATP 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 Intune and configured in accordance with the corporate policy.
•Configure Windows Information Protection (W1P) for the Windows 10 devices.

NEW QUESTION 138
You need to meet the compliance requirements for the Windows 10 devices. What should you create from the Intune admin center?

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

Answer: D

NEW QUESTION 139
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://www.windowscentral.com/whats-difference-HYPERLINK "https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10"between-quality-updates-and-feature-updates-windows-10

NEW QUESTION 144
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 rote.
B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.

C. From the Intune admin center, add User1 as a device enrollment manager.
D. From the Intune admin center, configure the Enrollment restrictions.

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrHYPERLINK "https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager"ollment-manager

NEW QUESTION 148
You need to create the Microsoft Store for Business. Which user can create the store?

A. User2
B. User3
C. User4
D. User5

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for- business
Case Study: 2
A. Datum Case Study: Overview
Existing Environment
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. When you are ready to answer a question, click the Question button to return to the question. Current Infrastructure
A. Datum recently purchased a Microsoft 365 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.ad3tum.com.
Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.
A. Datum uses and processes Personally Identifiable Information (PII).
Problem Statements Requirements
A. Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365. Business Goals
A. Datum warns to be fully compliant with all the relevant data privacy laws in the regions where it operates.
A. Datum wants to minimize the cost of hardware and software whenever possible.
Technical Requirements
A. Datum 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 Office 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 Microsoft 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 36S users signed in Based on the report, the security administrator will 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 US. 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.

NEW QUESTION 150
You need to meet the technical requirement for the EU PII data. What should you create?

A. a retention policy from the Security & Compliance admin center.
B. a retention policy from the Exchange admin center
C. a data loss prevention (DLP) policy from the Exchange admin center
D. a data loss prevention (DLP) policy from the Security & Compliance admin center

Answer: A

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

NEW QUESTION 152
You need to meet the technical requirement for large-volume document retrieval. What should you create?

A. a data loss prevention (DLP) policy from the Security & Compliance admin center
B. an alert policy from the Security & Compliance admin center
C. a file policy from Microsoft Cloud App Security
D. an activity policy from Microsoft Cloud App Security

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

NEW QUESTION 155
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your MS-101 Exam with Our Prep Materials Via below:

https://www.certleader.com/MS-101-dumps.html