

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.

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 2

You have a Microsoft 365 subscription.

Your company purchases a new financial application named App1.

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

You need to prevent the missing information from affecting the 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 3

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

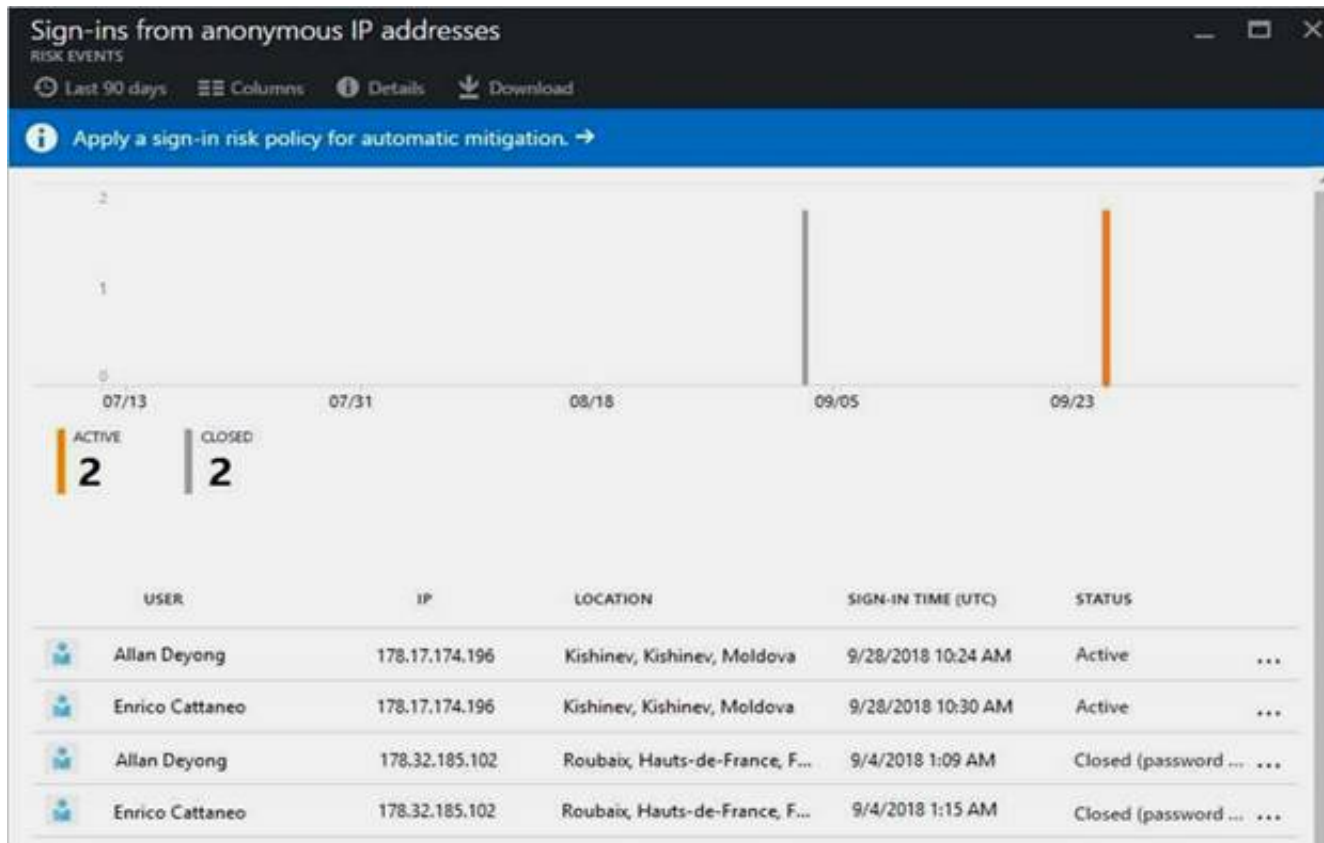
Explanation:

References:

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

NEW QUESTION 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

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

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 6

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)	Not applicable

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 7

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> [HYPERLINK "https://docs.micros](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints)
[oft.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)windows-

defender-advanced-threat-protection

NEW QUESTION 8

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 9

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 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	Role	Member of
User1	Cloud device administrator	Group1
User2	Intune administrator	Group2
User3	None	None

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

Priority	Name	Device limit	Assigned to
1	Policy1	15	Group2
2	Policy2	10	Group1
Default	All users	5	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 a maximum of 10 devices in Intune.	<input type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Intune.	<input type="radio"/>	<input type="radio"/>
User3 can enroll an unlimited number of devices in Intune.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager>

NEW QUESTION 10

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	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

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

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

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

Name	Assigned to
Policy1	Group3
Policy2	Group2

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

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 12

You have Windows 10 Pro devices that are joined to an Active Directory domain. You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise. You are evaluating whether to deploy Windows Hello for Business for SSO to Microsoft 365 services. What are two prerequisites of the deployment? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Microsoft Azure Active Directory (Azure AD)
- B. smartcards
- C. Microsoft Intune enrollment
- D. TPM-enabled devices
- E. computers that have biometric hardware features

Answer: AC

Explanation:

References:

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

NEW QUESTION 13

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 14

HOTSPOT

Your company is based in the United Kingdom (UK).

Users frequently handle data that contains Personally Identifiable Information (PII).

You create a data loss prevention (DLP) policy that applies to users inside and outside the company. The policy is configured as shown in the following exhibit.

New DLP policy

Review your settings

Template name
U.K. Personally Identifiable Information (PII) Data [Edit](#)

Policy name
U.K. Personally Identifiable Information (PII) Data [Edit](#)

Description [Edit](#)

Applies to content in these locations [Edit](#)
Exchange email
SharePoint sites
OneDrive accounts

Policy settings [Edit](#)
If the content contains these types of sensitive info: U.K., National Insurance Number (NINO)U.S. / U.K. Passport Number then notify people with a policy tip and email message.
If there are at least 10 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override.

Turn policy on after it's created? [Edit](#)
Yes

[Back](#) [Create](#) [Cancel](#)

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

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

NEW QUESTION 16
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 20

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains the file servers shown in the following table.

Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

A file named File1.abc is stored on Server1. A file named File2.abc is stored on Server2. Three apps named App1, App2, and App3 all open files that have the .abc file extension.

You implement Windows Information Protection (WIP) by using the following configurations:

Exempt apps: App2

Protected apps: App1

Windows Information Protection mode: Block
Network boundary: IPv4 range of: 192.168.1.1-192.168-1.255
You need to identify the apps from which you can open File1.abc.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
You can open File1.abc in App1.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App2.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure>

NEW QUESTION 22

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 23

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the OLP policy.

You need to prevent the users from bypassing the DLP policy. What should you configure?

- A. incident reports
- B. actions
- C. exceptions
- D. user overrides

Answer: D

Explanation:

References:

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

NEW QUESTION 24

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 29

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 30

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 an Apple Configurator enrollment profile. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 35

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 37

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 40

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 44

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 46

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 49

HOTSPOT

From the Security & Compliance admin center, you create a retention policy named Policy1. You need to prevent all users from disabling the policy or reducing the retention period.

Which command should you run? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

▼	-Identity "Policy1"	▼	\$true
Set-ComplianceTag		-enabled	
Set-HoldCompliancePolicy		-Force	
Set-RetentionCompliancePolicy		-RestrictiveRetention	
Set-RetentionPolicy		-RetentionPolicyTagLinks	
Set-RetentionPolicyTag		-SystemTag	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-pHYPERLINK>
"https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps"s

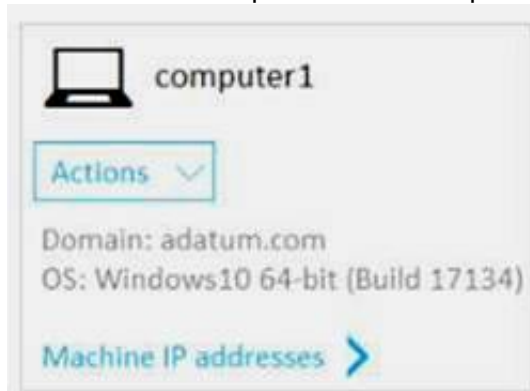
NEW QUESTION 52

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)	<i>Not applicable</i>

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 55

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 59

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint site.

What should you do?

- A. From the Security & Compliance admin center, create an alert policy.
- B. From the SharePoint site, create an alert.
- C. From the SharePoint admin center, modify the sharing settings.
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/create-activity-alerts>

NEW QUESTION 62

HOTSPOT

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

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

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

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

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

Name	Include	Exclude
Policy1	Group3	None
Policy2	Group2	Group3

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

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 66

HOTSPOT

Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain. You update the Windows 10 devices by using Windows Update for Business.

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

NOTE: Each correct selection is worth one point.

Quality updates:

14 days

30 days

60 days

120 days

Feature updates:

60 days

180 days

365 days

540 days

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 67

Your company uses Microsoft System Center Configuration Manager (Current Branch) and Microsoft Intune to co-manage devices.

Which two actions can be performed only from Intune? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

Answer: BD

Explanation:

References:

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

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

NEW QUESTION 70

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. You have a Microsoft 365 subscription.

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

What should you configure?

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

Answer: B

Explanation:

References:

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

NEW QUESTION 71

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 76

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 78

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 83

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 86

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

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

You have a Microsoft 365 subscription.

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

Solution: From the Device Management admin center, you create a trusted location and a compliance policy Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

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

NEW QUESTION 88

HOTSPOT

You have Microsoft 365 subscription.

You create an alert policy as shown in the following exhibit.

Policy1 [X]

[Edit policy](#) [Delete policy](#)

Status ☒ On

Description Description

Severity Low [Edit](#)

Category Threat management

Conditions Activity is Detected malware in file

Aggregation Aggregated

Threshold 20 activities [Edit](#)

Window 120 minutes

Scope All users

Email recipients User1@sk190107outlook.onmicrosoft.com

Daily notification limit 100 [Edit](#)

[Close](#)

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Policy1 will trigger an alert if malware is detected in

- Exchange Online only
- SharePoint Online only
- SharePoint Online or OneDrive only
- Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is

- 5
- 12
- 20
- 100

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Note: The Aggregation settings has a 120 minute window

NEW QUESTION 93

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 96

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com. The domain contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2

The domain contains the devices shown in the following table.

Name	Compliance status
Device1	Compliant
Device2	Noncompliant

The domain contains conditional access policies that control access to a cloud app named App1. The policies are configured as shown in the following table.

Name	Includes	Excludes	Device state includes	Device state excludes	Grant
Policy1	Group1	None	All device states	Device marked as compliant	Block access
Policy2	Group1	Group2	None	None	Block Access
Policy3	Group1	None	All device states	None	Grant access

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

Statements	Yes	No
User1 can access App1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from Device2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 98

HOTSPOT

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

A user named User1 has files on a Windows 10 device as shown in the following table.

Name	Text in file
File1.docx	Importing and exporting is easy. For import, you need a source, and for export, you need a destination.
File2.docx	You must declare what you want to import. Dangerous items cannot be imported. If you want to import valuables, you must pay customs.
File3.docx	IM are initials for instant messaging. You can use Microsoft Skype for IM, but there are also other IM programs.

In Azure Information Protection, you create a label named Label1 that is configured to apply automatically. Label1 is configured as shown in the following exhibit.

Condition: Condition1

Default Directory – Azure Information Protection

Save

Discard

Delete

Choose the type of condition

Information Types

Custom

Name

Condition1

Match exact phrase or pattern

im

Match as a regular expression

Off

On

Match with case sensitivity

Off

On

Minimum number of occurrences

2

Count occurrences with unique values only

Off

On

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

Statements	Yes	No
Label1 applies to File1.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File2.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File3.docx.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 100

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have 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 105

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 108

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:

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 109

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 automatically.
- 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 (WIP) for the Windows 10 devices.

NEW QUESTION 112

On which server should you install the Azure ATP sensor?

- A. Server 1
- B. Server 2
- C. Server 3
- D. Server 4
- E. Server 5

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning>

NEW QUESTION 117

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 121

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

- A. 1
- B. 4
- C. 7
- D. 31

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager>

NEW QUESTION 125

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 127

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/s>[HYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies"](https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies)ecuritycompliance/data-loss- prevention-policies

NEW QUESTION 128

You need to recommend a solution for the security administrator. The solution must meet the technical requirements.

What should you include in the recommendation?

- A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- B. Microsoft Azure Active Directory (Azure AD) Identity Protection
- C. Microsoft Azure Active Directory (Azure AD) conditional access policies
- D. Microsoft Azure Active Directory (Azure AD) authentication methods

Answer: C

Explanation:

References:

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

NEW QUESTION 132

.....

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>