

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 Intune. Solution: You create an Apple Configurator enrollment profile. Does this meet the goal?

A. Yes

B. No

Answer: A

NEW QUESTION 2

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

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

You have a Microsoft 365 subscription.

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

You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the SharePoint site, you create an alert.

Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 3

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	None

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

Statements

Yes

No

User1 can view Device1 in Windows Defender Security Center.

☐
☐

User2 can sign in to Windows Defender Security Center.

☐
☐

User3 can view Device1 in Windows Defender Security Center.

☐
☐

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Statements

Yes

No

User1 can view Device1 in Windows Defender Security Center.

☒
☐

User2 can sign in to Windows Defender Security Center.

☐
☒

User3 can view Device1 in Windows Defender Security Center.

☒
☐

NEW QUESTION 4

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.

Platform:

▼
Android
iOS
Windows 10 and later
Windows 8.1 and later

Settings:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 5

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 6

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 7

A user receives the following message when attempting to sign in to <https://myapps.microsoft.com>: "Your sign-in was blocked. We've detected something unusual about this sign-in. For example, you might be signing in from a new location device, or app. Before you can continue, we need to verify your identity. Please contact your admin."

Which configuration prevents the users from signing in?

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

Answer: B

Explanation:

References:

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

NEW QUESTION 8

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 9

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 10

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 10

Your company has a Microsoft 365 subscription.

You need to identify which users performed the following privileged administration tasks:

- Deleted a folder from the second-stage Recycle Bin of Microsoft SharePoint
 - Opened a mailbox of which the user was not the owner
 - Reset a user password
- What should you use?

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

Answer: A

Explanation:

References:

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

NEW QUESTION 14

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 17

In Microsoft 365, you configure a data loss prevention (DLP) policy named Policy1. Policy1 detects the sharing of United States (US) bank account numbers in email messages and attachments.

Policy1 is configured as shown in the exhibit. (Click the Exhibit tab.)

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content

- ☒ Block people from sharing and restrict access to shared content
By default, users are blocked from sending email messages to people. You can choose who has access to shared SharePoint and OneDrive content. Block these people from accessing SharePoint and OneDrive content
- ☐ Everyone. Only the content owner, the last modifier, and the site admin will continue to have access
- ☒ Only people outside your organization. People inside your organization will continue to have access.
- ☐ Encrypt email messages (applies only to content in Exchange)

You need to ensure that internal users can email documents that contain US bank account numbers to external users who have an email suffix of contoso.com. What should you configure?

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

Answer: A

Explanation:

References:

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

NEW QUESTION 18

HOTSPOT

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

You have three applications named App1, App2, and App3 that have the same file format.

Your company uses Windows Information Protection (WIP). WIP has the following configurations: Windows Information Protection mode: Silent

Protected apps: App1 Exempt apps: App2

From App1, you create a file named File1.

What is the effect of the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

You can open File1 from:

▼
App1 only
App1 and App2 only
App1 and App3 only
App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

▼
App1 only
App3 only
App1 and App2 only
App2 and App3 only
App1, App2, and App3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

You can open File1 from:

▼
App1 only
App1 and App2 only
App1 and App3 only
App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

▼
App1 only
App3 only
App1 and App2 only
App2 and App3 only
App1, App2, and App3

NEW QUESTION 23

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.

To meet the goal for the manager, create:

<input type="checkbox"/>	A label policy
<input type="checkbox"/>	A retention policy
<input type="checkbox"/>	A supervisor policy
<input type="checkbox"/>	An alert policy
<input type="checkbox"/>	MyAnalytics

To review the messages, the manager must use:

<input type="checkbox"/>	A message trace
<input type="checkbox"/>	An eDiscovery case
<input type="checkbox"/>	MyAnalytics
<input type="checkbox"/>	Outlook Web App

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 24

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 28

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:

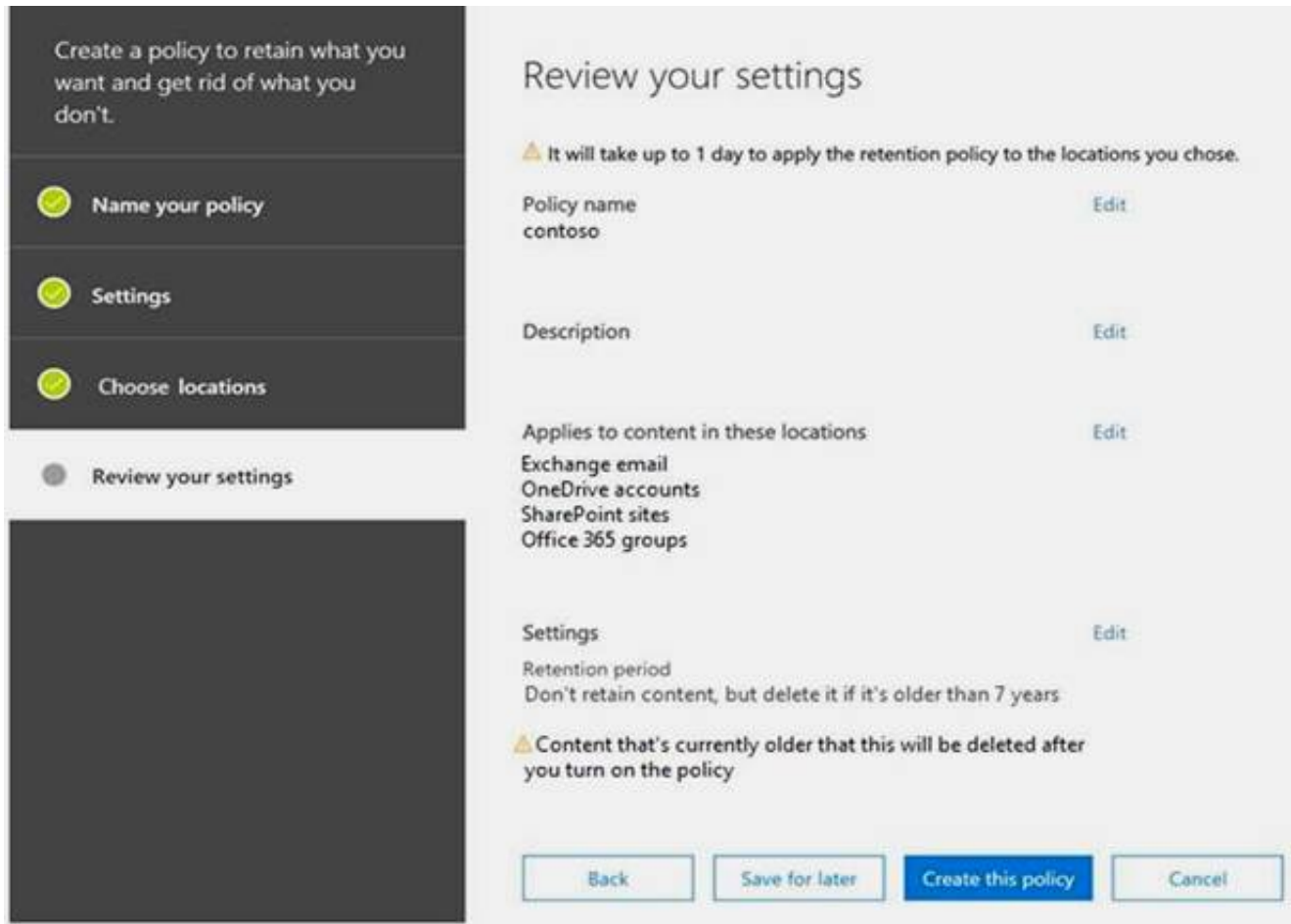
<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

NEW QUESTION 31

HOTSPOT

You have a Microsoft 365 tenant.

You plan to create a retention policy 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.

Microsoft SharePoint files that are affected by the policy will be [answer choice].	<div>▼</div> <div>recoverable for up to seven years</div> <div>deleted seven years after they were created</div> <div>retained for only seven years from when they were created</div>
Once the policy is created, [answer choice].	<div>▼</div> <div>some data may be deleted immediately</div> <div>data will be retained for a minimum of seven years</div> <div>users will be prevented from permanently deleting email messages for seven years</div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Microsoft SharePoint files that are affected by the policy will be [answer choice].	<div>▼</div> <div>recoverable for up to seven years</div> <div>deleted seven years after they were created</div> <div>retained for only seven years from when they were created</div>
Once the policy is created, [answer choice].	<div>▼</div> <div>some data may be deleted immediately</div> <div>data will be retained for a minimum of seven years</div> <div>users will be prevented from permanently deleting email messages for seven years</div>

NEW QUESTION 35

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 39

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

Set-ComplianceTag

Set-HoldCompliancePolicy

Set-RetentionCompliancePolicy

Set-RetentionPolicy

Set-RetentionPolicyTag

-Identity "Policy1"

-enabled

-Force

-RestrictiveRetention

-RetentionPolicyTagLinks

-SystemTag

\$true

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

NEW QUESTION 41
HOTSPOT
You have a Microsoft 365 tenant.
You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

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

Name your label

Label settings

Review your settings

Review your settings

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

Name

6Months

Edit

Description for admins

Edit

Description for users

Edit

Retention

6 months

Retain and Delete

Based on when it was created

Edit

Back

Create this label

Cancel

You create a label policy as shown in the Label Policy Exhibit. (Click the Label Policy tab.)

Automatically apply a label to content

Choose label to auto-apply

Choose conditions

Name your policy

Locations

Review your settings

Close

Detect content that matches this query:

Conditions

We'll apply this policy to content that matches these conditions.

Keyword query editor

ProjectX

Back

Next

Cancel

The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 44

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 48

Your company has a Microsoft 365 tenant.

The company sells products online and processes credit card information.

You need to be notified if a file stored in Microsoft SharePoint Online contains credit card information. The file must be removed automatically from its current location until an administrator can review its contents.

What should you use?

- A. a Security & Compliance data loss prevention (DLP) policy
B. a Microsoft Cloud App Security access policy
C. a Security & Compliance retention policy
D. a Microsoft Cloud App Security file policy

Answer: A

Explanation:

References:

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

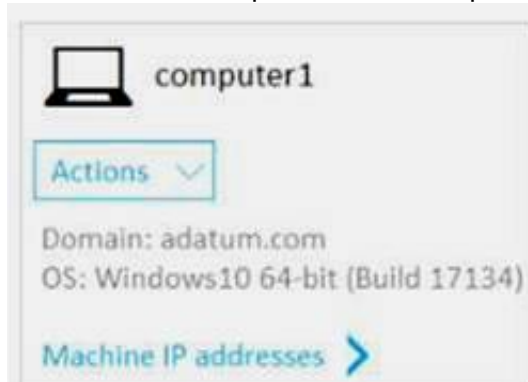
NEW QUESTION 52

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 Policies
- 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 56

Your company uses Microsoft Azure Advanced Threat Protection (ATP) and Windows Defender ATP. You need to integrate Windows Defender ATP and Azure ATP.
What should you do?

- A. From Azure ATP, configure the notifications and reports.
- B. From Azure ATP, configure the data sources.
- C. From Windows Defender Security Center, configure the Machine management settings.
- D. From Windows Defender Security Center, configure the General settings.

Answer: B

Explanation:

References:

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

NEW QUESTION 61

You have a Microsoft 365 tenant.
All users are assigned the Enterprise Mobility + Security license.
You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the device is enrolled in Microsoft Intune automatically.
What should you configure?

- A. Enrollment restrictions from the Intune admin center

- B. device enrollment managers from the Intune admin center
- C. MAM User scope from the Azure Active Directory admin center
- D. MDM User scope from the Azure Active Directory admin center

Answer: D

Explanation:

References:

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

NEW QUESTION 63

HOTSPOT

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

Name	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 have the Android devices shown in the following table.

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

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

User	Group
User1	Group1
User2	Group1, Group2
User3	Group2

The users enroll their device in Microsoft 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
The device of User1 is compliant.	<input type="radio"/>	<input type="radio"/>
The device of User2 is compliant.	<input type="radio"/>	<input type="radio"/>
The device of User3 is compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 67

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-wuufb>**NEW QUESTION 69**

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.

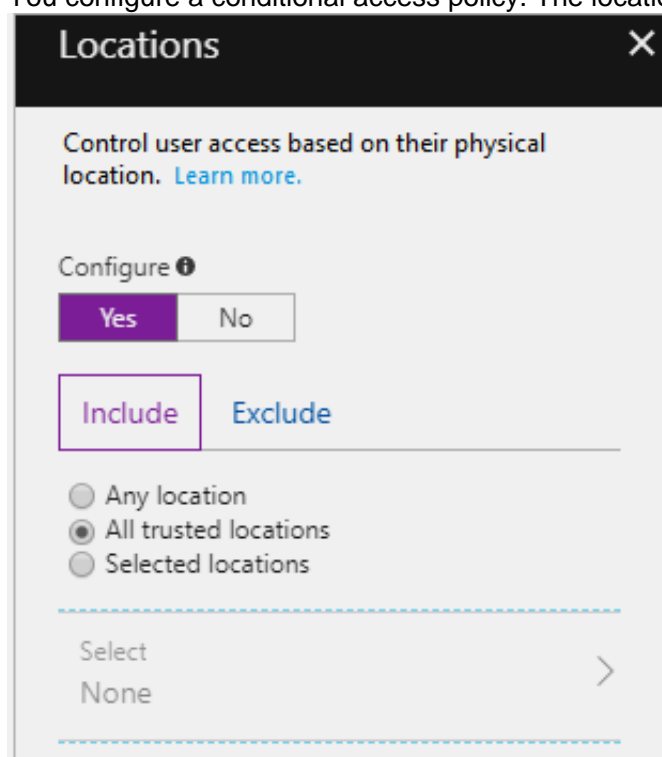
- A. Deploy applications to Windows 10 devices.
- B. Deploy VPN profiles to iOS devices.
- C. Deploy VPN profiles to Windows 10 devices.
- D. Publish applications to Android devices.

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 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 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

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
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 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:

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

NEW QUESTION 81

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 82

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 84

You have a Microsoft 365 subscription.

You recently configured a Microsoft SharePoint Online tenant in the subscription. You plan to create an alert policy.

You need to ensure that an alert is generated only when malware is detected in more than five documents stored in SharePoint Online during a period of 10 minutes.

What should you do first?

- A. Enable Microsoft Office 365 Cloud App Security.
- B. Deploy Windows Defender Advanced Threat Protection (Windows Defender ATP)
- C. Enable Microsoft Office 365 Analytics.

Answer: B

NEW QUESTION 85

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 90

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 92

HOTSPOT


You have a Microsoft 365 subscription that uses a default domain named contoso.com. Three files were created on February 1, 2019, as shown in the following table.

Name	Stored in
File1	Microsoft OneDrive
File2	A Microsoft SharePoint library
File3	Microsoft Exchange Online email

On March 1, 2019, you create two retention labels named Label1 and Label2.


The settings for Lable1 are configured as shown in the Label1 exhibit. (Click the Label1 tab.)


Label settings

Retention 


☒ On


When this label is applied to content...

☒ Retain the content 


For this long... years 


What do you want to do after this time?


☐ Delete the content automatically. 


☒ Trigger a disposition review. 


Notify these people when there are items ready to review




☐ Nothing. Leave the content as is. 

☐ Don't retain the content. Just delete it if it's older than 

years 

Retain or delete the content based on 

Label classification

☐ Use label to classify content as a "Record" 

The settings for Lable2 are configured as shown in the Label2 exhibit. (Click the Label2 tab.)

You apply the retention labels to Exchange email, SharePoint sites, and OneDrive accounts.

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

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	<input type="radio"/>	<input type="radio"/>
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input type="radio"/>
File3 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/labels> <https://docs.microsoft.com/en-us/office365/securitycompliance/disposition-reviews>

NEW QUESTION 96

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. You sign for Microsoft Store for Business. The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	None
User2	Basic Purchaser	None
User3	None	Application administrator
User4	None	Cloud application administrator
User5	None	None

Microsoft Store for Business has the following Shopping behavior settings: Allow users to shop is set to On

Make everyone a Basic Purchaser is set to Off

You need to identify which users can install apps from the Microsoft for Business private store.

Which users should you identify?

- A. User1, User2, User3, User4, and User5
- B. User1 only
- C. User1 and User2 only
- D. User3 and User4 only
- E. User1, User2, User3, and User4 only

Answer: C

Explanation:

References:

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

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 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 104

HOTSPOT

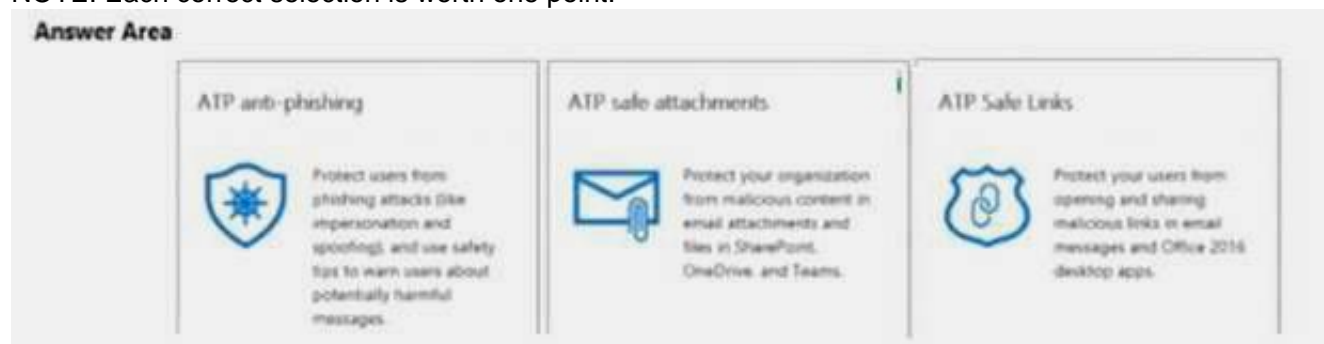
Your company has a Microsoft 365 subscription.

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

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

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

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 106

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 107

HOTSPOT

You need to configure a conditional access policy to meet the compliance requirements. You add Exchange Online as a cloud app.

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

NOTE: Each correct selection is worth one point.

New

Conditions

Device state (preview)

Info

Name

Policy1

Assignments

Users and groups

0 users and groups selected

Cloud apps

1 app included

Conditions

0 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

On Off

Info

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps (preview)

Not configured

Device state (preview)

Not configured

Info

Configure

Yes No

Include Exclude

Select the device state condition used to exclude devices from policy.

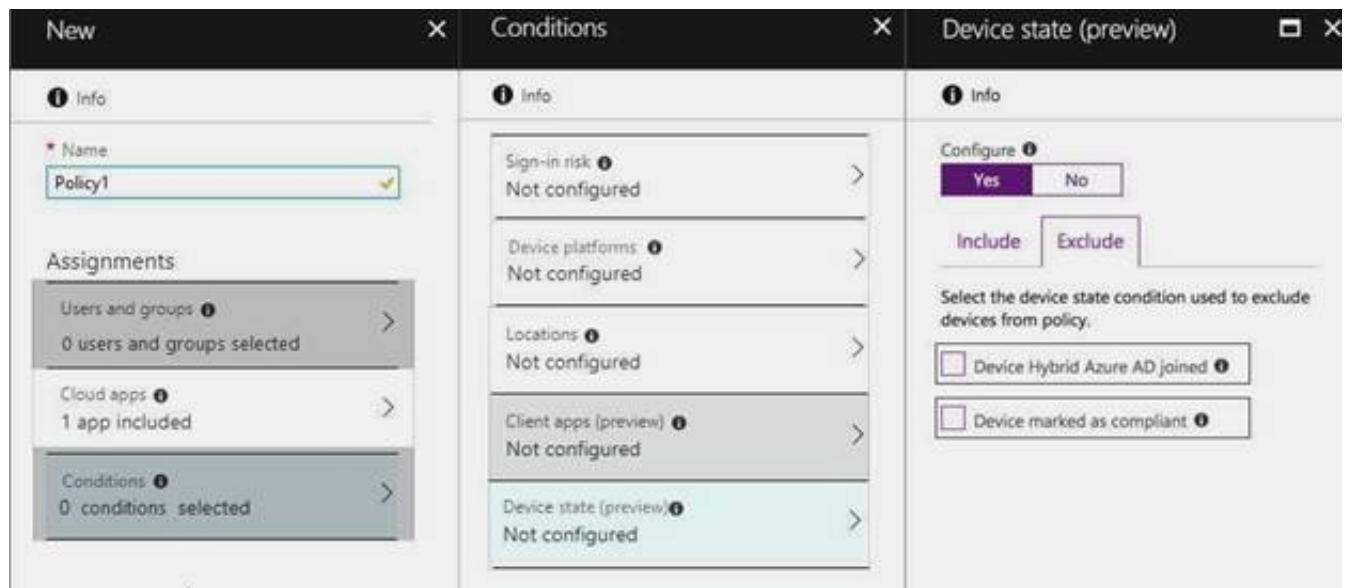
Device Hybrid Azure AD joined

Device marked as compliant

- A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 112

HOTSPOT

You need to meet the Intune requirements for the Windows 10 devices.

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

Settings to configure in Azure AD:	<div><div></div><div>Device settings</div><div>Mobility (MDM and MAM)</div><div>Organizational relationships</div><div>User settings</div></div>
Settings to configure in Intune:	<div><div></div><div>Device compliance</div><div>Device configuration</div><div>Device enrollment</div><div>Mobile Device Management Authority</div></div>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 113

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.

Seattle:	<div><div></div><div>6 months</div><div>18 months</div><div>24 months</div><div>30 months</div><div>5 years</div></div>
New York:	<div><div></div><div>6 months</div><div>18 months</div><div>24 months</div><div>30 months</div><div>5 years</div></div>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

[https://www.windowcentral.com/whats-difference-HYPERLINK "https://www.windowcentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10"between-quality-updates-and-feature-updates-windows-10](https://www.windowcentral.com/whats-difference-HYPERLINK-https://www.windowcentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10/between-quality-updates-and-feature-updates-windows-10)

NEW QUESTION 118

You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?

- A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator role.
- B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
- C. From the 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-enrollment-manager>

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 122

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/ediscovery-office-365/>

NEW QUESTION 126

HOTSPOT

You need to meet the technical requirement for log analysis.

What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Minimum number of data sources:	<div><div>▼</div><div>1</div><div>3</div><div>6</div></div>
Minimum number of log collectors:	<div><div>▼</div><div>1</div><div>3</div><div>6</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 128

You need to protect the U.S. PII data to meet the technical requirements. What should you create?

- A. a data loss prevention (DLP) policy that contains a domain exception
- B. a Security & Compliance retention policy that detects content containing sensitive data
- C. a Security & Compliance alert policy that contains an activity
- D. a data loss prevention (DLP) policy that contains a user override

Answer: C

Explanation:

References:

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

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>