



Microsoft

Exam Questions MS-101

Microsoft 365 Mobility and Security (beta)

NEW QUESTION 1

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

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

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

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

Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 2

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

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

You have a Microsoft 365 subscription.

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

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

Solution: From the Security & Compliance admin center, you create a threat management policy. Does this meet the goal?

A. Yes

B. No

Answer: A

NEW QUESTION 3

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

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

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 4

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

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

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

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

You configure pilot co-management

You add a new device named Device 1 to the domain. You install the Configuration Manager client on Device1.

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

Solution: You create a device configuration profile from the Intune admin center. Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 5

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 is a member of Group1.

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

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

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

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

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

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 6

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 Application 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 7

DRAG DROP

You create a Microsoft 365 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 8

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 9

You have a Microsoft 365 tenant

You have a line-of-business application named App1 that users access by using the My Apps portal. After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control,

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

What should you do?

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

Answer: A

Explanation:

References:

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

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

NEW QUESTION 10

HOTSPOT

You plan to allow users from the engineering department to enroll their mobile device in mobile device management (MDM).

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Device limit:

▼
5
10
15

Allowed platform:

▼
Android only
iOS only
All platforms

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Device limit:

▼
5
10
15

Allowed platform:

▼
Android only
iOS only
All platforms

NEW QUESTION 13

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 18

You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content. What should you do?

- A. From the AADRM PowerShell module, run the set-AadrmOnboardingControlPolicy cmdlet.
- B. From Azure Information Protection, create a policy.

- C. From the AAORM PowerShell module, run the Add-AadrmRoleBasedAdministrator cmdlet.
- D. From Azure Information Protection, configure the protection activation status.

Answer: B

Explanation:

References:

<https://blogs.technet.microsoft.com/kemckinn/2018/05/17/creating-labels-for-azure-information- protection/>

NEW QUESTION 21

HOTSPOT

You have retention policies in Microsoft 365 as shown in the following table.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

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

Decide if you want to retain content, delete it, or both

Do you want to retain content?

☐ Yes, I want to retain it

For this long... 7 years

☒ No, just delete content that's older than

2 years

Delete the content based on when it was created

Need more options?

☐ Use advanced retention settings

Back

Next

Cancel

Policy2 is configured as shown in the Policy2 exhibit. (Click the Policy2 tab.)

Decide if you want to retain content, delete it, or both

Do you want to retain content?

☒ Yes, I want to retain it

For this long... 4 years

Retain the content based on when it was created

Do you want us to delete it after this time?

☐ Yes ☒ No

☐ No, just delete content that's older than

2 years

Need more options?

☐ Use advanced retention settings

Back

Next

Cancel

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

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or-what-takes-precedence>

NEW QUESTION 24

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 28

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 31

HOTSPOT

You have a data loss prevention (DLP) policy.

You need to increase the likelihood that the DLP policy will apply to data that contains medical terms from the International Classification of Diseases (ICD-9-CM).

The solution must minimize the number of false positives.

Which two settings should you modify? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

Content contains

Any of these ▾

PII Identifiers

Sensitive info type

U.S. Social Security Number (SSN)

Instance count

min 1 max any

Match accuracy

min 50 max 100

Add ▾

and ▾

Any of these ▾

Medical Terms

Sensitive info type

International Classification of Diseases (ICD-9-CM)

Instance count

min 1 max any

Match accuracy

min 50 max 100

Add ▾

A. Mastered

B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies> <https://docs.microsoft.com/en-us/office365/securitycompliance/what-the-sensitive-information-types-look-for#international-classification-of-diseases-icd-9-cm>

NEW QUESTION 35

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

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

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

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

You configure pilot co-management.

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

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

Solution: You add Device1 to an Active Directory group. Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

References:

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

NEW QUESTION 38

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 40

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

NEW QUESTION 45

You create a new Microsoft 365 subscription and assign Microsoft 365 E3 licenses to 100 users. From the Security & Compliance admin center, you enable auditing.

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. An administrator creates a new Microsoft SharePoint site collection.
- B. An administrator creates a new mail flow rule.
- C. A user shares a Microsoft SharePoint folder with an external user.
- D. A user delegates permissions to their mailbox.
- E. A user purges messages from their mailbox.

Answer: ABC

Explanation:

References:

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

NEW QUESTION 46

DRAG DROP

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

Workspace

Manage Azure ATP user roles

Create Workspace

NAME	TYPE	INTEGRATION	GEOLOCATION
testworkspace	Primary	Windows Defender ATP	Europe

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

Sensors

Configure Directory Services to install the first Sensor or Standalone Sensor.

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

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

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

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 47

HOTSPOT

You configure an anti-phishing policy as shown in the following exhibit.

Policy setting	Policy name Description Applied to	Managers
		If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.OnMicrosoft.com
Impersonation	Users to protect Protect all domains I own Protect specific domains Action > User impersonation Action > Domain impersonation Safety tips > User impersonation Safety tips > Domain impersonation Safety tips > Unusual characters Mailbox intelligence	On - 3 User(s) specified On On - 2 Domain(s) specified Move message to the recipients' Junk Email folders Delete the message before it's delivered Off Off Off Off
Spoof	Enable antispoofting protection Action	On Quarantine the message
Advanced settings	Advanced phishing thresholds	3 - More Aggressive

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

If a message is identified as a domain impersonation, [answer choice].	<div>the message is delivered to the Inbox folder</div> <div>the message is moved to the Deleted Items folder</div> <div>the messages are moved to the Junk Email folder</div>
To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].	<div>Advanced phishing thresholds</div> <div>Domain impersonation</div> <div>Enable antispoofting protection</div> <div>Mailbox intelligence</div>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

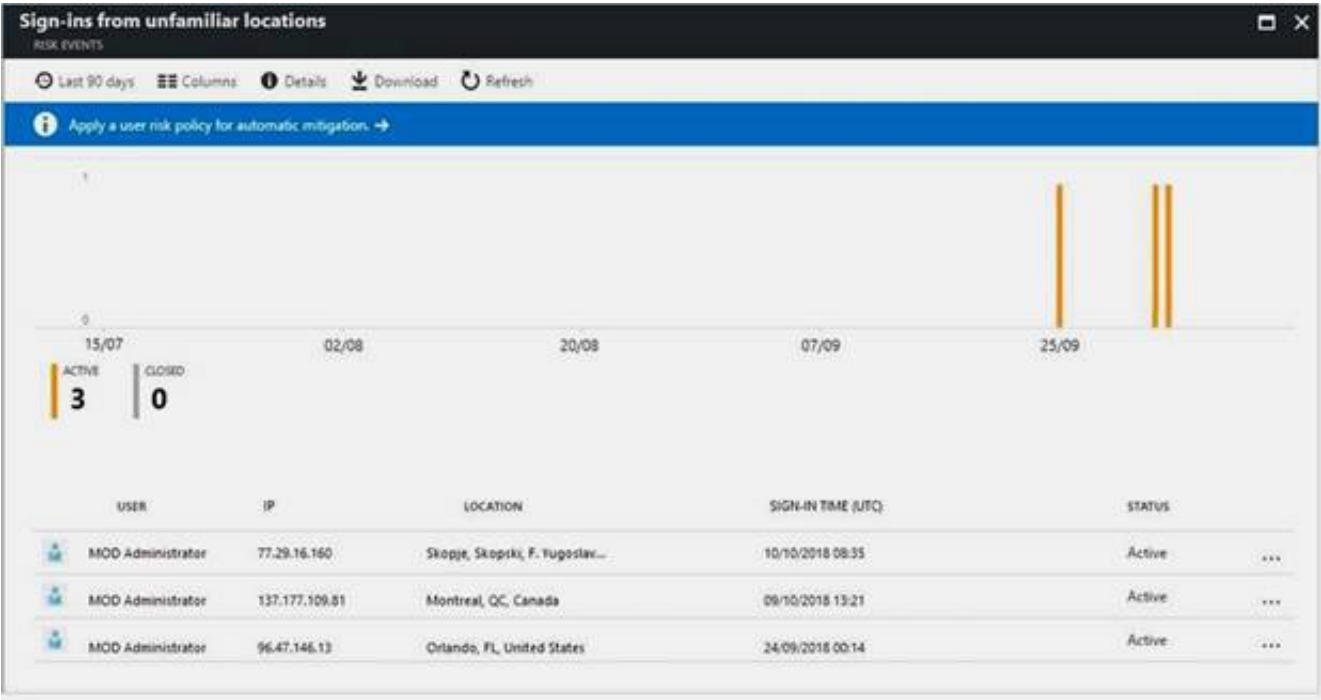
References:

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

NEW QUESTION 48

HOTSPOT

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



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

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

named location in Azure AD

sign-in risk policy

user risk policy

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

a named location in Azure AD

a sign-in risk policy

a user risk policy

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

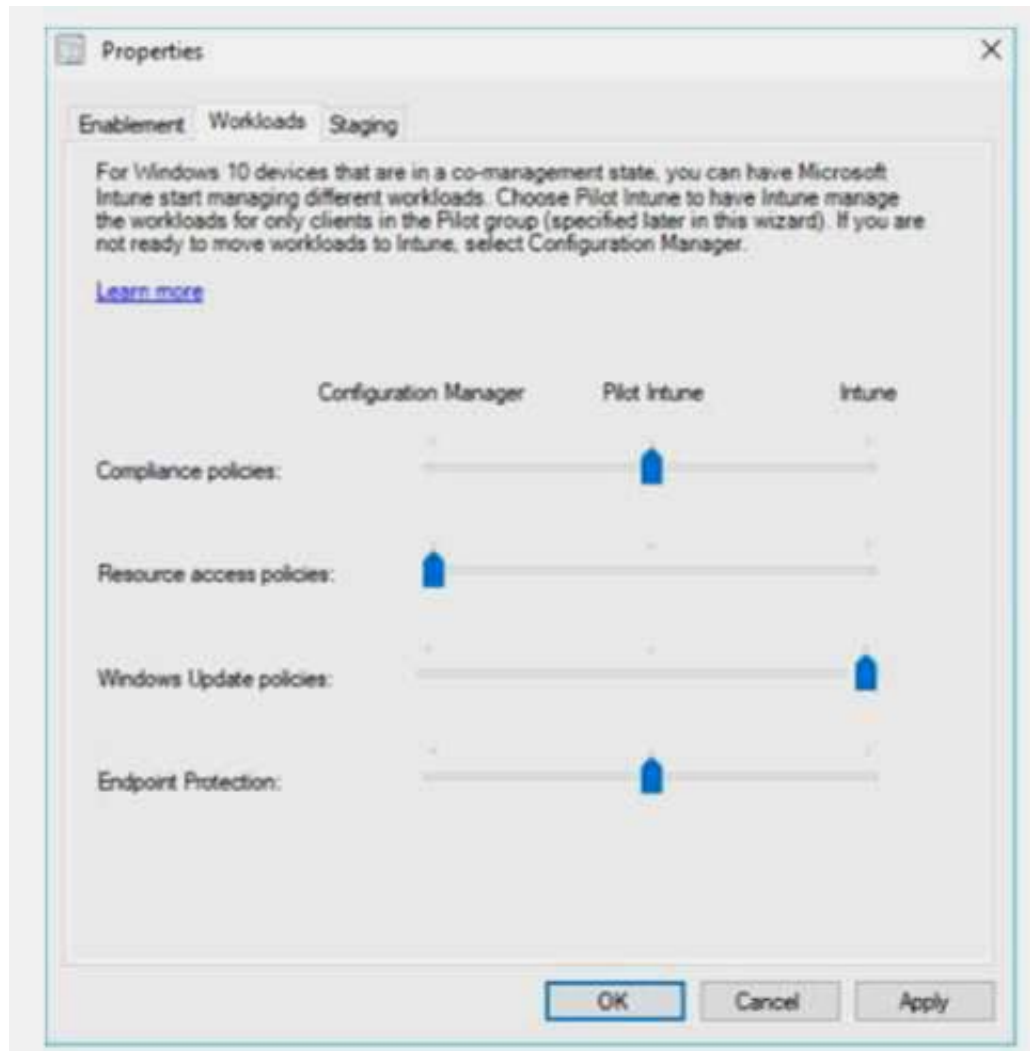
References:
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy>
<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations>

NEW QUESTION 53
HOTSPOT

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

Name	Collection
Device1	Collection1
Device2	Collection2

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



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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 58

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 59

HOTSPOT

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

You have Windows 10 and Windows 8.1 devices.

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

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

First action to perform:

<input type="checkbox"/>	Enroll the devices in Microsoft Intune.
<input type="checkbox"/>	Configure device compliance in Microsoft Intune.
<input type="checkbox"/>	Create a Microsoft Azure Log Analytics workspace.
<input type="checkbox"/>	Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:

<input type="checkbox"/>	Configure all the devices to have a commercial ID.
<input type="checkbox"/>	Configure software inventory in Configuration Manager.
<input type="checkbox"/>	Configure all the devices to join the Windows Insider Program.
<input type="checkbox"/>	Configure and restart the Windows Update service on all the devices.

A. Mastered

B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 63

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 68

Your company uses on-premises Windows Server File Classification Infrastructure (FCI). Some documents on the on-premises file servers are classified as Confidential.

You migrate the files from the on-premises file servers to Microsoft SharePoint Online.

You need to ensure that you can implement data loss prevention (DLP) policies for the uploaded file based on the Confidential classification.

What should you do first?

A. From the SharePoint admin center, configure hybrid search.

B. From the SharePoint admin center, create a managed property.

C. From the Security & Compliance Center PowerShell, run the New-DataClassification cmdlet.

D. From the Security & Compliance Center PowerShell, run the New-DlpComplianceRule cmdlet.

Answer: D

Explanation:

References:

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

NEW QUESTION 70

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 71

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

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

You have a Microsoft 365 subscription.

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

Solution: From the Microsoft 365 admin center, you configure the Organization profile settings. Does this meet the goal?

- A. Yes
B. No

Answer: B

Explanation:

References:

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

NEW QUESTION 72

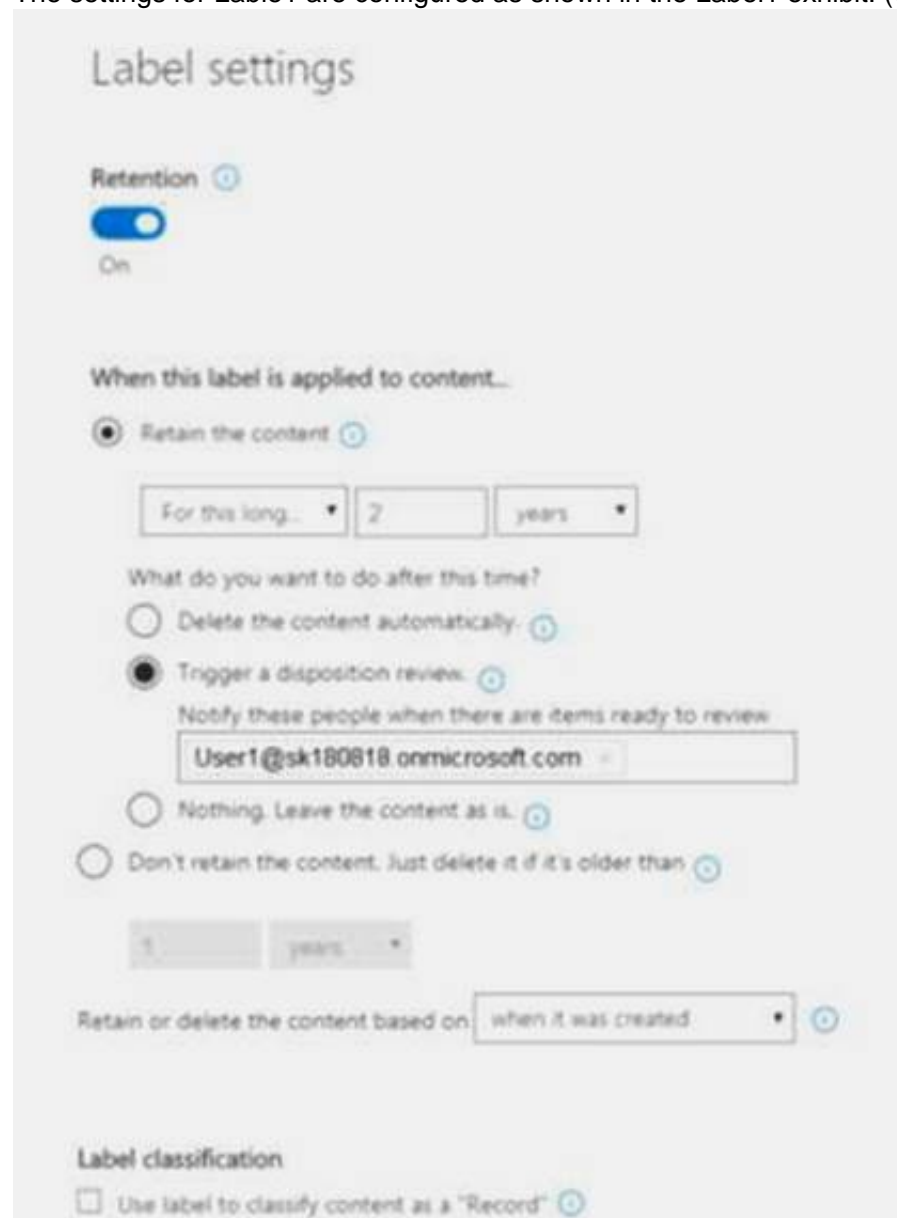
HOTSPOT

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

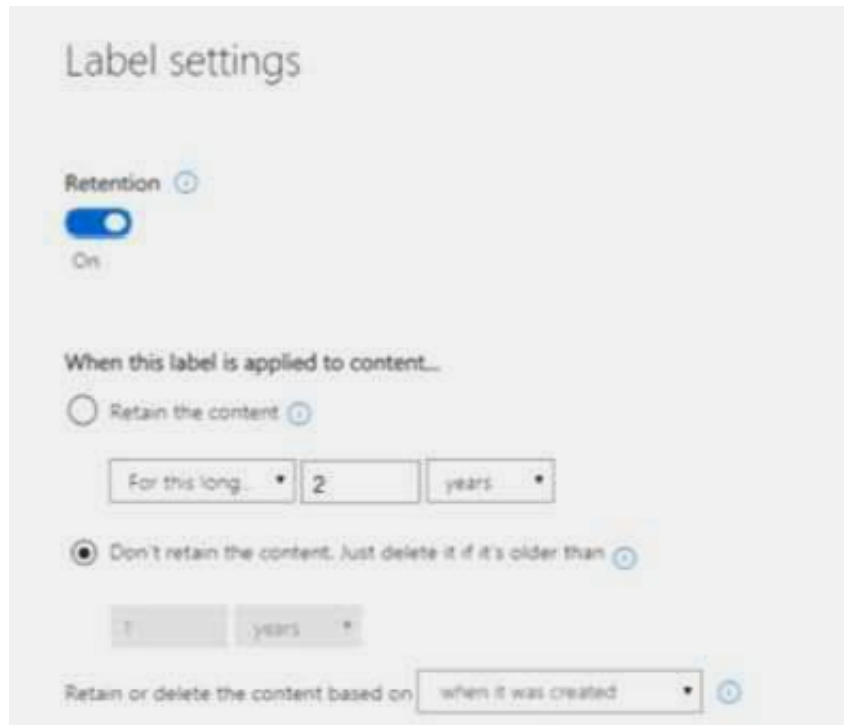
Name	Stored in
File1	Microsoft OneDrive
File2	A Microsoft SharePoint library
File3	Microsoft Exchange Online email

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

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



The settings for Label2 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 76

You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content. What should you do?

- A. Run the Add-AadrmRoleBasedAdministrator cmdlet.
- B. Create an Azure Information Protection policy.
- C. Configure the protection activation status for Azure Information Protection.
- D. Run the Set-AadrmOnboardingControlPolicy cmdlet.

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/information-protection/activate-service>

NEW QUESTION 80

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

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

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-AzureRmRoleAssignment cmdlet with the appropriate parameters.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/azurerms/resources/new-azurermroleassignment?view=azurermps-6.13.0>

NEW QUESTION 82

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

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

You configure the Microsoft 365 subscription to ensure that the new devices enroll in Microsoft Intune automatically.

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

Answer: C

NEW QUESTION 83

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 (W1P) for the Windows 10 devices.

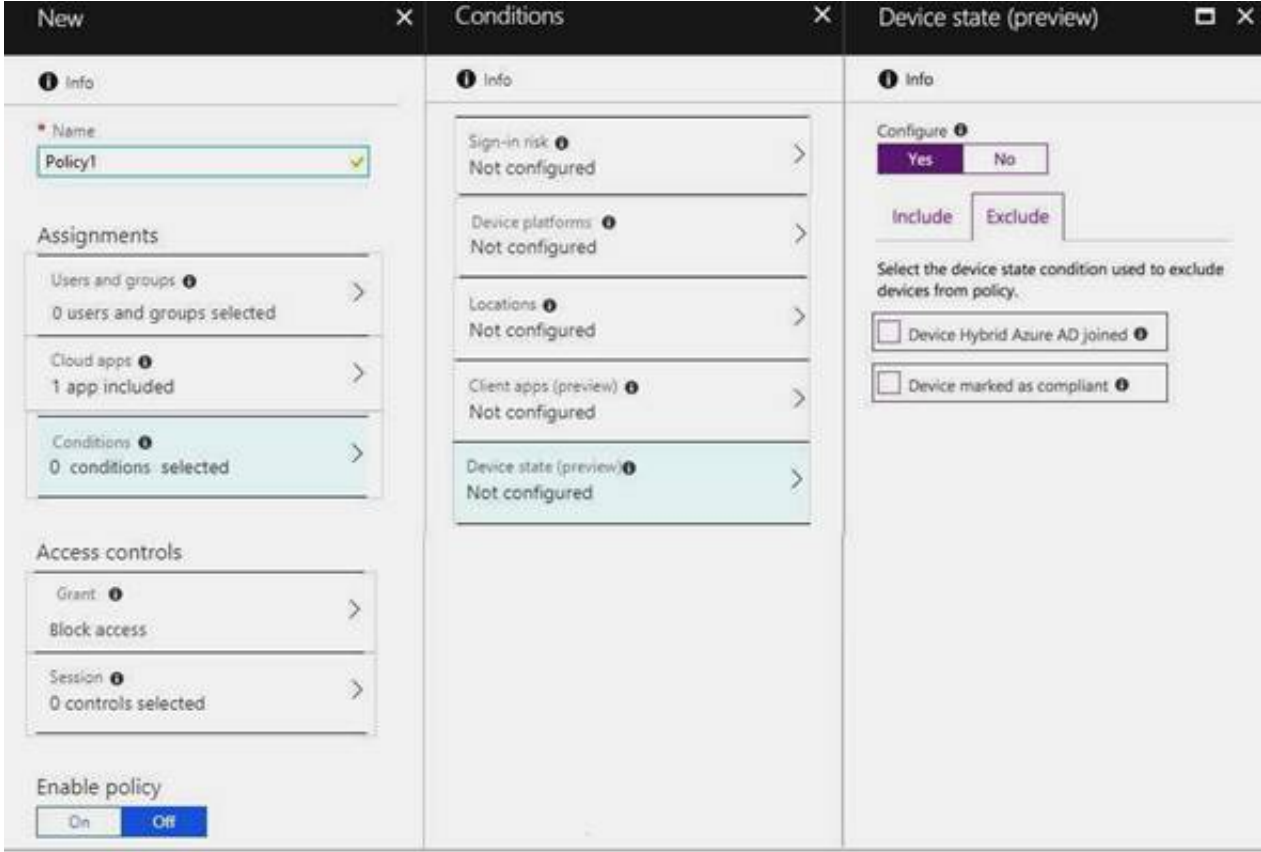
NEW QUESTION 85

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.

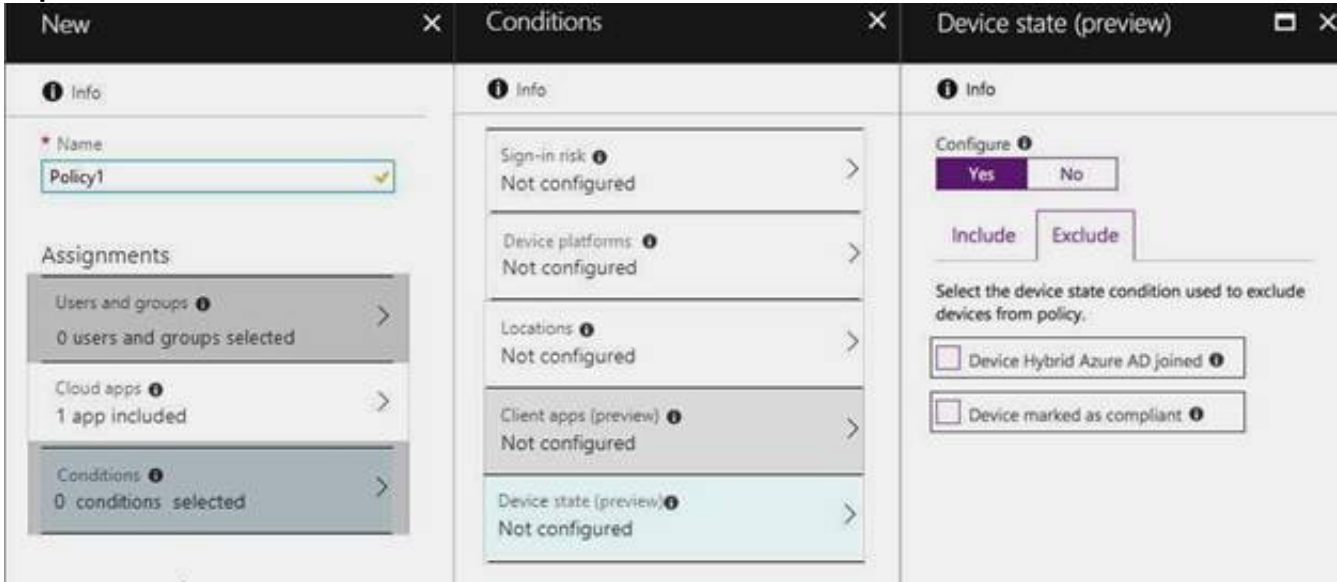
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

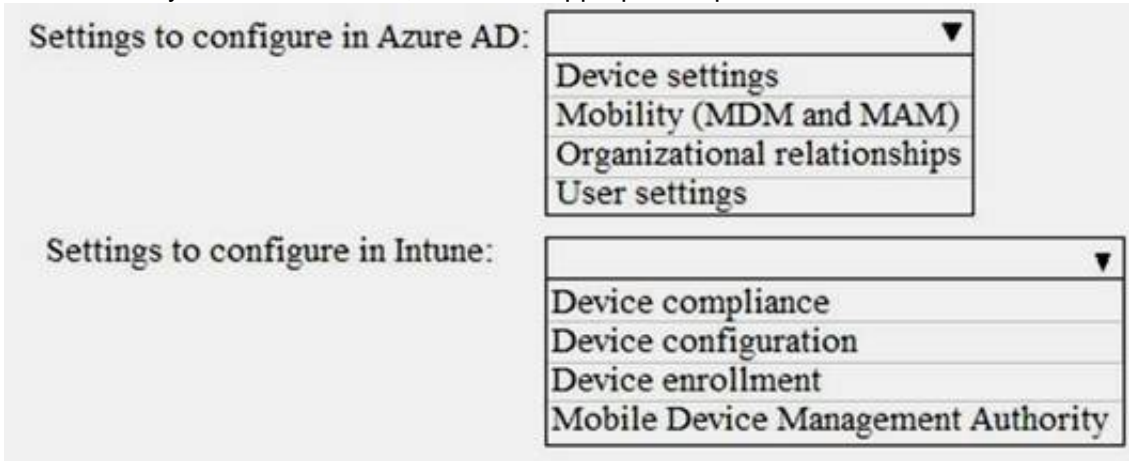


NEW QUESTION 86

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.



- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 90

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

NEW QUESTION 95

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/edisHYPERLINK \"https://www.sherweb.com/blog/ediscovery-office-365/\"covery-office-365/](https://www.sherweb.com/blog/edisHYPERLINK \)

NEW QUESTION 96

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 101

.....

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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

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

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

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

Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 2

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

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

You have a Microsoft 365 subscription.

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

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

Solution: From the Security & Compliance admin center, you create a threat management policy. Does this meet the goal?

A. Yes

B. No

Answer: A

NEW QUESTION 3

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

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

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 4

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

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

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

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

You configure pilot co-management

You add a new device named Device 1 to the domain. You install the Configuration Manager client on Device1.

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

Solution: You create a device configuration profile from the Intune admin center. Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 5

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 is a member of Group1.

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

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

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

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

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

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 6

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 Application 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 7

DRAG DROP

You create a Microsoft 365 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 8

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 9

You have a Microsoft 365 tenant

You have a line-of-business application named App1 that users access by using the My Apps portal. After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control,

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

What should you do?

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

Answer: A

Explanation:

References:

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

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

NEW QUESTION 10

HOTSPOT

You plan to allow users from the engineering department to enroll their mobile device in mobile device management (MDM).

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Device limit:

▼
5
10
15

Allowed platform:

▼
Android only
iOS only
All platforms

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Device limit:

▼
5
10
15

Allowed platform:

▼
Android only
iOS only
All platforms

NEW QUESTION 13

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 18

You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content. What should you do?

- A. From the AADRM PowerShell module, run the set-AadrmOnboardingControlPolicy cmdlet.
- B. From Azure Information Protection, create a policy.

- C. From the AAORM PowerShell module, run the Add-AadrmRoleBasedAdministrator cmdlet.
D. From Azure Information Protection, configure the protection activation status.

Answer: B

Explanation:

References:

<https://blogs.technet.microsoft.com/kemckinn/2018/05/17/creating-labels-for-azure-information- protection/>

NEW QUESTION 21

HOTSPOT

You have retention policies in Microsoft 365 as shown in the following table.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

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

Decide if you want to retain content, delete it, or both

Do you want to retain content?

☐ Yes, I want to retain it

For this long...7years

☒ No, just delete content that's older than

2years

Delete the content based onwhen it was created

Need more options?

☐ Use advanced retention settings

BackNextCancel

Policy2 is configured as shown in the Policy2 exhibit. (Click the Policy2 tab.)

Decide if you want to retain content, delete it, or both

Do you want to retain content?

☒ Yes, I want to retain it

For this long...4years

Retain the content based onwhen it was created

Do you want us to delete it after this time?

☐ Yes☒ No

☐ No, just delete content that's older than

2years

Need more options?

☐ Use advanced retention settings

BackNextCancel

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
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or-what-takes-precedence>

NEW QUESTION 24

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 28

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 31

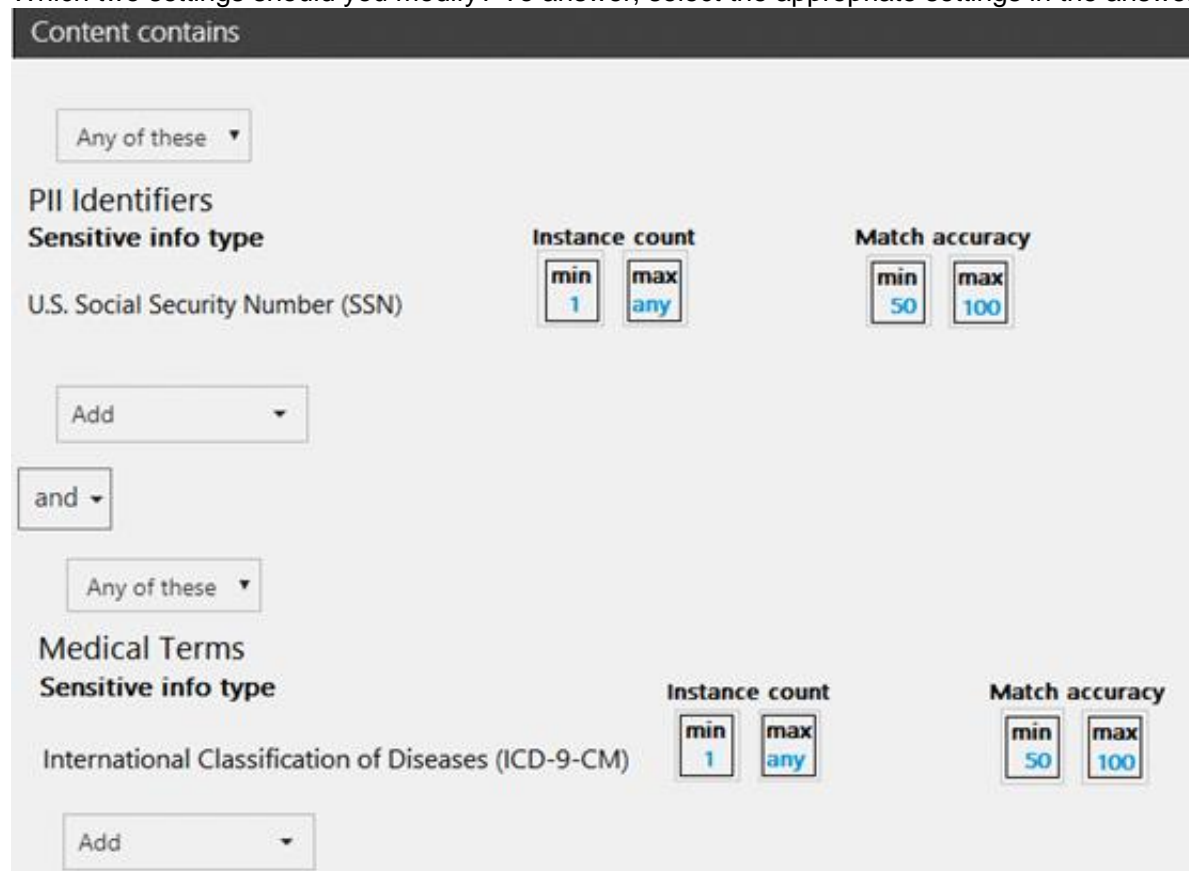
HOTSPOT

You have a data loss prevention (DLP) policy.

You need to increase the likelihood that the DLP policy will apply to data that contains medical terms from the International Classification of Diseases (ICD-9-CM).

The solution must minimize the number of false positives.

Which two settings should you modify? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered

B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies> <https://docs.microsoft.com/en-us/office365/securitycompliance/what-the-sensitive-information-types-look-for#international-classification-of-diseases-icd-9-cm>

NEW QUESTION 35

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

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

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

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

You configure pilot co-management.

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

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

Solution: You add Device1 to an Active Directory group. Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

References:

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

NEW QUESTION 38

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 40

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

<div><div></div><div>Set-ComplianceTag</div></div> <div><div></div><div>Set-HoldCompliancePolicy</div></div> <div><div></div><div>Set-RetentionCompliancePolicy</div></div> <div><div></div><div>Set-RetentionPolicy</div></div> <div><div></div><div>Set-RetentionPolicyTag</div></div>	<code>-Identity "Policy1"</code>	<div><div></div><div>-enabled</div></div> <div><div></div><div>-Force</div></div> <div><div></div><div>-RestrictiveRetention</div></div> <div><div></div><div>-RetentionPolicyTagLinks</div></div> <div><div></div><div>-SystemTag</div></div>	<code>\$true</code>
--	----------------------------------	--	---------------------

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 45

You create a new Microsoft 365 subscription and assign Microsoft 365 E3 licenses to 100 users. From the Security & Compliance admin center, you enable auditing.

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. An administrator creates a new Microsoft SharePoint site collection.
- B. An administrator creates a new mail flow rule.
- C. A user shares a Microsoft SharePoint folder with an external user.
- D. A user delegates permissions to their mailbox.
- E. A user purges messages from their mailbox.

Answer: ABC

Explanation:

References:

[https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%25HYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%2farticle%2f0d4d0f35-390b-4518-800e-0c7ec95e946c"2farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c](https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%25HYPERLINK%2Fhttps%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Foffice365%2Fsecuritycompliance%2Fsearch-the-audit-log-in-security-andcompliance%3FredirectSourcePath%3D%252Farticle%2F0d4d0f35-390b-4518-800e-0c7ec95e946c%2Farticle%252F0d4d0f35-390b-4518-800e-0c7ec95e946c)

NEW QUESTION 46

DRAG DROP

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



NAME	TYPE	INTEGRATION	GEOLOCATION
testworkspace	Primary	Windows Defender ATP	Europe

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



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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 47

HOTSPOT

You configure an anti-phishing policy as shown in the following exhibit.

Policy setting	Policy name Description Applied to	Managers
		If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.OnMicrosoft.com
Impersonation	Users to protect Protect all domains I own Protect specific domains Action > User impersonation Action > Domain impersonation Safety tips > User impersonation Safety tips > Domain impersonation Safety tips > Unusual characters Mailbox intelligence	On - 3 User(s) specified On On - 2 Domain(s) specified Move message to the recipients' Junk Email folders Delete the message before it's delivered Off Off Off Off
Spoof	Enable antispoofting protection Action	On Quarantine the message
Advanced settings	Advanced phishing thresholds	3 - More Aggressive

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

If a message is identified as a domain impersonation, [answer choice].	<div>the message is delivered to the Inbox folder</div> <div>the message is moved to the Deleted Items folder</div> <div>the messages are moved to the Junk Email folder</div>
To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].	<div>Advanced phishing thresholds</div> <div>Domain impersonation</div> <div>Enable antispoofting protection</div> <div>Mailbox intelligence</div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

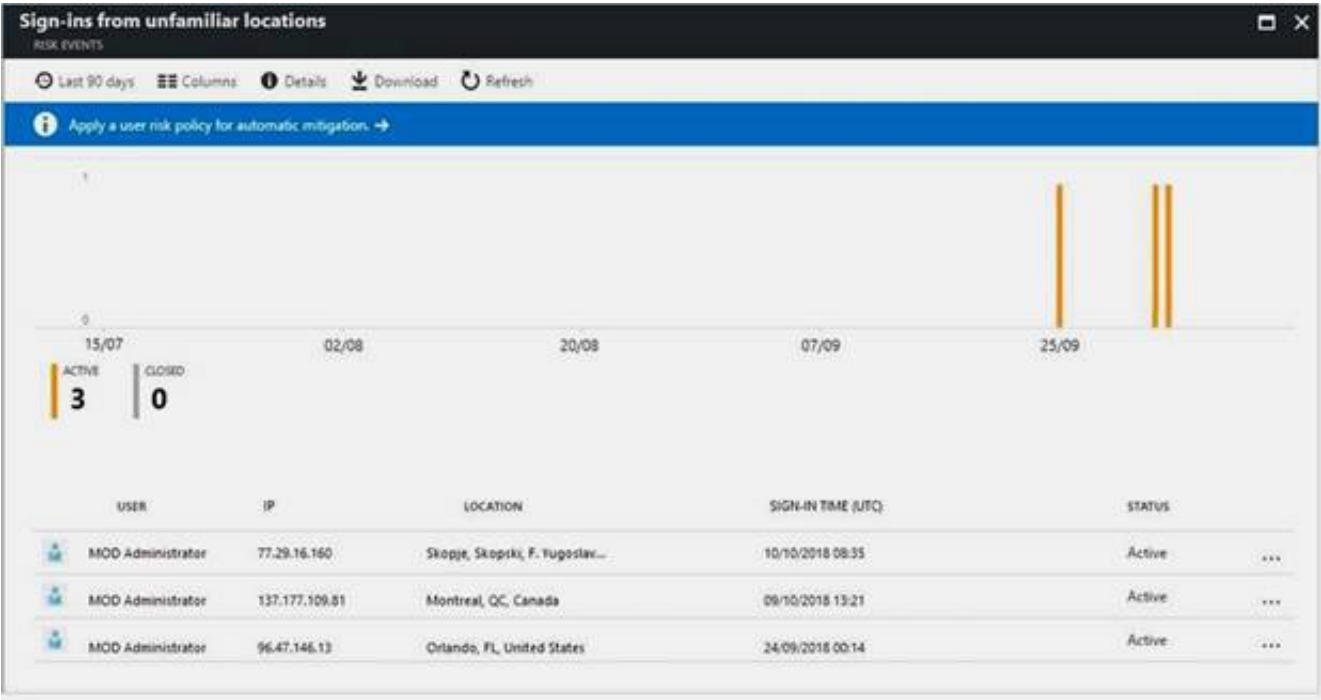
References:

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

NEW QUESTION 48

HOTSPOT

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



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

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

named location in Azure AD

sign-in risk policy

user risk policy

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

a named location in Azure AD

a sign-in risk policy

a user risk policy

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

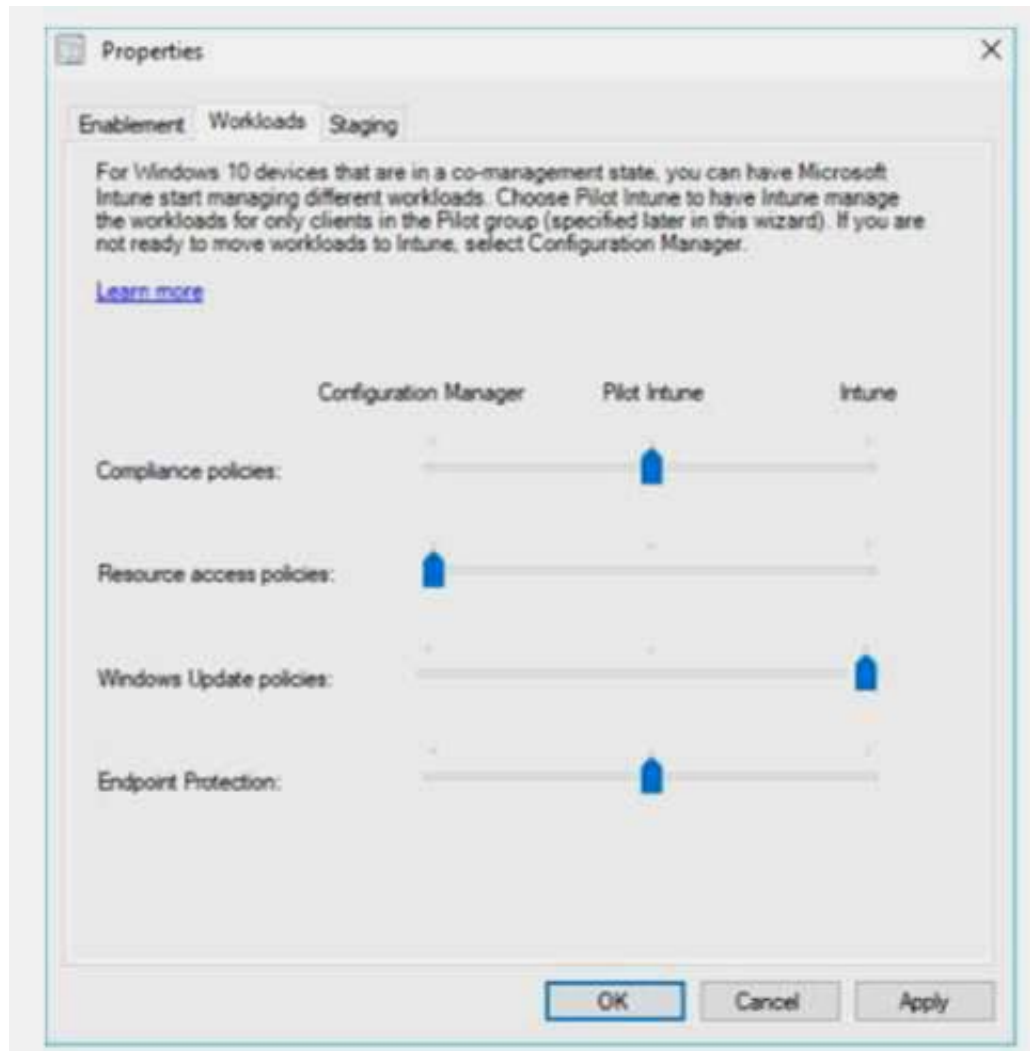
References:
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy>
<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations>

NEW QUESTION 53
HOTSPOT

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

Name	Collection
Device1	Collection1
Device2	Collection2

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



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

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 58

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-wuflb>

NEW QUESTION 59

HOTSPOT

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

You have Windows 10 and Windows 8.1 devices.

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

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

First action to perform:

<input type="checkbox"/>	Enroll the devices in Microsoft Intune.
<input type="checkbox"/>	Configure device compliance in Microsoft Intune.
<input type="checkbox"/>	Create a Microsoft Azure Log Analytics workspace.
<input type="checkbox"/>	Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:

<input type="checkbox"/>	Configure all the devices to have a commercial ID.
<input type="checkbox"/>	Configure software inventory in Configuration Manager.
<input type="checkbox"/>	Configure all the devices to join the Windows Insider Program.
<input type="checkbox"/>	Configure and restart the Windows Update service on all the devices.

A. Mastered

B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 63

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 68

Your company uses on-premises Windows Server File Classification Infrastructure (FCI). Some documents on the on-premises file servers are classified as Confidential.

You migrate the files from the on-premises file servers to Microsoft SharePoint Online.

You need to ensure that you can implement data loss prevention (DLP) policies for the uploaded file based on the Confidential classification.

What should you do first?

A. From the SharePoint admin center, configure hybrid search.

B. From the SharePoint admin center, create a managed property.

C. From the Security & Compliance Center PowerShell, run the New-DataClassification cmdlet.

D. From the Security & Compliance Center PowerShell, run the New-DlpComplianceRule cmdlet.

Answer: D

Explanation:

References:

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

NEW QUESTION 70

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 71

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

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

You have a Microsoft 365 subscription.

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

Solution: From the Microsoft 365 admin center, you configure the Organization profile settings. Does this meet the goal?

- A. Yes
B. No

Answer: B

Explanation:

References:

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

NEW QUESTION 72

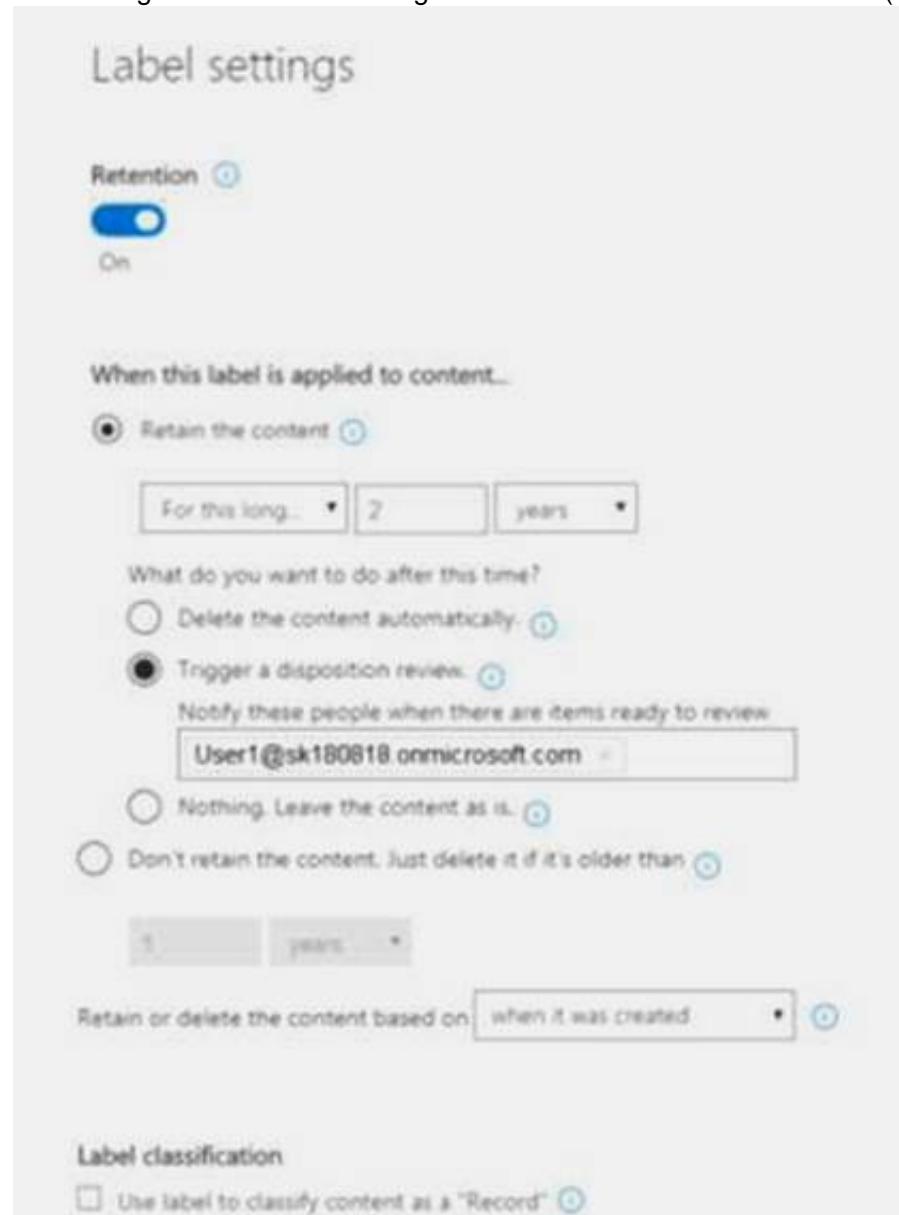
HOTSPOT

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

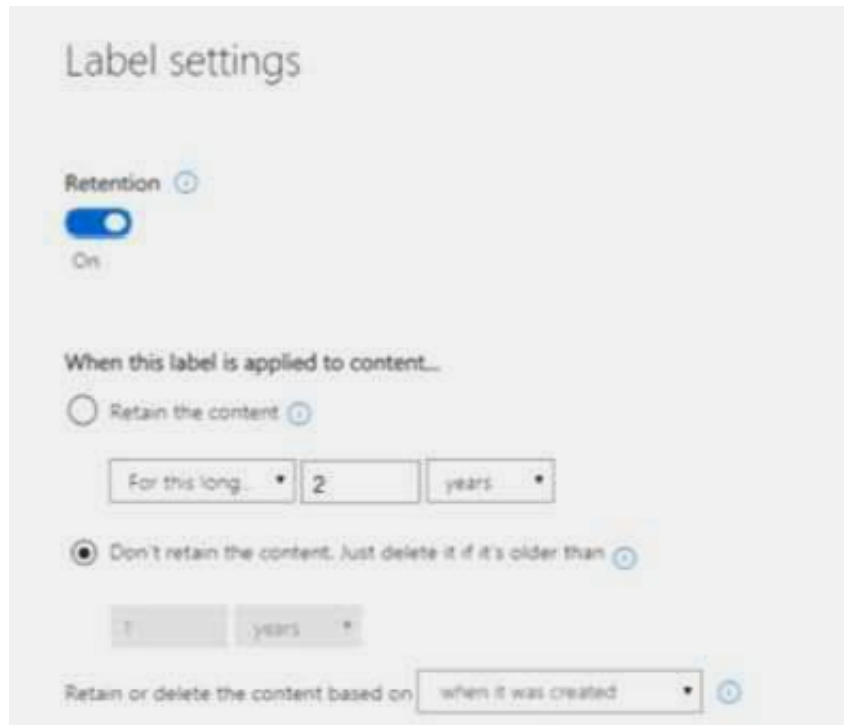
Name	Stored in
File1	Microsoft OneDrive
File2	A Microsoft SharePoint library
File3	Microsoft Exchange Online email

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

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



The settings for Label2 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 76

You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content. What should you do?

- A. Run the Add-AadrmRoleBasedAdministrator cmdlet.
- B. Create an Azure Information Protection policy.
- C. Configure the protection activation status for Azure Information Protection.
- D. Run the Set-AadrmOnboardingControlPolicy cmdlet.

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/information-protection/activate-service>

NEW QUESTION 80

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

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

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-AzureRmRoleAssignment cmdlet with the appropriate parameters.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/azurerms.resources/new-azurermroleassignment?view=azurermps-6.13.0>

NEW QUESTION 82

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

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

You configure the Microsoft 365 subscription to ensure that the new devices enroll in Microsoft Intune automatically.

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

Answer: C

NEW QUESTION 83

You have a Microsoft 365 subscription that uses a default domain named contoso.com.

You have two users named User 1 and User2.

From the Security & Compliance admin center, you add User1 to the ediscovery Manager role group. From the Security & Compliance admin center, User1 creates a case named Case1

You need to ensure that User1 can add User2 as a case member. The solution must use the principle of least privilege.

To which role group should you add User2?

- A. eDiscovery Manager
- B. eDiscovery Administrator
- C. Security Administrator

Answer: C

Explanation:

Case Study: 1 Contoso, Ltd Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 ES subscription.

Existing Environment Requirement

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops are Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Planned Changes

Contoso plans to implement the following changes:

- Implement Microsoft 365.
- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

Technical Requirements

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automaticaiy.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must NOT use port mirroring.
- Whenever possible, the principle of least privilege must be used.

- A Microsoft Store for Business must be created.
- Compliance Requirements
- Contoso identifies the following compliance requirements:
- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
 - Configure Windows Information Protection (W1P) for the Windows 10 devices.

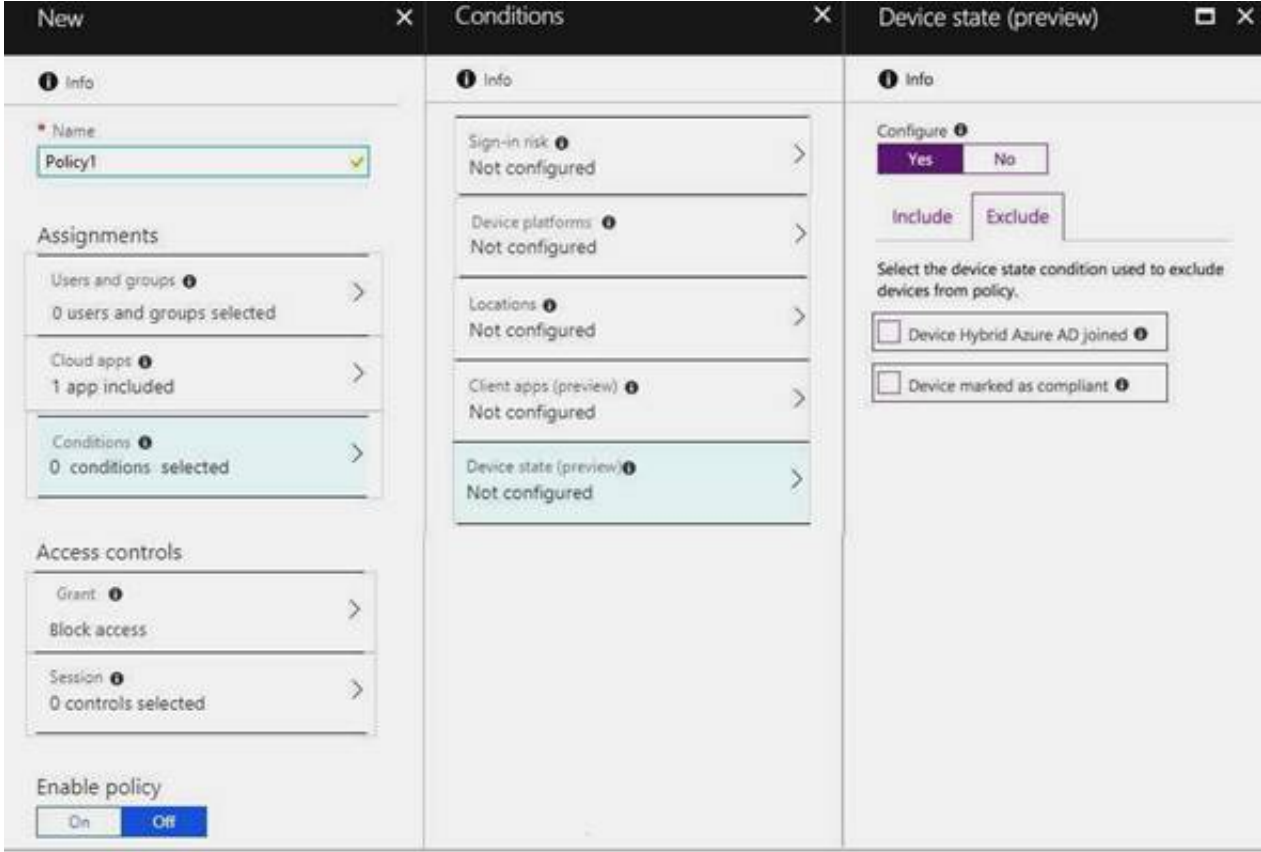
NEW QUESTION 85

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.

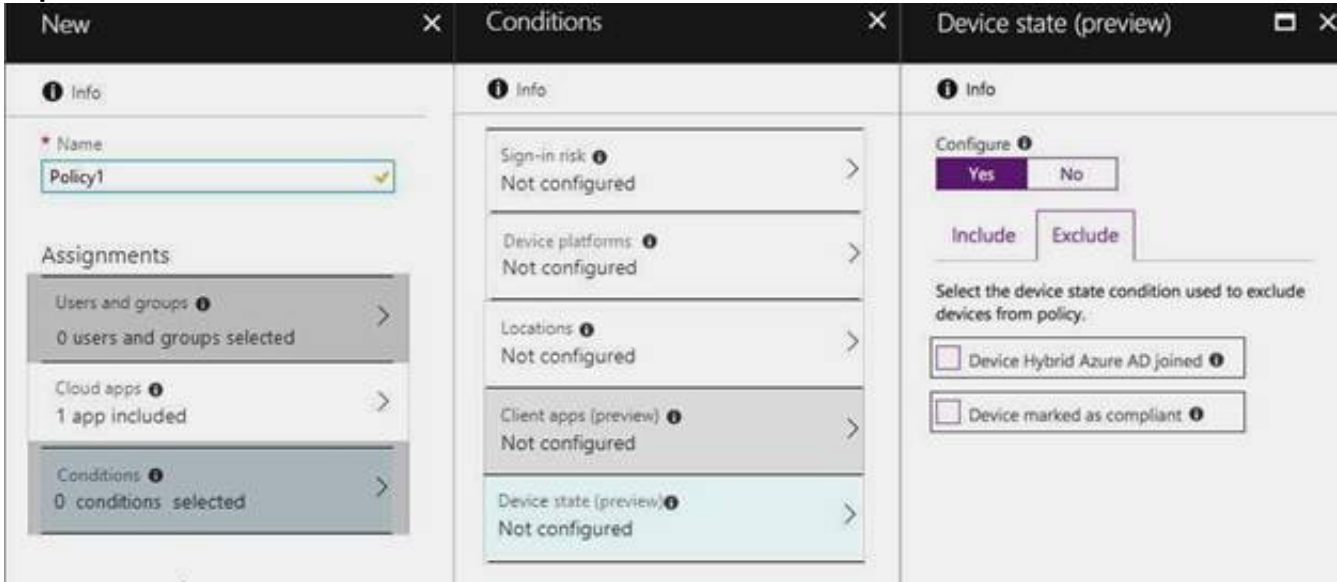
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

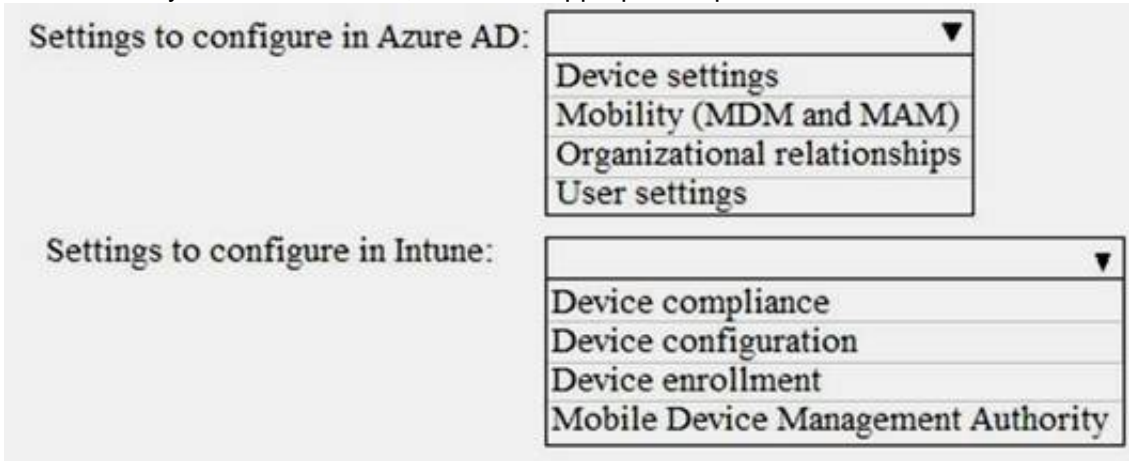


NEW QUESTION 86

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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 90

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

NEW QUESTION 95

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/edisHYPERLINK \"https://www.sherweb.com/blog/ediscovery-office-365/\"covery-office-365/](https://www.sherweb.com/blog/edisHYPERLINK \)

NEW QUESTION 96

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 101

.....

Relate Links

100% Pass Your MS-101 Exam with Examible Prep Materials

<https://www.exambible.com/MS-101-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>