# Exam Questions MS-101

Microsoft 365 Mobility and Security (beta)

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

**NEW QUESTION 1**
- (Exam Topic 4)
Your company has a Microsoft 365 subscription that uses an Azure Directory (Azure AD0 tenant named Contoso.com. The tenant contains the users shown in the following table.
You create a relation label named Label1 that has the following configurations: Retains content for five years.
Automatically deletes all content that is older than five years.
You turn on Auto labeling for Label1 b using a policy named Policy1. Policy1 has the following configurations:
• Retains content for five years
• Automatically deletes all content that is older than five years
You turn on Auto labeling for Label 1 by using a policy named Policy1. Policy has the following configurations:
• Applies to content that contains the word Merger
• Specifies the OneDrive accounts and SharePoint sites locations You run the following command
Set RetentionConpliancePolicy Policy1 RestrictiveRelention $true Force
For each of the following statements select Yes if the statement is true Otherwise, select No NOTE: Each correct selection is worth one point.

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 can add Exchange email as a location to Policy1. | ○ | ○ |
| User2 can remove SharePoint sites from Policy1. | ○ | ○ |
| User2 can add the word Acquisition to Policy1. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 can add Exchange email as a location to Policy1. | ○ | [○] |
| User2 can remove SharePoint sites from Policy1. | [○] | ○ |
| User2 can add the word Acquisition to Policy1. | ○ | [○] |

**NEW QUESTION 2**
- (Exam Topic 4)
DRAG DROP
You have a Microsoft 365 subscription.
In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:
➢ Block emails that contain financial data.
➢ Display the following policy tip text: Message blocked.
From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:
➢ Use the following location: Exchange email.
➢ Display the following policy tip text: Message contains sensitive data.
➢ When a user sends an email, notify the user if the email contains health records.
What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

**Results**

| |
|---|
| The email will be blocked, and the user will receive the policy tip: Message blocked. |
| The email will be blocked, and the user will receive the policy tip: Message contains sensitive data. |
| The email will be allowed, and the user will receive the policy tip: Message blocked. |
| The email will be allowed, and the user will receive the policy tip: Message contains sensitive data. |
| The email will be allowed, and a message policy tip will NOT be displayed. |

**Answer Area**

When the user sends an email that contains financial data and health records: [Result]

When the user sends an email that contains only financial data: [Result]

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked.
If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.
Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data. Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers

**NEW QUESTION 3**
- (Exam Topic 4)
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:**
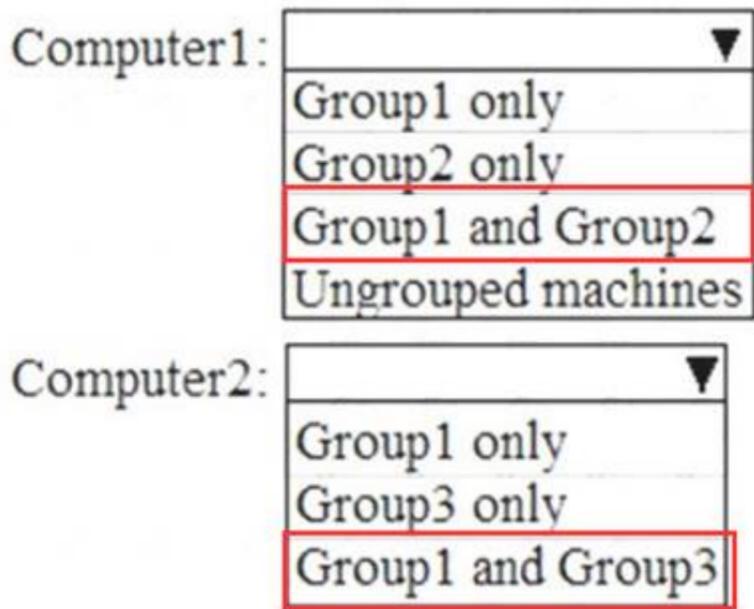


**NEW QUESTION 4**
- (Exam Topic 4)
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector. Where can you store data from the LinkedIn connector?

A. a Microsoft OneDrive for Business folder
B. a Microsoft SharePoint Online document library
C. a Microsoft 365 mailbox
D. Azure Files

**Answer:** C

**Explanation:**

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin-data?view=o365-worldwide

**NEW QUESTION 5**
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You have the devices shown in the following table.

| Name | TPM version | Operating system | BIOS/UEFI | BitLocker Drive Encryption (BitLocker) |
|------|-------------|------------------|-----------|----------------------------------------|
| Device1 | TPM 1.2 | Windows 10 Pro | BIOS | Enabled |
| Device2 | TPM 2 | Windows 10 Home | BIOS | Not applicable |
| Device3 | TPM 2 | Windows 8.1 Pro | UEFI | Enabled |

You plan to join the devices to Azure Active Directory (Azure AD)
What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, of not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

| Device1: | Disable BitLocker. |
| Device2: | Switch to UEFI. |
| Device3: | Upgrade to Windows 10 Enterprise. |

**NEW QUESTION 6**
- (Exam Topic 4)
You have a Microsoft 365 subscription and an on-premises Active Directory domain named contoso.com. All client computers run Windows 10 Enterprise and are joined to the domain.
You need to enable Windows Defender Credential Guard on all the computers. What should you do?

A. From the Security & Compliance admin center, configure the DKIM signatures for the domain
B. domain controller, create a Group Policy object (GPO) that enables the Restrict delegation of credentials to remote servers setting.
C. From the Security & Compliance admin center, create a device security policy.
D. From a domain controller, create a Group Policy object (GPO) that enables the Turn On Virtualization Based Security setting.

**Answer:** A


**NEW QUESTION 7**
- (Exam Topic 4)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.onmicrost.com. You have a Microsoft 365 subscription.
You need to ensure that administrations in your organization can manage the configuration settings for the Windows 10 device in your organization.
What should you configure?

A. Windows enrollment settings
B. Mobile device management (MDM) authority
C. Exchange on-permission access settings
D. Enrollment restriction

**Answer:** D


**NEW QUESTION 8**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP). You need to create a detection exclusion in Azure ATP.
Which tool should you use?

A. the Security & Compliance admin center
B. Microsoft Defender Security Center
C. the Microsoft 365 admin center
D. the Azure Advanced Threat Protection portal
E. the Cloud App Security portal

**Answer:** D

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/what-is https://docs.microsoft.com/en-us/defender-for-identity/excluding-entities-from-detections


**NEW QUESTION 9**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.
You need to ensure that users can enroll devices in Microsoft Endpoint Manager without manually entering the address of Microsoft Endpoint Manager.
Which two DNS records should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a CNAME record for AutoDiscover.contoso.com
B. a CNAME record for EnterpriseEnrollment.contoso.com
C. a TXT record for EnterpriseRegistration.contoso.com
D. an SRV record for _SIP._TLS.contoso.com
E. an SRV record for _SIPfederationTLS.contoso.com
F. a CNAME record for EnterpriseRegistration.contoso.com
G. a TXT record for EnterpriseEnrollment.contoso.com

**Answer:** BF


**NEW QUESTION 10**
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).
All the devices in your organization are onboarded to Microsoft Defender ATP.
You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.

What should you do?

A. From Alerts queue, create a suppression rule and assign an alert
B. From the Security & Compliance admin center, create an audit log search
C. From Advanced hunting, create a query and a detection rule
D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detectionru

**NEW QUESTION 10**
- (Exam Topic 4)
You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.
You have the devices shown in the following table.

| Name | Platform | Configuration |
|------|----------|---------------|
| Device1 | Windows 10 | Hybrid joined to on-premises Active Directory and Azure AD only |
| Device2 | Windows 10 | Joined to Azure AD and enrolled in Configuration Manager only |
| Device3 | Windows 10 | Enrolled in Microsoft Endpoint Manager and has the Configuration Manager agent installed only |

You plan to enable co-management.
You need to identify which devices support co-management without requiring the installation of additional software.
Which devices should you identify?

A. Device1 only
B. Device2 only
C. Device3 only
D. Device2 and Device3 only
E. Device1, Device2, and Device3

**Answer:** D

**NEW QUESTION 14**
- (Exam Topic 4)
Your company has a Microsoft 365 subscription.
You implement Microsoft Azure Information Protection.
You need to automatically protect email messages that contain the word Confidential in the subject line. What should you create?

A. a mail flow rule from the Exchange admin center
B. a message trace from the Security & Compliance admin center
C. a supervision policy from the Security & Compliance admin center
D. a sharing policy from the Exchange admin center

**Answer:** A

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

**NEW QUESTION 15**
- (Exam Topic 4)
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 20**
- (Exam Topic 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.
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 tenet contains the 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 User 3 to modify the Azure ATP sensor configuration- Does this meet the goal?

A. Yes
B. No

**Answer:** A

**Explanation:**
Access to the Defender for Identity portal is granted only to users within the Defender for Identity security groups, within your Azure Active Directory, as well as global and security admins of the
tennant.

**NEW QUESTION 21**
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains the compliance policies shown in the following table.

| Name | Require BitLocker | Require the device to be at or under the machine risk score |
|------|-------------------|------------------------------------------------------------|
| Policy1 | Required | High |
| Policy2 | Not configured | Medium |
| Policy3 | Required | Low |

The tenant contains the devices shown in the following table.

| Name | BitLocker Drive Encryption (BitLocker) | Microsoft Defender for Endpoint risk status | Policies applied |
|------|----------------------------------------|---------------------------------------------|------------------|
| Device1 | Configured | High | Policy1, Policy3 |
| Device2 | Not configured | Medium | Policy2, Policy3 |
| Device3 | Not configured | Low | Policy1, Policy2 |

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

| Statements | Yes | No |
|------------|-----|-----|
| Device1 is marked as compliant. | ○ | ○ |
| Device2 is marked as compliant. | ○ | ○ |
| Device3 is marked as compliant. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text, application Description automatically generated

**NEW QUESTION 26**
- (Exam Topic 4)
HOTSPOT
You configure an anti-phishing policy as shown in the following exhibit.

| Policy setting | Policy name | Managers |
| --- | --- | --- |
| | Description | |
| | Applied to | If the email is sent to: |
| | | IrvinS@M365x289755.OnMicrosoft.com |
| | | MiriamG@M365x289755.OnMicrosoft.com |
| | | Except if the email is sent to member of: |
| | | test1ww@M365x289755.OnMicrosoft.com |

| Impersonation | Users to protect | On - 3 User(s) specified | |
| --- | --- | --- | --- |
| | Protect all domains I own | On | |
| | Protect specific domains | On - 2 Domain(s) specified | |
| | Action > User impersonation | Move message to the recipients' Junk Email folders | |
| | Action > Domain impersonation | Delete the message before it's delivered | Edit |
| | Safety tips > User impersonation | Off | |
| | Safety tips > Domain impersonation | Off | |
| | Safety tips > Unusual characters | Off | |
| | Mailbox intelligence | Off | |

| Spoof | Enable antispoofing protection | On | |
| --- | --- | --- | --- |
| | Action | Quarantine the message | Edit |

| Advanced settings | Advanced phishing thresholds | 3 - More Aggressive | Edit |
| --- | --- | --- | --- |

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

If a message is identified as a domain impersonation, **[answer choice]**.

- the message is delivered to the Inbox folder
- the message is moved to the Deleted Items folder
- the messages are moved to the Junk Email folder

To reduce the likelihood of the impersonation policy generating false positives, configure **[answer choice]**.

- Advanced phishing thresholds
- Domain impersonation
- Enable antispoofing protection
- Mailbox intelligence

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies#learn-about-atp-an

**NEW QUESTION 28**
- (Exam Topic 4)
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 App1 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:**
https://docs.microsoft.com/en-us/cloud-app-security/discovered-app-queries

**NEW QUESTION 29**
- (Exam Topic 4)
You have a Microsoft Office 365 subscription.
You need to delegate eDiscovery tasks as shown in the following table.

| User | Task |
|------|------|
| User1 | • Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content.<br>• View the eDiscovery cases created by User1.<br>• Configure case settings.<br>• Place content on hold. |
| User2 | • View the eDiscovery cases created by User1.<br>• Export data from Advanced eDiscovery. |

The solution must follow the principle of the least privilege.
To which role group should you assign each user? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User1:
eDiscovery Administrator
eDiscovery Manager
Records Management
Reviewer
Security Administrator

User2:
eDiscovery Administrator
eDiscovery Manager
Records Management
Reviewer
Security Administrator

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 34**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

| Name | Platform |
|------|----------|
| Device1 | MacOS |
| Device2 | Windows 10 Pro |
| Device3 | Windows 10 Enterprise |
| Device4 | Ubuntu 18.04 LTS |

You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?

A. Device 1, Device2, and Device3 only
B. Device3 only
C. Device2 and Device3 only
D. Device1, Device2, Devices and Device4

**Answer:** C

**Explanation:**

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?vie

**NEW QUESTION 37**
- (Exam Topic 4)
You have a Microsoft 365 F5 subscription.
You plan to deploy 100 new Windows 10 devices.
You need to order the appropriate version of Windows 10 for the new devices. The version must Meet the following requirements.
Be serviced for a minimum of 24 moths.
Support Microsoft Application Virtualization (App-V) Which version should you identify?

A. Window 10 Pro, version 1909
B. Window 10 Pro, version 2004
C. Window 10 Pro, version 1909
D. Window 10 Enterprise, version 2004

**Answer:** D

**Explanation:**

Reference:
https://docs.microsoft.com/en-us/windows/release-health/release-information https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported-configurations

**NEW QUESTION 40**
- (Exam Topic 4)
HOTSPOT
You have a Microsoft 365 tenant named contoso.com. The tenant contains the users shown in the following table.

| Name | Azure AD role | Office 365 role group |
|------|---------------|------------------------|
| User1 | Application administrator | eDiscovery Administrator |
| User2 | Application administrator | Organization Management |
| User3 | Cloud application administrator | Global Administrator |
| User4 | Compliance administrator | eDiscovery Manager |

You have the eDiscovery cases shown in the following table.

| Name | Created by |
|------|-----------|
| Case1 | User1 |
| Case2 | User2 |
| Case3 | User3 |
| Case4 | User4 |

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 delete Case4. | ○ | ○ |
| User3 can add members to Case2. | ○ | ○ |
| User4 can close Case3. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
References:
https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions

**NEW QUESTION 41**
- (Exam Topic 4)
From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit. (Click the Exhibit tab.)
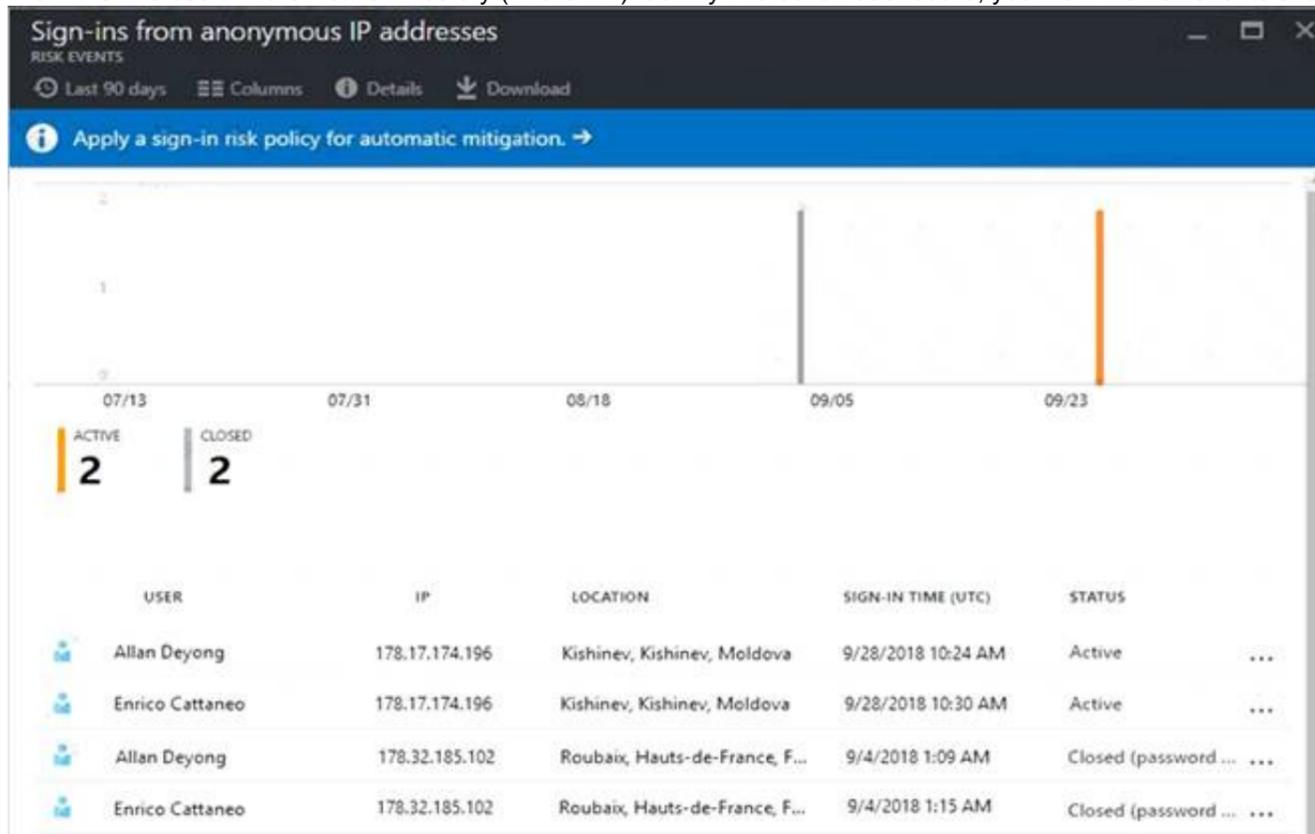
You need to reduce the likelihood that the sign-ins are identified at risky. What should you do?

A. From the Security & Compliance admin center, create a classification label.
B. From the Security & Compliance admin center, add the users to the Security Readers role group.
C. From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.
D. From the Conditional access blade in the Azure Active Directory admin center, create named locations.

**Answer:** D

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


**NEW QUESTION 42**
- (Exam Topic 4)
HOTSPOT
You have a Microsoft 365 subscription.
Your network uses an IP address space of 51.40.15.0/24.
An Exchange Online administrator recently created a role named Role1 from a computer on the network. You need to identify the name of the administrator by using an audit log search.
For which activities should you search and by which field should you filter in the audit log search? 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 46**
- (Exam Topic 4)
You have a Microsoft 365 subscription.
From the Security & Compliance admin center, you create a content search of a mailbox.
You need to view the content of the mail messages found by the search as quickly as possible. What should you select from the Content search settings?

A. Export report
B. Export results
C. Re-run
D. View results

**Answer:** B

**Explanation:**
There is no 'View Results" option. You can preview results but that will only show up to 100 emails. To
guarantee you're getting all results, you'll need to export them to a PST file.
References:
https://docs.microsoft.com/en-us/microsoft-365/compliance/limits-for-content-search


**NEW QUESTION 47**
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains the groups shown in the following table.

| Name | Type |
|--------|---------------------|
| Group1 | Distribution |
| Group2 | Mail-enabled security |
| Group3 | Security |

You plan to create a new Windows 10 Security Baseline profile. To which groups can you assign to the profile?

A. Group3 only
B. Group1 and Group3 only
C. Group2 and Group3 only
D. Group1. Group2. and Group3

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

**NEW QUESTION 49**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft intune.
in the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices, You enable device clean-up rules
What can you configure as the minimum number of days before a device a removed automatically?

A. 10
B. 30
C. 45
D. 90

**Answer:** D

**NEW QUESTION 50**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices. You plan to attack surface reduction (ASR) rules for the Windows 10 devices.
You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.
You need to find the ASR rules that match the activities on the devices.
How should you complete the Kusto query? 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:**
Graphical user interface, application Description automatically generated
Reference:
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction

**NEW QUESTION 53**
- (Exam Topic 4)
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

A. Android
B. CentOS Linux
C. iOS
D. Window 10

**Answer:** D

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure


**NEW QUESTION 58**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant.
You have the alerts shown in the following exhibit.

View alerts

| | Severity | Alert name | Status | Tags | Category | Activity count | Last occurrence... |
|---|---|---|---|---|---|---|---|
| ☐ | ● Medium | Alert1 | Active | - | Threat management | 2 | 3 minutes ago |
| ☐ | ● High | Alert5 | Resolved | - | Permissions | 1 | 8 minutes ago |

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.

Answer Area

For Alert1, you can change Status to
- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

For Alert5, you can
- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Answer Area

For Alert1, you can change Status to
- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

For Alert5, you can
- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active


**NEW QUESTION 63**
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.
Company policy requires that the devices have the following configurations:

➢ Require complex passwords.

➢ Require the encryption of removable data storage devices.

➢ Have Microsoft Defender Antivirus real-time protection enabled.
You need to configure the devices to meet the requirements.
What should you use?

A. an app configuration policy
B. a compliance policyC a security baseline profile D a conditional access policy

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

**NEW QUESTION 64**
- (Exam Topic 4)
You have a document in Microsoft OneDrive that is encrypted by using Microsoft Azure Information Protection as shown in the following exhibit.

**Protection settings** ❶

| Azure (cloud key) | HYOK (AD RMS) |

Select the protection action type ❶
- ⦿ 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

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 68**
- (Exam Topic 4)
You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that User1 can place a hold on all mailbox content. Which rote should you assign to User1?

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

**Answer:** A

**Explanation:**

References:
https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions

**NEW QUESTION 70**
- (Exam Topic 4)
You use Windows Defender Advanced Threat Protection (Windows Defender ATP). You have the Windows Defender ATP machine groups shown in the following table.

| Name | Rank | Members |
|------|------|---------|
| Group1 | 1 | Operating system in Windows 10 |
| Group2 | 2 | Name ends with London |
| Group3 | 3 | Operating system in Windows Server 2016 |
| Ungrouped machines (default) | Last | Not applicable |

You plan to onboard computers to Windows Defender ATP as shown in the following table.

| Name | Operating system |
|------|------------------|
| Computer1-London | Windows 10 |
| Server1-London | Windows Server 2016 |

To which machine group will each computer be added? To answer, select the appropriate options in the answer are.
NOTE: Each correct selection is worth one point.

Computer1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

Server1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

Computer1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

Server1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

**NEW QUESTION 71**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).
When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

This website is blocked by your organization. Contact your administrator for more information.

Hosted by www.contoso.com

Back to safety

Windows Defender SmartScreen

You need to enable user access to the partner company's portal. Which Microsoft Defender ATP setting should you modify?

A. Custom detections
B. Advanced hunting

C. Alert notifications
D. Indicators
E. Alert suppression

**Answer:** D

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators

**NEW QUESTION 75**
- (Exam Topic 4)
You need to grant a user a named User1 access to download compliance reports from the Security & Compliance reports from the Security from the Security & Compliance admin center. The solution must use the principle of least privilege.
What should you do?

A. Add User1 to the Security Reader role group
B. Create a new role group that has the Preview role and add User1 to the role group.
C. Add user1 to the Compliance Administrator role group.
D. Add User1 to the Service Assurance User role group.

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/download-existing-reports?view=o365-worldwide

**NEW QUESTION 77**
- (Exam Topic 4)
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

A. Ubuntu Linux
B. macOS
C. iOS
D. Android

**Answer:** B

**Explanation:**
Intune device configuration profiles can be applied to Windows 10 devices and macOS devices Note:
There are several versions of this question in the exam. The question has two possible correct answers:
≫ Windows 10
≫ macOS
Other incorrect answer options you may see on the exam include the following:
≫ Android Enterprise
≫ Windows 8.1 Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

**NEW QUESTION 81**
- (Exam Topic 4)
Your company has a Microsoft 365 subscription that contains the domains shown in the following table.

| Name | Can enroll devices to Microsoft Intune by using auto-discovery |
|---|---|
| Contoso.com | Yes |
| Contoso.onmicrosoft.com | Yes |

The company plans to add a custom domain named fabrikam.com to the subscription and then to enable enrollment of devices to Intune by using auto discovery for Tabrikam.com.
You need to add a DNS record to the fabrikam.com zone. Which record type should you use for the new record?

A. SRV
B. PTR
C. CNAME
D. TXT

**Answer:** C

**NEW QUESTION 83**
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

| Name | Platform |
|---|---|
| Device1 | Windows 10 |
| Device2 | Android |
| Device3 | iOS |

You plan to perform the following device management tasks in Microsoft Endpoint Manager:

≫ Deploy a VPN connection by using a VPN device configuration profile.

≫ Configure security settings by using an Endpoint Protection device configuration profile.

You support the management tasks.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

VPN device configuration profile:

| Device1 only |
| Device1 and Device2 only |
| Device1 and Device3 only |
| Device1, Device2 and Device3 |

Endpoint Protection device configuration profile:

| Device1 only |
| Device1 and Device2 only |
| Device1 and Device3 only |
| Device1, Device2 and Device3 |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos

**NEW QUESTION 84**
- (Exam Topic 4)
You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User 1. You need to preserve a copy of all the email messages that contain the word Project X.
WDM should you do?

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

**Answer:** D

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

**NEW QUESTION 88**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have devices enrolled in Intune as shown in the following table.

| Name | Platform | Member of | Scope (Tags) |
|---|---|---|---|
| Device1 | Windows 10 | Group1, Group3 | Tag1 |
| Device2 | Android | Group2 | Tag2 |

You create the device configuration profiles shown in the following table.

| Name | Platform | Assignments: Included groups | Assignments: Excluded groups | Scope tags |
|------|----------|------------------------------|------------------------------|------------|
| Profile1 | Windows 10 and later | Group1 | Group3 | Tag1, Tag2 |
| Profile2 | Android Enterprise | All devices | Group2 | Tag1, Tag2 |
| Profile3 | Android Enterprise | Group2, Group3 | Group3 | Tag1 |
| Profile4 | Windows 10 and later | Group3 | None | Default |

Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Device1:
| No profiles |
| Profile1 only |
| Profile4 only |
| Profile1 and Profile4 only |
| Profile1, Profile1, and Profile4 only |

Device2:
| No profiles |
| Profile1 only |
| Profile2 only |
| Profile3 only |
| Profile1 and Profile2 only |
| Profile2 and Profile3 only |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text, application, table Description automatically generated

**NEW QUESTION 91**
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.

| Name | Platform |
|------|----------|
| Device1 | MacOS |
| Device2 | Windows 10 Pro for Workstations |
| Device3 | Windows 10 Enterprise |
| Device4 | iOS |
| Device5 | Android |

You plan to enable VPN access for the devices.
What is the minimum number of configuration policies required?

A. 3
B. 5
C. 4
D. 1

**Answer:** D

**NEW QUESTION 92**
- (Exam Topic 4)
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 97**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.
You deploy a third-party antivirus solution to the devices. You need to ensure that the devices are marked as compliant.
Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows


**NEW QUESTION 100**
- (Exam Topic 4)
HOTSPOT
You have a Microsoft 365 tenant.
You need to create a custom Compliance Manager assessment template.
Which application should you use to create the template, and in which file format should the template be saved? 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:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-create?view=o365

**NEW QUESTION 104**
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.
From Microsoft Defender Security Center, you perform a security investigation. You need to run a PowerShell script on the device to collect forensic information.
Which action should you select on the device page?

A. Initiate Live Response Session
B. Initiate Automated Investigation
C. Collect investigation package
D. Go hunt

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwid

**NEW QUESTION 105**
- (Exam Topic 4)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

| Name | Microsoft 365 role |
| --- | --- |
| User1 | Cloud application administrator |
| User2 | Application administrator |
| User3 | Application developer |
| User4 | None |

Users are assigned Microsoft Store for Business roles as shown in the following table.

| User | Role |
| --- | --- |
| User1 | None |
| User2 | Basic Purchaser |
| User3 | Purchaser |
| User4 | Device Guard signer |

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Add apps to the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Install apps from the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User2, User3 and User4 only
- User1, User2, User3, and User4

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

**NEW QUESTION 109**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?

A. From the Cloud App Security admin center, select Users and accounts.
B. From the Microsoft 365 security center, view the Threat tracker.
C. From the Microsoft 365 admin center, view the Security & compliance report.
D. From the Azure Active Directory admin center, view the Risky sign-ins report.

**Answer:** A

**NEW QUESTION 112**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.
Devices are onboarded by using Microsoft Defender for Endpoint.
You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.
What should you create first?

A. a device configuration policy
B. a device compliance policy
C. a conditional access policy
D. an endpoint detection and response policy

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

**NEW QUESTION 113**
- (Exam Topic 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.
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 114**
- (Exam Topic 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.
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:**
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access. References:
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Onlinea

**NEW QUESTION 119**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant.
You need to evaluate compliance with European Union privacy regulations for customer data. What should you do in the Microsoft 365 compliance center?

A. Create a Data Subject Request (DSR)
B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data
C. Create an assessment based on the EU GDPR assessment template
D. Create an assessment based on the Data Protection Baseline assessment template

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan

**NEW QUESTION 121**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant.
You configure a device compliance policy as shown in the following exhibit.

**Compliance settings** Edit

## Microsoft Defender ATP

| | |
|---|---|
| Require the device to be at or under the machine risk score. | Low |

## Device Health

| | |
|---|---|
| Rooted devices | Block |
| Require the device to be at or under the Device Threat Level | |

## System Security

| | |
|---|---|
| Require a password to unlock mobile devices | Require |
| Required password type | Device default |
| Encryption of data storage on device. | Require |
| Block apps from unknown sources | Block |

**Actions for noncompliance** Edit

| Action | Schedule |
|---|---|
| Mark device noncompliant | Immediately |
| Retire the noncompliant device | Immediately |

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.

When a device reports a medium threat level, the device will ▼

| |
|---|
| be locked remotely |
| display a notification |
| marked as compliant |
| marked as noncompliant |
| removed from the database |

Rooted devices will be ▼

| |
|---|
| allowed to access company resources |
| marked as compliant |
| prevented from accessing company resources |
| reported with a low device threat |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android

**NEW QUESTION 123**
- (Exam Topic 4)
Your company has a Microsoft 365 tenant
You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM)
The device type restriction 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 restriction are configured as shown in the following table.

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

Answer Area

Device limit:
| 5 |
| 10 |
| 15 |

Allowed platform
| Android only |
| iOS only |
| All platforms |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restricti
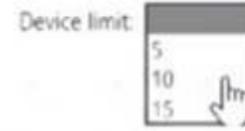
**NEW QUESTION 128**
- (Exam Topic 4)
Your company has a Microsoft 365 E3 subscription.
All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).
You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution 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:** C

**Explanation:**
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

**NEW QUESTION 129**
- (Exam Topic 4)
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. | ○ | ○ |
| User2 can enroll a maximum of 10 devices in Intune. | ○ | ○ |
| User3 can enroll an unlimited number of devices in Intune. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 134**
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.
Does this meet the goal?

A. Yes
B. No

**Answer:** A

**NEW QUESTION 137**
- (Exam Topic 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.
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/newcomp

**NEW QUESTION 139**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant that contains four devices enrolled in Microsoft Intune as shown in the following table.

| Name | Platform |
|---|---|
| Device1 | Windows 10 |
| Device2 | Android |
| Device3 | macOS |
| Device4 | iOS |

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager. To which devices can you deploy Microsoft 365 Apps for enterprise?

A. Device1 only
B. Device1 and Device3 only
C. Device2 and Device4 only
D. Device1, Device2. and Device3 only
E. Device1, Device2, Device3, and Device4

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

**NEW QUESTION 143**
- (Exam Topic 4)
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 log search

**Answer:** D

**NEW QUESTION 147**
- (Exam Topic 4)
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 | -Identity "Policy1" | -enabled | $true |
| Set-HoldCompliancePolicy | | -Force | |
| Set-RetentionCompliancePolicy | | -RestrictiveRetention | |
| Set-RetentionPolicy | | -RetentionPolicyTagLinks | |
| Set-RetentionPolicyTag | | -SystemTag | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentionco

**NEW QUESTION 148**
- (Exam Topic 4)
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. Your company implements Windows Information Protection (WIP).
You need to modify which users and applications are affected by WIP.
What should you do? To answer, select the appropriate options m the answer area. NOTE: Each correct selection is worth one point.

To modify which users are affected by WIP, configure:

| The Azure AD app registration |
| The Azure AD device settings |
| The MAM User scope |
| The mobile device management (MDM) authority |

To modify which applications are affected by WIP, configure:

| App configuration policies |
| App protection policies |
| Compliance policies |
| Device configuration profiles |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
References:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/crea

**NEW QUESTION 153**
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses a default domain named contoso.com. The domain contains the users shown in the following table.

| Name | Member of |
| --- | --- |
| User1 | Group1 |
| User2 | Group1, Group2 |

The domain contains the devices shown in the following table.

| Name | Compliance status |
| --- | --- |
| Device1 | Compliant |
| Device2 | Noncompliant |

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

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

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

| Statements | Yes | No |
|------------|-----|-----|
| User1 can access App1 from Device1. | ○ | ○ |
| User2 can access App1 from Device1. | ○ | ○ |
| User2 can access App1 from Device2. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Yes Yes No


**NEW QUESTION 156**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant.
industry regulations require that the tenant comply with the ISO 27001 standard. You need to evaluate the tenant based on the standard

A. From Policy in the Azure portal, select Compliance, and then assign a pokey
B. From Compliance Manager, create an assessment
C. From the Microsoft J6i compliance center, create an audit retention pokey.
D. From the Microsoft 365 admin center enable the Productivity Score.

**Answer:** B


**NEW QUESTION 160**
- (Exam Topic 4)
From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

| Role | Member |
|------|--------|
| Site owner | Prvi |
| Site member | User1 |
| Site visitor | User2 |

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)
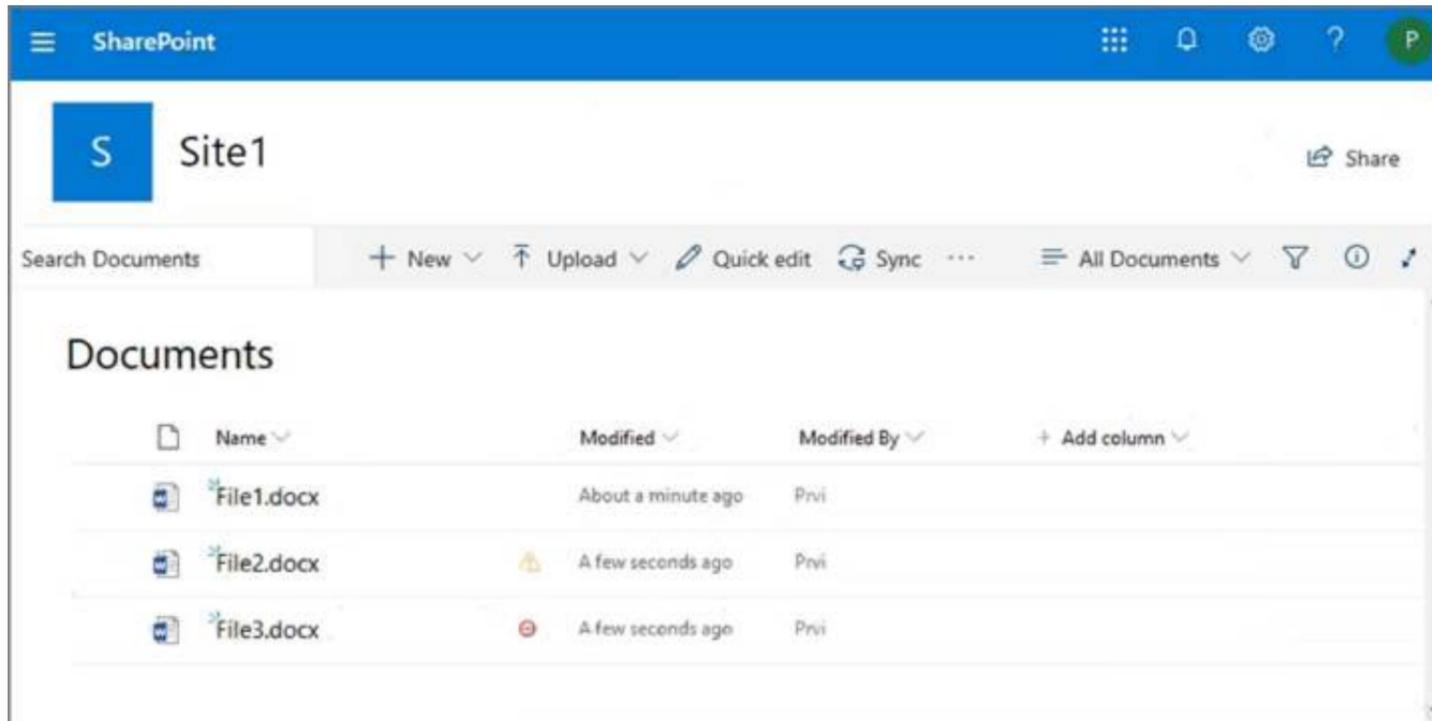
Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**User1:**

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

**User2:**

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text, application, email Description automatically generated
Reference:
https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/ https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/

**NEW QUESTION 164**
- (Exam Topic 4)
You have a Microsoft 365 tenant.
You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Save the audit logs to: _____ ▼

Azure Active Directory admin center blade to use to view the _____ ▼
saved audit logs:

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

| | |
|---|---|
| Save the audit logs to: | Azure Log Analytics ▼ |
| Azure Active Directory admin center blade to use to view the saved audit logs: | Audit logs ▼ |

## NEW QUESTION 167
- (Exam Topic 4)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.
The tenant contains the users shown in the following table.

| Name | Member of group | Azure AD role |
|---|---|---|
| User1 | Defender for Identity Contoso Administrators | None |
| User2 | Defender for Identity Contoso Users | None |
| User3 | None | Security administrator |
| User4 | Defender for Identity Contoso Users | Global administrator |

You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User3 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes
B. No

**Answer:** A

## NEW QUESTION 170
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains the users shown in the following table.

| Name | Member of | Azure Active Directory (Azure AD) role |
|---|---|---|
| User1 | Group1 | Global administrator |
| User2 | Group2 | Cloud device administrator |

You configure an Enrollment Status Page profile as shown in the following exhibit.

## Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

| | |
|---|---|
| Show app and profile installation progress. | **Yes** No |
| Show time limit error when installation takes longer than specified number of minutes. | 60 |
| Show custom message when time limit error occurs. | Yes **No** |
| Allow users to collect logs about instalattion errors. | Yes **No** |
| Only show page to devices provisioned by out-of-box experience (OOBE) | **Yes** No |
| Block device use until all apps and profiles are installed | Yes **No** |

You assign the policy to Group1.
You purchase the devices shown in the following table.

| Name | Platform |
|---|---|
| Device1 | Windows 10 |
| Device2 | Android |

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 User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show. | O | O |
| If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show. | O | O |
| If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show. | O | O |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

**NEW QUESTION 175**
- (Exam Topic 4)
You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).
The tenant has two Compliance Manager assessments as shown in the following table.

| Name | Score | Status | Assessment progress | Your improvement actions | Microsoft actions | Group | Product | Regulation |
|---|---|---|---|---|---|---|---|---|
| SP800 | 15444 | Incomplete | 72% | 3 of 450 completed | 887 of 887 completed | Group1 | Microsoft 365 | NIST 800-53 |
| Data Protection Baseline | 14370 | Incomplete | 70% | 3 of 489 completed | 835 of 835 completed | Group2 | Microsoft 365 | Data Protection Baseline |

The SP800 assessment has the improvement actions shown in the following table.

| Improvement action | Test status | Impact | Points achieved | Regulations |
|---|---|---|---|---|
| Establish a threat intelligence program | None | +9 points | 0/9 | NIST 800-53, Data Protection Baseline |
| Establish and document a configuration management program | None | +9 points | 0/9 | NIST 800-53, Data Protection Baseline |

You perform the following actions:

≫ For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.

≫ Enable multi-factor authentication (MFA) for all users.
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 |
|---|---|---|
| Establish a threat intelligence program will appear as Implemented in the SP800 assessment. | O | O |
| The SP800 assessment score will increase by 54 points. | O | O |
| The Data Protection Baseline score will increase by 9 points. | O | O |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-assessments?view=o365-worl https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwid

**NEW QUESTION 176**
- (Exam Topic 4)

You have a Microsoft 365 E5 tenant.
You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.
Which two policies can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. a data loss prevention (DLP) policy
B. a sensitivity label policy
C. a Microsoft Cloud App Security file policy
D. a communication compliance policy
E. a retention label policy

**Answer:** AD

**NEW QUESTION 178**
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

| Name | Username | Type |
|------|----------|------|
| User1 | User1@contoso.com | Member |
| User2 | User2@sub.contoso.com | Member |
| User3 | User3@adatum.com | Member |
| User4 | User4@outlook.com | Guest |
| User5 | User5@gmail.com | Guest |

You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (PII) from being emailed to users outside your organization.
To which users can User1 send documents that contain PII?

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

**Answer:** B

**Explanation:**
Guest accounts are considered "outside your organization". Users who have non-guest accounts in a host organization's Active Directory or Azure Active Directory tenant are considered as people inside the organization.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwid

**NEW QUESTION 182**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

| Name | Windows 10 edition | Azure Active Directory (Azure AD) | Mobile device management (MDM) enrollment |
|------|--------------------|-----------------------------------|-------------------------------------------|
| Device1 | Windows 10 Pro | Registered | Microsoft Intune |
| Device2 | Windows 10 Enterprise | Joined | Microsoft Intune |
| Device3 | Windows 10 Pro | Joined | Not enrolled |
| Device4 | Windows 10 Enterprise | Registered | Microsoft Intune |
| Device5 | Windows 10 Enterprise | Joined | Not enrolled |

You add custom apps to the private store in Microsoft Store Business.
You plan to create a policy to show only the private store in Microsoft Store for Business. To which devices can the policy be applied?

A. Device2 only
B. Device1 and Device3 only
C. Device2 and Device4 only
D. Device2, Device3, and Device5 only
E. Device1, Device2, Device3, Device4, and Device5

**Answer:** C

**NEW QUESTION 184**
- (Exam Topic 4)
The users at your company use Dropbox to store documents. The users access Dropbox by using the MyApps portal.
You need to ensure that user access to Dropbox is authenticated by using a Microsoft 365 identify. The documents must be protected if the data is downloaded to an untrusted device.
What should you do?

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

**Answer:** B

**NEW QUESTION 189**
- (Exam Topic 4)
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:** C

**Explanation:**
Editing Policy settings > +New Rule > Exceptions We won't apply this rule to content that matches any of these exceptions. > +Add an exception > [Dropdownbox] Except if the recipient domain is.
---------------------------- Except if recipient domain is Detects when content is sent in an email message to the recipient domains you specify.

**NEW QUESTION 192**
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Security & Compliance retention policies. You implement a preservation lock on a retention policy that is assigned to all executive users.
Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point?

A. Add locations to the policy
B. Reduce the duration of policy
C. Remove locations from the policy
D. Extend the duration of the policy
E. Disable the policy

**Answer:** AD

**NEW QUESTION 194**
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

A. From the Exchange admin center, create a spam filter policy.
B. From the Security & Compliance admin center, create a data governance event.
C. From the Security & Compliance admin center, create an alert policy.
D. From the Exchange admin center, create a mail-flow rule.

**Answer:** D

**Explanation:**
You can inspect email attachments in your Exchange Online organization by setting up mail flow rules. Exchange Online offers mail flow rules that provide the ability to examine email attachments as a part of your messaging security and compliance needs. When you inspect attachments, you can then take action on the messages that were inspected based on the content or characteristics of those attachments.

**NEW QUESTION 197**
- (Exam Topic 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.
You are deploying Microsoft Intune.
You successfully enroll Windows 10 devices in Intune.
When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intuen. Solution: You create an Apple Configurator enrollment profile. Does this meet the goal?

A. Yes
B. No

**Answer:** A

**NEW QUESTION 200**
- (Exam Topic 4)
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<br>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. | ○ | ○ |
| The device of User2 is compliant. | ○ | ○ |
| The device of User3 is compliant. | ○ | ○ |

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 204**
- (Exam Topic 4)
Your company uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP). The devices onboarded to Microsoft Defender ATP are shown in the following table.

| Name | Machine group |
|---|---|
| Device1 | ATP1 |
| Device2 | ATP1 |
| Device3 | ATP2 |

The alerts visible in the Microsoft Defender ATP alerts queue are shown in the following table.

| Name | Machine |
|---|---|
| Alert1 | Device1 |
| Alert2 | Device2 |
| Alert3 | Device3 |

You create a suppression rule that has the following settings:
➤ Triggering IOC: Any IOC
➤ Action: Hide alert
➤ Suppression scope: Alerts on ATP1 machine group
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 |
|---|---|---|
| After you create the suppression rule, Alert1 is visible in the alerts queue. | ○ | ○ |
| After you create the suppression rule, Alert3 is visible in the alerts queue. | ○ | ○ |
| After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
A suppression rule will not affect alerts that are already in the alerts queue. Only new alerts will be suppressed.

**NEW QUESTION 205**
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You need to be notified if users receive email containing a file that has a virus. What should you do?

A. From the Exchange admin center, create an in-place eDiscovery & hold.
B. From the Security & Compliance admin center, create a data governance event.
C. From the Exchange admin center, create an anti-malware policy.
D. From the Security & Compliance admin center, create a safe attachments policy.

**Answer:** C

**Explanation:**
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-attachments-policie

**NEW QUESTION 208**
- (Exam Topic 4)
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:
- Enroll the devices in Microsoft Intune.
- Configure device compliance in Microsoft Intune.
- Create a Microsoft Azure Log Analytics workspace.
- Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:
- Configure all the devices to have a commercial ID.
- Configure software inventory in Configuration Manager.
- Configure all the devices to join the Windows Insider Program.
- 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 210**
- (Exam Topic 4)
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:** D


**NEW QUESTION 215**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant.
You create a retention label named Retention1 as shown in the following exhibit.

## Review your settings

**Name**                                    Edit
Retention1

**Description for admins**                  Edit

**Description for users**                   Edit

**File plan descriptors**                   Edit
Reference Id:1
Business function/department Legal
Category: Compliance
Authority type: Legal

**Retention**                               Edit
7 years
Retain only
Based on when it was created

[ Back ]    [ Create this label ]    [ Cancel ]

When users attempt to apply Retention1, the label is unavailable. You need to ensure that Retention1 is available to all the users. What should you do?

A. Create a new label policy
B. Modify the Authority type setting for Retention!
C. Modify the Business function/department setting for Retention 1.
D. Use a file plan CSV template to import Retention1.

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwid


**NEW QUESTION 219**
- (Exam Topic 4)
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. | ○ | ○ |
| Device2 is compliant. | ○ | ○ |
| Device3 is compliant. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Yes Yes Yes


**NEW QUESTION 222**
- (Exam Topic 4)
Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains computers that run Windows 10 Enterprise and are managed by using Microsoft Intune. The computers are configured as shown in the following table.

| Name | CPU | Cores | RAM | TPM |
|---|---|---|---|---|
| Computer1 | 64-bit | 2 | 12 GB | Enabled |
| Computer2 | 64-bit | 4 | 12 GB | Enabled |
| Computer3 | 64-bit | 8 | 16 GB | Disabled |
| Computer4 | 32-bit | 4 | 4 GB | Disabled |

You plan to implement Windows Defender Application Guard for contoso.com.
You need to identify on which two Windows 10 computers Windows Defender Application Guard can be installed.
Which two computers should you identify? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Computer1
B. Computer3
C. Computer2
D. Computer4

**Answer:** BC

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs


**NEW QUESTION 226**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).
You need to configure Microsoft Defender ATP on the computers. What should you create from the Endpoint Management admin center?

A. a device configuration profile
B. an update policy for iOS
C. a Microsoft Defender ATP baseline profile
D. a mobile device management (MDM) security baseline profile

**Answer:** A

**Explanation:**

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure


**NEW QUESTION 228**
- (Exam Topic 4)
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You need to provide a user with the ability to sign up for Microsoft Store for Business for contoso.com. The solution must use the principle of least privilege.
Which role should you assign to the user?

A. Cloud application administrator
B. Application administrator
C. Global administrator
D. Service administrator

**Answer:** C

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


**NEW QUESTION 230**
- (Exam Topic 4)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

| Name | Role |
|------|------|
| User1 | Global admin |
| User2 | None |
| User3 | None |

You provision the private store in Microsoft Store for Business.
You assign Microsoft Store for Business roles to the users as shown in the following table.

| Name | Role |
|------|------|
| User1 | None |
| User2 | Purchaser |
| User3 | Basic Purchaser |

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.
Which users should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Can add apps to the private store:

| |
|---|
| User2 only |
| User1 and User2 only |
| User2 and User3 only |
| User1, User2, and User3 |

Can assign apps from Microsoft Store for Business:

| |
|---|
| User2 only |
| User1 and User2 only |
| User2 and User3 only |
| User1, User2, and User3 |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-rol


**NEW QUESTION 234**
- (Exam Topic 4)
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

**Explanation:**
https://docs.microsoft.com/en-us/cloud-app-security/use-case-admin-quarantine


**NEW QUESTION 237**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
Users have the devices shown in the following table.

| Name | Platform | Owner | Enrolled in Microsoft Endpoint Manager |
|---------|------------|-------|----------------------------------------|
| Device1 | Android | User1 | Yes |
| Device2 | Android | User1 | No |
| Device3 | iOS | User1 | No |
| Device4 | Windows 10 | User2 | Yes |
| Device5 | Windows 10 | User2 | No |
| Device6 | iOS | User2 | Yes |

On which devices can you manage apps by using app configuration policies in Microsoft Endpoint Manager?

A. Device1, Device4, and Device6
B. Device2, Device3, and Device5
C. Device1, Device2, Device3, and Device6
D. Device1, Device2, Device4, and Device5

**Answer:** C

**Explanation:**
You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

**NEW QUESTION 241**
- (Exam Topic 4)
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.)



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

Label settings

Retention ⓘ

On

When this label is applied to content...

○ Retain the content ⓘ

For this long... ▾ 2 years ▾

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

1 years ▾

Retain or delete the content based on [ when it was created ▾ ] ⓘ

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 February 1, 2020. | ○ | ○ |
| If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021. | ○ | ○ |
| File3 will be deleted automatically after February 1, 2021. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: No
Retention overrides deletion.
Box 2: No
Content in a document library will be moved to the first-stage Recycle Bin within 7 days of disposition, and then permanently deleted another 93 days after that. Thus 100 days in total.
Box 3: No
Items in an Exchange mailbox will be permanently deleted within 14 days of disposition. References:
https://docs.microsoft.com/en-us/office365/securitycompliance/labels https://docs.microsoft.com/en-us/office365/securitycompliance/disposition-reviews

**NEW QUESTION 242**
- (Exam Topic 4)
You have a Microsoft 365 tenant.
You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.
What should you use?

A. an attack surface reduction (ASR) policy
B. an app configuration policy
C. a device compliance policy
D. a device configuration profile

**Answer:** D

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

**NEW QUESTION 243**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.

| Name | Platform |
|---|---|
| Device1 | Windows 10 |
| Device2 | Android 8.1.0 |
| Device3 | Android 10 |
| Device4 | iOS 12 |
| Device5 | iOS 14 |

All the devices have an app named App1 installed.
You need to prevent users from copying data from App1 and pasting the data into other apps.
Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Policy to create in Microsoft Endpoint Manager:

- An app configuration policy
- An app protection policy
- A conditional access policy
- A device compliance policy

Minimum number of required policies:

- 1
- 2
- 3
- 5

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, application, table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

**NEW QUESTION 245**
- (Exam Topic 4)
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          Edit
6Months

Description for admins          Edit

Description for users          Edit

Retention          Edit
6 months
Retain and Delete
Based on when it was created

Back    Create this label    Cancel

You create a label policy as shown in the Label Policy Exhibit. (Click the Label Policy tab.)
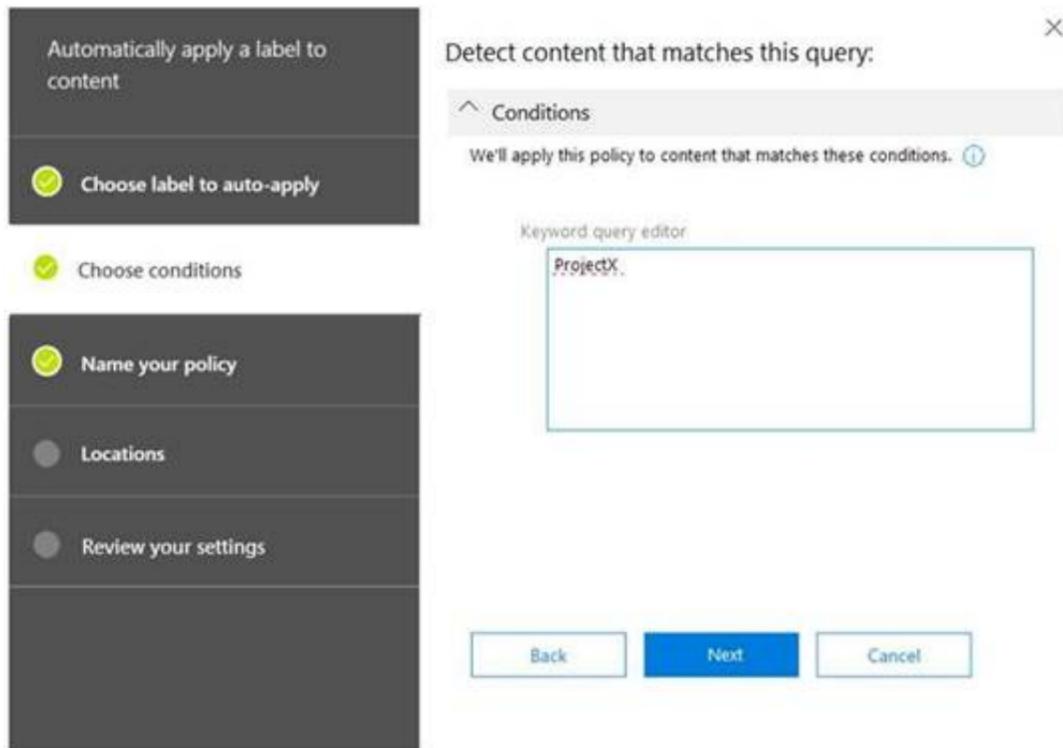
The label policy is configured as shown in the following table.

| 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. | ○ | ○ |
| Any sent email message that contains the word ProjectX will be retained for six months. | ○ | ○ |
| Users are required to manually apply a label to email messages that contain the work ProjectX. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 249**
- (Exam Topic 4)
You have Windows 10 devices that are managed by using Microsoft Endpoint Manager. You need to configure the security settings in Microsoft Edge.
What should you create in Microsoft Endpoint Manager?

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

**Answer:** C

**Explanation:**

Reference:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

**NEW QUESTION 252**
- (Exam Topic 4)
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.

Answer Area



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area



**NEW QUESTION 255**
- (Exam Topic 4)
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 257**
- (Exam Topic 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.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select Update & Security to view the update history.
Does this meet the goal?

A. Yes
B. No

**Answer:** B

**NEW QUESTION 260**
- (Exam Topic 4)
You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1. You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:
• Assign licenses to users.
• Procure apps from Microsoft Store.
• Manage private store availability for all items.
The solution must use the principle of least privilege.
Which Microsoft Store for Business role should you assign to User1?

A. Basic Purchaser
B. Device Guard signer
C. Admin
D. Purchaser

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

**NEW QUESTION 261**
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

| Name | Type | Block execution of potentially obfuscated scripts (js/vbs/ps) |
| --- | --- | --- |
| Policy1 | Attack surface reduction (ASR) | Audit mode |
| Policy2 | Microsoft Defender ATP Baseline | Disable |
| Policy3 | Device configuration profile | Not configured |

A. only the settings of Policy!
B. only the settings of Policy2
C. only the settings of Policy3
D. no settings

**Answer:** C

**NEW QUESTION 265**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains a user named User1.
The subscription has a single anti-malware policy as shown in the following exhibit.
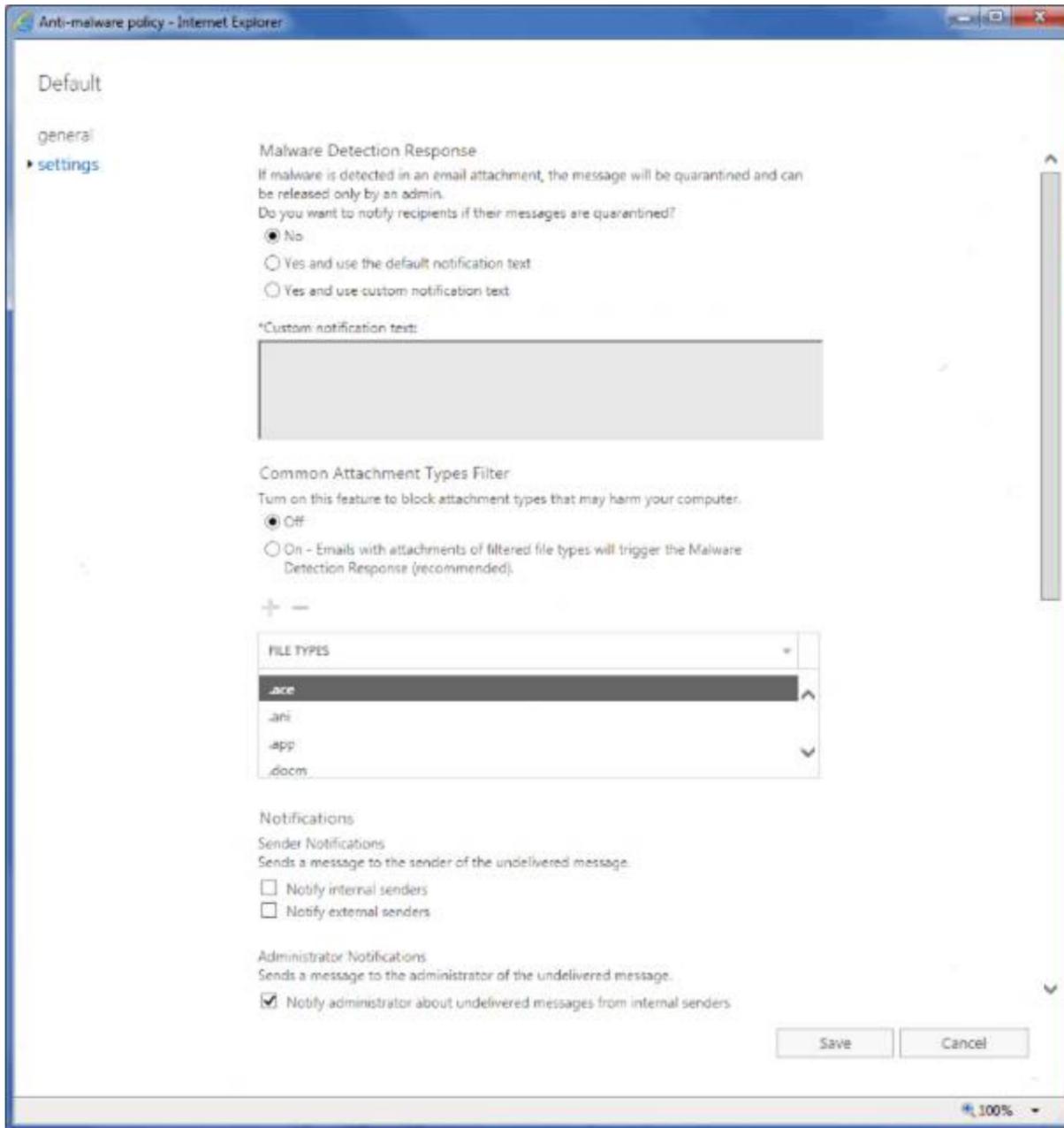
An email message that contains text and two attachments is sent to User1. One attachment is infected with malware.
How will the email message and the attachments be processed?

A. Both attachments will be remove
B. The email message will be quarantined, and Used will receive an email message without any attachments and an email message that includes the following text: 'Malware was removed.'
C. The email message will be quarantined, and the message will remain undelivered.
D. Both attachments will be remove
E. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: 'Malware was removed."
F. The malware-infected attachment will be remove
G. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o36


**NEW QUESTION 268**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You run an eDiscovery search that returns the following Azure Rights Management (Azure RMS) – encrypted content:

≫ Microsoft Exchange emails

≫ Microsoft OneDrive documents

≫ Microsoft SharePoint documents

Which content can be decrypted when you export the eDiscovery search results?

A. Exchange emails only
B. SharePoint documents, OneDrive documents, and Exchange emails
C. OneDrive documents only
D. SharePoint documents and OneDrive documents only
E. SharePoint documents only

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/export-search-results?view=o365-worldwide

**NEW QUESTION 270**
- (Exam Topic 4)
Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.
The tenant is configured to use Azure AD Identity Protection.
You plan to use an application named App1 that creates reports of Azure AD Identity Protection usage. You register App1 in the tenant.
You need to ensure that App1 can read the risk event information of contoso.com.
To which API should you delegate permissions?

A. Windows Azure Service Management API
B. Windows Azure Active Directory
C. Microsoft Graph
D. Office 365 Management

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/graph/api/resources/identityprotection-root?view=graph-rest-beta

**NEW QUESTION 274**
- (Exam Topic 4)
Your company has a Microsoft 365 subscription. you implement sensitivity Doris for your company.
You need to automatically protect email messages that contain the word Confidential m the subject line. What should you create?

A. a sharing policy from the Exchange admin center
B. a mall flow rule from the Exchange admin center
C. a message Dace from the Microsoft 365 security center
D. a data loss prevention (DLP) policy from the Microsoft 365 compliance center

**Answer:** B

**NEW QUESTION 277**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant that contains a user named User1. You plan to implement insider risk management.
You need to ensure that User1 can perform the following tasks:
> Review alerts.
> Manage cases.
> Create notice templates.
> Review user emails by using Content explorer. The solution must use the principle of least privilege. To which role group should you add User1?

A. Insider Risk Management
B. Insider Risk Management Analysts
C. Insider Risk Management Investigators
D. Insider Risk Management Admin

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-wo

**NEW QUESTION 280**
- (Exam Topic 4)
Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.
The company purchases a cloud app named App1 that supports Microsoft (loud App Security monitoring. You configure App1 to be available from the My Apps portal.
You need to ensure that you can monitor App1 from Cloud App Security What should you do?

A. From the Device Management admin center, create an app configuration policy.
B. From the Azure Active Directory admin center, create an app registration.
C. From the Device Management admin center, create an app protection policy.
D. From the Azure Active Directory admin center, create a conditional access policy.

**Answer:** C

**Explanation:**
https://docs.microsoft.com/en-us/intune/apps/app-protection-policies

**NEW QUESTION 284**
- (Exam Topic 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.
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.
Does this meet the goal?

A. Yes
B. No

**Answer:** A

**Explanation:**
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/pe

**NEW QUESTION 288**
- (Exam Topic 4)
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-alertswi defender-advanced-threat-protection
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automatedinvestigat windows-defender-advanced-threat-protection

**NEW QUESTION 289**
- (Exam Topic 4)
Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD) Password hash synchronization is disabled.
You plan to implement co-management.
You need to configure Azure AD Connect and the domain to support co-management. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**



**NEW QUESTION 293**
- (Exam Topic 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.
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Security & Compliance admin center, you assign the Security Administrator role to User1. Does this meet the goal?

A. Yes

B. No

**Answer:** B

**Explanation:**
References:
https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

**NEW QUESTION 296**
- (Exam Topic 4)
Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

| Name | Role | Office 365 role group |
|------|------|------------------------|
| User1 | *None* | Compliance data administrator |
| User2 | Global administrator | *None* |

You create a retention label named Label1 that has the following configurations:

≫ Retains content for five years

≫ Automatically deletes all content that is older than five years
You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

≫ Applies to content that contains the word Merger

≫ Specifies the OneDrive accounts and SharePoint sites locations You run the following command.
Set-RetentionCompliancePolicy Policy1 –RestrictiveRetention $true
-Force
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 add Exchange email as a location to Policy1. | ○ | ○ |
| User2 can remove SharePoint sites from Policy1. | ○ | ○ |
| User2 can add the word Acquisition to Policy1. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentionco

**NEW QUESTION 299**
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You discover that some external users accessed center for 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:** B

**NEW QUESTION 304**
- (Exam Topic 4)
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 306**
- (Exam Topic 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.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed. Solution: From Device Manager, you view the computer properties. Does this meet the goal?

A. Yes
B. No

**Answer:** B

**Explanation:**
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628be


**NEW QUESTION 308**
- (Exam Topic 4)
You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the Locations tab.)
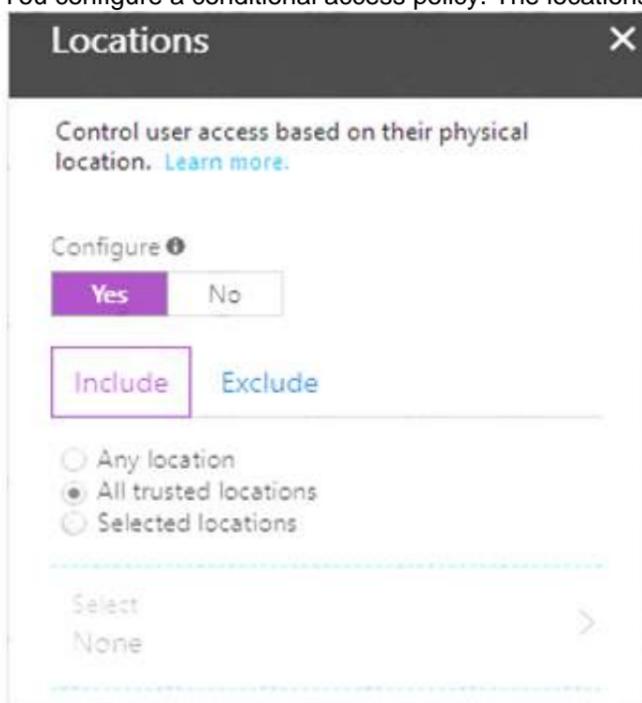


The users and groups settings are configured as shown in the Users and Groups exhibit. (Click Users and Groups tab.)
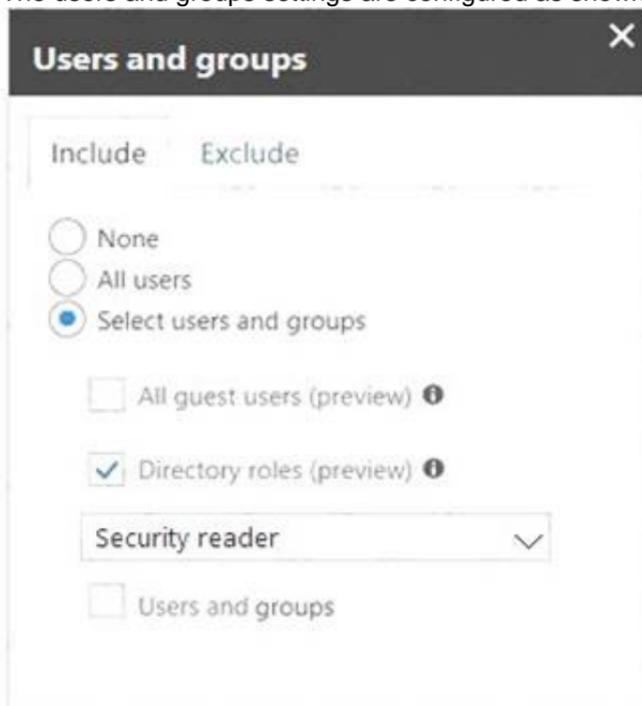


Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office.
You need to ensure that the members of the Security reader group can sign in in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege.
What should you do?

A. From the conditional access policy, configure the device state.
B. From the Azure Active Directory admin center, create a custom control.
C. From the Intune admin center, create a device compliance policy.
D. From the Azure Active Directory admin center, create a named location.

**Answer:** D

**Explanation:**

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

**NEW QUESTION 312**
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You are planning a threat management solution for your organization.
You need to minimize the likelihood that users will be affected by the following threats:

≫ Opening files in Microsoft SharePoint that contain malicious content

≫ Impersonation and spoofing attacks in email messages

Which policies should you create in the Security & Compliance admin center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Opening files in SharePoint that contain malicious content: ▼
| Anti-spam |
| ATP anti-phishing |
| ATP safe attachments |
| ATP Safe Links |

Impersonation and spoofing attacks in email messages: ▼
| Anti-spam |
| ATP anti-phishing |
| ATP safe attachments |
| ATP Safe Links |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: ATP Safe Attachments
ATP Safe Attachments provides zero-day protection to safeguard your messaging system, by checking email attachments for malicious content. It routes all messages and attachments that do not have a virus/malware signature to a special environment, and then uses machine learning and analysis techniques to detect malicious intent. If no suspicious activity is found, the message is forwarded to the mailbox.
Box 2: ATP anti-phishing
ATP anti-phishing protection detects attempts to impersonate your users and custom domains. It applies machine learning models and advanced impersonation-detection algorithms to avert phishing attacks.
ATP Safe Links provides time-of-click verification of URLs, for example, in emails messages and Office files. Protection is ongoing and applies across your messaging and Office environment. Links are scanned for each click: safe links remain accessible and malicious links are dynamically blocked.
References:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp#configure-atp-polici

**NEW QUESTION 316**
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?

A. Microsoft Store for Business
B. Apple Business Manager
C. Apple iTunes Store
D. Apple Configurator

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios

**NEW QUESTION 317**
- (Exam Topic 4)
You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.

**Choose the types of content to protect**

This policy will protect that matches these requirements. You can choose sensitive info types and existing labels

**Content contains**

Any of these ▾

| Sensitive info type | Match accuracy | |
| --- | --- | --- |
| | min | max |
| Credit Card Number | 85 | 100 | ✕ |

**Retention labels**
1 year

Add ▾

+ Add group

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.

DLP1 cannot be applied to [answer choice].

| ▼ |
| --- |
| Exchange email |
| SharePoint sites |
| OneDrive accounts |

DLP1 will be applied only to documents that have [answer choice].

| ▼ |
| --- |
| both a credit card number and the 1 year label applied |
| either a credit card number or the 1 year label applied |
| between 85 and 100 credit card numbers |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwid

**NEW QUESTION 321**
- (Exam Topic 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.
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 Endpoint Management admin center, you create a device configuration profile. Does this meet the goal?

A. Yes
B. No

**Answer:** B

**Explanation:**
You need to create a trusted location and a conditional access policy.

**NEW QUESTION 325**
- (Exam Topic 4)
You have a new Microsoft 365 subscription.
A user named User1 has a mailbox in Microsoft Exchange Online.
You need to log any changes to the mailbox folder permissions of User1.
Which command should you run? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

| ▼ | User1 | ▼ | $true |
| --- | --- | --- | --- |
| Set-AdminAuditLogConfig | | -AdminAuditLogEnabled | |
| Set-Mailbox | | -AuditEnabled | |
| Set-UnifiedAuditSetting | | -UnifiedAuditLogIngestionEnabled | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
To enable auditing for a single mailbox (in this example, belonging to Holly Sharp), use this PowerShell command: Set-Mailbox username -AuditEnabled $true
References:
https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps

**NEW QUESTION 329**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

| Name | Member of |
|------|-----------|
| User1 | Group1 |
| User2 | Group2 |

You purchase the devices shown in the following table.

| Name | Platform |
|------|----------|
| Device1 | Windows 10 |
| Device2 | Android |

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:

➢ Show app and profile configuration progress: Yes

➢ Allow users to collect logs about installation errors: Yes

➢ Only show page to devices provisioned by out-of-box experience (OOBE): No

➢ Assignments: Group2
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

| Statements | Yes | No |
|------------|-----|-----|
| If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear. | ○ | ○ |
| If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear. | ○ | ○ |
| If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

**NEW QUESTION 332**
- (Exam Topic 4)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.
The tenant contains the users shown in the following table.

| Name | Member of group | Azure AD role |
|------|-----------------|---------------|
| User1 | Defender for identity Contoso Administrators | None |
| User2 | Defender for identity Contoso Users | None |
| User3 | None | Security administrator |
| User4 | Defender for identity Contoso Users | Global administrator |

You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User1 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes
B. No

**Answer:** A

**NEW QUESTION 335**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You plan to implement records management and enable users to designate documents as regulatory records. You need to ensure that the option to mark content as a regulatory record is visible when you create retention
labels.

What should you do first?

A. Configure custom detection rules.
B. Create an Exact Data Match (EDM) schema.
C. Run the Sec-RegulacoryComplianceUI cmdlet.
D. Run the Sec-LabelPolicy cmdlet.

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide

**NEW QUESTION 337**
- (Exam Topic 4)
You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.
During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint Online.
You need to prevent the user from sharing the credit card information by using email and SharePoint. What should you configure?

A. the locations of the DLP policy
B. the user overrides of the DLP policy rule
C. the status of the DLP policy
D. the conditions of the DLP policy rule

**Answer:** A

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

**NEW QUESTION 339**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant.
You need to ensure that when a document containing a credit card number is added to the tenant, the document is encrypted.
Which policy should you use?

A. a retention policy
B. a retention label policy
C. an auto-labeling policy
D. an insider risk policy

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-w

**NEW QUESTION 344**
- (Exam Topic 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.
You are deploying Microsoft Intune.
You successfully enroll Windows 10 devices in Intune.
When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intuen. Solution: You configure the Mobility (MDM and MAM) settings. Does this meet the goal?

A. Yes
B. No

**Answer:** B

**NEW QUESTION 349**
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You need to identify which administrative users performed eDiscovery searches during the past week. What should you do from the Security & Compliance admin center?

A. Perform a content search
B. Create a supervision policy
C. Create an eDiscovery case
D. Perform an audit log search

**Answer:** D

**NEW QUESTION 350**
- (Exam Topic 4)

You have a Microsoft 365 tenet named Contoso.com. the tenant contains the users shown in the following table.

| Name | Azure AD role | Office 365 role group |
|------|---------------|----------------------|
| User1 | Application administrator | eDiscovery Administrator |
| User2 | Application administrator | Organization Management |
| User3 | Cloud application administrator | Global Administrator |
| User4 | Compliance administrator | eDiscovery Manager |

You have an eDiscovery case shown in the follow table.

| Name | Created by |
|------|-----------|
| Case1 | User1 |
| Case2 | User2 |
| Case3 | User3 |
| Case4 | User4 |

For each of the following statements select yes of the statements is true. Otherwise, select NO. NOTE: each correct selection is worth one point.

**Answer Area**

| Statements | Yes | No |
|------------|-----|-----|
| User1 can delete Case4. | ○ | ○ |
| User3 can add members to Case2. | ○ | ○ |
| User4 can close Case3. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

| Statements | Yes | No |
|------------|-----|-----|
| User1 can delete Case4. | ○ | [○] |
| User3 can add members to Case2. | ○ | [○] |
| User4 can close Case3. | [○] | ○ |

**NEW QUESTION 352**
- (Exam Topic 4)
Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP includes the machine groups shown in the following table.

| Rank | Machine group | Members |
|------|---------------|---------|
| 1 | Group1 | Tag Equals demo And OS In Windows 10 |
| 2 | Group2 | Tag Equals demo |
| 3 | Group3 | Domain Equals adatum.com |
| 4 | Group4 | Domain Equals adatum.com And OS In Windows 10 |
| Last | Ungrouped machines (default) | *Not applicable* |

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

🖥 **computer1**

[Actions ⌄]

Domain: adatum.com
OS: Windows10 64-bit (Build 17134)

**Machine IP addresses** ❯

Use the drop-down menus to select the answer choice that completes each statement.
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:**
According to this article
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/machine-groups
- If a machine is also matched to other groups, it is added only to the highest ranked machine group. Part 1 answer should be - computer 1 will be a member of - Group 3 only.
Because its the highest rank and the machine is part of adatum.com Part 2 - if you add the tag demo to computer 1. then the answer should be group 1 only.
Because the machine is tagged "demo" and OS is windows 10.

**NEW QUESTION 353**
- (Exam Topic 4)
Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.
You update the Windows 10 devices by using Windows Update for Business.
What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Quality updates:

14 days
30 days
60 days
120 days

Feature updates:

60 days
180 days
365 days
540 days

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
References:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

**NEW QUESTION 356**
- (Exam Topic 4)
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 security center.
Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

A. Microsoft Cloud App Security
B. Azure Sentinel
C. Azure Web Application Firewall
D. Azure Defender

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

**NEW QUESTION 358**
- (Exam Topic 4)
You have the Microsoft Azure Advanced Threat Protection (ATP) workspace shown in the Workspace exhibit. (Click the Workspace tab.)

Workspace ⑦

Create Workspace

Manage Azure ATP user roles ⑦

| NAME | TYPE | INTEGRATION | GEOLOCATION |
|------|------|-------------|-------------|
| testwrkspace ☐ | Primary | Windows Defender ATP | Europe |

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

Sensors ⑦

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

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

You need to ensure that Azure ATP stores data in Asia.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

**Actions**

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

**Answer Area**

| |
| |
| |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step1

**NEW QUESTION 361**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft 365 compliance policies to meet the following requirements:

≫ Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).

≫ Report on shared documents that contain PII. What should you create?

A. an alert policy
B. a data loss prevention (DLP) policy
C. a retention policy
D. a Microsoft Cloud App Security policy

**Answer:** B

**Explanation:**

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

**NEW QUESTION 366**
- (Exam Topic 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 on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings. You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You raise the forest functional level to Windows Server 2016. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.
Does this meet the goal?

A. yes
B. No

**Answer:** B

**NEW QUESTION 368**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune.
You plan to use Endpoint analytics to identify hardware issues.
You need to enable Window health monitoring on the devices to support Endpoint analytics What should you do?

A. Configure the Endpoint analytics baseline regression threshold.
B. Create a configuration profile.
C. Create a Windows 10 Security Baseline profile
D. Create a compliance policy.

**Answer:** B


**NEW QUESTION 370**
- (Exam Topic 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.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and
OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Security administrator role.
Does this meet the goal?

A. Yes
B. No

**Answer:** A


**NEW QUESTION 371**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant.
You plan to deploy a monitoring solution that meets the following requirements:

> Captures Microsoft Teams channel messages that contain threatening or violent language.

> Alerts a reviewer when a threatening or violent message is identified.
What should you include in the solution?

A. Data Subject Requests (DSRs)
B. Insider risk management policies
C. Communication compliance policies
D. Audit log retention policies

**Answer:** C


**NEW QUESTION 373**
- (Exam Topic 4)
You have a Microsoft 365 E5 tenant
You create a data toss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.
To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

## Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

ⓘ Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites.

| Status | Location | Included | Excluded |
|--------|----------|----------|----------|
| Off | Exchange email | ✓ | |
| Off | SharePoint sites | | |
| Off | OneDrive accounts | ✓ | |
| Off | Teams chat and channel messages | | |
| Off | Devices | | |
| Off | Microsoft Cloud App Security | | |
| Off | On-premises repositories | | |
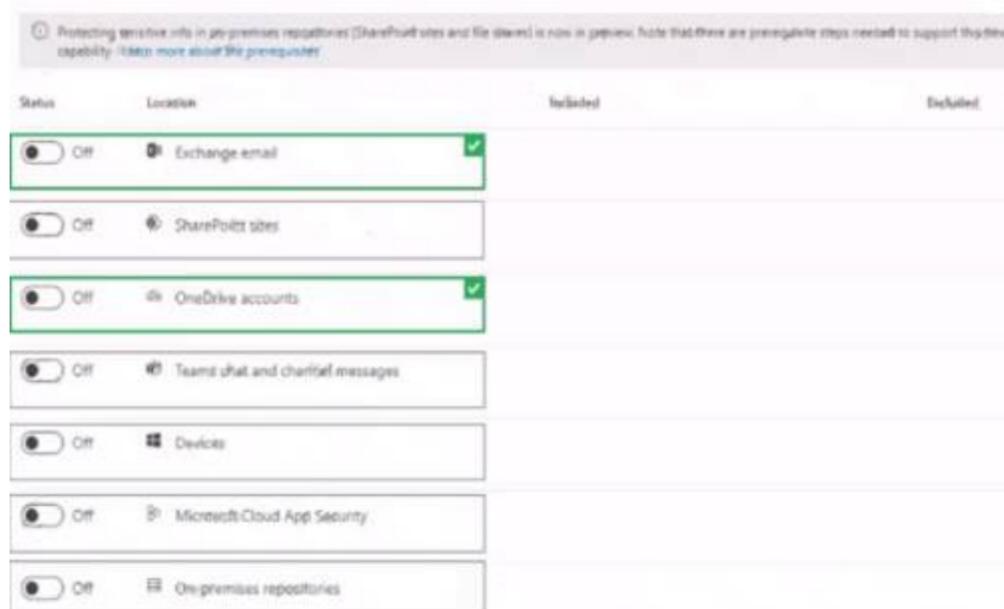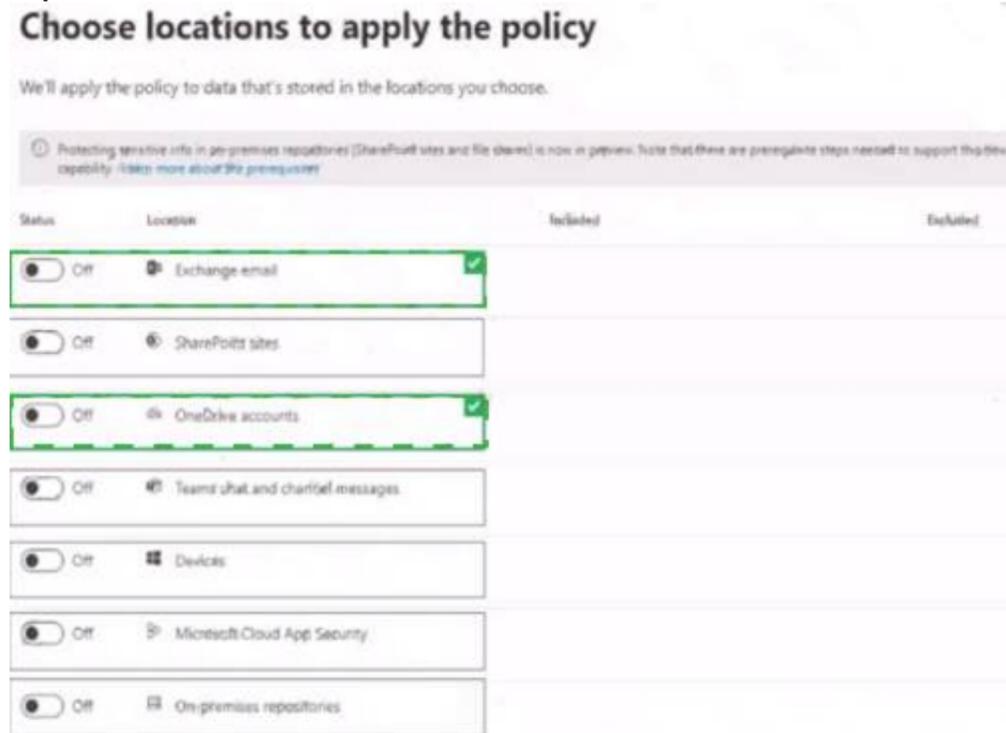
**NEW QUESTION 375**
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have 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.
You are deploying Microsoft Intune.
You successfully enroll Windows 10 devices in Intune.
When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intune. Solution: You configure the Apple MDM Push certificate.
Does this meet the goal?

A. Yes
B. No

**Answer:** A

**Explanation:**
 References:
https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get

**NEW QUESTION 380**
- (Exam Topic 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.
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Cloud App Security admin center, you assign the App/instance admin role for all Microsoft Online Services to User1.
Does this meet the goal?

A. Yes
B. No

**Answer:** B

**Explanation:**
App/instance admin: Has full or read-only permissions to all of the data in Microsoft Cloud App Security that deals exclusively with the specific app or instance of an app selected.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

**NEW QUESTION 385**
- (Exam Topic 4)
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 386**
- (Exam Topic 4)
Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The company stores 2 TBs of data in SharePoint Online document libraries. The tenant has the labels shown in the following table.

| Name | Type |
|------|------|
| Label1 | Sensitivity label |
| Label2 | Retention label |
| Label3 | Azure Information Protection label |

| Statements | Yes | No |
|------------|-----|-----|
| Label1 can now be used as a sensitivity label or an Azure Information Protection label. | ○ | ○ |
| Label2 can now be used as a retention label or an Azure Information Protection label. | ○ | ○ |
| Label3 can now be used as a sensitivity label or an Azure Information | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

| Statements | Yes | No |
|------------|-----|-----|
| Label1 can now be used as a sensitivity label or an Azure Information Protection label. | ○ | ○ |
| Label2 can now be used as a retention label or an Azure Information Protection label. | ○ | ○ |
| Label3 can now be used as a sensitivity label or an Azure Information | ○ | ○ |

**NEW QUESTION 387**
- (Exam Topic 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.
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance admin role. Does this meet the goal?

A. Yes
B. No

**Answer:** B

**Explanation:**
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/pe

**NEW QUESTION 392**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:

≫ Name: Case1

≫ Included content: Group1, User1, Site1

≫ Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders
The investigation for Case1 completes, and you close the case.
What occurs after you close Case1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

| Holds are turned off for: | ▼ |
|---|---|
| | User1 only |
| | All locations |
| | Site1 and Group1 only |

| Holds are placed on a delay hold for: | ▼ |
|---|---|
| | 30 days |
| | 90 days |
| | 120 days |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/close-or-delete-case?view=o365-worldwide

**NEW QUESTION 396**
- (Exam Topic 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.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange admin role. Does this meet the goal?

A. Yes
B. No

**Answer:** B

**Explanation:**
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwi

**NEW QUESTION 400**
......

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

# Money Back Guarantee

## MS-101 Practice Exam Features:

* MS-101 Questions and Answers Updated Frequently

* MS-101 Practice Questions Verified by Expert Senior Certified Staff

* MS-101 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* MS-101 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year