

# Exam Questions MS-102

Microsoft 365 Administrator Exam

<https://www.2passeasy.com/dumps/MS-102/>



### NEW QUESTION 1

- (Topic 6)

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 2

DRAG DROP - (Topic 6)

DRAG DROP

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.

You need to ensure that each group can perform the tasks shown in the following table.

Group	Task
Group1	<ul style="list-style-type: none"> <li>• Manage service requests.</li> <li>• Purchase new services.</li> <li>• Manage subscriptions.</li> <li>• Monitor service health.</li> </ul>
Group2	<ul style="list-style-type: none"> <li>• Assign licenses.</li> <li>• Add users and groups.</li> <li>• Create and manage user views.</li> <li>• Update password expiration policies.</li> </ul>

The solution must use the principle of least privilege.

Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role 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.

### Roles

- ☐ Billing Administrator
- ☐ Global Administrator
- ☐ Helpdesk Administrator
- ☐ License Administrator
- ☐ Service Support Administrator
- ☐ User Administrator

### Answer Area

- Group1:
- Group2:

- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

Box 1: Billing admin manage service request Purchase new services Etc.

Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.

Box 2: User admin User admin

Assign the User admin role to users who need to do the following for all users:

- Add users and groups
- Assign licenses
- Manage most users properties
- Create and manage user views
- Update password expiration policies
- Manage service requests
- Monitor service health

### NEW QUESTION 3

- (Topic 6)

You have a Microsoft 365 E5 subscription that contains a user named User1.

User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.

You need to remove User1 from the Restricted entities list. What should you use?

- A. the Exchange admin center
- B. the Microsoft Purview compliance portal
- C. the Microsoft 365 admin center
- D. the Microsoft 365 Defender portal
- E. the Microsoft Entra admin center

**Answer:** D

#### Explanation:

Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.

Remove a user from the Restricted entities page in the Microsoft 365 Defender portal In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use <https://security.microsoft.com/restrictedentities>.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam>

### NEW QUESTION 4

- (Topic 6)

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/permissions-in-the-security-and-compliance-center.md>

### NEW QUESTION 5

- (Topic 6)

You have a Microsoft 365 tenant.

You plan to implement device configuration profiles in Microsoft Intune. Which platform can you manage by using the profiles?

- A. Ubuntu Linux
- B. macOS
- C. Android Enterprise
- D. Windows 8.1

**Answer:** D

### NEW QUESTION 6

- (Topic 6)

Your company has offices in five cities. The company has a Microsoft 365 tenant.

Each office is managed by a local administrator. You plan to deploy Microsoft Intune.

You need to recommend a solution to manage resources in Intune that meets the following requirements:

? Local administrators must be able to manage only the resources in their respective office.

? Local administrators must be prevented from managing resources in other offices.

? Administrative effort must be minimized.

What should you include in the recommendation?

- A. device categories
- B. scope tags
- C. configuration profiles
- D. conditional access policies

**Answer:** B

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags>

### NEW QUESTION 7

- (Topic 6)

Your company has 10,000 users who access all applications from an on-premises data center.

You plan to create a Microsoft 365 subscription and to migrate data to the cloud. You plan to implement directory synchronization.

User accounts and group accounts must sync to Azure AD successfully. You discover that several user accounts fail to sync to Azure AD.

You need to resolve the issue as quickly as possible. What should you do?

- A. From Active Directory Administrative Center, search for all the users, and then modify the properties of the user accounts.
- B. Run idfix.exe, and then click Edit.
- C. From Windows PowerShell, run the start-AdSyncSyncCycle -PolicyType Delta command.
- D. Run idfix.exe, and then click Complete.

**Answer:** B

**Explanation:**

IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for-synch-with-idfix>

**NEW QUESTION 8**

- (Topic 6)

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: At a command prompt, you run the winver.exe command. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

Reference:

<https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808>

**NEW QUESTION 9**

- (Topic 6)

You have a Microsoft 365 subscription.

You register two applications named App1 and App2 to Azure AD.

You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

- A. From the Microsoft Entra admin center, create a conditional access policy
- B. From the Microsoft 365 admin center, configure the Modern authentication settings.
- C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.
- D. From Multi-Factor Authentication, configure the service settings.

**Answer:** A

**Explanation:**

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication>

**NEW QUESTION 10**

- (Topic 6)

Your company has a Microsoft 365 E5 tenant that contains a user named User1. You review the company's compliance score.

You need to assign the following improvement action to User1:Enable self-service password reset.

What should you do first?

- A. From Compliance Manager, turn off automated testing.
- B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
- C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
- D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

**Answer:** D

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide>

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal>

**NEW QUESTION 10**

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



Name	Role
User1	Global Administrator
User2	Service Support Administrator
User3	Cloud Application Administrator
User4	None

You plan to provide User4 with early access to Microsoft 365 feature and service updates. You need to identify which Microsoft 365 setting must be configured, and which user can

modify the setting. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

## Answer Area

Microsoft 365 setting:

▼

Office installation options

Privileged access

Release preferences

User:

▼

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area

Microsoft 365 setting:

▼

Office installation options

Privileged access

Release preferences

User:

▼

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

## NEW QUESTION 14

- (Topic 6)

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

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

Your network contains an Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the Azure AD credentials.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

The question states that “all the user account synchronizations completed successfully”. Therefore, the Azure AD credentials are configured correctly in Azure AD Connect. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering>

**NEW QUESTION 18**

- (Topic 6)

From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)

SharePoint Content\_Export

↓ Restart report

↓ Download report

🗑 Delete

**Status:**  
The export has completed. You can start downloading the results.

**Items included from the search:**  
All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

**Exchange content format:**  
One PST file for each mailbox.

**De-duplication for Exchange content:**  
Not enabled.

**SharePoint document versions:**  
Included

**Export files in a compressed (zipped) folder:**  
Yes

**The export data was prepared within region:**  
Default region

Close

Feedback

What will be excluded from the export?

- A. a 10-MB XLSX file
- B. a 5-MB MP3 file
- C. a 5-KB RTF file
- D. an 80-MB PPTX file

**Answer:** B

**Explanation:**

Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide>

<https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report>

**NEW QUESTION 21**

HOTSPOT - (Topic 6)

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:**

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

#### NEW QUESTION 24

- (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. A Built-in protection preset security policy is applied to the subscription.

Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Anti-malware
- B. Anti-phishing
- C. Safe Attachments
- D. Anti-spam
- E. Safe Links

**Answer:** CE

#### NEW QUESTION 26

- (Topic 6)

You have a Microsoft 365 subscription.

You plan to use Adoption Score and need to ensure that it can obtain device and software metrics.

What should you do?

- A. Enable Endpoint analytics.
- B. Run the Microsoft 365 network connectivity test on each device.



- C. Enable privileged access.
- D. Configure Support integration.

**Answer:** A

#### NEW QUESTION 29

HOTSPOT - (Topic 6)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.

### Configure

Microsoft Intune

Save
 Discard
 Delete

MDM user scope

None
 Some
 All

Groups

Select groups
 Group1

MDM terms of use URL

<https://portal.manage.microsoft.com/TermsofUse.aspx>

MDM discovery URL

<https://enrollment.manage.microsoft.com/enrollmentserver/discovery>

MDM compliance URL

<https://portal.manage.microsoft.com/?portalAction=Compliance>

Restore default MDM URLs

MAM User scope

None
 Some
 All

Groups

Select groups
 Group2

MAM Terms of use URL

MAM Discovery URL

<https://wip.mam.manage.microsoft.com/Enroll>

MAM Compliance URL

Restore default MAM URLs

You purchase a Windows 10 device named Device1.

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 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>

#### NEW QUESTION 34

- (Topic 6)

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 months.

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 36

- (Topic 6)

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

The policies are assigned to Device1.

Which policy settings will be applied to Device1?

- A. only the settings of Policy1
- B. only the settings of Policy2
- C. only the settings of Policy3
- D. no settings

**Answer:** D

#### NEW QUESTION 37

- (Topic 6)

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 41

HOTSPOT - (Topic 6)

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

Credit Card Number

min

max

x

Retention labels

1 year

x

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.

#### NEW QUESTION 44

- (Topic 6)

Your network contains an Active Directory forest named Contoso. Local. You have a Microsoft 365 subscription.

You plan to implement a directory synchronization solution that will use password hash synchronization.

From the Microsoft 365 admin center, you successfully verify the contoso.com domain name.

You need to prepare the environment for the planned directory synchronization solution. What should you do first?

- A. From Active Directory Domains and Trusts, add contoso.com as a UPN suffix.
- B. From the Microsoft 365 admin center verify the Contos
- C. Local domain name.
- D. From the public DNS zone of contoso.com, add a new mail exchanger (MX) record.
- E. From Active Directory Users and Computers, modify the UPN suffix for all users.

Answer: A

#### NEW QUESTION 45

DRAG DROP - (Topic 6)

DRAG DROP

You have a Microsoft 365 E5 subscription. Several users have iOS devices.

You plan to enroll the iOS devices in Microsoft Endpoint Manager.

You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.

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

#### Actions

#### Answer Area

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Create a certificate from the Apple Push Certificates Portal.

From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Create a certificate from the Apple Push Certificates Portal.

From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

Answer Area

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Create a certificate from the Apple Push Certificates Portal.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

NEW QUESTION 46

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy. You need to identify the following information:

- The number of email messages quarantined by zero-hour auto purge (ZAP)
- The number of times users clicked a malicious link in an email message

Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

To identify the number of times users clicked a malicious link in an email:

Mailflow status report

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

To identify the number of times users clicked a malicious link in an email:

Mailflow status report

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

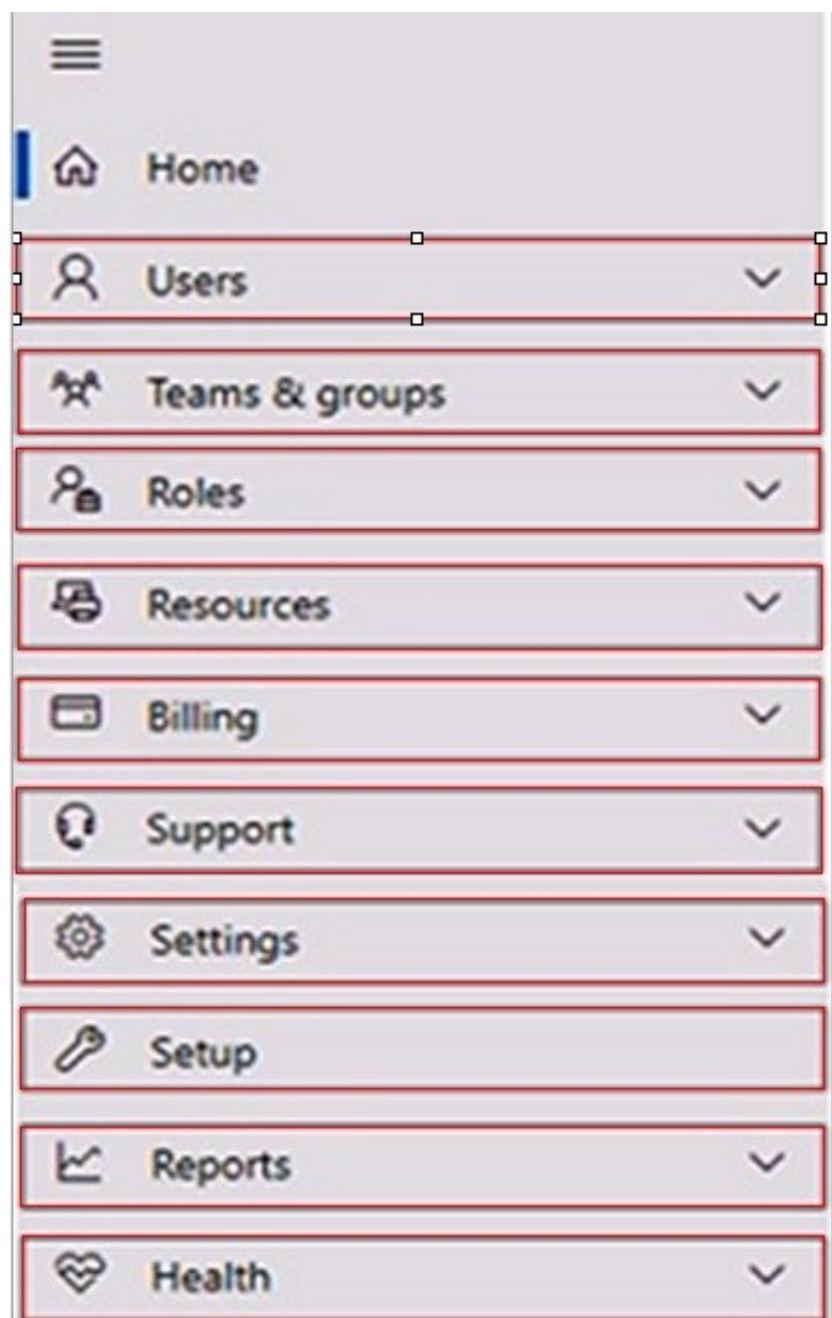
NEW QUESTION 48

HOTSPOT - (Topic 6)

HOTSPOT

Your company has a Microsoft 365 E5 subscription. You need to perform the following tasks: View the Adoption Score of the company. Create a new service request to Microsoft. Which two options should you use in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.





- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Reports

View the Adoption Score of the company.

How to enable Adoption Score To enable Adoption Score:

? Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score

? Select enable Adoption Score. It can take up to 24 hours for insights to become available.

Box 2: Support

Create a new service request to Microsoft.

Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request. If you're in the admin center, select Support > New service request.

**NEW QUESTION 50**

- (Topic 6)

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.

To which location can the policy be applied?

- A. OneDrive accounts
- B. Exchange email
- C. Teams chat and channel messages
- D. SharePoint sites

**Answer:** B

**NEW QUESTION 53**

- (Topic 6)

You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.

You need to prevent the members of Group1 from communicating with the members of Group2 by using Microsoft Teams. The solution must comply with regulatory requirements and must not affect other user in the tenant.

What should you use?

- A. information barriers
- B. communication compliance policies
- C. moderated distribution groups
- D. administrator units in Azure Active Directory (Azure AD)



Answer: A

#### NEW QUESTION 55

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Role
User1	Global admin
User2	<i>None</i>
User3	<i>None</i>

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	<i>None</i>
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:

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

#### NEW QUESTION 58

- (Topic 6)

You have a Microsoft 365 subscription.

You need to configure a compliance solution that meets the following requirements: Defines sensitive data based on existing data samples  
 Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages  
 Which two components should you configure? Each correct answer presents part of the solution.  
 NOTE: Each correct selection is worth one point.

- A. a trainable classifier
- B. a sensitive info type
- C. an insider risk policy
- D. an adaptive policy scope
- E. a data loss prevention (DLP) policy

**Answer:** AE

**Explanation:**

A: Classifiers

This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.

Where you can use classifiers

Classifiers are available to use as a condition for: Office auto-labeling with sensitivity labels

Auto-apply retention label policy based on a condition Communication compliance

Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.

Data loss prevention

E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about> <https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp>

**NEW QUESTION 63**

HOTSPOT - (Topic 6)

HOTSPOT

Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

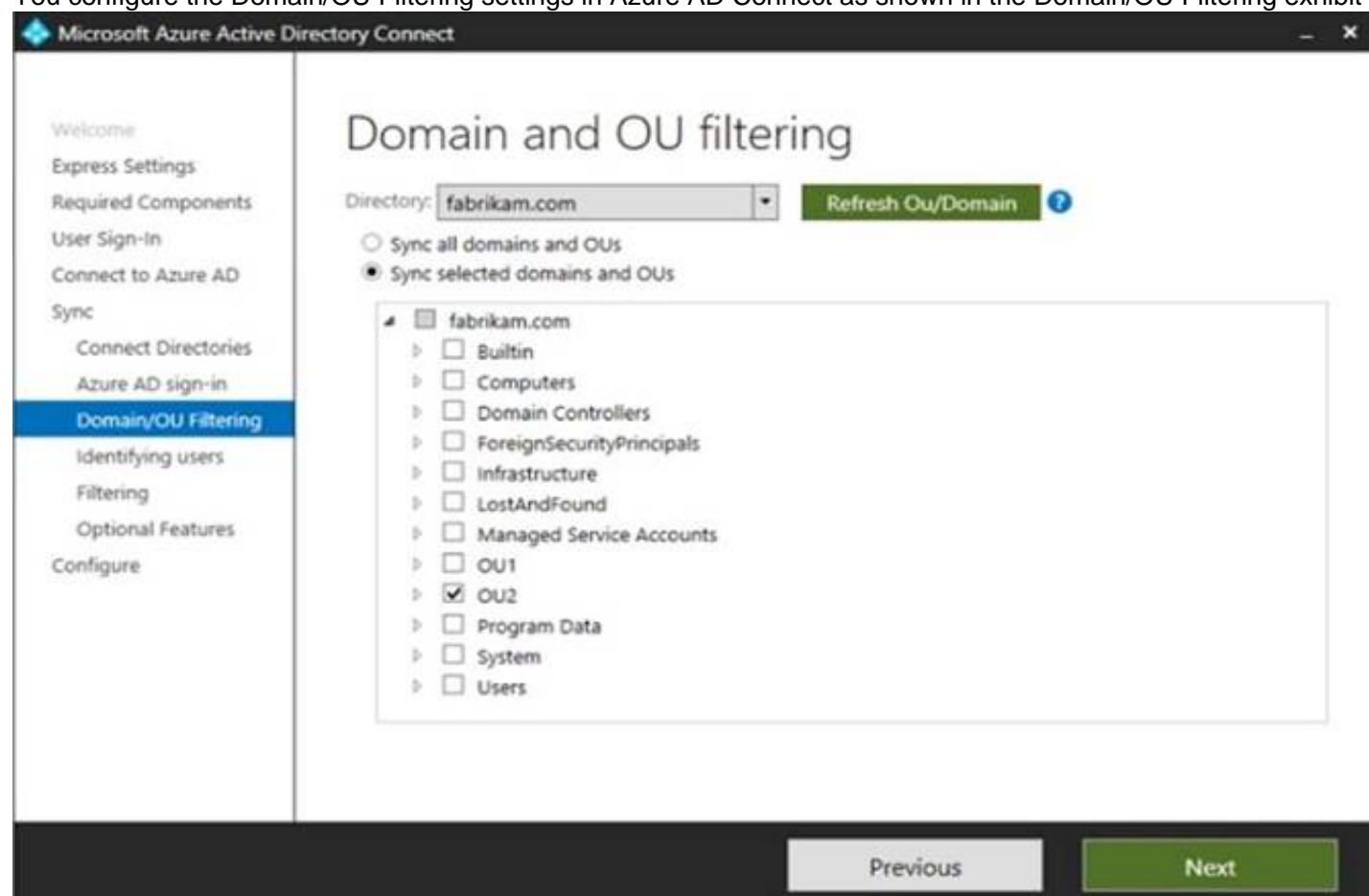
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.

You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)



You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)

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
User2 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>
Group2 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>
User3 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

### Explanation:

Box 1: No

The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized. User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD.

Box 2: Yes

Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.

Box 3: Yes

User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD.

### NEW QUESTION 68

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

Defender for Endpoint has the device groups shown in the following table.



Rank	Name	Matching rule
1	Group1	Tag Contains Inventory And OS in Android
2	Group2	Name Starts with Device And Tag Contains Inventory
Last	Ungrouped devices (default)	Not applicable

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@contoso.com

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

If a high-severity incident is triggered for Device1, an incident email notification will be sent.

Yes

☒

No

☐

If a low-severity incident is triggered for Computer1, an incident notification email will be sent.

☐
☐

If a low-severity incident is triggered for Device3, an incident notification email will be sent.

☐
☐

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Box 1: No

Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.

Box 2: No

Computer1 does not belong to either Group1 or Group2

Box 3: Yes

Device3 belongs to both Group1 and Group2.

Note: Understanding alert severity

Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.

The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

#### NEW QUESTION 71

- (Topic 6)

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert occurs only on a Windows 10 device. The solution must minimize administrative effort. What should you do first?

- A. From the Microsoft 365 admin center, create a mail-enabled security group.
- B. From the Microsoft 365 Defender portal, create a device group.
- C. From the Microsoft Endpoint Manager admin center, create a device category.
- D. From the Azure Active Directory admin center, create a dynamic device group.

Answer: B

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide>

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide>



NEW QUESTION 72

DRAG DROP - (Topic 6)

You have a Microsoft 365 subscription.

You need to meet the following requirements:

- Report a Microsoft 365 service issue.
- Request help on how to add a new user to an Azure AD tenant.

What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature 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.

Features

Message center

New service request

Product feedback

Service health

Answer Area

To report issues regarding a Microsoft 365 service:

To request help on how to add a new user to the tenant:

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Features

Message center

New service request

Product feedback

Service health

Answer Area

To report issues regarding a Microsoft 365 service:

New service request

To request help on how to add a new user to the tenant:

Message center

NEW QUESTION 75

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to use a mailbox named Mailbox1 to analyze malicious email messages. You need to configure Microsoft Defender for Office 365 to meet the following requirements:

- Ensure that incoming email is NOT filtered for Mailbox1.
- Detect impersonation and spoofing attacks on all other mailboxes in the subscription. Which two settings should you configure? To answer, select the appropriate settings in the answer area.

Answer Area

Policies

Anti-phishing

Anti-spam

Anti-malware

Safe Attachments

Safe Links

Rules

Tenant Allow/Block Lists

Email authentication settings

DKIM

Advanced delivery

Enhanced filtering

Quarantine policies

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

? Safe Attachments policy: This policy allows you to specify how to handle email attachments that might contain malware. You can create a custom policy for Mailbox1 and set the action to Do not scan attachments. This will ensure that incoming email is not filtered for Mailbox1. You can also enable the Redirect attachment option to send a copy of the original attachment to another mailbox for analysis1.

? Anti-phishing policy: This policy helps you protect your organization from impersonation and spoofing attacks. You can create a default policy for all other mailboxes in the subscription and enable the following features: Impersonation protection, Spoof intelligence, and Domain authentication. These features will help you detect and block emails that try to impersonate your users, domains, or trusted senders2.

# NEW QUESTION 78

HOTSPOT - (Topic 6)

You have a Microsoft 365 tenant that contains the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to create a compliance policy named Compliance1.

You need to identify the groups that meet the following requirements:

? Can be added to Compliance1 as recipients of noncompliance notifications

? Can be assigned to Compliance1

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Can be added to Compliance1 as recipients of noncompliance notifications:

▼

Group1 and Group4 only

Group3 and Group4 only

Group1, Group2 and Group3 only

Group1, Group3, and Group4 only

Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

▼

Group1 and Group4 only

Group3 and Group4 only

Group1, Group2 and Group3 only

Group1, Group3, and Group4 only

Group1, Group2, Group3, and Group4

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Can be added to Compliance1 as recipients of noncompliance notifications:

▼

Group1 and Group4 only

Group3 and Group4 only

Group1, Group2 and Group3 only

Group1, Group3, and Group4 only

Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

▼

Group1 and Group4 only

Group3 and Group4 only

Group1, Group2 and Group3 only

Group1, Group3, and Group4 only

Group1, Group2, Group3, and Group4

# NEW QUESTION 81

- (Topic 6)

Your network contains an on-premises Active Directory domain named contoso.com.

For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.

You plan to sync contoso.com to an Azure AD tenant.

You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.

What should you include in the recommendation?

A. pass-through authentication

B. conditional access policies

C. password synchronization

D. Azure AD Identity Protection policies

Answer: A

**Explanation:**  
Reference:  
<https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/>

**NEW QUESTION 83**  
HOTSPOT - (Topic 6)  
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	None	Purchaser	Group2
User3	None	Basic Purchaser	Group3

You perform the following actions:  
? Provision the private store in Microsoft Store for Business.  
? Add an app named App1 to the private store.  
? Set Private store availability for App1 to Specific groups, and then select 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
User1 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>
User2 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>
User3 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Statements	Yes	No
User1 can install App1 from the private store.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can install App1 from the private store.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can install App1 from the private store.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 85**  
DRAG DROP - (Topic 6)  
You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.  
All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.  
You plan to implement self-service password reset (SSPR).  
You need to ensure that when a user resets or changes a password, the password syncs with AD DS.  
Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action 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.

Actions	Answer Area
<div>From the Microsoft Entra admin center, configure on-premises integration password writeback.</div>	Step 1: Validate permissions for the Microsoft Entra Connect account.
<div>From the Microsoft Entra admin center, configure the authentication methods for SSPR.</div>	Step 2: <div></div>
<div>From the Microsoft Entra admin center, configure the registration settings for SSPR.</div>	Step 3: <div></div>
<div>Select Group writeback in Microsoft Entra Connect.</div>	
<div>Select Password writeback in Microsoft Entra Connect.</div>	



- A. Mastered  
B. Not Mastered

Answer: A

#### Explanation:

**Actions**

From the Microsoft Entra admin center, configure on-premises integration password writeback.

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

**Answer Area**

Step 1: Validate permissions for the Microsoft Entra Connect account.

Step 2: From the Microsoft Entra admin center, configure on-premises integration password writeback.

Step 3: Select Password writeback in Microsoft Entra Connect.

#### NEW QUESTION 90

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

You deploy the anti-phishing policy shown in the following exhibit.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

Add trusted senders and domains
Enable domains to protect
Enable users to protect
Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

Add trusted senders and domains
Enable intelligence for impersonation protection
Enable spoof intelligence

- A. Mastered  
B. Not Mastered

Answer: A

#### Explanation:

Box 1: Enable users to protect

Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.

User impersonation protection

User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.

You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation

is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).

When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender's email address, the action for impersonated users is applied to the message.

Box 2: Add trusted senders and domains Trusted senders and domains

Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren't applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.

#### NEW QUESTION 92

- (Topic 6)

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Department
User1	Human resources
User2	Research
User3	Human resources
User4	Marketing



You need to configure group-based licensing to meet the following requirements:

? To all users, deploy an Office 365 E3 license without the Power Automate license option.

? To all users, deploy an Enterprise Mobility + Security E5 license.

? To the users in the research department only, deploy a Power BI Pro license.

? To the users in the marketing department only, deploy a Visio Plan 2 license.

What is the minimum number of deployment groups required?

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

**Answer: C**

**Explanation:**

One for all users, one for the research department, and one for the marketing department.

Note: What are Deployment Groups?

With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers on-premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.

Reference:

<https://devblogs.microsoft.com/devops/deployment-groups-is-now-generally-available-sharing-of-targets-and-more>

**NEW QUESTION 94**

HOTSPOT - (Topic 6)

HOTSPOT

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 Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Opening files in SharePoint that contain malicious content:

<input type="checkbox"/>	Anti-spam
<input type="checkbox"/>	Anti-Phishing
<input type="checkbox"/>	Safe Attachments
<input type="checkbox"/>	Safe Links

Impersonation and spoofing attacks in email messages:

<input type="checkbox"/>	Anti-spam
<input type="checkbox"/>	Anti-Phishing
<input type="checkbox"/>	Safe Attachments
<input type="checkbox"/>	Safe Links

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Opening files in SharePoint that contain malicious content:

<input type="checkbox"/>	Anti-spam
<input type="checkbox"/>	Anti-Phishing
<input checked="" type="checkbox"/>	Safe Attachments
<input type="checkbox"/>	Safe Links

Impersonation and spoofing attacks in email messages:

<input type="checkbox"/>	Anti-spam
<input checked="" type="checkbox"/>	Anti-Phishing
<input type="checkbox"/>	Safe Attachments
<input type="checkbox"/>	Safe Links

**NEW QUESTION 98**

- (Topic 6)

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant includes a user named User1.

You enable Azure AD Identity Protection.

You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege. To which role should you add User1?

- A. Security Reader
- B. Global Administrator
- C. Owner
- D. User Administrator

Answer: A

NEW QUESTION 102

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1. Azure AD Password Protection is configured as shown in the following exhibit.

Custom smart lockout

Lockout threshold ⓘ

15

✓

Lockout duration in seconds ⓘ

600

✓

Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

3hundred  
Eleven  
Falcon  
Project  
Tailspin

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

User1 attempts to update their password to the following passwords:

? F@lcon

? Project22

? T4il\$pin45dg4

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

[Answer choice] will be accepted as a password.

Only T4il\$pin45dg4

Only F@lcon and T4il\$pin45dg4

Only Project22 and T4il\$pin45dg4

F@lcon, Project22, and T4il\$pin45dg4

If User1 enters the same wrong password 15 times, waits 11 minutes, and then enters the same wrong password again, the user [answer choice].

will be locked out

will trigger a user risk

can attempt to sign in again immediately

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Only T4il\$pin45dg4

Box 2: can attempt to sign in immediately Note: Manage Azure AD smart lockout values

Based on your organizational requirements, you can customize the Azure AD smart lockout values. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users. Customization of the smart lockout settings is not available for Azure China 21Vianet tenants.

To check or modify the smart lockout values for your organization, complete the following steps:

? Sign in to the Entra portal.

? Search for and select Azure Active Directory, then select Security > Authentication methods > Password protection.

? Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.

? The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.

? Set the Lockout duration in seconds, to the length in seconds of each lockout.

? The default is 60 seconds (one minute).

If the first sign-in after a lockout period has expired also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases.

#### NEW QUESTION 107

- (Topic 6)

You have a Microsoft 365 E5 subscription that contains a user named User1. You create a retention label named Retention1 that is published to all locations. You need to ensure that User1 can label email messages by using Retention1 as soon as possible. Which cmdlet should you run in Microsoft Exchange Online PowerShell?

- A. Start-MpScan
- B. Start-Process
- C. Start-ManagedFolderAssistant
- D. Start-AppBackgroundTask

**Answer: C**

#### NEW QUESTION 111

HOTSPOT - (Topic 6)

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.

Activities to search for:

	▼
Exchange mailbox activities	
Site administration activities	
Show results for all activities	
Role administration activities	

Field to filter by:

	▼
Item	
User	
Detail	
IP address	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Activities to search for:

	▼
Exchange mailbox activities	
Site administration activities	
Show results for all activities	
Role administration activities	

Field to filter by:

	▼
Item	
User	
Detail	
IP address	

#### NEW QUESTION 113

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.

You need to deploy the policy. What should you do first?

- A. Review the sensitive information in Activity explorer
- B. Turn on the policy
- C. Run the policy in simulation mode
- D. Configure Azure Information Protection analytics



Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide>

NEW QUESTION 118

- (Topic 6)

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 123

DRAG DROP - (Topic 6)

Your company has an Azure AD tenant named contoso.onmicrosoft.com.

You purchase a domain named contoso.com from a registrar and add all the required DNS records.

You create a user account named User1. User1 is configured to sign in as user1@contoso.onmicrosoft.com.

You need to configure User1 to sign in as user1@contoso.com.

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

Run update-rgdomain -DomainId contoso.com.

Modify the email address of User1.

Add contoso.com as a SAN for an X.509 certificate.

Add a custom domain name.

Verify the custom domain.

Modify the username of User1.

>

<

Answer Area

&u2191

&u2193

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Run update-rgdomain -DomainId contoso.com.

Modify the email address of User1.

Add contoso.com as a SAN for an X.509 certificate.

Add a custom domain name.

Verify the custom domain.

Modify the username of User1.

>

<

Answer Area

Add a custom domain name.

Verify the custom domain.

Modify the username of User1.

&u2191

&u2193

NEW QUESTION 126

DRAG DROP - (Topic 6)

Your company purchases a cloud app named App1.

You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls.

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



## Actions

## Answer Area

- Deploy Azure Active Directory (Azure AD) Application Proxy.
- From the Cloud App Security admin center, add an app connector.
- Sign in to App1.
- Create a conditional access policy.
- From the Azure Active Directory admin center, configure the Diagnostic settings.
- From the Azure Active Directory admin center, add an app registration for App1.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Actions

## Answer Area

- Deploy Azure Active Directory (Azure AD) Application Proxy.
- From the Cloud App Security admin center, add an app connector.
- Sign in to App1.
- Create a conditional access policy.
- From the Azure Active Directory admin center, configure the Diagnostic settings.
- From the Azure Active Directory admin center, add an app registration for App1.



- From the Cloud App Security admin center, add an app connector.
- Create a conditional access policy.
- Sign in to App1.

### NEW QUESTION 129

- (Topic 6)

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

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

Your network contains an Active Directory forest. You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant. Does this meet the goal?

- A. Yes
- B. No

Answer: B

### NEW QUESTION 132

- (Topic 6)

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 133

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

At 08:00, you create an incident notification rule that has the following configurations:

- Name: Notification!
- Notification settings
  - o Notify on alert severity: Low
  - o Device group scope: All (3)
  - o Details: First notification per incident
- Recipients: User1@contoso.com, User2@contoso.com

At 08:02, you create an incident notification rule that has the following configurations:

- Name: Notification
- Notification settings
  - o Notify on alert severity: Low, Medium
  - o Device group scope: DeviceGroup1, DeviceGroup2
- Recipients: User1@contoso.com

In Microsoft 365 Defender, alerts are logged as shown in the following table.

Time	Alert name	Severity	Impacted assets
08:05	Activity1	Low	Device1
08:07	Activity1	Low	Device1
08:08	Activity1	Medium	Device1
08:15	Activity2	Medium	Device2
08:16	Activity2	Medium	Device2
08:20	Activity1	High	Device1
08:30	Activity3	Medium	Device2
08:35	Activity2	High	Device2

For each of the following statements, select Yes if the statement is true. Otherwise, select No1.

NOTE: Each correct selection is worth one point.

#### Answer Area

##### Statements

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

Yes

☐

No

☐

User2@contoso.com will receive an incident notification email for the alert at 08:07.

☐
☐

User1@contoso.com will receive an incident notification email for the alert at 08:20.

☐
☐

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

#### Answer Area

##### Statements

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

Yes

☐

No

☒

User2@contoso.com will receive an incident notification email for the alert at 08:07.

☒
☐

User1@contoso.com will receive an incident notification email for the alert at 08:20.

☐
☒

### NEW QUESTION 137

- (Topic 6)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the



stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.  
 After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.  
 Your network contains an Active Directory domain. You deploy an Azure AD tenant.  
 Another administrator configures the domain to synchronize to Azure AD.  
 You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.  
 You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.  
 You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: You run idfix.exe and export the 10 user accounts.  
 Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

The question states that “all the user account synchronizations completed successfully”. If there were problems with the 10 accounts that needed fixing with idfix.exe, there would have been synchronization errors in Azure AD Connect Health.  
 It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.  
 Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering>

**NEW QUESTION 138**

- (Topic 6)

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 140**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of Microsoft 365 role group
Admin1	Content Explorer List viewer Content Explorer Content viewer
Admin2	Security Administrator Content Explorer List Viewer

You have labels in Microsoft 365 as shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

The content in Microsoft 365 is assigned labels as shown in the following table.

Name	Type	Label
File1	File in SharePoint Online	Label1
Mail1	Email message in Exchange Online	Label2

You have labels In Microsoft 365 as shown in the following table.

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

Answer Area		
Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	<input type="radio"/>	<input type="radio"/>
Admin2 can view the contents of File1 by using Content explorer.	<input type="radio"/>	<input type="radio"/>
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**



Explanation:

Answer Area

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can view the contents of File1 by using Content explorer.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 145

- (Topic 6)

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels   Label policies   Auto-labeling (preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label   Publish labels   Refresh

Name	Order	Created by	Last modified
Label1	0 - highest	Prvi	04/24/2020
Label2	1	Prvi	04/24/2020
Label3	0 - highest	Prvi	04/24/2020
Label4	0 - highest	Prvi	04/24/2020
Label5	5	Prvi	04/24/2020
Label6	0 - highest	Prvi	04/24/2020

Which labels can users apply to content?

- A. Label1, Label2, and Label5 only
- B. Label3, Label4, and Label6 only
- C. Label1, Label3, Label2, and Label6 only
- D. Label1, Label2, Label3, Label4, Label5, and Label6

Answer: C

NEW QUESTION 150

HOTSPOT - (Topic 6)

HOTSPOT

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Device 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 devices (default)	Not applicable

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

Settings > Endpoints > computer1



## computer1

### Device summary

Risk level ⓘ

None

### Device details

Domain

adatum.com

OS

Windows 10 64-bit

Version 21H2

Build 19044.2130

Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.

#### Answer Area

Computer1 will be a member of [answer choice].

▼

Group3 only

Group4 only

Group3 and Group4 only

Ungrouped devices

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 devices

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Box 1: Group3 and Group4 only Computer1 has no Demo Tag.

Computer1 is in the adatum domain and OS is Windows 10. Box 2: Group1, Group2, Group3 and Group4

#### NEW QUESTION 155

- (Topic 6)

You have the sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels

Label policies

Auto-labeling(preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label    Publish labels    Refresh

Name ↑		Order	Created by	Last modified
Label1	...	0-highest	Pri	04/24/2020
- Label2	...	1	Pri	04/24/2020
Label3	...	0-highest	Pri	04/24/2020
Label4	...	0-highest	Pri	04/24/2020
- Label5	...	5	Pri	04/24/2020
Label6		0-highest	Pri	04/24/2020

Which labels can users apply to content?

- A. Label3, Label4, and Label6 only
- B. Label1, Label2, Label3, Label4, Label5, and Label6
- C. Label1, Label2, and Label5 only
- D. Label1, Label3, Label4, and Label6 only

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

#### NEW QUESTION 156

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription.

All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.

You need to configure Defender for Endpoint to meet the following requirements:

? Block a vulnerable app until the app is updated.

? Block an application executable based on a file hash.

The solution must minimize administrative effort.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

Block a vulnerable app until the app is updated:

An allow or block file

A file indicator

A remediation request

An update ring

Block an application executable based on a file hash:

An allow or block file

A file indicator

A remediation request

An update ring

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



Box 1: A remediation request  
 Block a vulnerable app until the app is updated.  
 Block vulnerable applications  
 How to block vulnerable applications  
 ? Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.  
 ? Select a security recommendation to see a flyout with more information.  
 ? Select Request remediation.  
 ? Select whether you want to apply the remediation and mitigation to all device groups or only a few.  
 ? Select the remediation options on the Remediation request page. The remediation options are software update, software uninstall, and attention required.  
 ? Pick a Remediation due date and select Next.  
 ? Under Mitigation action, select Block or Warn. Once you submit a mitigation action, it is immediately applied.  
 ? Review the selections you made and Submit request. On the final page you can choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.

Box 2: A file indicator  
 Block an application executable based on a file hash.  
 While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.  
 The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

#### NEW QUESTION 160

- (Topic 6)  
 You have a Microsoft 365 subscription.  
 You need to receive a notification each time a user in the service desk department grants Full Access permissions for a user mailbox.  
 What should you configure?

- A. a data loss prevention (DLP) policy
- B. an alert policy
- C. an audit search
- D. an insider risk management policy

**Answer: B**

#### NEW QUESTION 162

HOTSPOT - (Topic 6)  
 Your company uses Microsoft Defender for Endpoint.  
 The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

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

Name	Device
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 device 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

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

#### Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input checked="" type="radio"/>

#### NEW QUESTION 163

- (Topic 6)

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 Administrator 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>

#### NEW QUESTION 168

- (Topic 6)

Your company has a Microsoft E5 tenant.

The company must meet the requirements of the ISO/IEC 27001:2013 standard. You need to assess the company's current state of compliance.

What should you use?

- A. eDiscovery
- B. Information governance
- C. Compliance Manager
- D. Data Subject Requests (DSRs)

**Answer: C**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001>

#### NEW QUESTION 171

- (Topic 6)

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 Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

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

Solution: From the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### NEW QUESTION 174

- (Topic 6)

You have a Microsoft 365 E5 tenant. Users store data in the following locations:

- ? Microsoft Teams
- ? Microsoft OneDrive
- ? Microsoft Exchange Online
- ? Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.

What is the minimum number of retention policies that you should create?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: C

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide>

**NEW QUESTION 177**

- (Topic 6)

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 named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

## PROVISION FROM ACTIVE DIRECTORY



### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

### Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

## USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.

Solution: From the Microsoft Entra admin center, you assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com.

Does this meet the goal?

A. Yes

B. No

Answer: B

**Explanation:**

This is not a permissions issue so you do not need to assign the Security Reader role. The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

**NEW QUESTION 182**

- (Topic 6)

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 186

DRAG DROP - (Topic 6)

DRAG DROP

You have a Microsoft 365 E5 tenant.

You need to implement compliance solutions that meet the following requirements:

- Use a file plan to manage retention labels.
- Identify, monitor, and automatically protect sensitive information.
- Capture employee communications for examination by designated reviewers.

Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Solutions

Data loss prevention

Information governance

Insider risk management

Records management

Answer Area

Identify, monitor, and automatically protect sensitive information:

Capture employee communications for examination by designated reviewers:

Use a file plan to manage retention labels:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Solutions

Data loss prevention

Information governance

Insider risk management

Records management

Answer Area

Identify, monitor, and automatically protect sensitive information: Data loss prevention

Capture employee communications for examination by designated reviewers: Insider risk management

Use a file plan to manage retention labels: Information governance

NEW QUESTION 187

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

The subscription has the following two anti-spam policies:

- Name: AntiSpam1
- Priority: 0
- Induce these users, groups and domains o Users: User3
- o Groups: Group1
- Exclude these users, groups and domains o Groups: Group2
- Message limits
- o Set a daily message limit 100
- Name: AntiSpam2
- Priority: 1
- Include these users, groups and domains o Users: User1 o Groups: Group2
- Exclude these users, groups and domains o Users: User3
- Message limits
- o Set a daily message limit 50

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 send a maximum of 150 email messages per day.	<input type="radio"/>	<input type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input type="radio"/>	<input type="radio"/>
User3 can send a maximum of 100 email messages per day.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can send a maximum of 100 email messages per day.	<input checked="" type="radio"/>	<input type="radio"/>

#### NEW QUESTION 189

- (Topic 6)

Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.

Your company purchases Microsoft 365 and creates an Azure AD tenant named contoso.onmicrosoft.com.

You plan to install Azure AD Connect on a member server and implement pass-through authentication.

You need to prepare the environment for the planned implementation of pass-through authentication.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From a domain controller install an Authentication Agent
- B. From the Microsoft Entra admin center, configure an authentication method.
- C. From Active Director,' Domains and Trusts add a UPN suffix
- D. Modify the email address attribute for each user account.
- E. From the Microsoft Entra admin center, add a custom domain name.
- F. Modify the User logon name for each user account.

**Answer:** ABE

#### Explanation:

Deploy Azure AD Pass-through Authentication Step 1: Check the prerequisites

Ensure that the following prerequisites are in place. In the Entra admin center

\* 1. Create a cloud-only Hybrid Identity Administrator account or a Hybrid Identity administrator account on your Azure AD tenant. This way, you can manage the configuration of your tenant should your on-premises services fail or become unavailable.

(E) 2. Add one or more custom domain names to your Azure AD tenant. Your users can sign in with one of these domain names.

(A) In your on-premises environment

\* 1. Identify a server running Windows Server 2016 or later to run Azure AD Connect. If not enabled already, enable TLS 1.2 on the server. Add the server to the same Active Directory forest as the users whose passwords you need to validate. It should be noted that installation of Pass-Through Authentication agent on Windows Server Core versions is not supported.

\* 2. Install the latest version of Azure AD Connect on the server identified in the preceding step. If you already have Azure AD Connect running, ensure that the version is supported.

\* 3. Identify one or more additional servers (running Windows Server 2016 or later, with TLS 1.2 enabled) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.

\* 4. Etc.

(B) Step 2: Enable the feature

Enable Pass-through Authentication through Azure AD Connect.

If you're installing Azure AD Connect for the first time, choose the custom installation path. At the User sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect. In addition, the Pass-through Authentication feature is enabled on your tenant.

Incorrect:

Not C: From Active Directory Domains and Trusts, add a UPN suffix Not D. Modify the email address attribute for each user account. Not F. Modify the User logon name for each user account.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start>

#### NEW QUESTION 194

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:

- Support KQL for querying data.
- Retain report data for at least one year.

What should you include in the recommendation?

- A. a security report in Microsoft 365 Defender
- B. End point analytics
- C. Microsoft 365 usage analytics
- D. Azure Monitor workbooks

**Answer:** D

#### NEW QUESTION 195

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription. You need to meet the following requirements:

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label. Which two settings should you use in the Microsoft Purview compliance portal? To answer,

select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

## Answer Area

Solutions	
	Catalog
	Audit
	Content search
	Communication compliance
	Data loss prevention
	eDiscovery 
	Data lifecycle management
	Information protection
	Information barriers 
	Insider risk management
	Records management
	Privacy Risk Management 
	Privacy Subject Rights Requests
<hr/>	
	Settings

- A. Mastered  
B. Not Mastered

Answer: A

### Explanation:

Box 1: Information protection

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection

All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.

To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels:

In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information Protection -> Microsoft Information Protection.

Note: Encryption of data at rest

Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.

BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology. Box 2: Settings

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.

- \* 1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
- \* 2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
- \* 3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
- \* 4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
- \* 5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.

## NEW QUESTION 196



- (Topic 6)

Your company has three main offices and one branch office. The branch office is used for research.

The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.

You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.

What should you include in the recommendation?

- A. Azure AD password protection
- B. a Microsoft Intune device configuration profile
- C. a Microsoft Intune device compliance policy
- D. Azure AD conditional access

**Answer: D**

#### NEW QUESTION 199

- (Topic 6)

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. What permission should you assign to User1?

- A. the Information Protection administrator role from the Azure Active Directory admin center.
- B. the eDiscovery Manager role from the Microsoft 365 compliance center.
- C. the Compliance Management role from the Exchange admin center.
- D. the User management administrator role from the Microsoft 365 admin center.

**Answer: B**

#### NEW QUESTION 203

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You need to create a policy that will generate an email alert when a banned app is detected requesting permission to access user information or data in the subscription.

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

**Answer Area**

Policy type: Activity, App discovery, OAuth app, Session. Callout: These are the selections for Policy type.

Filter type: App, App state, App tag, Permission level. Callout: These are the selections for Filter type.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Policy type: Activity, App discovery, OAuth app, Session. Callout: These are the selections for Policy type.

Filter type: App, App state, App tag, Permission level. Callout: These are the selections for Filter type.

#### NEW QUESTION 208

- (Topic 6)

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

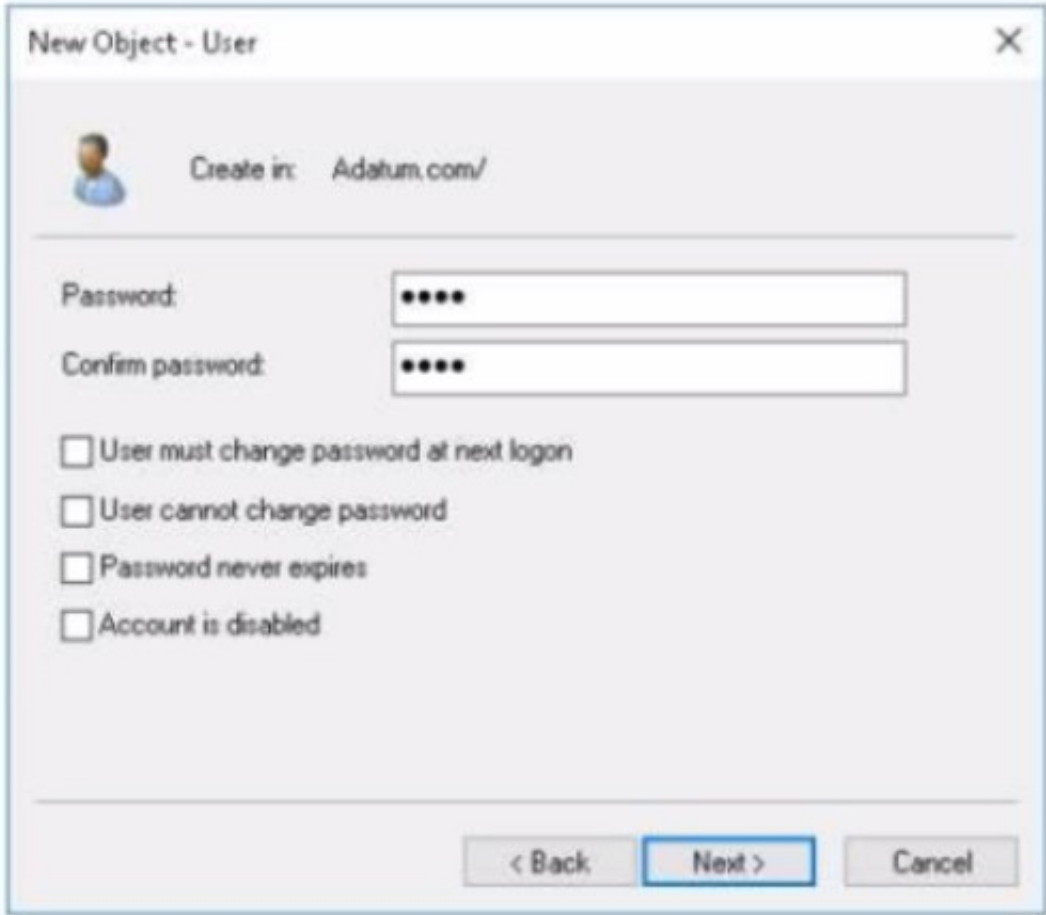
Explanation:

Reference:  
<https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide>

NEW QUESTION 209

HOTSPOT - (Topic 6)

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure AD by using the Azure AD Connect Express Settings. Password write back is disabled. You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.



The Azure AD password policy is configured as shown in the following exhibit. Password policy Set the password policy for all users in your organization. Days before passwords expire 90 Days before a user is notified about 14 expiration You confirm that User1 is synced to Azure AD. 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 sign in to Azure AD.	<input type="radio"/>	<input type="radio"/>
		User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input type="radio"/>
		From Azure AD, User1 must change the password every 90 days.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area				
		Statements	Yes	No
		User1 can sign in to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
		User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>
		From Azure AD, User1 must change the password every 90 days.	<input checked="" type="radio"/>	<input type="radio"/>

## NEW QUESTION 214

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 tenant.

You plan to create a retention policy as shown in the following exhibit.

Information governance > Create retention policy

✓ Name

✓ Locations

✓ Retention settings

● Finish

### Review and finish

It might take up to one day to apply this policy to the locations you selected.

**Policy name**  
contoso  
[Edit](#)

**Description**  
[Edit](#)

**Locations to apply the policy**  
Exchange email (All Recipients)  
SharePoint sites (All Sites)  
OneDrive accounts (All Accounts)  
Microsoft 365 Groups (All Groups)  
[Edit](#)

**Retention settings**  
Delete items at end of retention period  
Delete items that are older than 7 years based on when they were created  
[Edit](#)

⚠ Items that are currently older than 7 years will be deleted after you turn on this policy. This is especially important to note for locations scoped to 'All' sources (for example, 'All Teams chats') because all matching items in those locations across your organization will be permanently deleted.

[Back](#) [Submit](#) [Cancel](#)

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

NOTE: Each correct selection is worth one point.

### Answer Area

Microsoft SharePoint files that are affected by the policy will be **[answer choice]**.

Once the policy is created, **[answer choice]**.

- A. Mastered  
B. Not Mastered

Answer: A

### Explanation:

Box 1: Deleted seven years after they were created. From the exhibit:

The retention policy applies to SharePoint sites.

Delete items that are older than 7 years based on when they were created.

Box 2: data will retained for a minimum of seven years

The longest retention period wins. If content is subject to multiple retention settings that retain content for different periods of time, the content will be retained until the end of the longest retention period for the item.

Note: Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email).

For example, if all documents in a SharePoint site should be retained for 5 years, it's more efficient to do this with a retention policy than apply the same retention label to all documents in that site. However, if some documents in that site should be retained for 5

years and others retained for 10 years, a retention policy wouldn't be able to do this. When you need to specify retention settings at the item level, use retention labels.

## NEW QUESTION 219

- (Topic 6)

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 224

- (Topic 6)

You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.

## Domains

+ Add domain Buy domain Refresh		
Domain name ↑	Status	Choose columns
<input type="checkbox"/> Sub1.contoso221018.onmicrosoft.com (D...	Possible service issues	
<input type="checkbox"/> contoso.com	Incomplete setup	
<input type="checkbox"/> contoso221018.onmicrosoft.com	Healthy	
<input type="checkbox"/> Sub2.contoso221018.onmicrosoft.com	Incomplete setup	

Which domain name suffixes can you use when you create users?

- A. only Sub1.contoso221018.onmicrosoft.com
- B. only contoso.com and Sub2.contoso221018.onmicrosoft.com
- C. only contoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com
- D. all the domains in the subscription

Answer: B

#### NEW QUESTION 227

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Mailbox size
User1	5 MB
User2	15 MB
User3	25 MB
User4	55 MB

You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email.

You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2.

Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can assign Retention1:

	▼
User4 only	
User3 and User4 only	
User2, User3, and User4 only	
User1, User2, User3, and User4	

Users who can assign Retention2:

	▼
User4 only	
User3 and User4 only	
User2, User3, and User4 only	
User1, User2, User3, and User4	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Users who can assign Retention1:

	▼
User4 only	
User3 and User4 only	
User2, User3, and User4 only	
User1, User2, User3, and User4	

Users who can assign Retention2:

	▼
User4 only	
User3 and User4 only	
User2, User3, and User4 only	
User1, User2, User3, and User4	

#### NEW QUESTION 229

- (Topic 6)

You have an Azure AD tenant.

You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD. You purchase a Microsoft 365 E3 subscription.

You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort.

What should you do?

- A. From the Microsoft Endpoint Manager admin center, create a Windows Autopilot deployment profile
- B. Assign the profile to all the computer
- C. Instruct users to restart their computer and perform a network restart.
- D. Enroll the computers in Microsoft Intun
- E. Create a configuration profile by using the Edition upgrade and mode switch templat
- F. From the Microsoft Endpoint Manager admincenter, assign the profile to all the computers and instruct users to restart their computer.
- G. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online sit
- H. Instruct users to run the provisioning package from SharePoint Online.
- I. From the Azure Active Directory admin center, create a security group that has dynamic device membershi
- J. Assign licenses to the group and instruct users to sign in to their computer.

**Answer:** B

#### NEW QUESTION 230

DRAG DROP - (Topic 6)

DRAG DROP

Your network contains an on-premises Active Directory domain that syncs to Azure Active

Directory (Azure AD). The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2016	File Server Resource Manager (FSRM)
Server2	Windows Server 2016	None

You use Azure Information Protection.

You need to ensure that you can apply Azure Information Protection labels to the file stores on Server1.

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

Authorize Server1.

Install the Microsoft Rights Management connector on Server2.

Install a certificate on Server2.

Install a certificate on Server1.

Register a service principal name for Server1.

Run GenConnectorConfig.ps1 on Server1.

Run GenConnectorConfig.ps1 on Server2.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Authorize Server1.

Install the Microsoft Rights Management connector on Server2.

Install a certificate on Server2.

Install a certificate on Server1.

Register a service principal name for Server1.

Run GenConnectorConfig.ps1 on Server1.

Run GenConnectorConfig.ps1 on Server2.

Answer Area

Install the Microsoft Rights Management connector on Server2.

Authorize Server1.

Run GenConnectorConfig.ps1 on Server1.

NEW QUESTION 233

HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription that contains the administrative units shown in the following table.

Name	Members
AU1	Group1, User2
AU2	Group2, User3, User4

The groups contain the members shown in the following table.

Name	Members
Group1	User1
Group2	User2, User4

The users are assigned the roles shown in the following table.

Name	Role	Scope
User1	None	Not applicable
User2	Password Administrator	AU1
User3	License Administrator	Organization
User4	None	Not applicable

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

User2 can reset the password of User1.

☐

☐

User2 can reset the password of User4.

☐

☐

User3 can assign licenses to User1.

☐

☐



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User2 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can reset the password of User4.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can assign licenses to User1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 236

HOTSPOT - (Topic 5)

You need to configure the Office 365 service status notifications and limit access to the service and feature updates. The solution must meet the technical requirements.

What should you configure in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To configure the notifications:

Briefing email

Briefing email

Help desk information

Organization information

To limit access:

Release preferences

Privileged Access

Release preferences

Office installation options

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 237

HOTSPOT - (Topic 4)

HOTSPOT

You create the Microsoft 365 tenant.

You implement Azure AD Connect as shown in the following exhibit.

The screenshot shows the Azure Active Directory admin center interface. The left sidebar contains navigation icons. The main content area is titled 'Azure AD Connect' under the 'Home > Azure AD Connect' breadcrumb. Below the title are 'Troubleshoot' and 'Refresh' buttons. The 'SYNC STATUS' section shows a sync icon, 'Sync Status' as 'Enabled', 'Last Sync' as 'Less than 1 hour ago', and 'Password Hash Sync' as 'Enabled'. The 'USER SIGN-IN' section shows a sign-in icon and three options: 'Federation' (Disabled, 0 domains), 'Seamless single sign-on' (Disabled, 0 domains), and 'Pass-through authentication' (Disabled, 0 agents).

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

During Project1, sales department users can access [answer choice] applications by using SSO.

If Active Directory becomes unavailable during Project1, sales department users can access the resources [answer choice].

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Box 1: only on-premises

In the exhibit, seamless single sign-on (SSO) is disabled. Therefore, as SSO is disabled in the cloud, the Sales department users can access only on-premises applications by using SSO.

In the exhibit, directory synchronization is enabled and active. This means that the on- premises Active Directory user accounts are synchronized to Azure Active Directory user accounts. If the on-premises Active Directory becomes unavailable, the users can access resources in the cloud by authenticating to Azure Active Directory. They will not be able to access resources on-premises if the on-premises Active Directory becomes unavailable as they will not be able to authenticate to the on-premises Active Directory.

Box 2: in the cloud only

#### NEW QUESTION 239

- (Topic 4)

Which role should you assign to User1?

Available Choices (select all choices that are correct)

- A. Hygiene Management
- B. Security Reader
- C. Security Administrator
- D. Records Management

Answer: C

#### Explanation:

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.

Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in

Office 365 Security & Compliance Center.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles>

#### NEW QUESTION 242

- (Topic 3)

You create the planned DLP policies.

You need to configure notifications to meet the technical requirements. What should you do?

- A. From the Microsoft 365 security center, configure an alert policy.
- B. From the Microsoft Endpoint Manager admin center, configure a custom notification.
- C. From the Microsoft 365 admin center, configure a Briefing email.
- D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

**Answer:** D

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide>

#### NEW QUESTION 246

- (Topic 3)

You need to configure Office on the web to meet the technical requirements. What should you do?

- A. Assign the Global reader role to User1.
- B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.
- C. Configure an auto-labeling policy to apply the sensitivity labels.
- D. Assign the Office apps admin role to User1.

**Answer:** B

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide>

#### NEW QUESTION 248

- (Topic 3)

You need to create the Safe Attachments policy to meet the technical requirements. Which option should you select?

- A. Replace
- B. Enable redirect
- C. Block
- D. Dynamic Delivery

**Answer:** D

#### Explanation:

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/safe-attachments.md>

#### NEW QUESTION 253

HOTSPOT - (Topic 3)

You plan to implement the endpoint protection device configuration profiles to support the planned changes.

You need to identify which devices will be supported, and how many profiles you should implement.

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

NOTE: Each correct selection is worth one point.

Supported devices:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3
Device1, Device4, and Device5
Device1, Device2, Device3, Device4, and Device5

Number of required profiles:

1
2
3
4
5

- A. Mastered
- B. Not Mastered



Answer: A

Explanation:

Supported devices:

▼
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3
Device1, Device4, and Device5
Device1, Device2, Device3, Device4, and Device5

Number of required profiles:

▼
1
2
3
4
5

#### NEW QUESTION 255

- (Topic 2)

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

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

Answer: D

Explanation:

References:

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

#### NEW QUESTION 258

HOTSPOT - (Topic 2)

You need to meet the technical requirement for log analysis.

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

NOTE: Each correct selection is worth one point.

Minimum number of data sources:

▼
1
3
6

Minimum number of log collectors:

▼
1
3
6

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

#### NEW QUESTION 259

- (Topic 2)

You need to recommend a solution for the security administrator. The solution must meet the technical requirements. What should you include in the recommendation?

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

**Answer:** B

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#sign-in-risk> states clearly that Sign-in risk

**NEW QUESTION 264**

- (Topic 2)

Which report should the New York office auditors view?

- A. DLP policy matches
- B. DLP false positives and overrides
- C. DLP incidents
- D. Top Senders and Recipients

**Answer:** C

**Explanation:**

References:

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

This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

**NEW QUESTION 269**

- (Topic 1)

On which server should you install the Azure ATP sensor?

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

**Answer:** A

**Explanation:**

References:

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

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

**NEW QUESTION 273**

HOTSPOT - (Topic 1)

You need to meet the technical requirements and planned changes for Intune. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

## Answer Area

Settings to configure in Azure AD:

Device settings  
 Mobility (MDM and MAM)  
 Organizational relationships  
 User settings

Settings to configure in Intune:

Device compliance  
 Device configuration  
 Device enrollment  
 Mobile Device Management Authority

### NEW QUESTION 275

HOTSPOT - (Topic 1)

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

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

NOTE: Each correct selection is worth one point.

New	Conditions	Device state (preview)
<p><b>Info</b></p> <p>* Name                      Policy1 ✓</p> <p><b>Assignments</b></p> <p>Users and groups                      0 users and groups selected</p> <p>Cloud apps                      1 app included</p> <p>Conditions                      0 conditions selected</p> <p><b>Access controls</b></p> <p>Grant                      Block access</p> <p>Session                      0 controls selected</p> <p><b>Enable policy</b>                      On Off</p>	<p><b>Info</b></p> <p>Sign-in risk                      Not configured</p> <p>Device platforms                      Not configured</p> <p>Locations                      Not configured</p> <p>Client apps (preview)                      Not configured</p> <p>Device state (preview)                      Not configured</p>	<p><b>Info</b></p> <p>Configure                      Yes No</p> <p>Include Exclude</p> <p>Select the device state condition used to exclude devices from policy.</p> <p><input type="checkbox"/> Device Hybrid Azure AD joined</p> <p><input type="checkbox"/> Device marked as compliant</p>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References: <https://docs.microsoft.com/en-us/intune/create-conditional-access-intune>

### NEW QUESTION 276

- (Topic 1)

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

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

Answer: C

### NEW QUESTION 279

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You need to be notified when a single user downloads more than 50 files during any 60- second period.

What should you configure?

- A. a session policy
- B. a file policy
- C. an activity policy
- D. an anomaly detection policy

Answer: D



NEW QUESTION 280

DRAG DROP - (Topic 6)

You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune. You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices. Which four 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

Create an app configuration policy

Link the account to Intune

Create a Microsoft account

Configure a mobile device management (MDM) push certificate

Add the app

Create a Google account

Assign the app

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Create an app configuration policy

Link the account to Intune

Create a Microsoft account

Configure a mobile device management (MDM) push certificate

Add the app

Create a Google account

Assign the app

Answer Area

Create a Google account

Link the account to Intune

Add the app

Assign the app

NEW QUESTION 285

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription. You configure a new alert policy as shown in the following exhibit.

## How do you want the alert to be triggered?

- ☐ Every time an activity matches the rule
- ☐ When the volume of matched activities reaches a threshold

More than or equal to  activities

During the last  minutes

On

- ☒ When the volume of matched activities becomes unusual

On

You need to identify the following:

? How many days it will take to establish a baseline for unusual activity.

? Whether alerts will be triggered during the establishment of the baseline.

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

NOTE: Each correct selection is worth one point.

How many days it will take to establish the baseline:

1
5
7
10

Whether the alerts will be triggered during the establishment of the baseline:

Alerts will be triggered.
Alerts will not be triggered.
Alerts will be triggered only after the process to establish the baseline has been running for one day.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

How many days it will take to establish the baseline:

1
5
7
10

Whether the alerts will be triggered during the establishment of the baseline:

Alerts will be triggered.
Alerts will not be triggered.
Alerts will be triggered only after the process to establish the baseline has been running for one day.

NEW QUESTION 290

- (Topic 6)

You have a Microsoft 365 E5 subscription.  
 You create a Conditional Access policy that blocks access to an app named App1 when users trigger a high-risk sign-in event.  
 You need to reduce false positives for impossible travel when the users sign in from the corporate network.  
 What should you configure?

- A. exclusion groups
- B. multi-factor authentication (MFA)
- C. named locations
- D. user risk policies

**Answer:** C

#### NEW QUESTION 293

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Mail-enabled security
Group3	Microsoft 365
Group4	Distribution

All the groups are deleted.

Which groups can be restored, and what is the retention period? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Groups that can be restored:

Group3 only

Group1 and Group2 only

Group2 and Group4 only

Group1, Group2, and Group3 only

Group1, Group2, Group3, and Group4

Retention period:

24 hours

7 days

14 days

30 days

90 days

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Box 1: Group3 only

Box 2: 30 days

If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a "soft-delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

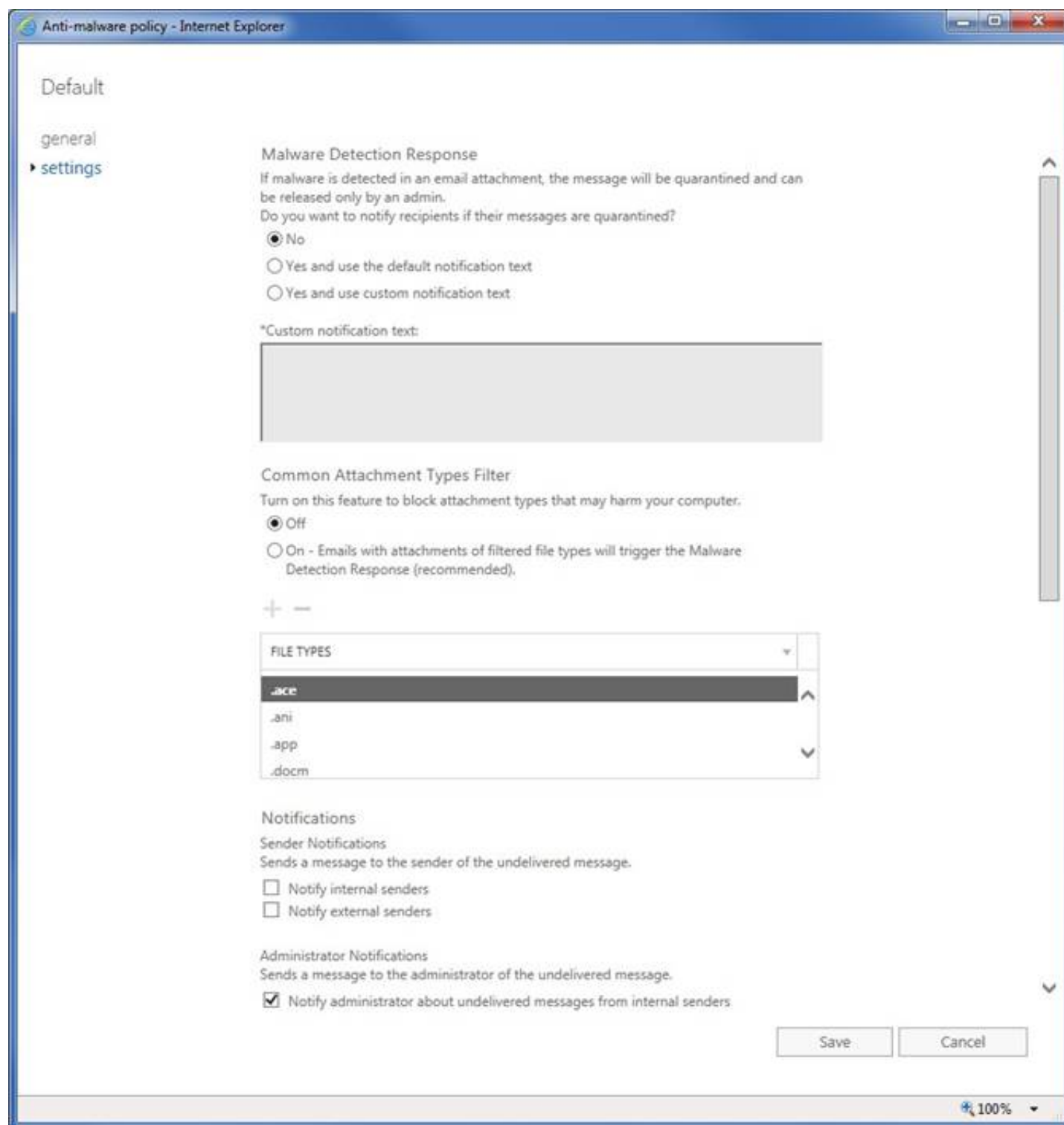
#### NEW QUESTION 297

- (Topic 6)

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=o365-worldwide#anti-malware-policies>

#### NEW QUESTION 301

HOTSPOT - (Topic 6)

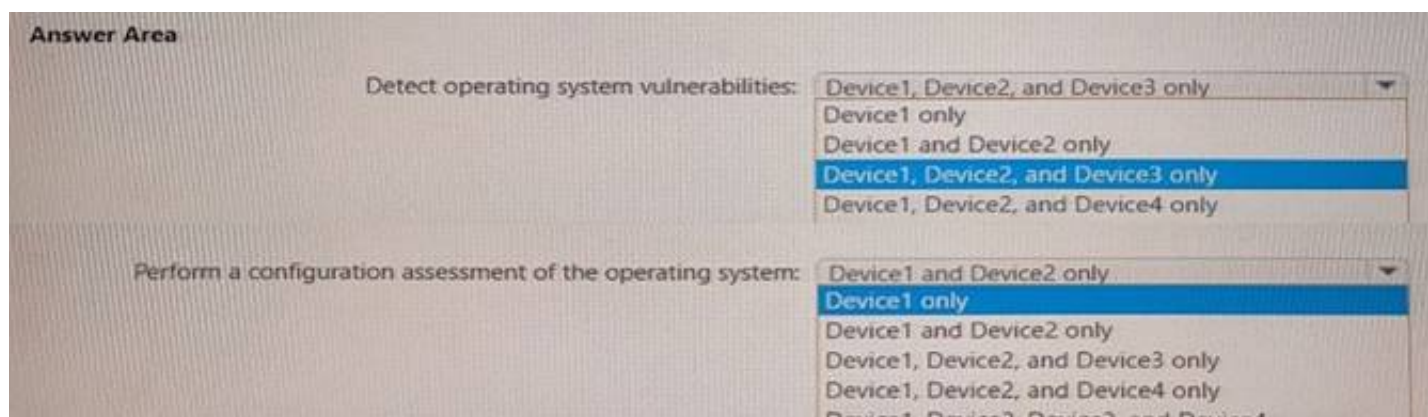
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

All the devices are onboarded To Microsoft Defender for Endpoint

You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:

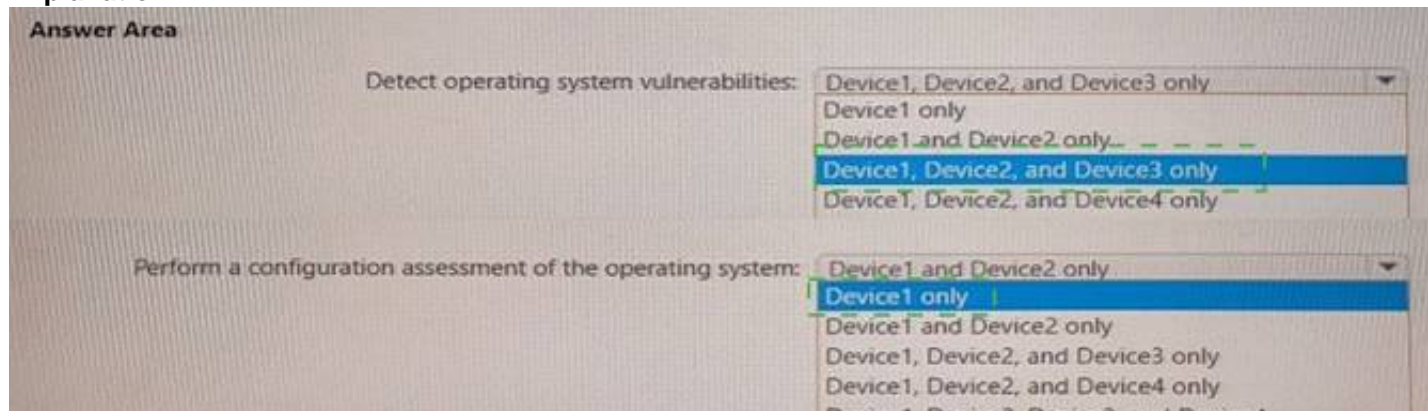
- Detect operating system vulnerabilities.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 305

- (Topic 6)

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 Defender for CloudUse the
- B. Microsoft Purview
- C. Azure Arc
- D. Microsoft Defender for Identity

**Answer:** D

**Explanation:**

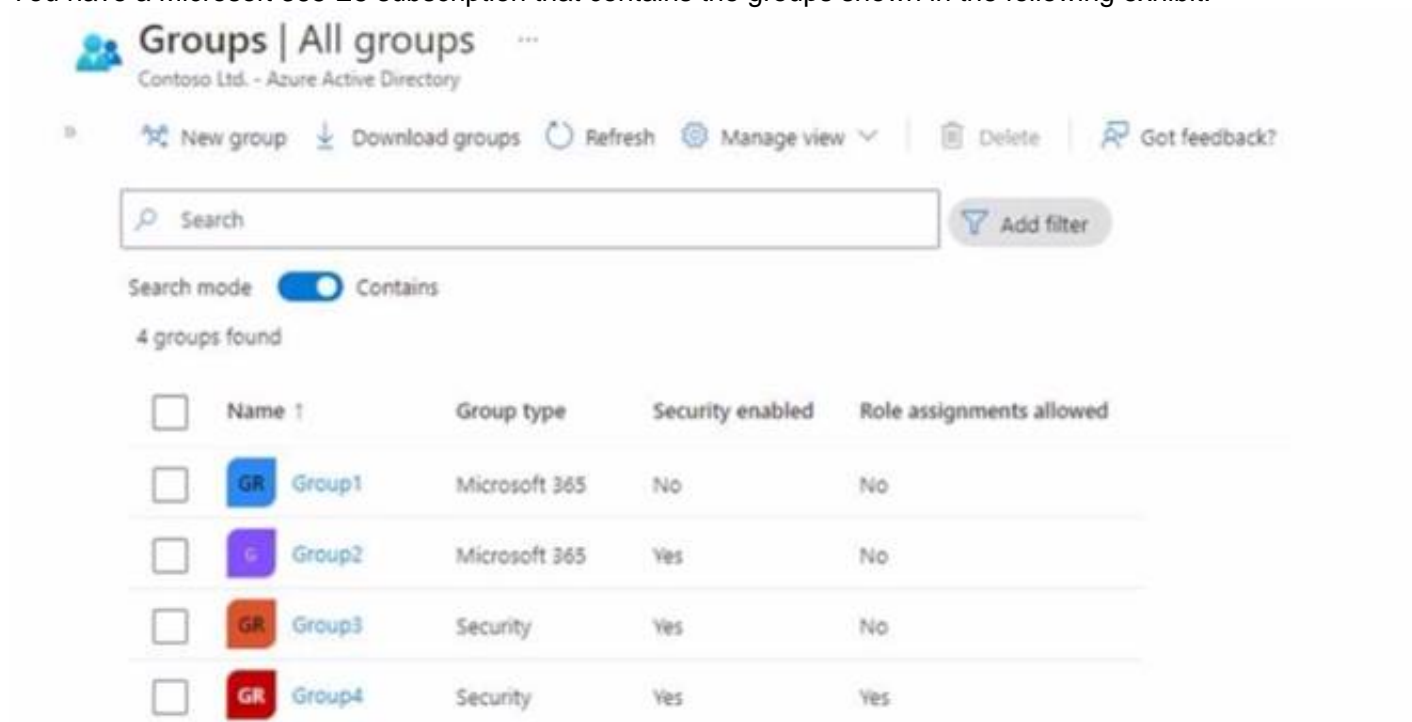
Reference:

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

#### NEW QUESTION 306

- (Topic 6)

You have a Microsoft 365 E5 subscription that contains the groups shown in the following exhibit.



To which groups can you assign Microsoft 365 E5 licenses?

- A. Group1 and Group2 only
- B. Group2 and Group3 only
- C. Group3 and Group4 only

- D. Group 1, Group2. and Group3 only  
E. Group2, Group3, and Group4 only

**Answer:** C

#### NEW QUESTION 309

- (Topic 6)

Your company has digitally signed applications.

You need to ensure that Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) considers the digitally signed applications safe and never analyzes them.

What should you create in the Microsoft Defender Security Center?

- A. a custom detection rule  
B. an allowed/blocked list rule  
C. an alert suppression rule  
D. an indicator

**Answer:** D

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators>

#### NEW QUESTION 312

- (Topic 6)

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 System, and then you select About to view information about the system.

Does this meet the goal?

- A. Yes  
B. No

**Answer:** A

#### Explanation:

Reference:

<https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808>

#### NEW QUESTION 314

- (Topic 6)

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 319

HOTSPOT - (Topic 6)

You have a hybrid deployment of Azure AD that contains the users shown in the following table.

Name	Description
User1	Azure AD Connect sync account
User2	Contributor for Azure AD Connect Health
User3	Application administrator in Azure AD

You need to identify which users can perform the following tasks:

- View sync errors in Azure AD Connect Health.
- Configure Azure AD Connect Health settings.

Which user should you identify for each task? To answer, select the appropriate options in the answer area.



NOTE: Each correct selection is worth one point.  
Answer Area

View sync errors in Azure AD Connect Health: 

User2  
User1  
User2  
User3

Configure Azure AD Connect Health settings: 

User1  
User1  
User2  
User3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Answer Area

View sync errors in Azure AD Connect Health: 

User2  
User1  
User2  
User3

Configure Azure AD Connect Health settings: 

User1  
User1  
User2  
User3

NEW QUESTION 322

- (Topic 6)  
You are reviewing alerts in the Microsoft 365 Defender portal. How long are the alerts retained in the portal?

- A. 30 days
- B. 60 days
- C. 3 months
- D. 6 months
- E. 12 months

Answer: C

Explanation:

Data retention information for Microsoft Defender for Office 365  
By default, data across different features is retained for a maximum of 30 days. However, for some of the features, you can specify the retention period based on policy. See the following table for the different retention periods for each feature.  
Defender for Office 365 Plan 1  
\* Alert metadata details (Microsoft Defender for Office alerts) 90 days.  
Note: By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the top of the list so you can see it first.

Alerts									
<div>Export 30 Days Manage alerts</div> <div>Filters: Status: New +1</div>									
Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity	
Email reported by ...		Informational		In progress	Others	MDO	Jenny Sivalingam	Apr 14, 2021	
Admin action sub...		Informational	Remediated	New	Suspicious activity	Automated investigation		Apr 14, 2021	
Custom detection ...		Medium		New	Execution	Custom detection	mario@outlook.com...	Apr 14, 2021	
"> <img src=x oner...> +3		High	No threats found	New	Exploit	Custom detection	cont-denmarks	Apr 14, 2021	
"> <img src=x oner...> +2		High	No threats found	New	Exploit	Custom detection	cont-mikelarden	Apr 7, 2021	
Unfamiliar sign-in ...		Low		New	Initial access	AAD Identity Protection	bbocadmin	Apr 14, 2021	
Admin action sub...		Informational	Remediated	New	Suspicious activity	Automated investigation		Apr 14, 2021	
Test email custom ...		Medium		New	Execution	Custom detection	Clare Love	Apr 14, 2021	

Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention>

NEW QUESTION 325

HOTSPOT - (Topic 6)  
HOTSPOT  
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support. How should you complete the membership rule? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

(user.userType

-eq "Guest"

-in "Guest"

-ne "Guest"

-notmatch "Member"

) and (user.department

-contains "Support"

-in "Support"

-match "Support"

-startsWith "Sup"

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: -eq "Guest"  
Dynamic membership rules for groups in Azure Active Directory  
Supported expression operators  
The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.  
\* Equals  
-eq  
\* Contains  
-contains  
\* Etc.  
Box 2: -contains "Support" Incorrect:  
\* -in  
If you want to compare the value of a user attribute against multiple values, you can use the -in or -notin operators.

NEW QUESTION 328

HOTSPOT - (Topic 6)  
You have a Microsoft 365 E5 tenant.  
You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege.  
Which type of policy should you create and which Microsoft 365 compliance center role is required to create the pokey? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

Alert

Threat

Compliance

  
Role:

Quarantine

Security Administrator

Organization Configuration

Communication Compliance Admin

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy type:

Alert

Threat

Compliance

  
Role:

Quarantine

Security Administrator

Organization Configuration

Communication Compliance Admin

NEW QUESTION 331

- (Topic 6)

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 334**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains 200 Android devices enrolled in Microsoft Intune.

You create an Android app protection policy named Policy1 that is targeted to all Microsoft apps and assigned to all users.

Policy1 has the Data protection settings shown in the following exhibit.

**Data Transfer**

Backup org data to Android backup services ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Block
Send org data to other apps ⓘ	Policy managed apps
Select apps to exempt	<input type="button" value="Select"/>
Save copies of org data ⓘ	<input type="radio"/> Allow <input checked="" type="radio"/> Block
Allow user to save copies to selected services ⓘ	SharePoint
Transfer telecommunication data to ⓘ	Any dialer app
Dialer App Package ID	
Dialer App Name	
Receive data from other apps ⓘ	All Apps
Open data into Org documents ⓘ	<input type="radio"/> Allow <input type="radio"/> Block
Allow users to open data from selected services ⓘ	3 selected
Restrict cut, copy, and paste between other apps ⓘ	Policy managed apps with paste in
Screen capture and Google Assistant ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Block
Approved keyboards ⓘ	<input type="radio"/> Require <input checked="" type="radio"/> Not required
Select keyboards to approve	<input type="button" value="Select"/>

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

**Answer Area**

A user can copy files from Microsoft OneDrive to [answer choice] only.

Microsoft SharePoint Online  
OneDrive  
local storage  
Microsoft SharePoint Online  
Microsoft SharePoint Online and OneDrive

A user can copy and paste text from [answer choice] to a Microsoft Word document stored in Microsoft OneDrive.

any app  
any app  
only managed apps  
only unmanaged apps

- A. Mastered
- B. Not Mastered

**Answer: A**



Explanation:

A user can copy files from Microsoft OneDrive to [answer choice] only.

A user can copy and paste text from [answer choice] to a Microsoft Word document stored in Microsoft OneDrive.

NEW QUESTION 338

HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table. From the Sign-ins blade of the Microsoft Entra admin center for which users can User1 and User2 view the sign-ins? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1 can view the sign-ins for the following users:

User2 can view the sign-ins for the following users:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1 can view the sign-ins for the following users:

User2 can view the sign-ins for the following users:

NEW QUESTION 340

- (Topic 6)

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 345

- (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps. You configure a session control policy to block downloads from SharePoint

Online sites. Users report that they can still download files from SharePoint Online sites. You need to ensure that file download is blocked while still allowing users to browse SharePoint Online sites. What should you configure?

- A. an access policy
- B. a data loss prevention (DLP) policy
- C. an activity policy
- D. a Conditional Access policy

**Answer:** A

#### NEW QUESTION 350

- (Topic 6)

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 355

- (Topic 6)

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 Policy1
- B. only the settings of Policy2
- C. only the settings of Policy3
- D. no settings

**Answer:** C

#### NEW QUESTION 359

- (Topic 6)

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-RegulatoryComplianceUI 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 361

- (Topic 6)

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 upgrade Server1 to Windows Server 2019.

Does this meet the goal?

A. yes

B. No

**Answer: A**

#### NEW QUESTION 365

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MS-102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MS-102 Product From:

<https://www.2passeasy.com/dumps/MS-102/>

## Money Back Guarantee

### MS-102 Practice Exam Features:

- \* MS-102 Questions and Answers Updated Frequently
- \* MS-102 Practice Questions Verified by Expert Senior Certified Staff
- \* MS-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* MS-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year