

MS-102 Dumps

Microsoft 365 Administrator Exam

<https://www.certleader.com/MS-102-dumps.html>



NEW QUESTION 1

- (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 2

- (Topic 6)

You have a Microsoft 365 tenant.

You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.

What should you use?

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

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices>

NEW QUESTION 3

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to configure a group naming policy.

Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Portal:	<div><div>The Microsoft 365 admin center</div><div>The Microsoft 365 admin center</div></div>
Group types:	<div><div>The Microsoft 365 Defender portal</div><div>The Microsoft Entra admin center</div><div>The Microsoft Purview compliance portal</div></div>
Group types:	<div><div>Security only</div><div>Microsoft 365 only</div><div>Security only</div><div>Security and mail-enabled security only</div><div>Microsoft 365 and distribution only</div><div>Microsoft 365, mail-enabled security, and distribution only</div><div>Security, Microsoft 365, mail-enabled security, and distribution</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Portal:

The Microsoft 365 admin center

The Microsoft 365 admin center

The Microsoft 365 Defender portal

The Microsoft Entra admin center

The Microsoft Purview compliance portal

Group types:

Security only

Microsoft 365 only

Security only

Security and mail-enabled security only

Microsoft 365 and distribution only

Microsoft 365, mail-enabled security, and distribution only

Security, Microsoft 365, mail-enabled security, and distribution

NEW QUESTION 4

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

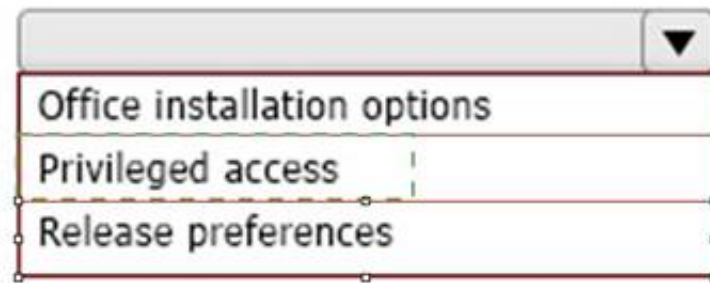
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

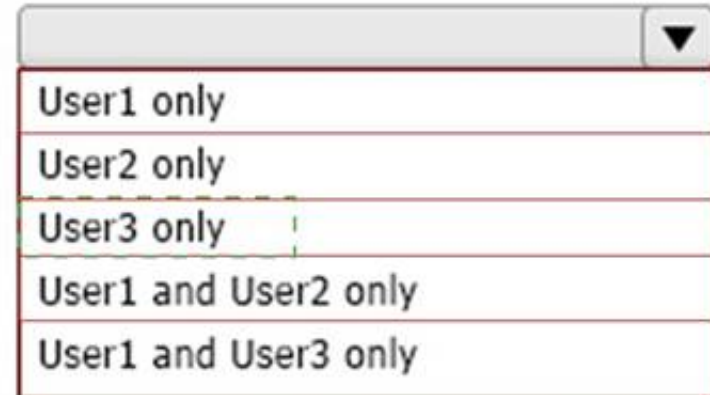
Answer Area

Microsoft 365 setting:



A screenshot of a dropdown menu for Microsoft 365 settings. The menu is open, showing three options: "Office installation options", "Privileged access", and "Release preferences". The "Privileged access" option is currently selected and highlighted.

User:



A screenshot of a dropdown menu for user selection. The menu is open, showing six options: "User1 only", "User2 only", "User3 only", "User1 and User2 only", and "User1 and User3 only". The "User3 only" option is currently selected and highlighted.

NEW QUESTION 5

- (Topic 6)

You have a Microsoft 365 tenant that contains 500 Windows 10 devices and a Microsoft Endpoint Manager device compliance policy. You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps. Which policy type should you configure?

- A. conditional access
- B. account protection
- C. attack surface reduction (ASR)
- D. Endpoint detection and response

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

NEW QUESTION 6

- (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 7

- (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 SharePoint Administrator role.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 8

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

- Retention period 7 years
- Start the retention period based on: When items were created

You need to prevent the removal of the label once the label is applied to an item. What should you select in the retention label settings?

- A. Retain items even if users delete
- B. Mark items as a record
- C. Mark items as a regulatory record
- D. Retain items forever

Answer: B

NEW QUESTION 9

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

A user named user1@contoso.com was recently provisioned.

You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```

Connect-AzureAD -Scopes User.ReadWrite.All, Organization.Read.All
Connect-MgGraph
Connect-MSOLService

$E3 = Get-MgSubscribedSku | Where SkuPartNumber -eq 'EnterprisePack'

$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
('MICROSOFTBOOKINGS') | select -ExcludeProperty ServicePlanID

$LicenseOptions= @(
    @{
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    }
)

Set-MgUserLicense -UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @{}

```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Connect-MgGraph

Assign Microsoft 365 licenses to user accounts with PowerShell Use the Microsoft Graph PowerShell SDK

First, connect to your Microsoft 365 tenant.

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the 'Assign license'

Microsoft Graph API reference page.

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All Box 2: Get-MgSubscribedSku

Run the Get-MgSubscribedSku command to view the available licensing plans and the

number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.

Box 3: Set-MgUserLicense Assigning licenses to user accounts

To assign a license to a user, use the following command in PowerShell.

Set-MgUserLicense -UserId \$userUPN -AddLicenses @{SkuId = "<SkuId>"} - RemoveLicenses @()

This example assigns a license from the SPE_E5 (Microsoft 365 E5) licensing plan to the unlicensed user belindan@litwareinc.com:

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
```

```
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId =
```

```
$e5Sku.SkuId} -RemoveLicenses @()
```

NEW QUESTION 10

- (Topic 6)

You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Security Operator
User3	Security Reader
User4	Compliance Administrator

You plan to implement Microsoft Defender for Endpoint.

You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.

You need to identify which user can view security incidents from the Microsoft 365 Defender portal.

Which user should you identify?

- A. User1
- B. User2
- C. User3
- D. User4

Answer: A

NEW QUESTION 10

- (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365 and contains a mailbox named Mailbox1.

You plan to use Mailbox1 to collect and analyze unfiltered email messages.

You need to ensure that Defender for Office 365 takes no action on any inbound emails delivered to Mailbox1.

What should you do?

- A. Configure a retention policy for Mailbox1.
- B. Create a mail flow rule.
- C. Configure Mailbox1 as a SecOps mailbox.
- D. Place a litigation hold on Mailbox1.

Answer: D

NEW QUESTION 12

HOTSPOT - (Topic 6)

HOTSPOT

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

? Contoso.com

? East.contoso.com

The forest contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	East.contoso.com
User3	Fabrikam.com

The forest 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	Disabled

USER SIGN-IN



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

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 authenticate to Azure AD by using a username of user1@contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	<input type="radio"/>	<input type="radio"/>
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes
The UPN of user1 is user1 @contoso.com so he can authenticate to Azure AD by using the username user1 @contoso.com.
Box 2: No
The UPN of user2 is user2 @east.contoso.com so he cannot authenticate to Azure AD by using the username user2 @contoso.com.
Box 3: No
The UPN of user3 is user3 @fabrikam.com so he cannot authenticate to Azure AD by using the username user3 @contoso.com.

NEW QUESTION 17

HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
On activation, require	Azure MFA
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	15 day(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

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

A user that is assigned the Global Administrator role as active [answer choice].

▼

will lose the role after eight hours

can reactivate the role every eight hours

can reactivate the role every 15 days

will lose the role after 15 days

You can make the Global Administrator role available to activation requests [answer choice].

▼

for up to eight hours

for up to three months

for up to 15 days

until the requests are revoked manually

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: will lose the role after eight hours

From exhibit: Activation, Activation maximum duration (hours): 8 hour(s)

Box 2: for up to three months

We see from exhibit: Assignment, Expire eligible assignment after: 3 month(s)

NEW QUESTION 18

- (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 User1 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
B. No

Answer: A

NEW QUESTION 21

HOTSPOT - (Topic 6)

HOTSPOT

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

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

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

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

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Add apps to the private store:

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

Install apps from the private store:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Add apps to the private store:

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

Install apps from the private store:

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

NEW QUESTION 26

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	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.
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.	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.	

NEW QUESTION 27

- (Topic 6)

You have a Microsoft 365 subscription.

You view the Service health Overview as shown in the following exhibit.

Service health

October 18, 2022 4:20 PM

Overview Issue history Reported issues

View the issues and health status of all services that are available with your current subscriptions. [Learn more about Service Health](#)






 Report an issue  Customize 

Active issues

Issue title	Affected service	Issue type
> Microsoft service health (6)		
Issues in your environment that require action (0)		

Microsoft service health

Shows the current health status of your Microsoft services, and updates when we fix issues.

Service	Status
Exchange Online	 3 advisories
Microsoft 365 suite	 2 advisories
Microsoft Teams	 1 advisory
OneDrive for Business	 1 advisory
SharePoint Online	 2 advisories

You need to ensure that a user named User1 can view the advisories to investigate service health issues. Which role should you assign to User1?

- A. Message Center Reader
- B. Reports Reader
- C. Service Support Administrator
- D. Compliance Administrator

Answer: B

Explanation:

Service Support admin

Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:

- Open and manage service requests
- View and share message center posts
- Monitor service health

Incorrect:

* Message center reader

Assign the Message center reader role to users who need to do the following:

- Monitor message center notifications
- Get weekly email digests of message center posts and updates
- Share message center posts
- Have read-only access to Azure AD services, such as users and groups

* Reports reader

Assign the Reports reader role to users who need to do the following:

- View usage data and the activity reports in the Microsoft 365 admin center
- Get access to the Power BI adoption content pack
- Get access to sign-in reports and activity in Azure AD
- View data returned by Microsoft Graph reporting API

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>

NEW QUESTION 31

- (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 33

- (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 37

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature. You need to block users from downloading a file named File1.exe.

What should you use?

- A. an indicator
- B. a suppression rule
- C. a device configuration profile

Answer: A

NEW QUESTION 41

- (Topic 6)

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

Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

The devices are managed by using Microsoft Intune.

You plan to use a configuration profile to assign the Delivery Optimization settings. Which devices will support the settings?

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

Answer: A

NEW QUESTION 43

HOTSPOT - (Topic 6)

HOTSPOT

You have a new Microsoft 365 E5 tenant. Enable Security defaults is set to Yes.

A user signs in to the tenant for the first time.

Which multi-factor authentication (MFA) method can the user use, and how many days does the user have to register for MFA? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

MFA method:

- Call to phone
- Email message
- Security questions
- Text message to phone
- Notification to Microsoft Authenticator app

Number of days:

- 7
- 14
- 30
- 60

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: Notification to Microsoft Authenticator app

Do users have 14 days to register for Azure AD Multi-Factor Authentication?

Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won't be able to sign in until MFA registration is completed.

Box 2: 14

Azure AD Identity Protection will prompt your users to register the next time they sign in interactively and they'll have 14 days to complete registration. During this 14-day period, they can bypass registration if MFA isn't required as a condition, but at the end of the period they'll be required to register before they can complete the sign-in process.

NEW QUESTION 48

HOTSPOT - (Topic 6)

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

Name	Member of
User1	Group1, Group2
User2	Group2, Group3
User3	Group1, Group3

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.

Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

The policies use the settings shown in the following table.

Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

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 has their cache cleared on close.	<input type="radio"/>	<input type="radio"/>
User2 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>
User3 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 has their cache cleared on close.	<input type="radio"/>	<input checked="" type="radio"/>
User2 has Cursor movement set to Visual.	<input type="radio"/>	<input checked="" type="radio"/>
User3 has Cursor movement set to Visual.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 50

- (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 54

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You onboard all devices to Microsoft Defender for Endpoint

You need to use Defender for Endpoint to block access to a malicious website at www.contoso.com.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

- A. Create a web content filtering policy.
- B. Configure an enforcement scope.
- C. Enable Custom network indicators.
- D. Create an indicator.
- E. Enable automated investigation.

Answer: AC

NEW QUESTION 56

- (Topic 6)

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the departments Microsoft SharePoint Online site. What should you do?

- A. From the SharePoint Online site, create an alert.
- B. From the SharePoint Online admin center, modify the sharing settings.
- C. From the Microsoft 365 Defender portal, create an alert policy.
- D. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.

Answer: D

NEW QUESTION 60

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 63

- (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 65

- (Topic 6)

You implement Microsoft Azure Advanced Threat Protection (Azure ATP). You have an Azure ATP sensor configured as shown in the following exhibit.



How long after the Azure ATP cloud service is updated will the sensor update?

- A. 20 hours
- B. 12 hours
- C. 7 hours
- D. 48 hours

Answer: B

NEW QUESTION 68

HOTSPOT - (Topic 6)

HOTSPOT

			progress	actions	summary			
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

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

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input checked="" type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input checked="" type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 70

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 tenant

You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM)

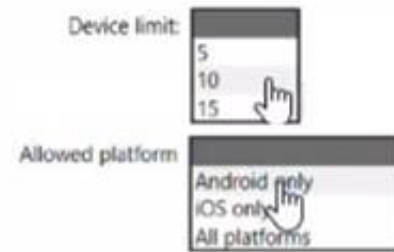
The device type restriction are configured as shown in the following table.

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

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

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

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restriction-priority>

NEW QUESTION 71

- (Topic 6)

You have a Microsoft 365 subscription.

You plan to implement Microsoft Purview Privileged Access Management. Which Microsoft Office 365 workloads support privileged access?

- A. Microsoft Exchange Online only
- B. Microsoft Teams only
- C. Microsoft Exchange Online and SharePoint Online only
- D. Microsoft Teams and SharePoint Online only
- E. Microsoft Teams, Exchange Online, and SharePoint Online

Answer: A

Explanation:

Privileged access management

Having standing access by some users to sensitive information or critical network configuration settings in Microsoft Exchange Online is a potential pathway for compromised accounts or internal threat activities. Microsoft Purview Privileged Access Management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. Instead of administrators having constant access, just-in-time access rules are implemented for tasks that need elevated permissions. Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.

Note: When will privileged access support Office 365 workloads beyond Exchange? Privileged access management will be available in other Office 365 workloads soon.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management-solution-overview>

<https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management>

NEW QUESTION 73

- (Topic 6)

You have a Microsoft 365 E5 subscription. You need to create a mail-enabled contact. Which portal should you use?

- A. the Microsoft 365 admin center
- B. the SharePoint admin center
- C. the Microsoft Entra admin center
- D. the Microsoft Purview compliance portal

Answer: A

NEW QUESTION 77

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1. Site1 contains the files shown in the following table.

Name	Number of IP addresses in the file
File1	2
File2	3

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	If there is a match, stop processing	Priority
Rule1	3 or more IP addresses	Tip1	No	0
Rule2	1 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

You apply DLP1 to Site1.
Which policy tip is displayed for each file? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

File1:

Tip2 only

Tip2 only

Tip3 only

Tip2 and Tip3

File2:

Tip1 and Tip2 only

Tip1 only

Tip3 only

Tip1 and Tip2 only

Tip1, Tip2, and Tip3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

File1:

Tip2 only

Tip2 only

Tip3 only

Tip2 and Tip3

File2:

Tip1 and Tip2 only

Tip1 only

Tip3 only

Tip1 and Tip2 only

Tip1, Tip2, and Tip3

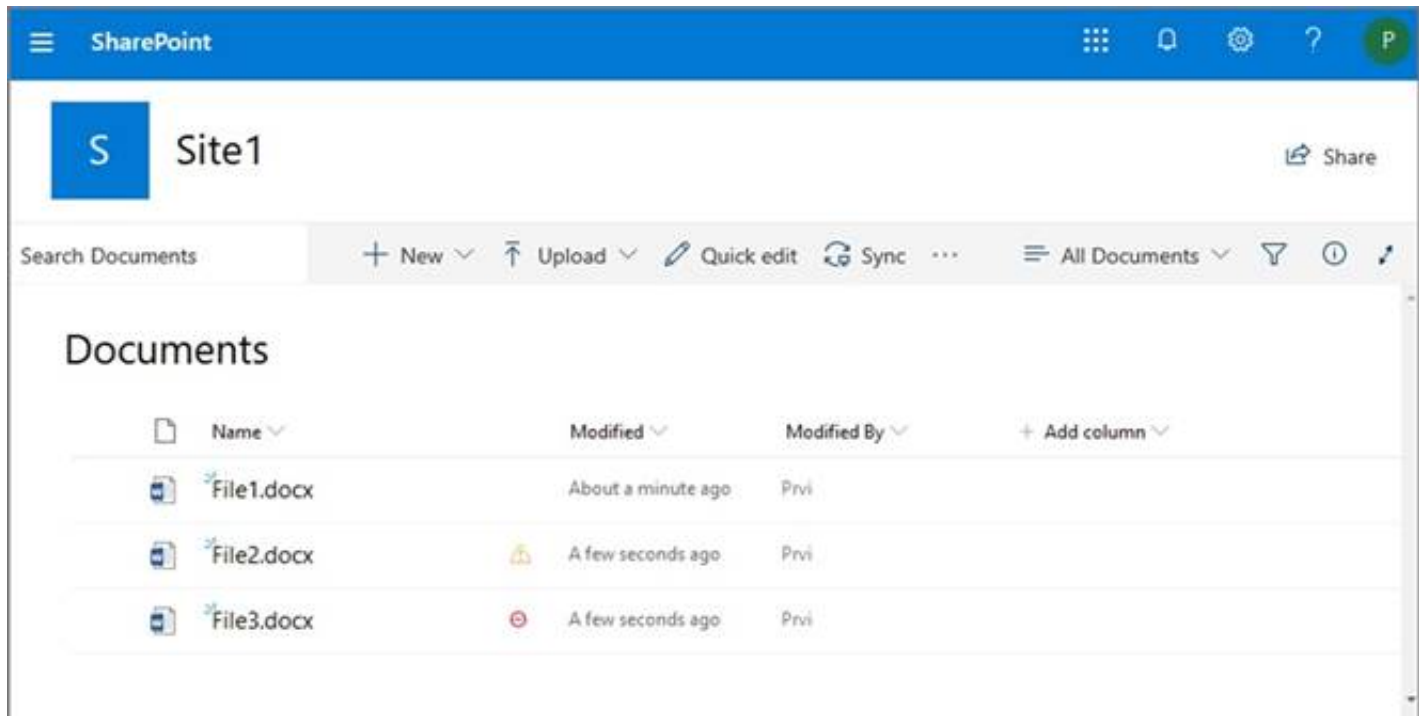
NEW QUESTION 78

HOTSPOT - (Topic 6)

From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)



Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

NEW QUESTION 82

DRAG DROP - (Topic 6)

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

Name	Operating system	Microsoft Intune
Device1	Windows 11 Enterprise	Enrolled
Device2	iOS	Enrolled
Device3	Android	Not enrolled

You install Microsoft Word on all the devices.

You plan to configure policies to meet the following requirements:

- Word files created by using Windows devices must be encrypted automatically.
- If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
- For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.

Which type of polio/ should you configure for each device? To answer, drag the appropriate policy types to the correct devices. Each policy type 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.

Policy Types		Answer Area
App configuration policy		Device1: <input type="text"/>
App protection policy	•	Device2: <input type="text"/>
Compliance policy	•	Device3: <input type="text"/>
Conditional Access policy	•	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policy Types		Answer Area
App configuration policy		Device1: App protection policy
App protection policy	•	Device2: Conditional Access policy
Compliance policy	•	Device3: Compliance policy
Conditional Access policy	•	

NEW QUESTION 85

- (Topic 6)

You have a Microsoft 365 tenant that contains two users named User1 and User2. You create the alert policy shown in the following exhibit.

Policy1

Edit policy

Delete policy

Status

On

Description

Add a description

Severity

Medium

Edit

Category

Information governance

Conditions

Activity is FileModified

Aggregation

Aggregated

Threshold

5 activities

Edit

Window

60 minutes

Scope

All users

Email recipients

User1@M365x082103.onmicrosoft.com

Daily notification limit

25

Edit

User2 runs a script that modifies a file in a Microsoft SharePoint Online library once every four minutes and runs for a period of two hours.
How many alerts will User1 receive?

- A. 2
- B. 5
- C. 10
- D. 25

Answer: D

NEW QUESTION 89

- (Topic 6)

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

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

Answer: AB

NEW QUESTION 94

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 97

- (Topic 6)

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.

You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory.

What should you configure in the profile?

- A. Microsoft Defender Credential Guard
- B. BitLocker Drive Encryption (BitLocker)
- C. Microsoft Defender
- D. Microsoft Defender Exploit Guard

Answer: A

NEW QUESTION 98

DRAG DROP - (Topic 6)

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

Type	Number of devices	Operating system	Enrollment status
Corporate	150	Windows 11	Azure AD-joined, Microsoft Intune- managed
Bring your own device (BYOD)	25	Windows 11	Unmanaged

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must minimize administrative effort.

What should you use to onboard each type of device? To answer, drag the appropriate onboarding methods to the correct device types. Each onboarding method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Onboarding method	Device Type
A local script	Corporate: <input type="text"/>
Group Policy	BYOD: <input type="text"/>
Integration with Microsoft Defender for Cloud	
Microsoft Intune	
Virtual Desktop Infrastructure (VDI) scripts	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Onboarding method	Device Type
A local script	Corporate: <input type="text" value="Microsoft Intune"/>
Group Policy	BYOD: <input type="text" value="Integration with Microsoft Defender for Cloud"/>
Integration with Microsoft Defender for Cloud	
Microsoft Intune	
Virtual Desktop Infrastructure (VDI) scripts	

NEW QUESTION 101

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

Site1 contains the files shown in the following table.

Name	Matched DLP rule
File1.docx	Rule1, Rule2, Rule3
File2.docx	Rule1, Rule3, Rule4

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

File1.docx:

- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Rule1 tip only

File1 matches Rule1, Rule2, and Rule3. Rule1 has the highest priority.

Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.

Box 2: Rule1 tip only

Note: User Override support

The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).

It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.

If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched.

NEW QUESTION 103

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices. You plan to attack surface reduction (ASR) rules for the Windows 10 devices.

You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.

You need to find the ASR rules that match the activities on the devices.

How should you complete the Kusto query? To answer, select the appropriate options in

the answer area.

NOTE: Each correct selection is worth one point.

	▼
AlertInfo	
DeviceEvents	
DeviceInfo	

		▼	ActionType startswith 'ASR'
	lookup		
	project		
	render		
	where		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

	▼
AlertInfo	
DeviceEvents	
DeviceInfo	

		▼	ActionType startswith 'ASR'
	lookup		
	project		
	render		
	where		

NEW QUESTION 106

- (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 109

HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to identify the settings that are below the Standard protection profile settings in the preset security policies.

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

Answer Area

Portal:	Microsoft 365 Defender portal	▼
	Microsoft 365 admin center	
	Microsoft 365 Defender portal	
	Microsoft Purview compliance portal	

Feature:	Configuration analyzer	▼
	Configuration analyzer	
	Preset security policies	
	Threat tracker	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

Portal: 

Feature: 

NEW QUESTION 110

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 111

- (Topic 6)

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

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

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

- A. User2only
B. User2and User3only
C. User2, User3, and User4 only
D. User2, User3, User4, and User5

Answer: B

NEW QUESTION 114

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 118

- (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 123

- (Topic 6)

: 241

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

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

Answer: B

Explanation:

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

NEW QUESTION 127

- (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 131

- (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 136

- (Topic 6)

You have a Microsoft 365 E5 tenant. You configure sensitivity labels.

Users report that the Sensitivity button is unavailable in Microsoft Word for the web. The sensitivity button is available in Word for Microsoft 365.

You need to ensure that the users can apply the sensitivity labels when they use Word for the web.

What should you do?

- A. Copy policies from Azure information Protection to the Microsoft 365 Compliance center
- B. Publish the sensitivity labels.
- C. Create an auto-labeling policy
- D. Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive.

Answer: B

NEW QUESTION 141

- (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 for Endpoint.

You need to configure Microsoft Defender for Endpoint on the computers. What should you create from the Endpoint Management admin center?

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

Answer: D

NEW QUESTION 142

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.

Which conditions can you use in the DLP rules of the policy?

- A. sensitive info types
- B. content search queries
- C. keywords
- D. sensitivity labels

Answer: C

Explanation:

Apply retention labels to content automatically if it matches specific conditions, that includes cloud attachments that are shared in email or Teams, or when the content contains:

Specific types of sensitive information.

Specific keywords that match a query you create.

Pattern matches for a trainable classifier.

Note: Retention policies can be applied to the following locations: Exchange mailboxes

SharePoint classic and communication sites OneDrive accounts

Microsoft 365 Group mailboxes & sites Skype for Business

Exchange public folders

Teams channel messages (standard channels and shared channels) Teams chats

Teams private channel messages Yammer community messages Yammer user messages

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention> <https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-exchange-conditions-and-actions>

NEW QUESTION 145

- (Topic 6)

You have a Microsoft 365 tenant.

Company policy requires that all Windows 10 devices meet the following minimum requirements:

? Require complex passwords.

? Require the encryption of data storage devices.

? Have Microsoft Defender Antivirus real-time protection enabled.

You need to prevent devices that do not meet the requirements from accessing resources in the tenant.

Which two components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a configuration policy

B. a compliance policy

C. a security baseline profile

D. a conditional access policy

E. a configuration profile

Answer: BD

Explanation:

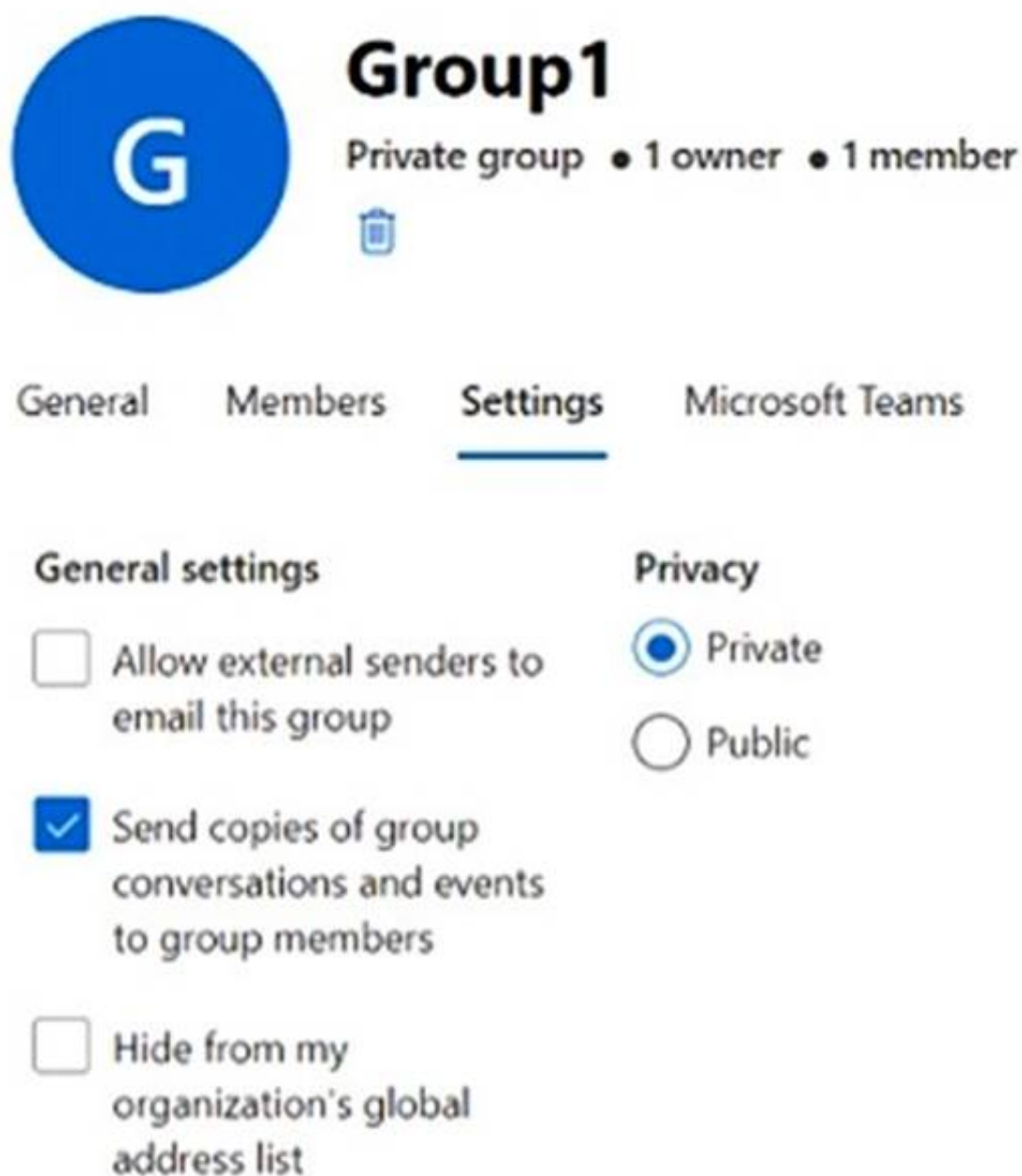
Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

NEW QUESTION 146

HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



An external user named User1 has an email address of user1@outlook.com. You need to add User1 to Group1.

What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Action:

Portal:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: Invite User1 to collaborate with your organization as a guest.

To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.

Navigate with your Web browser to <https://admin.microsoft.com>. On the left pane, click on “Users”, then click “Guest Users”.

On the “Guest Users” page, to create a new guest user, click on either the “Add a guest user” link on the top of the page or click on “Go to Azure Active Directory to add guest users” link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at <https://aad.portal.azure.com>.

On the “New user” page in the Microsoft Azure portal, you must choose to either “Create user” or “Invite user”. If you choose the “Create user” option, this will create a new user in your organization, which will have a login address with format username@tenantdomain.dot.com. If you choose the “Invite user” option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the “Invite user” option.

Box 2: The Microsoft Entra admin center

Microsoft Entra admin center unites Azure AD with family of identity and access products

Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.

Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).

NEW QUESTION 151

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You need to access service health alerts from a mobile phone.

What should you use?

- A. the Microsoft Authenticator app
B. the Microsoft 365 Admin mobile app
C. Intune Company Portal
D. the Intune app

Answer: B

NEW QUESTION 152

- (Topic 6)

You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de- fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.

D18912E1457D5D1DDCBD40AB3BF70D5D

What should you create to ensure that the DLP policy can detect the customer IDs?

- A. a sensitive information type
B. a sensitivity label
C. a supervision policy
D. a retention label

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide>

NEW QUESTION 154

- (Topic 6)

You have a Microsoft 365 E5 subscription.
Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.
You need to implement passwordless authentication. The solution must support all the devices.
Which authentication method should you use?

- A. Windows Hello
- B. FIDO2 compliant security keys
- C. Microsoft Authenticator app

Answer: C

NEW QUESTION 158

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

Priva Privacy Risk Managem...

Priva Subject Rights Requests

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 163

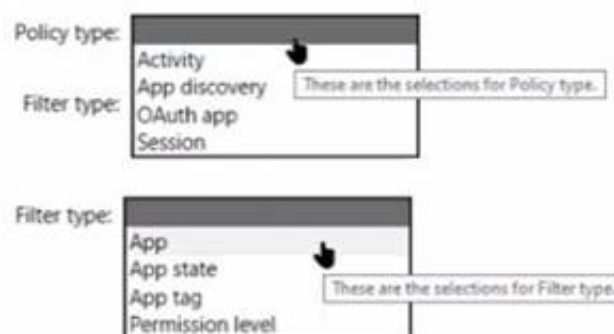
HOTSPOT - (Topic 6)

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

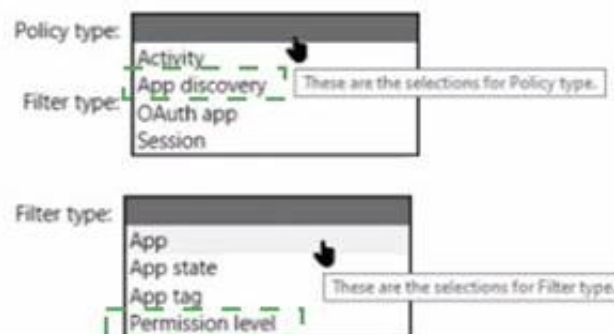


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 165

- (Topic 6)

You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.

Company policy requires that the devices have the following configurations:

- ? Require complex passwords.
- ? Require the encryption of removable data storage devices.
- ? Have Microsoft Defender Antivirus real-time protection enabled.

You need to configure the devices to meet the requirements.

What should you use?

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

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

NEW QUESTION 170

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 175

HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD). The tenant has two Compliance Manager assessments as shown in the following table.

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

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

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

You perform the following actions:

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

? Enable multi-factor authentication (MFA) for all users.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input checked="" type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input checked="" type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 180

- (Topic 6)

You have a Microsoft 365 subscription.

You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.

Which type of group should you use to assign the Reports Reader role and to access App1?

- A. a Microsoft 365 group that has assigned membership
- B. a Microsoft 365 group that has dynamic user membership
- C. a security group that has assigned membership
- D. a security group that has dynamic user membership

Answer: C

Explanation:

To grant permissions to assignees to manage users and group access for a specific enterprise app, go to that app in Azure AD and open in the Roles and Administrators list for

that app. Select the new custom role and complete the user or group assignment. The assignees can manage users and group access only for the specific app.

Note: You can add the following types of groups:

Assigned groups - Manually add users or devices into a static group.

Dynamic groups (Requires Azure AD Premium) - Automatically add users or devices to user groups or device groups based on an expression you create.

Note:

Security groups

Security groups are used for granting access to Microsoft 365 resources, such as SharePoint. They can make administration easier because you need only administer the group rather than adding users to each resource individually.

Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.

Security groups can be configured for dynamic membership in Azure Active Directory, allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device attributes such as operating system version.

Security groups can be added to a team.

Microsoft 365 Groups can't be members of security groups. Microsoft 365 Groups

Microsoft 365 Groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 Group, members get a group email and shared workspace for conversations, files, and calendar events, Stream, and a Planner.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps> <https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?> <https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy>

NEW QUESTION 184

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 187

HOTSPOT - (Topic 6)

You have device compliance policies shown in the following table.

Name	Platform	Assignment
Policy1	Windows 10 and later	Device1
Policy2	Windows 10 and later	Device1
Policy3	Windows 10 and later	Device2
Policy4	Windows 10 and later	Device2
Policy5	iOS/iPadOS	Device3
Policy6	iOS/iPadOS	Device3

The device compliance state for each policy is shown in the following table.

Policy	State
Policy1	Compliant
Policy2	In grace period
Policy3	Compliant
Policy4	Not compliant
Policy5	In grace period
Policy6	Compliant

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	<input type="radio"/>	<input type="radio"/>
Device2 has an overall compliance state of Not compliant.	<input type="radio"/>	<input type="radio"/>
Device3 has an overall compliance state of In grace period.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area





Statements	Yes	No
Device1 has an overall compliance state of Compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 has an overall compliance state of Not compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 has an overall compliance state of In grace period.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 188

- (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. onlycontoso.com and Sub2.contoso221018.onmicrosoft.com
C. onlvcontoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com
D. all the domains in the subscription

Answer: B

NEW QUESTION 190

HOTSPOT - (Topic 6)

You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.

In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

In Azure Active Directory (Azure AD), the Device settings are configured as shown in the following exhibit.

Users may register their devices with Azure AD ⓘ

All

None

Learn more on how this setting works

Require Multi-Factor Auth to join devices ⓘ

Yes

No

Maximum number of devices per user ⓘ

5

From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).
For each of the following statement, 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 enroll only five devices in Intune.	<input type="radio"/>	<input type="radio"/>
User1 can join only five devices to Azure AD.	<input type="radio"/>	<input type="radio"/>
User2 can enroll all the devices in Intune.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can join only five devices to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll all the devices in Intune.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 194

- (Topic 6)
You have a Microsoft 365 subscription.
You suspect that several Microsoft Office 365 applications or services were recently updated.
You need to identify which applications or services were recently updated.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. From the Microsoft 365 admin center review the Service health blade
- B. From the Microsoft 365 admin center, review the Message center blade.
- C. From the Microsoft 365 admin center review the Products blade.
- D. From the Microsoft 365 Admin mobile app, review the messages.

Answer: BD

Explanation:

The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where Microsoft posts official messages with information including new and changed features, planned maintenance, or other important announcements. The messages displayed in the Message center can also be viewed by using the Office 365 Admin mobile app. Reference:
https://docs.microsoft.com/en-us/office365/admin/manage/message-center https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app

NEW QUESTION 195

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	None	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	None	iOS	Not enrolled

You have the apps shown in the following table.

Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the users.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
App1 can be assigned as a required install for User3.	<input type="radio"/>	<input type="radio"/>
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
App3 can be installed automatically for UserGroup1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
App1 can be assigned as a required install for User3.	<input type="radio"/>	<input checked="" type="radio"/>
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
App3 can be installed automatically for UserGroup1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 197

- (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 Intune
- E. Create a configuration profile by using the Edition upgrade and mode switch template
- 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 site
- 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 membership

J. Assign licenses to the group and instruct users to sign in to their computer.

Answer: B

NEW QUESTION 199

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

Create retention label

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

Auto-labeling > Create auto-labeling policy

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

Box 2: Yes

Box 3: No

NEW QUESTION 204

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant.

You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)

Review your settings and finish

Name

Sensitivity1

Display name

Sensitivity1

Description for users

Sensitivity1

Scope

File.Email

Encryption

Content marking

Watermark: Watermark

Header: Header

Auto-labeling

Group settings

Site settings

Auto-labeling for database columns

None

You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)

Auto-labeling policy

 **Edit Policy**

 **Delete Policy**

Policy name

Auto-labeling policy

Description

Label in simulation

Sensitivity1

Info to label

IP Address

Apply to content in these locations

Exchange email All

Rules for auto-applying this label

Exchange email 1 rule

Mode

On

Comment

A user sends an email that contains the components shown in the following table.

Type	File	Includes IP address
Mail body	Not applicable	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

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
Sensitivity1 is applied to the email.	<input type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Sensitivity1 is applied to the email.	<input checked="" type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 207

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 E5 tenant.

Users at the company use the following versions of Microsoft Office:

- Microsoft 365 Apps for enterprise
- Office for the web
- Office 2016
- Office 2019

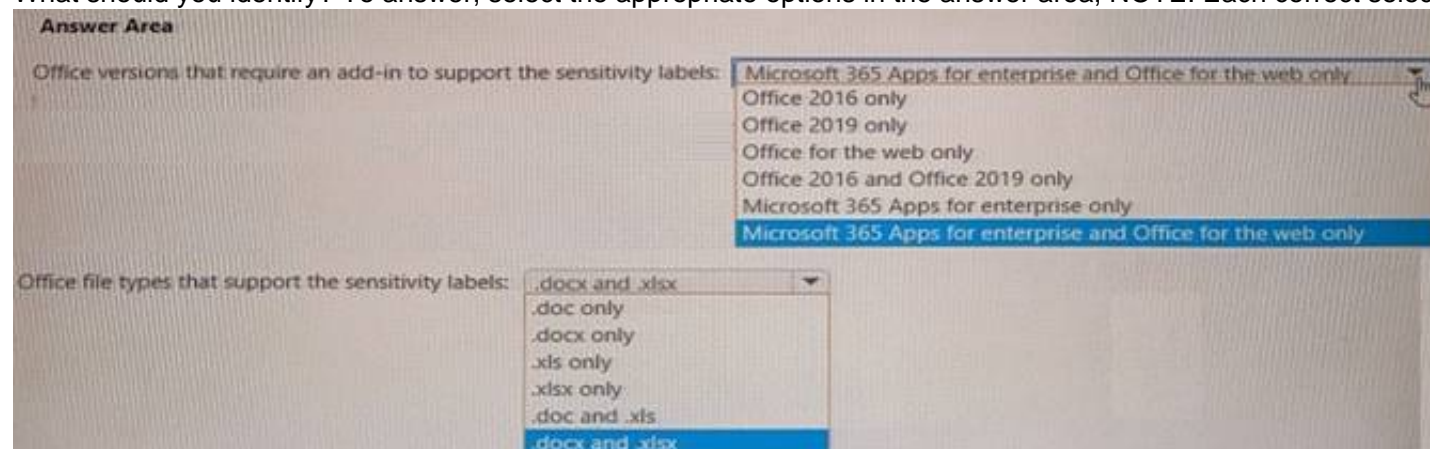
The company currently uses the following Office file types:

- .docx
- .xlsx
- .doc
- .xls

You plan to use sensitivity labels. You need to identify the following:

- Which versions of Office require an add-in to support the sensitivity labels.
- Which file types support the sensitivity labels.

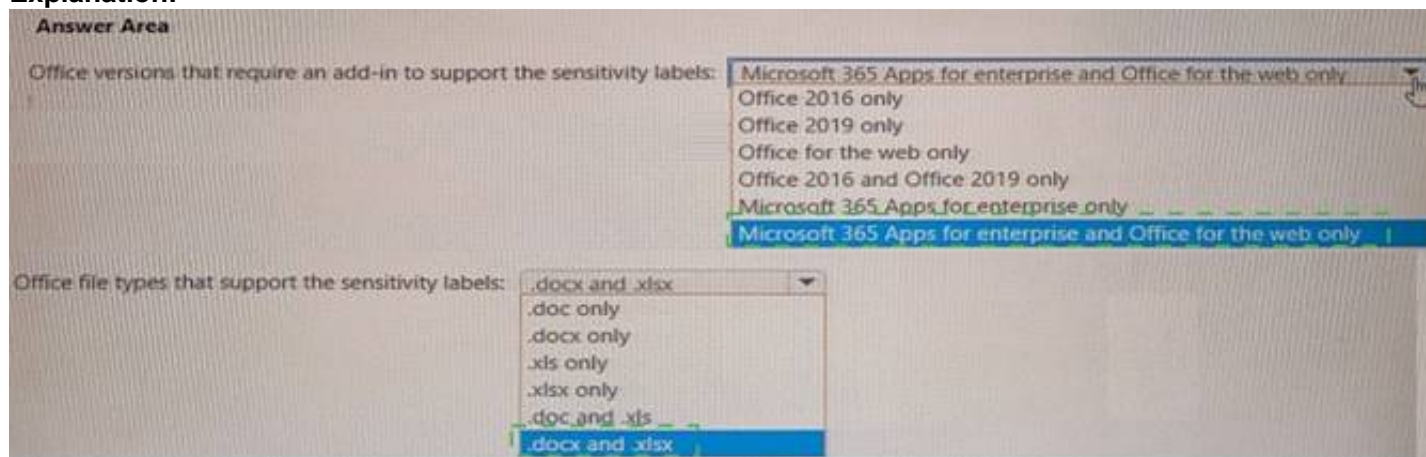
What should you identify? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.



- A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 209

- (Topic 6)

You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.

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

You plan to enable VPN access for the devices.

What is the minimum number of configuration policies required?

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

Answer: D

NEW QUESTION 213

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.	<input type="radio"/>	<input type="radio"/>
User2 can reset the password of User4.	<input type="radio"/>	<input type="radio"/>
User3 can assign licenses to User1.	<input type="radio"/>	<input type="radio"/>

- 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 216

HOTSPOT - (Topic 6)

HOTSPOT

Your company uses a legacy on-premises LDAP directory that contains 100 users. The company purchases a Microsoft 365 subscription.

You need to import the 100 users into Microsoft 365 by using the Microsoft 365 admin center.

Which type of file should you use and which properties are required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

File type to use:

CSV

JSON

PST

XML

Required properties for each user:

Display Name and Department

First Name and Last Name

User Name and Department

User Name and Display Name

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: CSV

Add multiple users in the Microsoft 365 admin center

? Sign in to Microsoft 365 with your work or school account.

? In the admin center, choose Users > Active users.

? Select Add multiple users.

? On the Import multiple users panel, you can optionally download a sample CSV file with or without sample data filled in.

? Etc.

Note: More information about how to add users to Microsoft 365 Not sure what CSV format is?

A CSV file is a file with comma separated values. You can create or edit a file like this with any text editor or spreadsheet program, such as Excel.

Box 2: User Name and Display Name

What if I don't have all the information required for each user? The user name and display name are required, and you cannot add a new user without this information. If you don't have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.

NEW QUESTION 217

HOTSPOT - (Topic 5)

You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.

Which users can review the incidents and advisories, and which blade should the users use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users:

Admin1 and Admin3 only	▼
Admin1 only	
Admin1 and Admin3 only	
Admin1, Admin2, and Admin3 only	
Admin1, Admin2, Admin3, and Admin4	

Blade:

Service Health	▼
Reports	
Service Health	
Message center	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Users:

Admin1 and Admin3 only	▼
Admin1 only	
Admin1 and Admin3 only	
Admin1, Admin2, and Admin3 only	
Admin1, Admin2, Admin3, and Admin4	

Blade:

Service Health	▼
Reports	
Service Health	
Message center	

NEW QUESTION 221

- (Topic 5)

You need to configure just in time access to meet the technical requirements. What should you use?

- A. entitlement management
- B. Azure AD Privileged Identity Management (PIM)
- C. access reviews
- D. Azure AD Identity Protection

Answer: B

NEW QUESTION 223

- (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 224

HOTSPOT - (Topic 3)

You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements.
To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Role group:

	▼
Reviewer	
Global reader	
Data Investigator	
Compliance Management	

Tool:

	▼
Exchange admin center	
SharePoint admin center	
Microsoft 365 admin center	
Microsoft 365 security center	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Role group:

	▼
Reviewer	
Global reader	
Data Investigator	
Compliance Management	

Tool:

	▼
Exchange admin center	
SharePoint admin center	
Microsoft 365 admin center	
Microsoft 365 security center	

NEW QUESTION 228

- (Topic 3)

You need to create the DLP policy to meet the technical requirements. What should you configure first?

- A. sensitive info types
- B. the Insider risk management settings
- C. the event types
- D. the sensitivity labels

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide>

NEW QUESTION 233

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 237

- (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 242

- (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 244

- (Topic 1)

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

- A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator role.
- B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
- C. From the Intune admin center, add User1 as a device enrollment manager.
- D. From the Intune admin center, configure the Enrollment restrictions.

Answer: C

Explanation:

References:

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

NEW QUESTION 248

- (Topic 6)

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

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

Answer: D

NEW QUESTION 249

- (Topic 6)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named site1. You need to ensure that site1 meets the following requirements:

- Retains all data for 10 years
- Prevents the sharing of data outside the organization

Which two items should you create and apply to site1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. a retention policy
- B. a sensitive info type
- C. a data loss prevention (DLP) policy
- D. a sensitivity label
- E. a retention label
- F. a retention label policy

Answer: CE

NEW QUESTION 253

- (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 257

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		Answer Area
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		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions		Answer Area
Create an app configuration policy		Create a Google account
Link the account to Intune		
Create a Microsoft account	➤	Link the account to Intune
Configure a mobile device management (MDM) push certificate	⬅	Add the app
Add the app		
Create a Google account		Assign the app
Assign the app		

NEW QUESTION 258

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant.

You configure a device compliance policy as shown in the following exhibit.

Compliance settings Edit	
Microsoft Defender ATP	
Require the device to be at or under the machine risk score:	Low
Device Health	
Rooted devices Require the device to be at or under the Device Threat Level	Block
System Security	
Require a password to unlock mobile devices	Require
Required password type	Device default
Encryption of data storage on device.	Require
Block apps from unknown sources	Block
Actions for noncompliance Edit	
Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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

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

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

Rooted devices will be

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

Rooted devices will be

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

NEW QUESTION 262

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 266

HOTSPOT - (Topic 6)

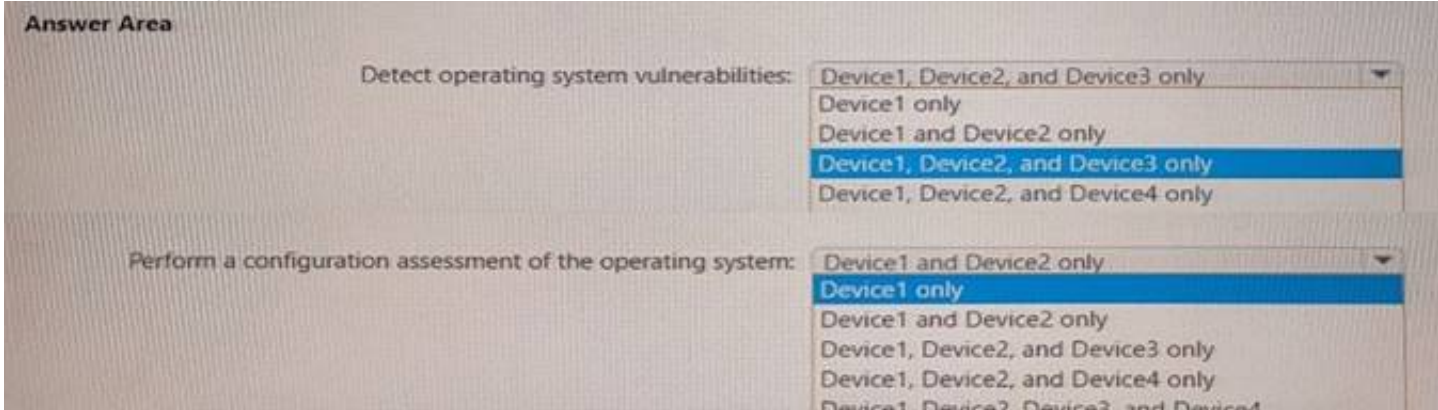
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

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:

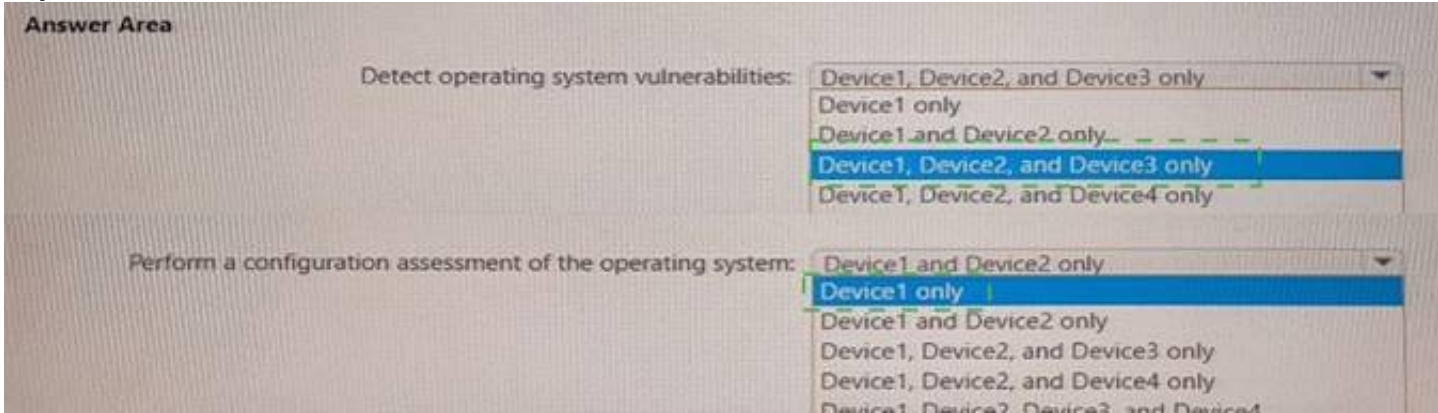
- Detect operating system vulnerabilities.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 268

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to create Conditional Access policies to meet the following requirements:

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.

Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must be blocked from signing in from outside the United States and Canada.

Only users in the R&D department must be blocked from signing in from both Android and iOS devices.

Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.

What is the minimum number of Conditional Access policies you should create?

- A. 3
- B. 4
- C. 5
- D. 6
- E. 7
- F. 8

Answer: B

Explanation:

* Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.

One Policy.

* Only users in the R&D department must be blocked from signing in from both Android and iOS devices.

One Policy.

* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.

One policy

* All users must be blocked from signing in from outside the United States and Canada. Only users in the R&D department must be blocked from signing in from both Android One Policy

Reference:

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

NEW QUESTION 269

- (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 273

- (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to ensure that users are prevented from opening or downloading malicious files from Microsoft Teams, OneDrive, or SharePoint Online.

What should you do?

- A. Create a new Anti-malware policy
- B. Configure the Safe Links global settings.
- C. Create a new Anti-phishing policy
- D. Configure the Safe Attachments global settings.

Answer: D

Explanation:

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams

In organizations with Microsoft Defender for Office 365, Safe Attachments for SharePoint,

OneDrive, and Microsoft Teams provides an additional layer of protection against malware. After files are asynchronously scanned by the common virus detection engine in Microsoft 365, Safe Attachments opens files in a virtual environment to see what happens (a process known as detonation). Safe Attachments for SharePoint, OneDrive, and Microsoft Teams also helps detect and block existing files that are identified as malicious in team sites and document libraries.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-about>

NEW QUESTION 278

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to be alerted when Microsoft 365 Defender detects high-severity incidents. What should you use?

- A. a custom detection rule
- B. a threat policy
- C. an alert policy
- D. a notification rule

Answer: C

NEW QUESTION 280

- (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 on-premises Active Directory domain, you set the UPN suffix for User2 to @contoso.com. You instruct User2 to sign in as user2@contoso.com. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

The on-premises Active Directory domain is named contoso.com. You can enable users to sign on using a different UPN (different domain), by adding the domain to Microsoft 365 as a custom domain. Alternatively, you can configure the user account to use the existing domain (contoso.com).

NEW QUESTION 282

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:

Configure Azure AD Connect Health settings:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 284

- (Topic 6)
You have a Microsoft 365 E5 tenant that uses Microsoft Intune.
You need to ensure that users can select a department when they enroll their device in Intune.
What should you create?

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

Answer: C

Explanation:
Reference:
<https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>

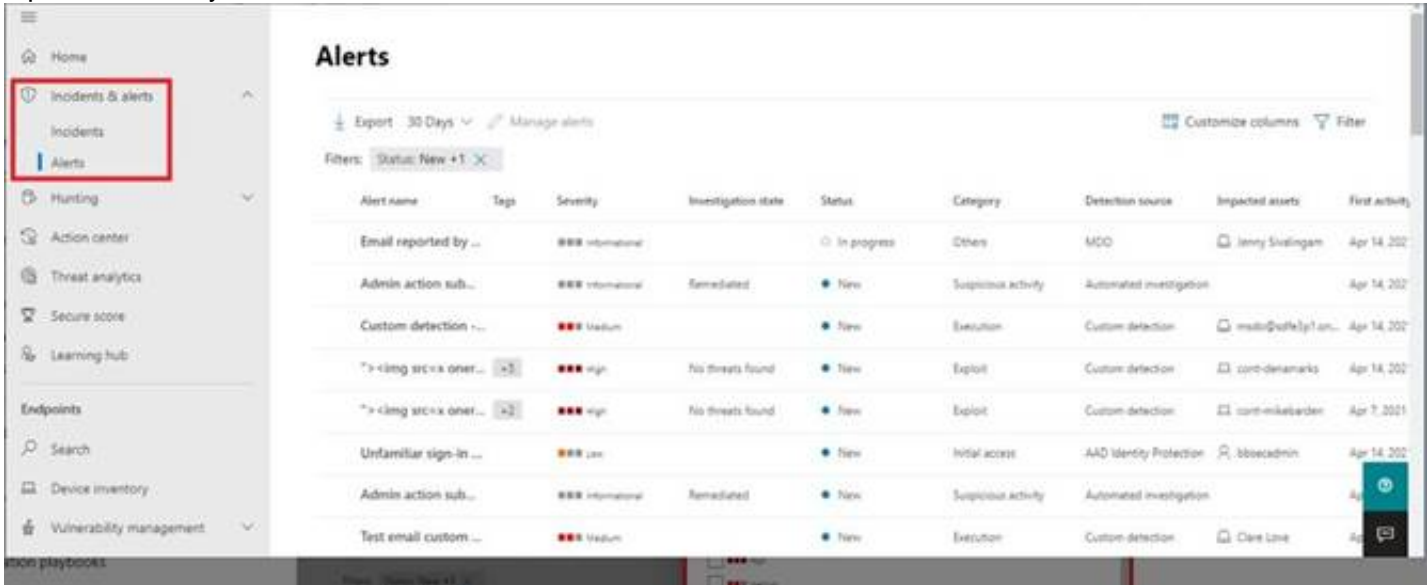
NEW QUESTION 285

- (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.



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

NEW QUESTION 290

HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:
? Name: Case1
? Included content: Group1, User1, Site1
? Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders
The investigation for Case1 completes, and you close the case.
What occurs after you close Case1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Holds are turned off for:

User1 only
All locations
Site1 and Group1 only

Holds are placed on a delay hold for:

30 days
90 days
120 days

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Holds are turned off for:

User1 only
All locations
Site1 and Group1 only

Holds are placed on a delay hold for:

30 days
90 days
120 days

NEW QUESTION 293

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:	<table border="1"><tr><td>Alert</td></tr><tr><td>Threat</td></tr><tr><td>Compliance</td></tr></table>	Alert	Threat	Compliance	
Alert					
Threat					
Compliance					
Role:	<table border="1"><tr><td>Quarantine</td></tr><tr><td>Security Administrator</td></tr><tr><td>Organization Configuration</td></tr><tr><td>Communication Compliance Admin</td></tr></table>	Quarantine	Security Administrator	Organization Configuration	Communication Compliance Admin
Quarantine					
Security Administrator					
Organization Configuration					
Communication Compliance Admin					

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 296

- (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 299

- (Topic 6)

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

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

You add custom apps to the private store in Microsoft Store Business.

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

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

Answer: C

NEW QUESTION 303

- (Topic 6)

Your company has a Microsoft 365 subscription.

You need to identify all the users in the subscription who are licensed for Office 365 through a group membership. The solution must include the name of the group used to assign the license.

What should you use?

- A. Active users in the Microsoft 365 admin center
- B. Reports in Microsoft Purview compliance portal
- C. the Licenses blade in the Microsoft Entra admin center
- D. Reports in the Microsoft 365 admin center

Answer: D

Explanation:

Microsoft 365 Reports in the admin center

You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.

Which activity reports are available in the admin center

Depending on your subscription, here are the available reports in all environments.

Report	Public	GCC	GCC-High	DoD	Office 365 operated by 21Vianet
Microsoft browser usage	Yes	No ¹	No ¹	No ¹	No ¹
Email activity	Yes	Yes	Yes	Yes	Yes
Email apps usage	Yes	Yes	Yes	Yes	Yes
Mailbox usage	Yes	Yes	Yes	Yes	Yes
Office activations	Yes	Yes	Yes	Yes	Yes

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports>

NEW QUESTION 305

- (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 310


HOTSPOT - (Topic 6)

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure Active Directory (Azure AD) role
User1	Purchaser	Billing administrator
User2	Admin	Global administrator
User3	Basic Purchaser	None
User4	Basic Purchaser, Device Guard signer	Global reader

All users have Windows 10 Enterprise devices.


The Products & services settings in Microsoft Store for Business are shown in the following exhibit.


Microsoft Remote Desktop
 Free • Online • [Product Details](#)
Install

Licenses
Unlimited licenses
 0 used

Billing
€0.00 (Free app)

Settings & Actions
 Not in private store
[More actions available on details page](#)


Excel Mobile
 Free • Online • [Product Details](#)
Install

Licenses
Unlimited licenses
 0 used

Billing
€0.00 (Free app)

Settings & Actions
 In private store
[More actions available on details page](#)

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
User2 can install the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	<input type="radio"/>	<input type="radio"/>
User4 can manage the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	<input checked="" type="radio"/>	<input type="radio"/>
User4 can manage the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 312

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your MS-102 Exam with Our Prep Materials Via below:

<https://www.certleader.com/MS-102-dumps.html>