



Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam

NEW QUESTION 1

DRAG DROP - (Topic 6)
DRAG DROP

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.
You need to ensure that each group can perform the tasks shown in the following table.

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

The solution must use the principle of least privilege.
Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Roles

Billing Administrator

Global Administrator

Helpdesk Administrator

License Administrator

Service Support Administrator

User Administrator

Answer Area

Group1:

Role

Group2:

Role

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Billing admin manage service request Purchase new services Etc.
Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.
Box 2: User admin User admin
Assign the User admin role to users who need to do the following for all users:

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

NEW QUESTION 2

- (Topic 6)
You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management. You need to add the phone number of the help desk to the Company Portal app. What should you do?

- A. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.
- B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.
- C. From the Microsoft 365 admin center, modify Organization information.
- D. From the Microsoft 365 admin center, modify Help desk information.

Answer: A

Explanation:

Reference:
<https://systemcenterdudes.com/intune-company-portal-customization/>

NEW QUESTION 3

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

Name	Type
Mailbox1	Microsoft Exchange Online mailbox
Account1	Microsoft OneDrive account
Site1	Microsoft SharePoint Online site
Channel	Microsoft Teams channel

To which resources can you apply a sensitivity label by using an auto-labeling policy?

- A. Mailbox1 and Site1 only
- B. Mailbox1, Account1, and Site1 only
- C. Account1 and Site1 only
- D. Mailbox1, Account1, Site1, and Channel1
- E. Account1, Site1, and Channel1 only

Answer: E

Explanation:

Reference:

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

NEW QUESTION 4

- (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 5

- (Topic 6)

You have a Microsoft 365 subscription.

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

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

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

Answer: A

Explanation:

Use Conditional Access policies

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

Reference:

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

NEW QUESTION 6

- (Topic 6)

You have a Microsoft 365 E5 subscription.

On Monday, you create a new user named User1.

On Tuesday, User1 signs in for the first time and perform the following actions:

- Signs in to Microsoft Exchange Online from an anonymous IP address
- Signs in to Microsoft SharePoint Online from a device in New York City.
- Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections

Which types of sign-in risks will Azure AD Identity Protection detect for User1?

- A. anonymous IP address only
- B. anonymous IP address and atypical travel
- C. anonymous IP address, atypical travel, and unfamiliar sign-in properties
- D. unfamiliar sign-in properties and atypical travel only

E. anonymous IP address and unfamiliar sign-in properties only

Answer: C

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

HOTSPOT - (Topic 6)

You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

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

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

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

You support the management tasks.

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

NOTE: Each correct selection is worth one point.

VPN device configuration profile:

▼

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2 and Device3

A. Mastered

B. Not Mastered

Answer: A

Explanation:

VPN device configuration profile:

▼

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2 and Device3

NEW QUESTION 9

- (Topic 6)

You purchase a new computer that has Windows 10, version 2004 preinstalled.

You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.

What should you do on the computer?

- A. Install all the feature updates released since version 2004 and all the quality updates released since version 2004 only.
- B. install the West feature update and the latest quality update only.
- C. install all the feature updates released since version 2004 and the latest quality update only.
- D. install the latest feature update and all the quality updates released since version 2004.

Answer: B

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. A Built-in protection preset security policy is applied to the subscription.

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

NOTE: Each correct selection is worth one point.

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

Answer: CE

NEW QUESTION 12

- (Topic 6)

You have a Microsoft 365 subscription.

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

What should you do?

- A. Enable Endpoint analytics.
- B. Run the Microsoft 365 network connectivity test on each device.
- C. Enable privileged access.
- D. Configure Support integration.

Answer: A

NEW QUESTION 13

- (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 15

- (Topic 6)
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

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

Answer: D

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

NEW QUESTION 16

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 19

HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.
The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.
You need to identify the following information:

- The number of email messages quarantined by zero-hour auto purge (ZAP)
 - The number of times users clicked a malicious link in an email message
- Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

• • • • •

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status ▼

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

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

Mailflow status report ▼

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

• • • • •

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status ▼

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

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

Mailflow status report ▼

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

NEW QUESTION 21

HOTSPOT - (Topic 6)

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

Name	Member of	Passwordless capable	Multi-factor authentication (MFA) method registered
User1	Group1	Capable	Microsoft Authenticator app (push notification)
User2	Group2	Capable	Microsoft Authenticator app (push notification)
User3	Group1, Group2	Capable	Mobile phone, Windows Hello for Business

Each user has a device with the Microsoft Authenticator app installed.
From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit tab.)

Microsoft Authenticator settings

Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. [Learn more](#)

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. [Learn more](#).

Enable and Target

Configure

Enable ☒

Include

Exclude

Target ☐ All users ☒ Select groups

[Add groups](#)

Name	Type	Registration	Authentication mode
Group1	Group	Optional ▼	Passwordless ▼

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 use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>
User3 can use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 22

- (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 25

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 28

- (Topic 6)

You have a Microsoft 365 E5 tenant.

industry regulations require that the tenant comply with the ISO 27001 standard. You need to evaluate the tenant based on the standard

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

Answer: B

NEW QUESTION 33

HOTSPOT - (Topic 6)

You have several devices enrolled in Microsoft Endpoint Manager

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown In the following table.

Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	None	None

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

Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All users

You add user as a device enrollment manager in Endpoint manager

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

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 37

- (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 41

- (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 Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to assign the Security Administrator role. Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide>

NEW QUESTION 43

HOTSPOT - (Topic 6)

You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.

You need to centrally monitor System log events from the computers.

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

NOTE: Each correct selection is worth one point.

In Azure:	<div><div></div><div><div>Add and configure the Diagnostics settings for the Azure Activity Log.</div><div>Add and configure an Azure Log Analytics workspace.</div><div>Add an Azure Storage account and Azure Cognitive Search</div><div>Add an Azure Storage account and a file share.</div></div></div>
On the computers:	<div><div></div><div><div>Create an event subscription.</div><div>Modify the membership of the Event Log Readers group.</div><div>Enroll in Microsoft Endpoint Manager.</div><div>Install the Microsoft Monitoring Agent.</div></div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

In Azure:	<div><div></div><div><div>Add and configure the Diagnostics settings for the Azure Activity Log.</div><div>Add and configure an Azure Log Analytics workspace.</div><div>Add an Azure Storage account and Azure Cognitive Search</div><div>Add an Azure Storage account and a file share.</div></div></div>
On the computers:	<div><div></div><div><div>Create an event subscription.</div><div>Modify the membership of the Event Log Readers group.</div><div>Enroll in Microsoft Endpoint Manager.</div><div>Install the Microsoft Monitoring Agent.</div></div></div>

NEW QUESTION 46

- (Topic 6)

Your on-premises network contains an Active Directory domain. You have a Microsoft 365 E5 subscription.

You plan to implement a hybrid configuration that has the following requirements:

- Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources

- Supports the use of Azure AD Identity Protection

You need to configure Azure AD Connect to support the planned implementation. Which two options should you select? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Password Hash Synchronization
- B. Password writeback
- C. Directory extension attribute sync
- D. Enable single sign-on
- E. Pass-through authentication

Answer: AB

NEW QUESTION 47

- (Topic 6)

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

Name	Role
User1	Exchange Administrator
User2	User Administrator
User3	Global Administrator
User4	None

You add another user named User5 to the User Administrator role. You need to identify which two management tasks User5 can perform.

Which two tasks should you identify? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Delete User2 and User4 only.
- B. Reset the password of User4 only
- C. Reset the password of any user in Azure AD.
- D. Delete User1, User2, and User4 only.
- E. Reset the password of User2 and User4 only.
- F. Delete any user in Azure AD.

Answer: AE

Explanation:

Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).

Only on users who are non-admins or in any of the following limited admin roles:

- Directory Readers
- Guest Inviter
- Helpdesk Administrator
- Message Center Reader
- Reports Reader
- User Administrator Reference:

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

NEW QUESTION 48

- (Topic 6)

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy. What should you configure?

- A. actions
- B. incident reports
- C. exceptions
- D. user overrides

Answer: D

Explanation:

A DLP policy can be configured to allow users to override a policy tip and report a false positive.

You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word.

If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.

Reference:

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

NEW QUESTION 53

- (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 55

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)

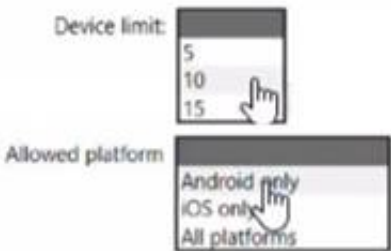
The device type restriction are configured as shown in the following table.

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 57

HOTSPOT - (Topic 6)

HOTSPOT

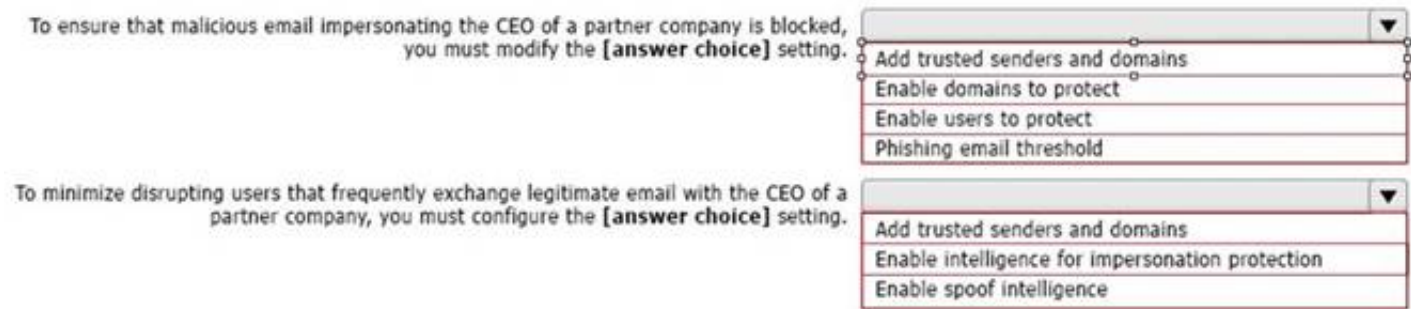
You have a Microsoft 365 subscription.

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

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

NOTE: Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Enable users to protect

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

User impersonation protection

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

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

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

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

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

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

NEW QUESTION 62

- (Topic 6)

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

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

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

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

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

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

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

What is the minimum number of deployment groups required?

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

Answer: C

Explanation:

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

Note: What are Deployment Groups?

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

Reference:

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

NEW QUESTION 65

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

You need to minimize the likelihood that users will be affected by the following threats:

? Opening files in Microsoft SharePoint that contain malicious content

? Impersonation and spoofing attacks in email messages

Which policies should you create in Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Opening files in SharePoint that contain malicious content:

▼

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

Impersonation and spoofing attacks in email messages:

▼

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Opening files in SharePoint that contain malicious content:

▼

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

Impersonation and spoofing attacks in email messages:

▼

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

NEW QUESTION 70

- (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 75

- (Topic 6)
You have a Microsoft 365 E5 tenant that contains four devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

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

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

Answer: B

Explanation:

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

NEW QUESTION 78

HOTSPOT - (Topic 6)
HOTSPOT

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

Custom smart logout

Lockout threshold ⓘ

15

✓

Lockout duration in seconds ⓘ

600

✓

Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

3hundred

Eleven

Falcon

Project

Tailspin

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

User1 attempts to update their password to the following passwords:

- ? F@lcon
- ? Project22
- ? T4il\$pin45dg4

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

Answer Area

[Answer choice] will be accepted as a password.

Only T4il\$pin45dg4

Only F@lcon and T4il\$pin45dg4

Only Project22 and T4il\$pin45dg4

F@lcon, Project22, and T4il\$pin45dg4

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

will be locked out

will trigger a user risk

can attempt to sign in again immediately

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

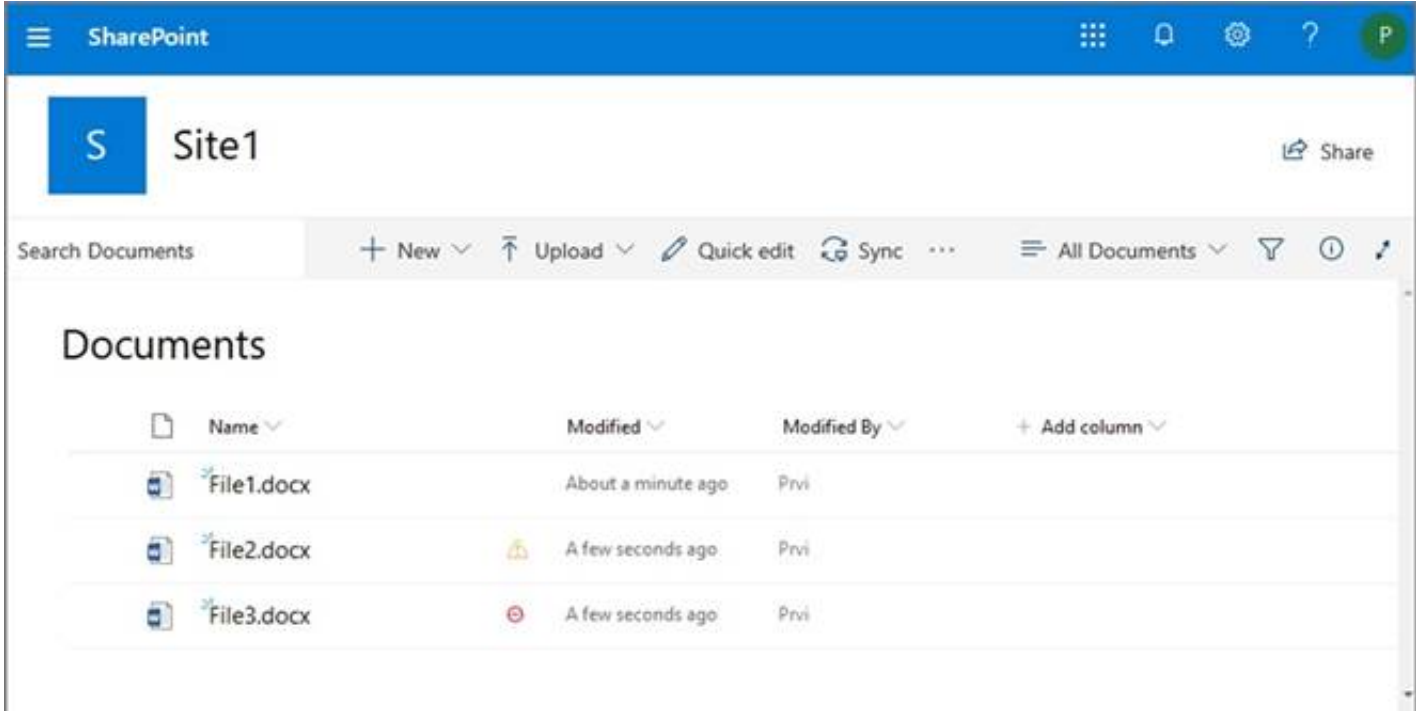
Box 1: Only T4il\$pin45dg4
Box 2: can attempt to sign in immediately Note: Manage Azure AD smart lockout values
Based on your organizational requirements, you can customize the Azure AD smart lockout values. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users. Customization of the smart lockout settings is not available for Azure China 21Vianet tenants.
To check or modify the smart lockout values for your organization, complete the following steps:
? Sign in to the Entra portal.
? Search for and select Azure Active Directory, then select Security > Authentication methods > Password protection.
? Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.
? The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.
? Set the Lockout duration in seconds, to the length in seconds of each lockout.
? The default is 60 seconds (one minute).
If the first sign-in after a lockout period has expired also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases.

NEW QUESTION 79

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

App configuration policy

App protection policy

Compliance policy

Conditional Access policy

Answer Area

Device1:

Device2:

Device3:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policy Types

App configuration policy

App protection policy

Compliance policy

Conditional Access policy

Answer Area

Device1:

App protection policy

Device2:

Conditional Access policy

Device3:

Compliance policy

NEW QUESTION 83

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.

Which two policies can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 86

HOTSPOT - (Topic 6)

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

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

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

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

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

- Name: Notification
- Notification settings
 - o Notify on alert severity: Low. Medium
 - o Device group scope: DevtceGroup1, DeviceGroup2
- Recipients: User1@contoso.com

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

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

For each of the following statements, select Yes if the statement is true. Otherwise, select No1.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	<input type="radio"/>	<input type="radio"/>
User2@contoso.com will receive an incident notification email for the alert at 08:07.	<input type="radio"/>	<input type="radio"/>
User1@contoso.com will receive an incident notification email for the alert at 08:20.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	<input type="radio"/>	<input checked="" type="radio"/>
User2@contoso.com will receive an incident notification email for the alert at 08:07.	<input checked="" type="radio"/>	<input type="radio"/>
User1@contoso.com will receive an incident notification email for the alert at 08:20.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 88

- (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 93

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

|

▼

lookup

project

render

where

ActionType startswith 'ASR'

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

▼

AlertInfo

DeviceEvents

DeviceInfo

|

▼

lookup

project

render

where

ActionType startswith 'ASR'

NEW QUESTION 98

HOTSPOT - (Topic 6)

Your company has 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"/> contoso221018.onmicrosoft.com (Default)	✓ Healthy	
<input type="checkbox"/> contoso.com	! Incomplete setup	
<input type="checkbox"/> east.contoso221018.onmicrosoft.com	! No services selected	

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

An administrator can create usernames that contain the [answer choice].

Exchange Online can receive inbound email messages sent to the [answer choice].

contoso221018.onmicrosoft.com domain only
contoso221018.onmicrosoft.com domain and all its subdomains only
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

contoso221018.onmicrosoft.com domain only
contoso221018.onmicrosoft.com domain and all its subdomains only
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

An administrator can create usernames that contain the [answer choice].

Exchange Online can receive inbound email messages sent to the [answer choice].

contoso221018.onmicrosoft.com domain only
contoso221018.onmicrosoft.com domain and all its subdomains only
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

contoso221018.onmicrosoft.com domain only
contoso221018.onmicrosoft.com domain and all its subdomains only
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

NEW QUESTION 100

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.

☐

☐

After you create the suppression rule, Alert3 is visible in the alerts queue.

☐

☐

After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.

☐

☐

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

Yes

No

After you create the suppression rule, Alert1 is visible in the alerts queue.

☒

☐

After you create the suppression rule, Alert3 is visible in the alerts queue.

☒

☐

After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.

☐

☒

NEW QUESTION 103

- (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 105

- (Topic 6)

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

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

You have a computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select Update & Security to view the update history. Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 108

HOTSPOT - (Topic 6)

Your network contains an Active Directory domain and an Azure AD tenant.

You implement directory synchronization for all 10,000 users in the organization. You automate the creation of 100 new user accounts.

You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.

Which command should you run? To answer, select the appropriate options in the answer area.

Answer Area

Start-ADSyncSyncCycle
Start-ADSyncSyncCycle
Set-ADSyncScheduler
Invoke-ADSyncRunProfile

-PolicyType

Delta
Delta
Initial
Full

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Start-ADSyncSyncCycle
Start-ADSyncSyncCycle
Set-ADSyncScheduler
Invoke-ADSyncRunProfile

-PolicyType

Delta
Delta
Initial
Full

NEW QUESTION 113

HOTSPOT - (Topic 6)

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.

What information must be configured for each user before the user can perform a self-service password reset? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:

Phone number and email address
Email address only
Phone number only
Security questions only
Phone number and email address

User2:

Phone number and email address
Email address only
Phone number only
Security questions only
Phone number and email address

User3:

Security questions only
Email address only
Phone number only
Security questions only
Phone number and email address

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1:

Phone number and email address
Email address only
Phone number only
Security questions only
Phone number and email address

User2:

Phone number and email address
Email address only
Phone number only
Security questions only
Phone number and email address

User3:

Security questions only
Email address only
Phone number only
Security questions only
Phone number and email address

NEW QUESTION 116

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.

Guaranteed success with Our exam guides

visit - https://www.certshared.com

NOTE: Each correct selection is worth one point.

Answer Area

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

recoverable for up to seven years
deleted seven years after they were created
retained for only seven years from when they were created

Once the policy is created, [answer choice].

some data may be deleted immediately
data will be retained for a minimum of seven years
users will be prevented from permanently deleting email messages for seven years

- 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 121

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

YesNo

Device1 has an overall compliance state of Compliant.

Device2 has an overall compliance state of Not compliant.

Device3 has an overall compliance state of In grace period.

- 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 125

DRAG DROP - (Topic 6)

You have a Microsoft 365 subscription.

You need to review reports to identify the following:

- The storage usage of files stored in Microsoft Teams
- The number of active users per team

Which report should you review for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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

Report

The device usage report in Teams

The OneDrive usage report

The SharePoint site usage report

The Teams usage report in Teams

The User activity report in Teams

Requirements

The storage usage of files stored in Microsoft Teams:

Number of active users per Microsoft Team:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Report

The device usage report in Teams

The OneDrive usage report

The SharePoint site usage report

The Teams usage report in Teams

The User activity report in Teams

Requirements

The storage usage of files stored in Microsoft Teams: The SharePoint site usage report

Number of active users per Microsoft Team: The Teams usage report in Teams

NEW QUESTION 126

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint. You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.

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

NOTE: Each correct selection is worth one point.

Devices that can onboard to Microsoft Defender for Endpoint:

Device 1 only
Device 1 and Device 2 only
Device 1 and Device 3 only
Device 1 and Device 4 only
Device 1, Device 2, and Device 4 only
Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

A conditional access policy only
A device compliance policy only
A device configuration profile only
A device configuration profile and a conditional access policy only
Device configuration profile, device compliance policy, and conditional access policy

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, table Description automatically generated with medium confidence

NEW QUESTION 131

- (Topic 6)

Your on-premises network contains an Active Directory domain named Contoso.com and 500 devices that run either macOS, Windows 8.1, Windows 10, or Windows 11. All the devices are managed by using Microsoft Endpoint Configuration Manager. The domain syncs with Azure Active Directory (Azure AD). You plan to implement a Microsoft 365 E5 subscription and enable co-management. Which devices can be co-managed after the implementation?

- A. Windows 11 and Windows 10 only
- B. Windows 11, Windows 10, Windows 8.1, and macOS
- C. Windows 11 and macOS only
- D. Windows 11 only
- E. Windows 11, Windows 10, and Windows 8.1 only

Answer: C

NEW QUESTION 135

HOTSPOT - (Topic 6)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Users who can assign Retention1:

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

Users who can assign Retention2:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Users who can assign Retention1:

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

Users who can assign Retention2:

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

NEW QUESTION 140

- (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?

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

Answer: A

NEW QUESTION 145

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

✓ Name

✓ Retention settings

● Finish

Review and finish

Name

Name

6Months

Edit

Retention settings

Retention period

6 months

Edit

Retention action

Retain and Delete

Edit

Based on

Based on when it was created

Edit

Back

Create label

Cancel

?

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

Auto-labeling > Create auto-labeling policy

✓ Name

● Info to label

● Create content query

○ Scope

○ Label

○ Finish

Apply label to content matching this query

Conditions

ProjectX

+ Add condition

Back

Next

Cancel

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

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

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

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 146

- (Topic 4)
Which role should you assign to User1?
Available Choices (select all choices that are correct)

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

Answer: C

Explanation:

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory- assign-admin-roles

NEW QUESTION 148

- (Topic 4)

You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.
 Which authentication strategy should you implement for the pilot projects?

- A. pass-through authentication
- B. pass-through authentication and seamless SSO
- C. password hash synchronization and seamless SSO
- D. password hash synchronization

Answer: C

Explanation:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

Fabrikam does NOT plan to implement identity federation.

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

NEW QUESTION 149

HOTSPOT - (Topic 3)

You need to configure the information governance settings to meet the technical requirements.

Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

- Label
- Retention**
- Auto-labeling

Number of required policies:

- 1
- 2**
- 3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy type:

- Label
- Retention**
- Auto-labeling

Number of required policies:

- 1
- 2**
- 3

NEW QUESTION 151

- (Topic 3)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 155

HOTSPOT - (Topic 3)

You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.

What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Configure:

	▼
Device configuration profiles Enrollment restrictions	
The mobile device management (MDM) user scope	
The mobile application management (MAM) user scope	

Group:

	▼
UserGroup1	
UserGroup2	
DeviceGroup1	
DeviceGroup2	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Configure:

	▼
Device configuration profiles Enrollment restrictions	
The mobile device management (MDM) user scope	
The mobile application management (MAM) user scope	

Group:

	▼
UserGroup1	
UserGroup2	
DeviceGroup1	
DeviceGroup2	

NEW QUESTION 160

- (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 164

- (Topic 1)

On which server should you use the Defender for identity sensor?

- A. Server1
- B. Server2
- C. Server3
- D. Server4
- E. Servers5

Answer: A

Explanation:

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

NEW QUESTION 165

- (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 167

- (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 identity sensors.

Solutions: You instruct User4 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 172

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You create a Conditional Access policy that blocks access to an app named App1 when users trigger a high-risk sign-in event.

You need to reduce false positives for impossible travel when the users sign in from the corporate network.

What should you configure?

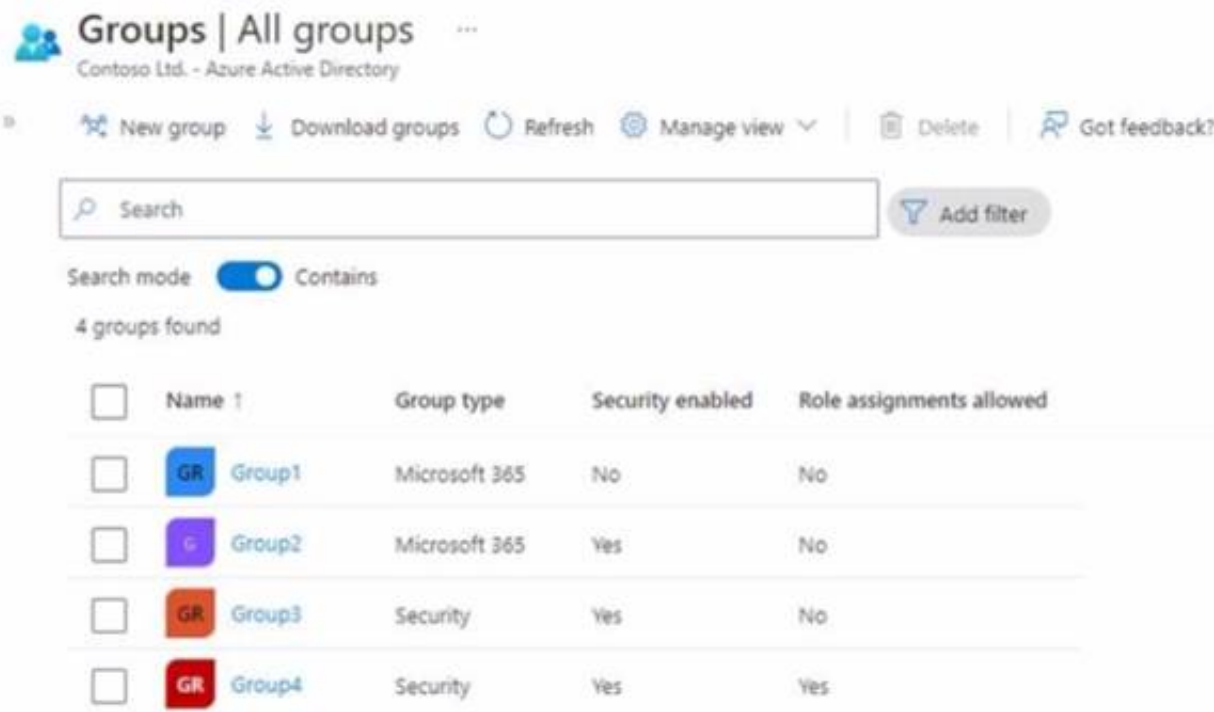
- A. exclusion groups
- B. multi-factor authentication (MFA)
- C. named locations
- D. user risk policies

Answer: C

NEW QUESTION 176

- (Topic 6)

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



	Name	Group type	Security enabled	Role assignments allowed
<input type="checkbox"/>	GR Group1	Microsoft 365	No	No
<input type="checkbox"/>	G Group2	Microsoft 365	Yes	No
<input type="checkbox"/>	GR Group3	Security	Yes	No
<input type="checkbox"/>	GR Group4	Security	Yes	Yes

To which groups can you assign Microsoft 365 E5 licenses?

- A. Group1 and Group2 only
- B. Group2 and Group3 only
- C. Group3 and Group4 only
- D. Group 1, Group2. and Group3 only
- E. Group2, Group3, and Group4 only

Answer: C

NEW QUESTION 179

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.

You need to export the existing template.

Which file format should you use for the exported template?

- A. CSV
- B. XLSX
- C. JSON
- D. XML

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldwide#export-a-template>

NEW QUESTION 180

- (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 184

- (Topic 6)

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

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

You have a computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select System, and then you select About to view information about the system.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

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

NEW QUESTION 188

- (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 193

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You need to evaluate compliance with European Union privacy regulations for customer data.

What should you do in the Microsoft 365 compliance center?

- A. Create a Data Subject Request (DSR)
- B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data

- C. Create an assessment based on the EU GDPR assessment template
- D. Create an assessment based on the Data Protection Baseline assessment template

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan>

NEW QUESTION 197

- (Topic 6)

You have a Microsoft 365 E5 subscription.

Your company's Microsoft Secure Score recommends the actions shown in the following exhibit.

Microsoft Secure Score

Overview Recommended actions History Metrics & trends

Export

	Rank	Recommended action	Score impact	Points achieved	Status
<input type="checkbox"/>	1	Require multifactor authentication for administrative roles	+4.15%	0/10	To address
<input type="checkbox"/>	2	Ensure all users can complete multifactor authentication	+3.73%	0/9	To address
<input type="checkbox"/>	3	Create Safe Links policies for email messages	+3.73%	0/9	To address
<input type="checkbox"/>	4	Enable policy to block legacy authentication	+3.32%	0/8	To address
<input type="checkbox"/>	5	Turn on Safe Attachments in block mode	+3.32%	0/8	To address
<input type="checkbox"/>	6	Ensure that intelligence for impersonation protection is enabled	+3.32%	0/8	To address
<input type="checkbox"/>	7	Move messages that are detected as impersonated users by mailbox intelligence	+3.32%	0/8	To address
<input type="checkbox"/>	8	Enable impersonated domain protection	+3.32%	0/8	To address

You select Create Safe Links policies for email messages and change Status to Risk accepted in the Status & action plan settings. How does the change affect the Secure Score?

- A. remains the same
- B. increases by 1 point
- C. increases by 9 points
- D. decreases by 1 point
- E. decreases by 9 points

Answer: A

NEW QUESTION 201

- (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 206

- (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:

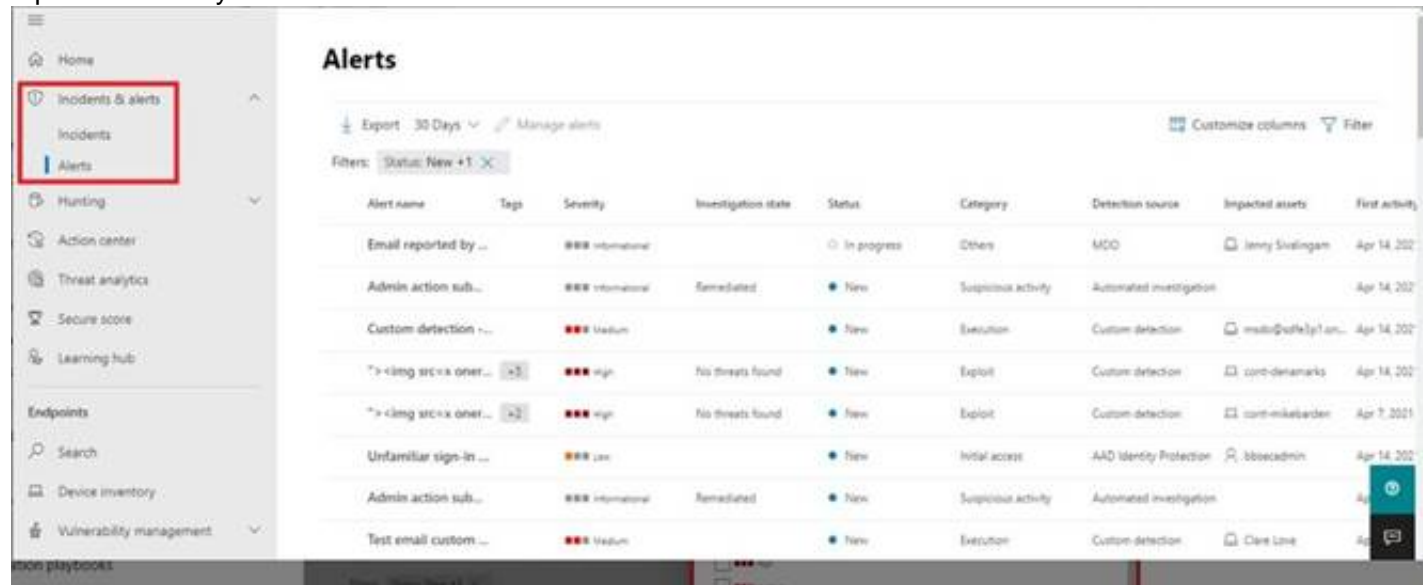
Data retention information for Microsoft Defender for Office 365

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.



Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity
Email reported by ...		High	Investigating	In progress	Others	MDO	Jenny Sivalingam	Apr 14, 2021
Admin action sub...		High	Remediated	New	Suspicious activity	Automated investigation		Apr 14, 2021
Custom detection ...		Medium		New	Execution	Custom detection	msal@outlook.com...	Apr 14, 2021
"> 3	High	No threats found	New	Exploit	Custom detection	cont-denmarks	Apr 14, 2021
"> 2	High	No threats found	New	Exploit	Custom detection	cont-mikebarden	Apr 7, 2021
Unfamiliar sign-in ...		Low		New	Initial access	AAD Identity Protection	bboecadmin	Apr 14, 2021
Admin action sub...		High	Remediated	New	Suspicious activity	Automated investigation		Apr 14, 2021
Test email custom ...		Medium		New	Execution	Custom detection	Clare Love	Apr 14, 2021

Reference:

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

NEW QUESTION 209

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 211

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that uses Microsoft Intune. You need to configure Intune to meet the following requirements:

? Prevent users from enrolling personal devices.

? Ensure that users can enroll a maximum of 10 devices.

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

NOTE: Each correct selection is worth one point.

Prevent users from enrolling
personal devices:

Conditional access policies
Device categories
Device limit restrictions
Device type restrictions

Ensure that users can enroll a
maximum of 10 devices:

Conditional access policies
Device categories
Device limit restrictions
Device type restrictions

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Prevent users from enrolling
personal devices:

Conditional access policies
Device categories
Device limit restrictions
Device type restrictions

Ensure that users can enroll a
maximum of 10 devices:

Conditional access policies
Device categories
Device limit restrictions
Device type restrictions

NEW QUESTION 215

- (Topic 6)

Your network contains an Active Directory forest named contoso.local. You purchase a Microsoft 365 subscription.

You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months.

You need to prepare for the planned move to Microsoft 365.

What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

- A. Purchase a third-party X.509 certificate.
- B. Create an external forest trust.
- C. Rename the Active Directory forest.
- D. Purchase a custom domain name.

Answer: D

Explanation:

The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on- premise Active Directory if it's a routable domain name, for example, contoso.com.

If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active Directory.

Incorrect:

Not C: No need to rename the Active Directory forest. As we use a non-routable domain name contoso.local, we just need to add the routable domain name as a UPN suffix in Active Directory.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization>

NEW QUESTION 220

- (Topic 6)

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles.

Which platform can you manage by using the profile?

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

Answer: B

Explanation:

Intune device configuration profiles can be applied to Windows 10 devices and macOS devices

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

? Windows 10

? macOS

Other incorrect answer options you may see on the exam include the following:

? Android Enterprise

? Windows 8.1

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure>

NEW QUESTION 223

HOTSPOT - (Topic 6)

You use Microsoft Defender for Endpoint.

You have the Microsoft Defender for Endpoint device groups shown in the following table

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

You plan to onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Answer Area

Computer1-London:	<input type="checkbox"/> Group1 <input type="checkbox"/> Group2 <input type="checkbox"/> Group3 <input type="checkbox"/> Ungrouped machines
Server1-London:	<input checked="" type="checkbox"/> Group1 <input type="checkbox"/> Group2 <input type="checkbox"/> Group3 <input type="checkbox"/> Ungrouped machines

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Computer1-London:	<input checked="" type="checkbox"/> Group1 <input checked="" type="checkbox"/> Group2 <input checked="" type="checkbox"/> Group3 <input type="checkbox"/> Ungrouped machines
Server1-London:	<input checked="" type="checkbox"/> Group1 <input checked="" type="checkbox"/> Group2 <input checked="" type="checkbox"/> Group3 <input type="checkbox"/> Ungrouped machines

NEW QUESTION 225

HOTSPOT - (Topic 6)

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

From the Sign-ins blade of the Microsoft Entra admin center for which users can User1 and User2 view the sign-ins? To answer, select the appropriate options in

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

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

User1, User2, User3, and User4

User1 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, User3, and User4

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

User1 and User2 only

User2 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

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

User1, User2, User3, and User4

User1 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, User3, and User4

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

User1 and User2 only

User2 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, User3, and User4

NEW QUESTION 227

- (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 228

- (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 232

HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription.

You need to create two groups named Group1 and Group2. The solution must meet the following requirements:

- Group1 must be mail-enabled and have an associated Microsoft SharePoint Online site.
- Group2 must support dynamic membership and role assignments but must NOT be mail-enabled.

Which types of groups should you create? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Group1:

Microsoft 365

Distribution

Dynamic distribution

Microsoft 365

Security

Group2:

Security

Distribution

Dynamic distribution

Microsoft 365

Security

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Group1:

Microsoft 365

Distribution

Dynamic distribution

Microsoft 365

Security

Group2:

Security

Distribution

Dynamic distribution

Microsoft 365

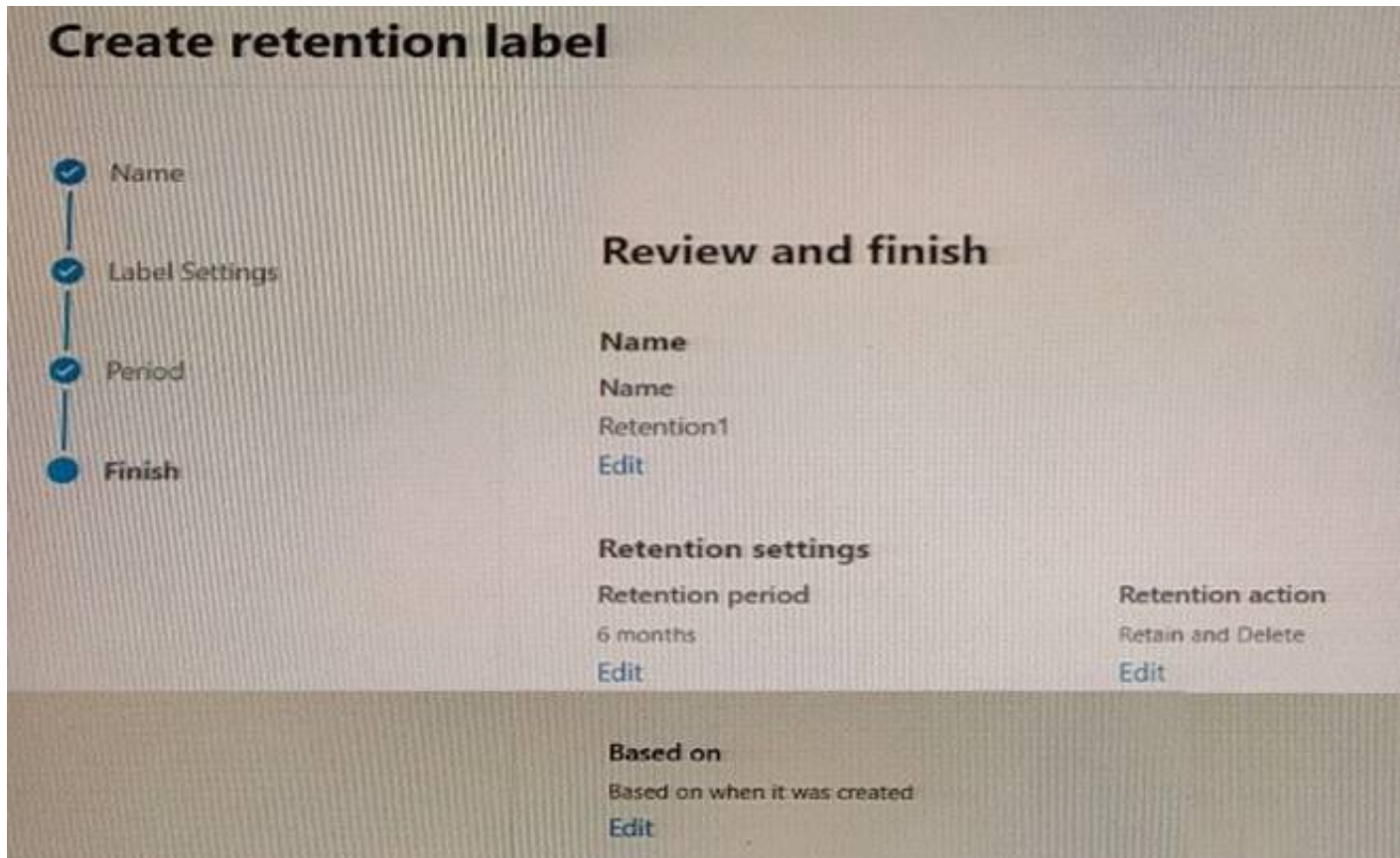
Security

NEW QUESTION 237

- (Topic 6)

You have a Microsoft 365 subscription.

You create a retention label named Retention1 as shown in the following exhibit.



You apply Retention1 to all the Microsoft OneDrive content.
 On January 1, 2020, a user stores a file named File1 in OneDrive.
 On January 10, 2020, the user modifies File1. On February 1, 2020, the user deletes File1.
 When will File1 be removed permanently and unrecoverable from OneDrive?

- A. February 1, 2020
- B. July 1, 2020
- C. July 10, 2020
- D. August 1, 2020

Answer: B

NEW QUESTION 239

- (Topic 6)
 You have a Microsoft 365 E5 subscription that contains the labels shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

You have the items shown in the following table.

Name	Stored in	Description
File1	Microsoft SharePoint	File document that has Label1 applied
File2	Microsoft Teams channel	File document that has Label2 applied
Mail1	Microsoft Exchange Online	Email message that has Label1 applied
Mail2	Microsoft Exchange Online	Email message that has Label2 applied

Which items can you view in Content explorer?

- A. File1 only
- B. File1 and File2 only
- C. File1 and Mail1 only
- D. File2 and Mail2 only
- E. File1, File2, Mail1, and Mail2

Answer: C

NEW QUESTION 242

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

MS-102 Practice Exam Features:

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

100% Actual & Verified — Instant Download, Please Click
[Order The MS-102 Practice Test Here](#)