MS-102 Dumps

Microsoft 365 Administrator Exam

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

NEW QUESTION 1
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription.
You need to review metrics for the following: The daily active users in Microsoft Teams Recent Microsoft service issues
What should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Teams daily active users:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

Recent Microsoft service issues:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Usage reports
The daily active users in Microsoft Teams
Microsoft 365 Reports in the admin center - Microsoft Teams usage activity
The brand-new Teams usage report gives you an overview of the usage activity in Teams, including the number of active users, channels and messages so you can quickly see how many users across your organization are using Teams to communicate and collaborate. It also includes other Teams specific activities, such as the number of active guests, meetings, and messages.
Box 2: Service Health
Recent Microsoft service issues
You can view the health of your Microsoft services, including Office on the web, Yammer, Microsoft Dynamics CRM, and mobile device management cloud services, on the Service health page in the Microsoft 365 admin center. If you are experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

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
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant
You create a data toss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.
To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.
NOTE: Each correct selection is worth one point.

Choose locations to apply the policy

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

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

Status	Location	Included	Excluded
⬤ Off	📧 Exchange email ✓		
⬤ Off	🌐 SharePoint sites		
⬤ Off	☁ OneDrive accounts ✓		
⬤ Off	📱 Teams chat and channel messages		
⬤ Off	⊞ Devices		
⬤ Off	☁ Microsoft Cloud App Security		
⬤ Off	🗄 On-premises repositories		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Choose locations to apply the policy

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

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

Status	Location	Included	Excluded
⬤ Off	📧 Exchange email ✓		
⬤ Off	🌐 SharePoint sites		
⬤ Off	☁ OneDrive accounts ✓		
⬤ Off	📱 Teams chat and channel messages		
⬤ Off	⊞ Devices		
⬤ Off	☁ Microsoft Cloud App Security		
⬤ Off	🗄 On-premises repositories		

NEW QUESTION 4
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.
You need to remove User1 from the Restricted entities list. What should you use?

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

E. the Microsoft Entra admin center

Answer: D

Explanation:
Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.
Remove a user from the Restricted entities page in the Microsoft 365 Defender portal In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use https://security.microsoft.com/restrictedentities.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam

NEW QUESTION 5
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

NEW QUESTION 6
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Configuration
Group1	Global security group
User1	Enabled user account
User2	Disabled user account

You configure Azure AD Connect to sync contoso.com to Azure AD.
Which objects will sync to Azure AD?

A. Group1 only
B. User1 and User2 only
C. Group1 and User1 only
D. Group1, User1, and User2

Answer: D

Explanation:
 Disabled accounts
Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.
The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts

NEW QUESTION 7
HOTSPOT - (Topic 6)
You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (default)	Device2	Group2

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

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	[○]
User2 can collect an investigation package from Device2.	○	[○]
User3 can isolate Device1.	[○]	○

NEW QUESTION 8
- (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 9
- (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 10
- (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 10
- (Topic 6)
Your network contains an Active Directory forest named Contoso. Local. You have a Microsoft 365 subscription.
You plan to implement a directory synchronization solution that will use password hash synchronization.
From the Microsoft 365 admin center, you successfully verify the contoso.com domain name.
You need to prepare the environment for the planned directory synchronization solution. What should you do first?

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

Answer: A

NEW QUESTION 15
DRAG DROP - (Topic 6)
Your company has a Microsoft 365 E5 tenant.
Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.
You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.
What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component 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.

Solutions	Answer Area	
An app configuration policy	Company-owned devices:	Solution
An app protection policy	Personal devices:	Solution
A compliance policy		
A configuration profile		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Solutions	Answer Area	
An app configuration policy	Company-owned devices:	A compliance policy
An app protection policy	Personal devices:	An app protection policy
A compliance policy		
A configuration profile		

NEW QUESTION 19
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.
You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for
10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.
You plan to onboard all the devices to Microsoft Defender for Endpoint. You need to store the Microsoft Defender for Endpoint data in Europe. What should you do first?

A. Delete the workspace.
B. Create a workspace.
C. Onboard a new device.
D. Offboard the test devices.

Answer: B

Explanation:
 Storage locations
Understand where Defender for Cloud stores data and how you can work with your data:
* Machine information
- Stored in a Log Analytics workspace.
- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data- workspace

NEW QUESTION 21
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that has auditing turned on. The subscription contains the users shown in the following table.

Name	License
Admin1	Microsoft Office 365 E5
Admin2	None

New audit retention policy   ✕

Name *:

Policy1

Description

Record Types

AzureActiveDirectory ▾

Activities

Added user ▾

Users:

Show results for all users

Duration *:
○ 90 Days
● 6 Months
○ 1 Year

Priority *:

100

You plan to create a new user named User1.
How long will the user creation audit event be available if Admin1 or Admin2 creates User1? To answer, select the appropriate options in the answer area.
Each correct selection is worth one point.

Answer Area

Admin1: 6 months ▾
         30 days
         90 days
         6 months
         1 year

Admin2: 90 days ▾
         30 days
         90 days
         6 months
         1 year

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Admin1: 6 months ▼
30 days
90 days
6 months   1
1 year

Admin2: 90 days ▼
30 days
90 days   ┘
6 months
1 year

NEW QUESTION 22
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You plan to perform device discovery and authenticated scans of network devices. You install and register the network scanner on a device named Device1.
What should you do next?

A. Connect Defender for Endpoint to Microsoft Intune.
B. Apply for Microsoft Threat Experts - Targeted Attack Notifications.
C. Create an assessment job.
D. Download and run an onboarding package.

Answer: C

NEW QUESTION 23
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

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

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

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Create a certificate from the Apple Push Certificates Portal.

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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

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

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

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Create a certificate from the Apple Push Certificates Portal.

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

Answer Area

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

Create a certificate from the Apple Push Certificates Portal.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

NEW QUESTION 24
- (Topic 6)

You have a Microsoft 365 subscription.
You view the Service health Overview as shown in the following exhibit.

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 25
HOTSPOT - (Topic 6)
HOTSPOT

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

☰

⌂ Home

Ⓡ Users ⌄

⚐ Teams & groups ⌄

⚑ Roles ⌄

⊞ Resources ⌄

▭ Billing ⌄

☏ Support ⌄

⚙ Settings ⌄

⚲ Setup

⚲ Reports ⌄

♡ Health ⌄
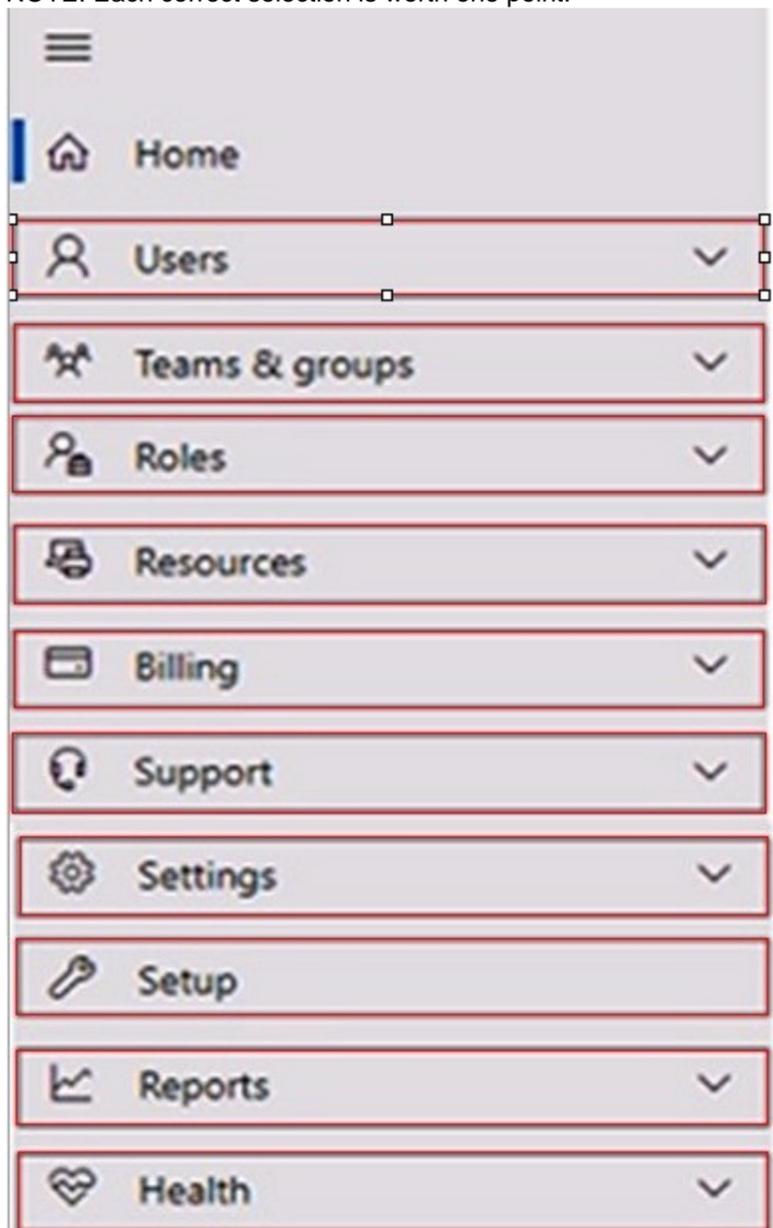
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Reports
View the Adoption Score of the company.
How to enable Adoption Score To enable Adoption Score:
? Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score
? Select enable Adoption Score. It can take up to 24 hours for insights to become
available.
Box 2: Support
Create a new service request to Microsoft.
Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request. If you're in the admin center, select Support > New service request.

NEW QUESTION 27
- (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 31
- (Topic 6)
Your network contains three Active Directory forests. There are forests trust relationships between the forests.
You create an Azure AD tenant.
You plan to sync the on-premises Active Directory to Azure AD.
You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a
single server fails.

What should you include in the recommendation?

A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode
B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode
C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode
D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

Answer: A

Explanation:
Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

NEW QUESTION 33
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft intune. The subscription contains the resources shown in the following table.

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.
You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table.
On Thursday, you review the results of the app deployments.

Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

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
Word is installed on Device1.	○	○ ▪
App3 is displayed in the Company Portal.	○	○
Excel is installed on Device1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Statements	Yes	No
Word is installed on Device1.	☐○	○ ▪
App3 is displayed in the Company Portal.	☐○	○
Excel is installed on Device1.	☐○	○

NEW QUESTION 38
- (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 39
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	None

You create an administrative unit named AU1 that contains the members shown in the following exhibit.

AU1

Members   Role assignments

Add users and groups, or select and remove them. The administrators assigned to this unit will
manage these users and groups. Adding groups doesn't add users to the unit, it lets the assigned
admins manage group settings.

R. Add users   ⅔ Add groups   ↑ Upload users   · · ·   ▽ Filter   🔍 Search this list   ≡

	Members	Email address	Last sign-in	Member type
☐	User1	User1@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:25 PM	User
☐	User3	User3@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:27 PM	User

General   **Assigned**   Permissions

You can assign this role to users and groups, and select users and groups to remove
or manage them.

Learn more about assigning admin roles

R. Add users   ⅔ Add groups

	Admin name	Last sign-in	Scope ⓘ
☐	**Group1**	Unavailable for groups	Organization
☐	**Group2**	Unavailable for groups	AU1

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 reset the password of User3.	○	○
User2 can reset the password of User3.	○	○
User2 can reset the password of User1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	○	⦿
User2 can reset the password of User3.	○	⦿
User2 can reset the password of User1.	○	⦿

NEW QUESTION 44
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You have the devices shown in the following table.

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

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

Actions		Answer Area	
Disable BitLocker.		Device1:	Action
Disable TPM.		Device2:	Action
Switch to UEFI.		Device3:	Action
Upgrade to Windows 10 Enterprise.			

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions		Answer Area	
Disable BitLocker.		Device1:	Disable BitLocker.
Disable TPM.		Device2:	Switch to UEFI.
Switch to UEFI.		Device3:	Upgrade to Windows 10 Enterprise.
Upgrade to Windows 10 Enterprise.			

NEW QUESTION 46
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.	○	○
User2 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User3 can enroll an unlimited number of devices in Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	☑	○
User2 can enroll a maximum of 10 devices in Endpoint Manager.	○	☑
User3 can enroll an unlimited number of devices in Endpoint Manager.	☑	○

NEW QUESTION 49
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

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

USER SIGN-IN

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

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

NEW QUESTION 53
- (Topic 6)
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.
Where can you store data from the LinkedIn connector?

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

Answer: C

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

NEW QUESTION 57
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 security center. Which Microsoft service source will appear on the Incidents page of the Microsoft 365
security center?

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

Answer: A

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

NEW QUESTION 59
HOTSPOT - (Topic 6)
HOTSPOT

			progress	actions	actions			
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.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

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.	○	▣
The SP800 assessment score will increase by 54 points.	○	▣
The Data Protection Baseline score will increase by 9 points.	○	▣

NEW QUESTION 60
HOTSPOT - (Topic 6)

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

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

You plan to create a compliance policy named Compliance1.
You need to identify the groups that meet the following requirements:
? Can be added to Compliance1 as recipients of noncompliance notifications
? Can be assigned to Compliance1
To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Can be added to Compliance1 as recipients of noncompliance notifications:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Can be added to Compliance1 as recipients of noncompliance notifications:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

NEW QUESTION 62
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it as a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the filtering settings.
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 65
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

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

You perform the following actions:
? Provision the private store in Microsoft Store for Business.
? Add an app named App1 to the private store.
? Set Private store availability for App1 to Specific groups, and then select Group3.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can install App1 from the private store.	○	○
User2 can install App1 from the private store.	○	○
User3 can install App1 from the private store.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can install App1 from the private store.	○	**○**
User2 can install App1 from the private store.	○	**○**
User3 can install App1 from the private store.	**○**	○

NEW QUESTION 69
DRAG DROP - (Topic 6)
You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.
All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.
You plan to implement self-service password reset (SSPR).
You need to ensure that when a user resets or changes a password, the password syncs with AD DS.
Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

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

A. Mastered
B. Not Mastered

Answer:

A

Explanation:

NEW QUESTION 71

HOTSPOT - (Topic 6)
From the Microsoft Purview compliance portal, you create a retention policy named Policy 1.
You need to prevent all users from disabling the policy or reducing the retention period. How should you configure the Azure PowerShell command? 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 73

- (Topic 6)
You have a Microsoft 365 E5 subscription.
You create an account tor 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 Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.
Does this meet the goal?

A. Yes
B. no

Answer: B

NEW QUESTION 74

- (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 Azure Active Directory admin center, you assign SecAdmin1 the
Security administrator role.

Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 79
HOTSPOT - (Topic 6)
HOTSPOT
Your network contains an on-premises Active Directory domain. You have a Microsoft 365 E5 subscription.
You plan to implement directory synchronization.
You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.
What should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Tool:

| AccessChk |
| Azure AD Connect |
| Active Directory Explorer |
| IdFix |

Required group membership:

| Domain Admins |
| Domain Users |
| Server Operators |
| Enterprise Admins |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: IdFix
Query and fix invalid object attributes with the IdFix tool
Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft 365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization tools such as Azure AD Connect and Azure AD Connect cloud sync. The focus of IdFix is to enable you to accomplish this task in a simple, expedient fashion.
The IdFix tool provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Window's Server AD forests in preparation for deployment to Microsoft 365. The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow you to successfully synchronize users, contacts, and groups from on-premises Active Directory into Microsoft 365. Note: IdFix might identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be synchronized to the cloud, the product group recommends that these errors be corrected.
Incorrect:
* AccessChk
Box 2: Enterprise Admins
IdFix permissions requirements
The user account that you use to run IdFix must have read and write access to the AD DS domain.
If you aren't sure if your user account meets these requirements, and you're not sure how to check, you can still download and run IdFix. If your user account doesn't have the right permissions, IdFix will simply display an error when you try to run it.
* Enterprise Admins
The Enterprise Admins group exists only in the root domain of an Active Directory forest of domains. The group is a Universal group if the domain is in native mode. The group is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, like adding child domains.
Incorrect:
* Domain Admins
Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that's created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.
* Server Operator
Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer. Any service that accesses the system has the Service identity.
* Domain Users - too few permissions
The Domain Users group includes all user accounts in a domain. When you create a user account in a domain, it's automatically added to this group.

NEW QUESTION 81
- (Topic 6)
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 84
- (Topic 6)
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant includes a user named User1.
You enable Azure AD Identity Protection.
You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.
To which role should you add User1?

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

Answer: A

NEW QUESTION 89
- (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 92
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. Site! 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
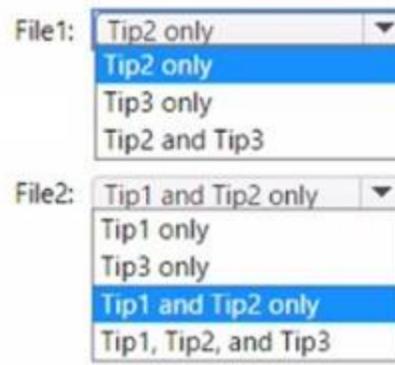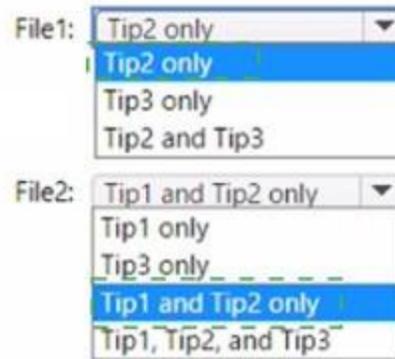
NEW QUESTION 94
HOTSPOT - (Topic 6)
From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

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

☰ SharePoint	⋮⋮⋮	◻	⚙	?	P

S	Site1		⤢ Share

Search Documents   + New ∨   ⬆ Upload ∨   ✎ Quick edit   ⟳ Sync   ⋯   ☰ All Documents ∨   ▽   ⓘ   ⤢

Documents

	Name ∨		Modified ∨	Modified By ∨	+ Add column ∨
🗎	File1.docx		About a minute ago	Prvi	
🗎	File2.docx	⚠	A few seconds ago	Prvi	
🗎	File3.docx	⊘	A few seconds ago	Prvi	
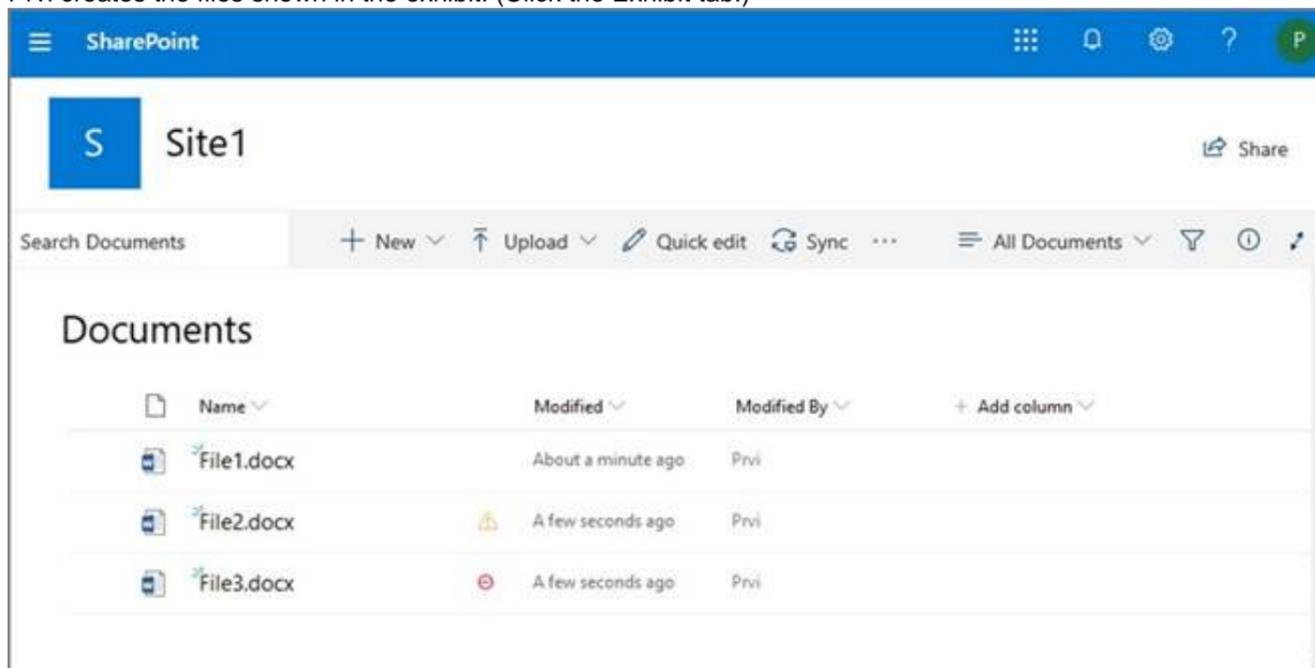
Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

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 99
- (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 100
HOTSPOT - (Topic 6)
You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.

```
Select Administrator: Windows PowerShell                        —    □    ×

Name               : Retention1
Priority           : 200
RecordTypes        : {MicrosoftTeams}
Operations         : {}
UserIds            : {}
RetentionDuration  : ThreeMonths

Name               : Retention2
Priority           : 150
RecordTypes        : {MicrosoftTeams}
Operations         : {teamcreated}
UserIds            : {User1@sk200628outlook.onmicrosoft.com}
RetentionDuration  : SixMonths

Name               : Retention3
Priority           : 100
RecordTypes        : {}
Operations         : {}
UserIds            : {User2@sk200628outlook.onmicrosoft.com}
RetentionDuration  : TwelveMonths



PS C:\>
```

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

If User1 creates a team in Microsoft Teams, the event is [**answer choice**].
- not retained
- retained for 90 days
- retained for six months
- retained for one year

If User2 adds a channel in Microsoft Teams, the event is [**answer choice**].
- not retained
- retained for 90 days
- retained for six months
- retained for one year

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

If User1 creates a team in Microsoft Teams, the event is [**answer choice**].
- not retained
- retained for 90 days
- retained for six months
- retained for one year

If User2 adds a channel in Microsoft Teams, the event is [**answer choice**].
- not retained
- retained for 90 days
- retained for six months
- retained for one year

NEW QUESTION 101
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

- 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.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

- 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.

Answer Area

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

NEW QUESTION 105
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:	
Group Policy		BYOD:	
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:	Microsoft Intune
Group Policy		BYOD:	Integration with Microsoft Defender for Cloud
Integration with Microsoft Defender for Cloud			
Microsoft Intune			
Virtual Desktop Infrastructure (VDI) scripts			

NEW QUESTION 106
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: You run idfix.exe and export the 10 user accounts.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 111
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
☐	contoso221018.onmicrosoft.com (Default)		✅ Healthy	
☐	contoso.com	⋮	ℹ Incomplete setup	
☐	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].

- contoso221018.onmicrosoft.com domain only
- 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

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

- contoso221018.onmicrosoft.com domain only
- 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].

- contoso221018.onmicrosoft.com domain only
- 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

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

- contoso221018.onmicrosoft.com domain only
- 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 114
- (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 116
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.
You need to configure Defender for Endpoint to meet the following requirements:
? Block a vulnerable app until the app is updated.
? Block an application executable based on a file hash.
The solution must minimize administrative effort.
What should you configure for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Block a vulnerable app until the app is updated:
- An alow or block file
- A file indicator
- A remediation request
- An update ring

Block an application executable based on a file hash:
- An alow or block file
- A file indicator
- A remediation request
- An update ring

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: A remediation request
Block a vulnerable app until the app is updated.
Block vulnerable applications

How to block vulnerable applications

? Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.

? Select a security recommendation to see a flyout with more information.

? Select Request remediation.

? Select whether you want to apply the remediation and mitigation to all device groups or only a few.

? Select the remediation options on the Remediation request page. The remediation options are software update, software uninstall, and attention required.

? Pick a Remediation due date and select Next.

? Under Mitigation action, select Block or Warn. Once you submit a mitigation action, it is immediately applied.

? Review the selections you made and Submit request. On the final page you can

choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.

Box 2: A file indicator

Block an application executable based on a file hash.

While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.

The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

NEW QUESTION 119

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected.

What should you use to create the policy?

A. the Microsoft 365 admin center

B. the Microsoft Purview compliance portal

C. the Microsoft Defender for Cloud Apps portal

D. the Microsoft Apps admin center

Answer: C

NEW QUESTION 120

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 125
- (Topic 6)
You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Source	Last sign in
User1	Azure AD	Yesterday
User2	Active Directory Domain Services (AD DS)	Two days ago
User3	Active Directory Domain Services (AD DS)	Never

Azure AD Connect has the following settings:
? Password Hash Sync: Enabled
? Pass-through authentication: Enabled
You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.
Which users should you identify?

A. none
B. Used only1
C. User1 and User2 only
D. User1. User2, and User3

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn¨

NEW QUESTION 130
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You need to ensure that when a document containing a credit card number is added to the tenant, the document is encrypted.
Which policy should you use?

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

Answer: C

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

NEW QUESTION 132
- (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 137
HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have devices enrolled in Intune as shown in the following table.
You create the device configuration profiles shown in the following table.

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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Device1:

No profiles	
Profile1 only	
Profile4 only	
Profile1 and Profile4 only	
Profile1, Profile1, and Profile4 only	

Device2:

No profiles	
Profile1 only	
Profile2 only	
Profile3 only	
Profile1 and Profile2 only	
Profile2 and Profile3 only	

NEW QUESTION 138
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

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

USER SIGN-IN

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

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 140
- (Topic 6)
Your on-premises network contains an Active Directory domain.
You have a Microsoft 365 subscription.
You need to sync the domain with the subscription. The solution must meet the following requirements:
On-premises Active Directory password complexity policies must be enforced. Users must be able to use self-service password reset (SSPR) in Azure AD. What should you use?

A. password hash synchronization
B. Azure AD Identity Protection
C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
D. pass-through authentication

Answer: D

Explanation:
Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.
This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations
wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.
Note: Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time by using either Azure AD Connect or Azure AD Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.
Password writeback is supported in environments that use the following hybrid identity models:
Password hash synchronization Pass-through authentication
Active Directory Federation Services
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback

NEW QUESTION 144
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	Member of
User1	Group1
User2	Group1, Group2
User3	None

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

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	○
User2 can enroll Android devices in Endpoint Manager.	○	○
User3 can enroll iOS devices in Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	⊙
User2 can enroll Android devices in Endpoint Manager.	○	⊙
User3 can enroll iOS devices in Endpoint Manager.	⊙	○

NEW QUESTION 148
- (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 151
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The question states that "all the user account synchronizations completed successfully". Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync- configure-filtering

NEW QUESTION 153
HOTSPOT - (Topic 6)
Your company has 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	Office 365 role group
User1	None	Compliance Data Administrator
User2	Global Administrator	None

You create a retention label named Label 1 that has the following configurations:
• Retains content for five years
• Automatically deletes all content that is older than five years
You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

• Applies to content that contains the word Merger
• Specifies the OneDrive accounts and SharePoint sites locations You run the following command.
Set-RetentionConpliancePolicy Policy1 -RestrictiveRetention Strue -Force
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 155
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table.
User1 reports that after sending 1,000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:
• Which administrators can unblock User1
• What to configure to allow User1 to send at least 2,000 emails per day without being blocked
What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Administrators: | Admin2 only ▼ |
Admin1 only
Admin2 only
Admin1 and Admin2 only
Admin2 and Admin3 only
Admin1, Admin2, and Admin3

Settings: | Anti-spam ▼ |
Anti-spam
Anti-phishing
Anti-malware
Advanced delivery
Enhanced filtering

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Administrators:
```
Admin2 only                    ▼
Admin1 only
Admin2 only
Admin1 and Admin2 only
Admin2 and Admin3 only
Admin1, Admin2, and Admin3
```

Settings:
```
Anti-spam                    ▼
Anti-spam
Anti-phishing
Anti-malware
Advanced delivery
Enhanced filtering
```
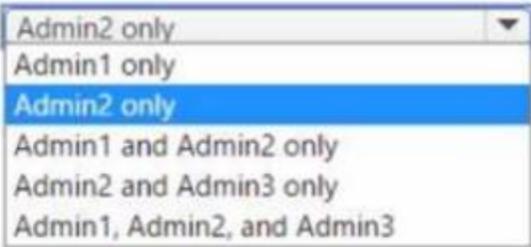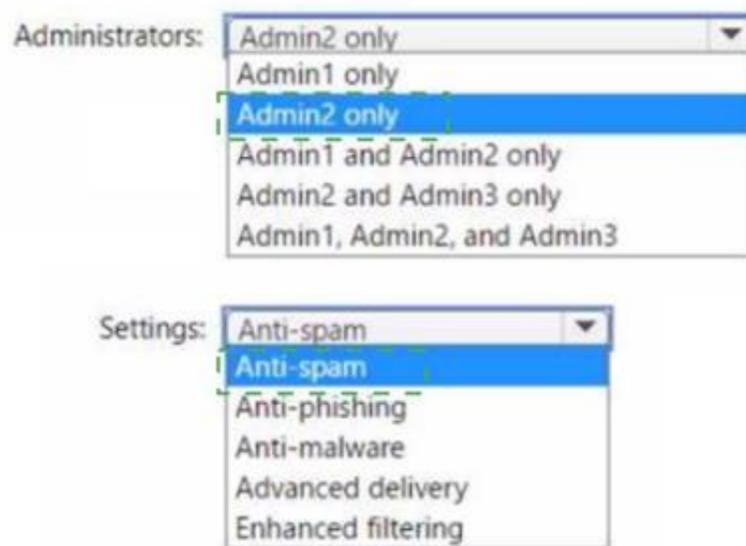
NEW QUESTION 158
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.
You need to implement passwordless authentication. The solution must support all the devices.
Which authentication method should you use?

A. Windows Hello
B. FID02 compliant security keys
C. Microsoft Authenticator app

Answer: C

NEW QUESTION 160
- (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 policyC a security baseline profile D a conditional access policy

Answer: B

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

NEW QUESTION 162
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.
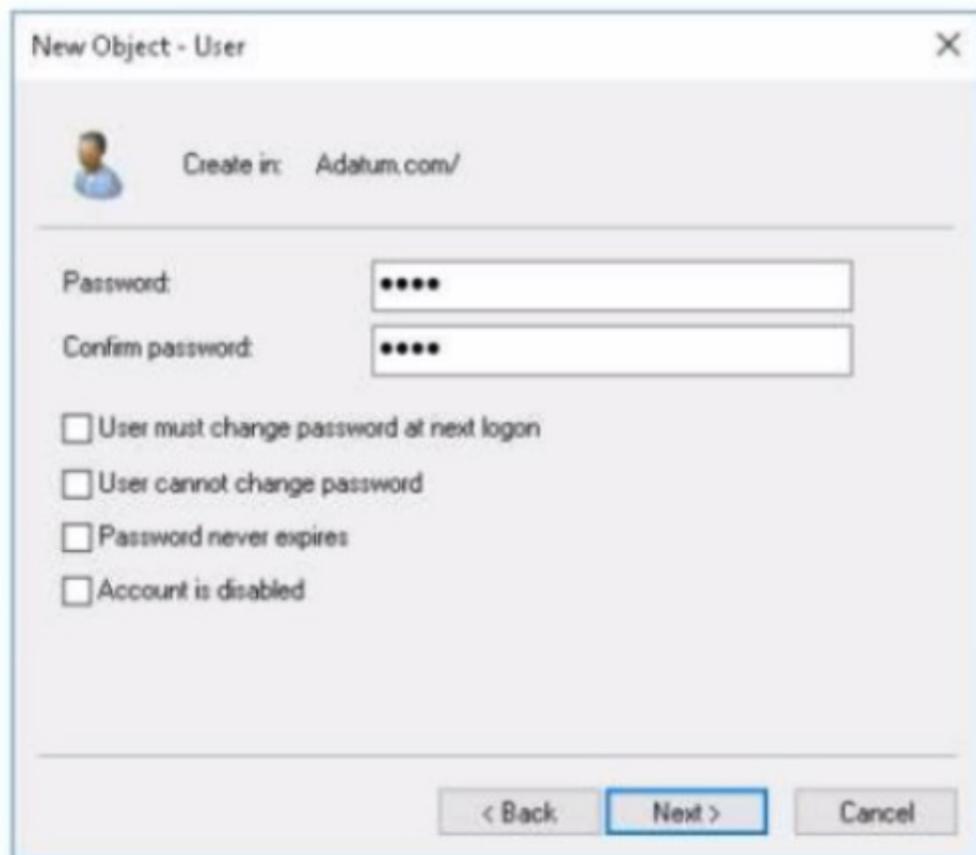
The Azure AD password policy is configured as shown in the following exhibit. Password policy
Set the password policy for all users in your organization. Days before passwords expire 90
Days before a user is notified about 14 expiration
You confirm that User1 is synced to Azure AD.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 166
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].

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

A. Yes
B. No

Answer: A

NEW QUESTION 169
- (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 assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
This is not a permissions issue.
The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

NEW QUESTION 173
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 onboarded 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 177
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.	○	○
User1 can join only five devices to Azure AD.	○	○
User2 can enroll all the devices in Intune.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	○	☑
User1 can join only five devices to Azure AD.	○	☑
User2 can enroll all the devices in Intune.	☑	○

NEW QUESTION 180
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant.
You have the alerts shown in the following exhibit.

View alerts

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

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

Answer Area

For Alert1, you can change Status to [Investigating only / Investigating or Resolved only / Investigating or Dismissed only / Investigating, Resolved, or Dismissed]

For Alert5, you can [not change Status / change Status to Dismissed only / change Status to Dismissed or Active only / change Status to Dismissed or Investigating only / change Status to Dismissed, Investigating, or Active]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

For Alert1, you can change Status to [Investigating only / Investigating or Resolved only / Investigating or Dismissed only / Investigating, Resolved, or Dismissed]

For Alert5, you can [not change Status / change Status to Dismissed only / change Status to Dismissed or Active only / change Status to Dismissed or Investigating only / change Status to Dismissed, Investigating, or Active]

NEW QUESTION 185
- (Topic 6)
You have a Microsoft 365 subscription.
You have the retention policies shown in the following table.

Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx.
File1.docx was created on January 1, 2022 and last modified on January 31, 2022. The file was NOT modified again.
When will File1.docx be deleted automatically?

A. January 1, 2023
B. January 1, 2024
C. January 31, 2023
D. January 31, 2024
E. never

Answer: D

Explanation:
Retention wins over deletion. Note:
Explanation for the four different principles:
* 1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system-initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.
* 2. Etc. Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

NEW QUESTION 187
- (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 Endpoinf Manager admin center, create a Windows Autopilot deployment profil
B. Assign the profile to all the computer
C. Instruct users to restart their computer and perform a network restart.
D. Enroll the computers in Microsoft Intun
E. Create a configuration profile by using the Edition upgrade and mode switch templat
F. From the Microsoft Endpoint Manager admincenter, assign the profile to all the computers and instruct users to restart their computer.
G. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online sit
H. Instruct users to run the provisioning package from SharePoint Online.
I. From the Azure Active Directory admin center, create a security group that has dynamic device membershi
J. Assign licenses to the group and instruct users to sign in to their computer.

Answer: B

NEW QUESTION 190
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.	○	○
A watermark is added to File1.docx.	○	○
A header is added to File2.xml.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Sensitivity1 is applied to the email.	○	○
A watermark is added to File1.docx.	○	○
A header is added to File2.xml.	○	○

NEW QUESTION 192
DRAG DROP - (Topic 6)
DRAG DROP

Your network contains an on-premises Active Directory domain that syncs to Azure Active
Directory (Azure AD). The domain contains the servers shown in the following table.

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

You use Azure Information Protection.
You need to ensure that you can apply Azure Information Protection labels to the file stores on Server1.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Authorize Server1.
Install the Microsoft Rights Management connector on Server2.
Install a certificate on Server2.
Install a certificate on Server1.
Register a service principal name for Server1.
Run GenConnectorConfig.ps1 on Server1.
Run GenConnectorConfig.ps1 on Server2.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

Authorize Server1.
Install the Microsoft Rights Management connector on Server2.
Install a certificate on Server2.
Install a certificate on Server1.
Register a service principal name for Server1.
Run GenConnectorConfig.ps1 on Server1.
Run GenConnectorConfig.ps1 on Server2.

Answer Area

Install the Microsoft Rights Management connector on Server2.
Authorize Server1.
Run GenConnectorConfig.ps1 on Server1.

NEW QUESTION 194
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains the administrative units shown in the following table.

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

The groups contain the members shown in the following table.

Name	Members
Group1	User1
Group2	User2, User4

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

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

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

Answer Area

Statements	Yes	No
User2 can reset the password of User1.	○	○
User2 can reset the password of User4.	○	○
User3 can assign licenses to User1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User2 can reset the password of User1.	⦿	○
User2 can reset the password of User4.	○	⦿
User3 can assign licenses to User1.	⦿	○

NEW QUESTION 198
- (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 202
- (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 206
- (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 208
- (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 210
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365 and contains a user named User1.
User1 emails a product catalog in the PDF format to 300 vendors. Only 200 vendors receive the email message, and User1 is blocked from sending email until the next day.
You need to prevent this issue from reoccurring. What should you configure?

A. anti-spam policies
B. Safe Attachments policies
C. anti-phishing policies
D. anti-malware policies

Answer: A

NEW QUESTION 213
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1.
The subscription has a single anti-malware policy as shown in the following exhibit.
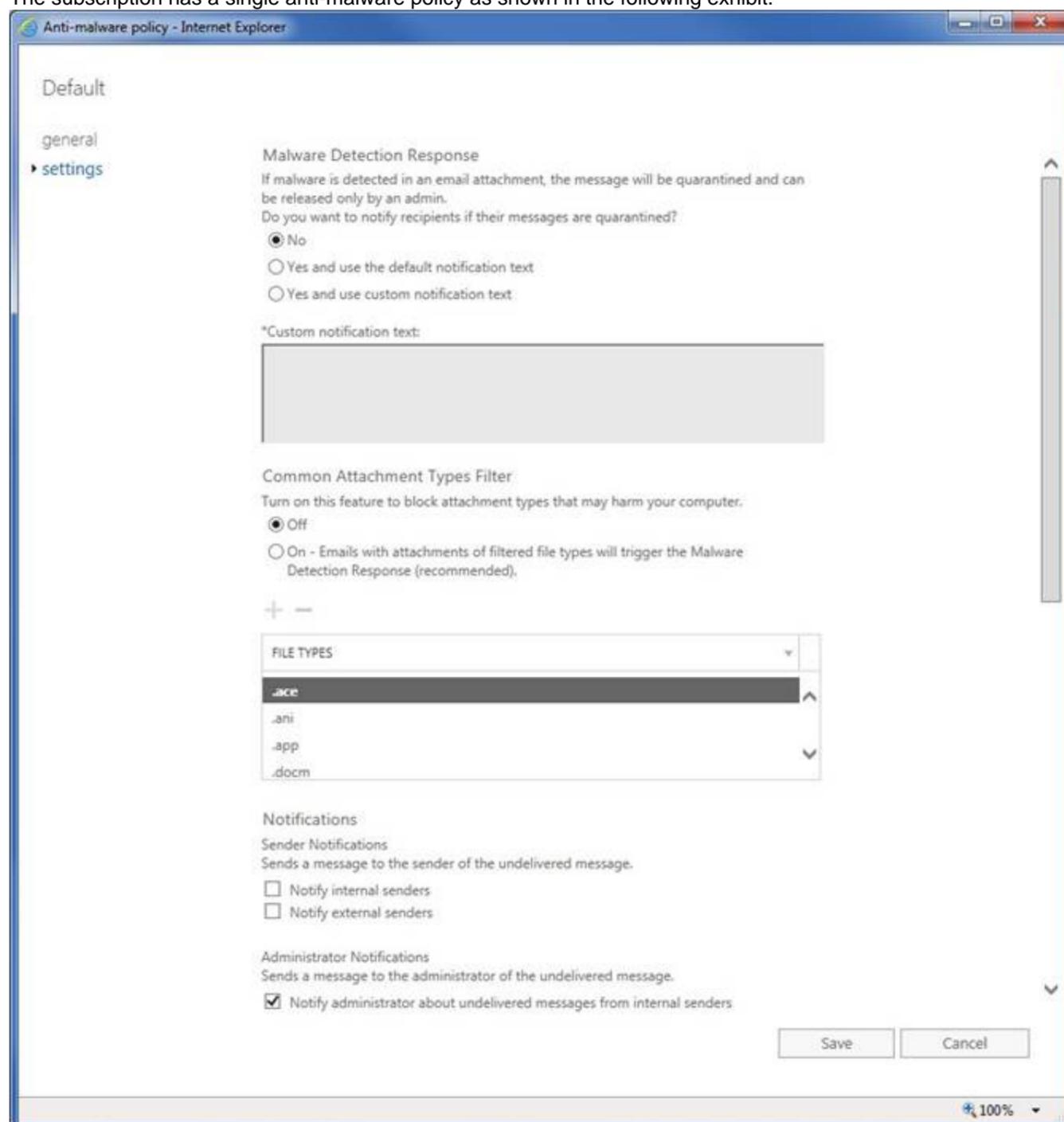
An email message that contains text and two attachments is sent to User1. One attachment is infected with malware.

How will the email message and the attachments be processed?

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

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies

NEW QUESTION 216
- (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 218
HOTSPOT - (Topic 6)
You have Microsoft 365 subscription.
You create an alert policy as shown in the following exhibit.

Policy1

✎ **Edit policy**   🗑 **Delete policy**

Status 🔵 On

Name your alert   ✎ ^

Description
Add a description

Severity
🔵 Low

Category
Threat management

Policy contains tags
-

Create alert settings   ✎ ^

Conditions
Activity is FileMalwareDetected

Aggregation
Aggregated

Scope
All users

Threshold
20

Window
2 hours

Severity
🔵 Low

Set your recipients   ✎ ^

Recipients
User1@sk220912outlook.onmicrosoft
.com

Daily notification limit
100

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

Policy1 will trigger an alert if malware is detected in **[answer choice]**.

SharePoint or OneDrive only ▼
Exchange Online only
SharePoint only
SharePoint or OneDrive only
Exchange Online, SharePoint , or OneDrive

The maximum number of email messages that Policy1 will generate per day is **[answer choice]**.

5 ▼
5
12
20
100

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy1 will trigger an alert if malware is detected in **[answer choice]**.

SharePoint or OneDrive only	▼
Exchange Online only	
SharePoint only	
SharePoint or OneDrive only	
Exchange Online, SharePoint , or OneDrive	

The maximum number of email messages that Policy1 will generate per day is **[answer choice]**.

5	▼
5	
12	
20	
100	

NEW QUESTION 223
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.
Each user has an Android device with the Microsoft Authenticator app installed and has set up phone sign-in.
The subscription has the following Conditional Access policy:
• Name: Policy1
• Assignments
o Users and groups: Group1, Group2 o Cloud apps or actions: All cloud apps
• Access controls
o Grant Require multi-factor authentication
• Enable policy: On
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   ⋯   ✕

ℹ 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 ∨	✕
Group2	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 sign in by using number matching in the Microsoft Authenticator app.	◯	◯
User2 can sign in by using a username and password.	◯	◯
User3 can sign in by using number matching in the Microsoft Authenticator app.	◯	◯

A. Mastered
B. Not Mastered

Answer: A

Explanation:

nswer Area

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	◯	◯
User2 can sign in by using a username and password.	◯	◯
User3 can sign in by using number matching in the Microsoft Authenticator app.	◯	◯

NEW QUESTION 224
- (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
☐	1	Require multifactor authentication for administrative roles	+4.15%	0/10	◯ To address
☐	2	Ensure all users can complete multifactor authentication	+3.73%	0/9	◯ To address
☐	3	Create Safe Links policies for email messages	+3.73%	0/9	◯ To address
☐	4	Enable policy to block legacy authentication	+3.32%	0/8	◯ To address
☐	5	Turn on Safe Attachments in block mode	+3.32%	0/8	◯ To address
☐	6	Ensure that intelligence for impersonation protection is enabled	+3.32%	0/8	◯ To address
☐	7	Move messages that are detected as impersonated users by mailbox intelligence	+3.32%	0/8	◯ To address
☐	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 229
HOTSPOT - (Topic 6)
You have a hybrid deployment of Azure AD that contains the users shown in the following table.

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

You need to identify which users can perform the following tasks:
• View sync errors in Azure AD Connect Health.
• Configure Azure AD Connect Health settings.
Which user should you identify for each task? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

View sync errors in Azure AD Connect Health: | User2 ▼
User1
User2
User3

Configure Azure AD Connect Health settings: | User1 ▼
User1
User2
User3

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

View sync errors in Azure AD Connect Health: | User2 ▼
User1
User2
User3

Configure Azure AD Connect Health settings: | User1 ▼
User1
User2
User3

NEW QUESTION 233
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 tenant.
You need to create a custom Compliance Manager assessment template.
Which application should you use to create the template, and in which file format should the template be saved? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Application: ▼
Microsoft Excel
Microsoft Forms
Microsoft Word
Visual Studio Code

File format: ▼
csv
dbx
docx
dotx
json
xlsx
xltx

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Application:

Microsoft Excel
Microsoft Forms
Microsoft Word
Visual Studio Code

File format:

csv
dbx
docx
dotx
json
xlsx
xltx

NEW QUESTION 236
- (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 238
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains 200 Android devices enrolled in Microsoft Intune.
You create an Android app protection policy named Policy! that is targeted to all Microsoft apps and assigned to all users.
Policy! has the Data protection settings shown in the following exhibit.

Data Transfer

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

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

Answer Area

A user can copy files from Microsoft OneDrive to **[answer choice]** only.
- OneDrive
- local storage
- **Microsoft SharePoint Online**
- Microsoft SharePoint Online and OneDrive

A user can copy and paste text from **[answer choice]** to a Microsoft Word document stored in Microsoft OneDrive.
- **any app**
- only managed apps
- only unmanaged apps

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

A user can copy files from Microsoft OneDrive to **[answer choice]** only.
- OneDrive
- local storage
- **Microsoft SharePoint Online**
- Microsoft SharePoint Online and OneDrive

A user can copy and paste text from **[answer choice]** to a Microsoft Word document stored in Microsoft OneDrive.
- **any app**
- only managed apps
- only unmanaged apps

NEW QUESTION 240
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	Not applicable

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

Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

Server1-London:
- Group1
- Group2
- Group3
- Ungrouped machines
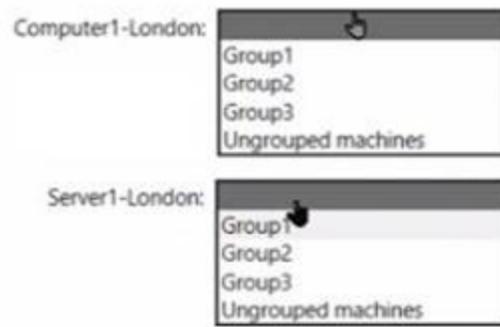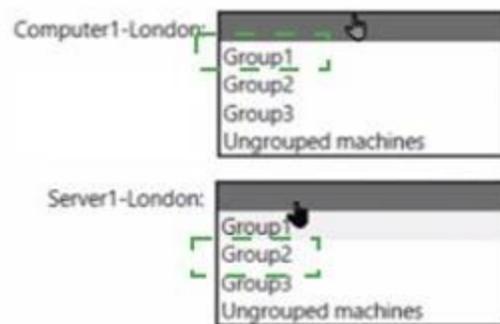
NEW QUESTION 245
- (Topic 6)
You have a Microsoft 365 E5 subscription.
All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).
You need to configure Microsoft Defender ATP on the 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 248
- (Topic 6)
You have a Microsoft 365 subscription that contains a user named User1.
You need to ensure that User1 can search the Microsoft 365 audit logs from the Security & Compliance admin center.
Which role should you assign to User1?

A. View-Only Audit Logs in the Security & Compliance admin center
B. View-Only Audit Logs in the Exchange admin center
C. Security reader in the Azure Active Directory admin center
D. Security Reader in the Security & Compliance admin center

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

NEW QUESTION 252
- (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 255
- (Topic 6)
You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.
You have the devices shown in the following table.

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

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

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

Answer: D

NEW QUESTION 260
......

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