Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam

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

A. Yes
B. No

Answer: A

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

NEW QUESTION 3
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You plan to deploy 1.000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.
You need to recommend a Microsoft Intune enrollment option that meets the following requirements:
• Minimizes user interaction
• Minimizes administrative effort
• Automatically installs corporate apps What should you recommend?

A. Automated Device Enrollment (ADE)
B. bring your own device (BYOD) user and device enrollment
C. Apple Configurator enrollment

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll

NEW QUESTION 4
- (Topic 6)
Your company has 10,000 users who access all applications from an on-premises data center.
You plan to create a Microsoft 365 subscription and to migrate data to the cloud. You plan to implement directory synchronization.
User accounts and group accounts must sync to Azure AD successfully. You discover that several user accounts fail to sync to Azure AD.
You need to resolve the issue as quickly as possible. What should you do?

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

Answer: B

Explanation:
IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for- synch-with-idfix

NEW QUESTION 5
- (Topic 6)
Your company has a Microsoft 365 E5 tenant that contains a user named User1. You review the company's compliance score.
You need to assign the following improvement action to User1:Enable self-service password reset.
What should you do first?

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

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

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

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

You plan to provide User4 with early access to Microsoft 365 feature and service updates. You need to identify which Microsoft 365 setting must be configured, and which user can
modify the setting. The solution must use the principle of least privilege.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Microsoft 365 setting:
▼
Office installation options
Privileged access
Release preferences

User:
▼
User1 only
User2 only
User3 only
User1 and User2 only
User1 and User3 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Microsoft 365 setting:
▼
Office installation options
Privileged access
Release preferences

User:
▼
User1 only
User2 only
User3 only
User1 and User2 only
User1 and User3 only

NEW QUESTION 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 E5 subscription.
On Monday, you create a new user named User1.
On Tuesday, User1 signs in for the first time and perform the following actions:
• Signs in to Microsoft Exchange Online from an anonymous IP address
• Signs in to Microsoft SharePoint Online from a device in New York City.
• Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections
Which types of sign-in risks will Azure AD Identity Protection detect for User1?

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

Answer: C

NEW QUESTION 9
- (Topic 6)
You have a Microsoft 365 E5 tenant.

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

Review your settings

Name   Edit
Retention1

Description for admins   Edit

Description for users   Edit

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

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

[Back]   [Create this label]   [Cancel]
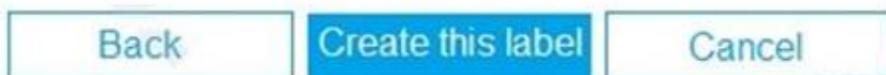
When users attempt to apply Retention1, the label is unavailable. You need to ensure that Retention1 is available to all the users. What should you do?

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

Answer: A

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

NEW QUESTION 10
- (Topic 6)
You purchase a new computer that has Windows 10, version 2004 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

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

Answer: B

NEW QUESTION 10
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. A Built-in protection preset security policy is applied to the subscription.
Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: CE

NEW QUESTION 14
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the resources shown in the following table.

Name	Type
Group1	Microsoft 365 group
Group2	Distribution group
Site1	Microsoft SharePoint site

You create a sensitivity label named Label1. To which resource can you apply Label1?

A. Group1 only
B. Group2 only
C. Site1 only
D. Group1 and Group2 only
E. Group1, Group2, and Site1

Answer: E

Explanation:
Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory
Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.
In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.
When you configure a label policy, you can:
Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams- groups-sites
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365- worldwide

NEW QUESTION 17
HOTSPOT - (Topic 6)
Your company has a Azure AD tenant named comoso.onmicrosoft.com that contains the users shown in the following table.

Name	Role
User1	Password Administrator
User2	Security Administrator
User3	User Administrator
User4	None

You need to identify which users can perform the following administrative tasks:
• Reset the password of User4.
• Modify the value for the manager attribute of User4.
Which users 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

Reset the password of User4: `User1 and User3 only` ▼
- User1 only
- User2 only
- User1 and User2 only
- **User1 and User3 only**
- User1, User2, and User3

Modify the value for the manager attribute of User4: `User3 only` ▼
- User2 only
- **User3 only**
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Reset the password of User4:	User1 and User3 only ▼
	User1 only
	User2 only
	User1 and User2 only
	User1 and User3 only
	User1, User2, and User3

Modify the value for the manager attribute of User4:	User3 only ▼
	User2 only
	User3 only
	User1 and User3 only
	User2 and User3 only
	User1, User2, and User3

NEW QUESTION 22
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365 and contains a mailbox named Mailbox1.
You plan to use Mailbox1 to collect and analyze unfiltered email messages.
You need to ensure that Defender for Office 365 takes no action on any inbound emails delivered to Mailbox1.
What should you do?

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

Answer: D

NEW QUESTION 27
- (Topic 6)
You have a Microsoft 365 E5 tenant that has sensitivity label support enabled for Microsoft and SharePoint Online.
You need to enable unified labeling for Microsoft 365 groups. Which cmdlet should you run?

A. set-unifiedGroup
B. Set-Labelpolicy
C. Execute-AzureAdLebelSync
D. Add-UnifiedGroupLinks

Answer: C

NEW QUESTION 29
- (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 30
- (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 32
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

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

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

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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 34
- (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 35
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. |

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 37
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.
The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.
You need to identify the following information:
• The number of email messages quarantined by zero-hour auto purge (ZAP)
• The number of times users clicked a malicious link in an email message
Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify the number of emails quarantined by ZAP: | Threat protection status ▼ |
Mailflow status report
Spoof detections
Threat protection status
URL threat protection

To identify the number of times users clicked a malicious link in an email: | Mailflow status report ▼ |
Mailflow status report
Spoof detections
Threat protection status
URL threat protection

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

To identify the number of emails quarantined by ZAP:
Threat protection status ▼
- Mailflow status report
- Spoof detections
- **Threat protection status**
- URL threat protection

To identify the number of times users clicked a malicious link in an email:
Mailflow status report ▼
- **Mailflow status report**
- Spoof detections
- Threat protection status
- URL threat protection

NEW QUESTION 41
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 ⌄
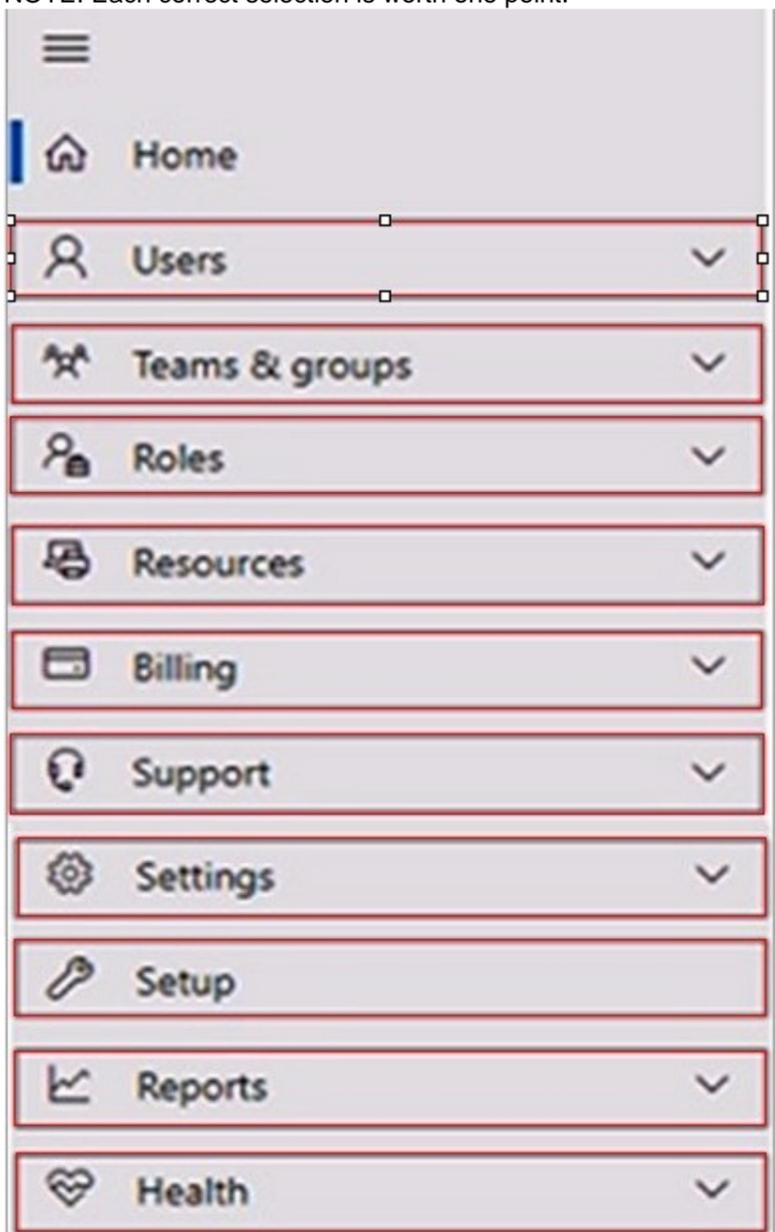
A. Mastered
B. Not Mastered

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 46
- (Topic 6)
You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.
You need to prevent the members or Group1 from communicating with the members of Group2 by using Microsoft Teams. The solution must comply with regulatory requirements and must not affect other user in the tenant.
What should you use?

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

Answer: A

NEW QUESTION 48
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature. You need to block users from downloading a file named File1.exe.
What should you use?

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

Answer: A

NEW QUESTION 53
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Role
User1	Global admin
User2	None
User3	None

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

Name	Role
User1	None
User2	Purchaser
User3	Basic Purchaser

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

Can add apps to the private store:
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Can assign apps from Microsoft Store for Business:
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

A. Mastered
B. Not Mastered

□ CertShared

Certshared now are offering 100% pass ensure MS-102 dumps!
https://www.certshared.com/exam/MS-102/ (312 Q&As)

Answer: A

Explanation:

Can add apps to the private store:

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

Can assign apps from Microsoft Store for Business:

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

NEW QUESTION 55
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Reports Reader
User2	Exchange Administrator
User3	User Experience Success Manager

Which users can review the Adoption Score in the Microsoft 365 admin center?

A. User! only
B. User2onry
C. User1 and User2 only
D. User! and User3 only
E. User1, User2. and User3

Answer: E

NEW QUESTION 60
- (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 65
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You onboard all devices to Microsoft Defender for Endpoint
You need to use Defender for Endpoint to block access to a malicious website at www.contoso.com.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

A. Create a web content filtering policy.
B. Configure an enforcement scope.

C. Enable Custom network indicators.
D. Create an indicator.
E. Enable automated investigation.

Answer: AC

NEW QUESTION 66
- (Topic 6)
You need to notify the manager of the human resources department when a user in the department shares a file or folder from the departments Microsoft SharePoint Online site. What should you do?

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

Answer: D

NEW QUESTION 68
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1. Solution: You raise the forest functional level to Windows Server 2016. You copy the Group
Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.
Does this meet the goal?

A. yes
B. No

Answer: B

NEW QUESTION 69
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

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

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

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

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

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

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

Answer Area

Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	○
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	○
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.
Box 2: No
Computer1 does not belong to either Group1 or Group2
Box 3: Yes
Device3 belongs to both Group1 and Group2.
Note: Understanding alert severity
Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.
The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

NEW QUESTION 71
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Role
User1	Group1	User Administrator
User2	Group1	None
User3	Group2	None
User4	None	Global Administrator

You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.
Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.
NOTE; Each correct selection is worth one point.

Answer Area

Users that can use SSPR: User1, User2, and User4 only ▼
- User1 and User2 only
- User1, User2, and User3 only
- **User1, User2, and User4 only**
- User1, User2, User3, and User4

Users that must answer security questions to reset their password: User1 and User2 only ▼
- User1 only
- User2 only
- **User1 and User2 only**
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Users that can use SSPR: | User1, User2, and User4 only ▼
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Users that must answer security questions to reset their password: | User1 and User2 only ▼
- User1 only
- User2 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4
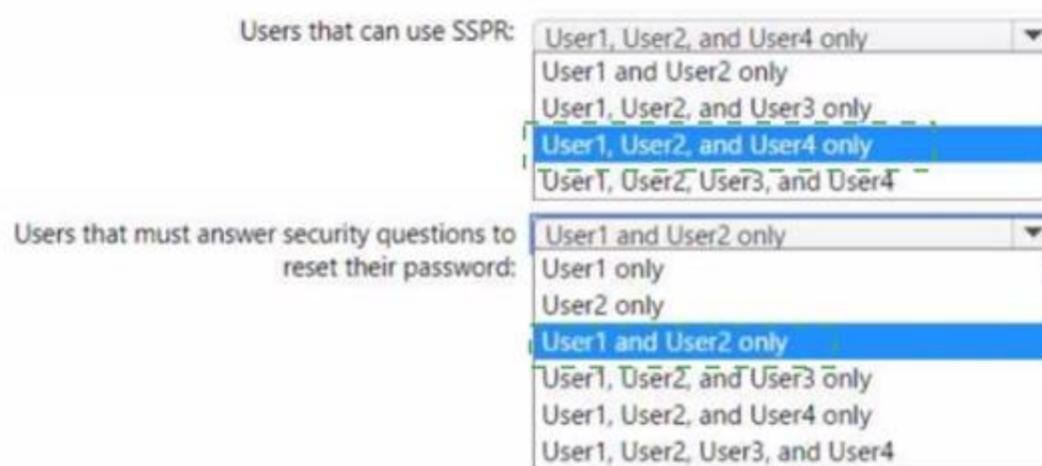
NEW QUESTION 72
- (Topic 6)
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.
Where can you store data from the LinkedIn connector?

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 75
- (Topic 6)
You have a Microsoft 365 subscription.
You configure a data loss prevention (DLP) policy.
You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.
You need to prevent the users from bypassing the DLP policy. What should you configure?

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

Answer: D

Explanation:
A DLP policy can be configured to allow users to override a policy tip and report a false positive.
You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word.
If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention- policies

---

NEW QUESTION 78
- (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 80**
HOTSPOT - (Topic 6)

Your company has a Microsoft 365 tenant

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

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

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

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

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

Answer Area

Device limit:
- 5
- 10
- 15

Allowed platform
- Android only
- iOS only
- All platforms

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restriction-priority
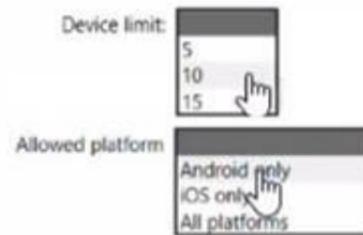
NEW QUESTION 83
HOTSPOT - (Topic 6)
From the Microsoft Purview compliance portal, you create a retention policy named Policy 1.
You need to prevent all users from disabling the policy or reducing the retention period. How should you configure the Azure PowerShell command? To answer select the
appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Set-RetentionCompliancePolicy ▼   -Identity "Policy1"   -RestrictiveRetention ▼ $true
- Set-ComplianceTag   -enabled
- Set-HoldCompliancePolicy   -Force
- **Set-RetentionCompliancePolicy**   -RestrictiveRetention
- Set-RetentionPolicy   -RetentionPolicyTagLinks
- Set-RetentionPolicyTag   -SystemTag

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Set-RetentionCompliancePolicy ▼   -Identity "Policy1"   -RestrictiveRetention ▼ $true
- Set-ComplianceTag   -enabled
- Set-HoldCompliancePolicy   -Force
- **Set-RetentionCompliancePolicy**   -RestrictiveRetention
- Set-RetentionPolicy   -RetentionPolicyTagLinks
- Set-RetentionPolicyTag   -SystemTag

NEW QUESTION 84
- (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 85
HOTSPOT - (Topic 6)
Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Member
1	Group1	Name starts with Comp
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped devices (default)	Not applicable

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

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer! and Computed members? To answer, select the appropriate options in The answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Computer1: Group1 only
- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped devices

Computer2: Group1 only
- Group1 only
- Group3 only
- Group1 and Group3

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Computer1: Group1 only
- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped devices

Computer2: Group1 only
- Group1 only
- Group3 only
- Group1 and Group3

NEW QUESTION 86
- (Topic 6)
You have a Microsoft 365 subscription.
You plan to implement Microsoft Purview Privileged Access Management. Which Microsoft Office 365 workloads support privileged access?

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

Answer: A

Explanation:

Privileged access management

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

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

Reference:

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

---

NEW QUESTION 87
- (Topic 6)
You have a Microsoft 365 E5 subscription. You need to create a mail-enabled contact. Which portal should you use?

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

Answer: A

NEW QUESTION 88
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

You ate implementing Microsoft Defender for Endpoint

You need to enable role-based access control (RBAQ to restrict access to the Microsoft 365 Defender portal.

Which users can enable RBAC, and winch users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Answer Area

Users that can enable RBAC: | Admin1 and Admin2 only |
Admin1 only
Admin1 and Admin2 only
Admin1, Admin2, and Admin5 only
Admin1, Admin2, Admin3, and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal: | Admin3, Admin4, and Admin5 only |
Admin5 only
Admin3 and Admin4 only
Admin4 and Admin5 only
Admin3, Admin4, and Admin5 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Users that can enable RBAC: | Admin1 and Admin2 only |
Admin1 only
Admin1 and Admin2 only
Admin1, Admin2, and Admin5 only
Admin1, Admin2, Admin3, and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal: | Admin3, Admin4, and Admin5 only |
Admin5 only
Admin3 and Admin4 only
Admin4 and Admin5 only
Admin3, Admin4, and Admin5 only

NEW QUESTION 89
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of	Device
User1	Group1	Device1
User2	Group1	Device2, Device3

The devices are configured as shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Joined
Device3	Android	Registered

You have a Conditional Access policy named CAPolicy1 that has the following settings: 1.Assignments
? Users or workload identities: Group1
? Cloud apps or actions: Office 365 SharePoint Online
? Conditions
- Filter for devices: Exclude filtered devices from the policy
- Rule syntax: device.displayName -startsWith "Device" 2.Access controls
? Grant
- Grant: Block access
? Session: 0 controls selected 3.Enable policy: On
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 access Site1 from Device1.	○	○
User2 can access Site1 from Device2.	○	○
User2 can access Site1 from Device3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
User1 is member of Group1 and has Device1.
Device1 is not Azure AD joined.
Note: Requiring a hybrid Azure AD joined device is dependent on your devices already being hybrid Azure AD joined.
Box 2: Yes
User2 is member of Group1 and has devices Device2 and Device3. Device2 is Azure AD joined.
Device2 is excluded from CAPolicy1 (which would block access to Site1). Box 3: Yes
User2 is member of Group1 and has devices Device2 and Device3.
Device3 is Android and is Azure AD registered.
Device3 is excluded from CAPolicy1 (which would block access to Site1).
Note: On Windows 7, iOS, Android, macOS, and some third-party web browsers, Azure AD identifies the device using a client certificate that is provisioned when the device is registered with Azure AD. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.

NEW QUESTION 91
- (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 95
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1 You create a retention label named Retention1 that is published to all locations.
You need to ensure that User1 can label email messages by using Retention1 as soon as possible.
Which cmdlet should you run in Microsoft Exchange Online PowerShell?

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

Answer: C

NEW QUESTION 96
HOTSPOT - (Topic 6)
From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

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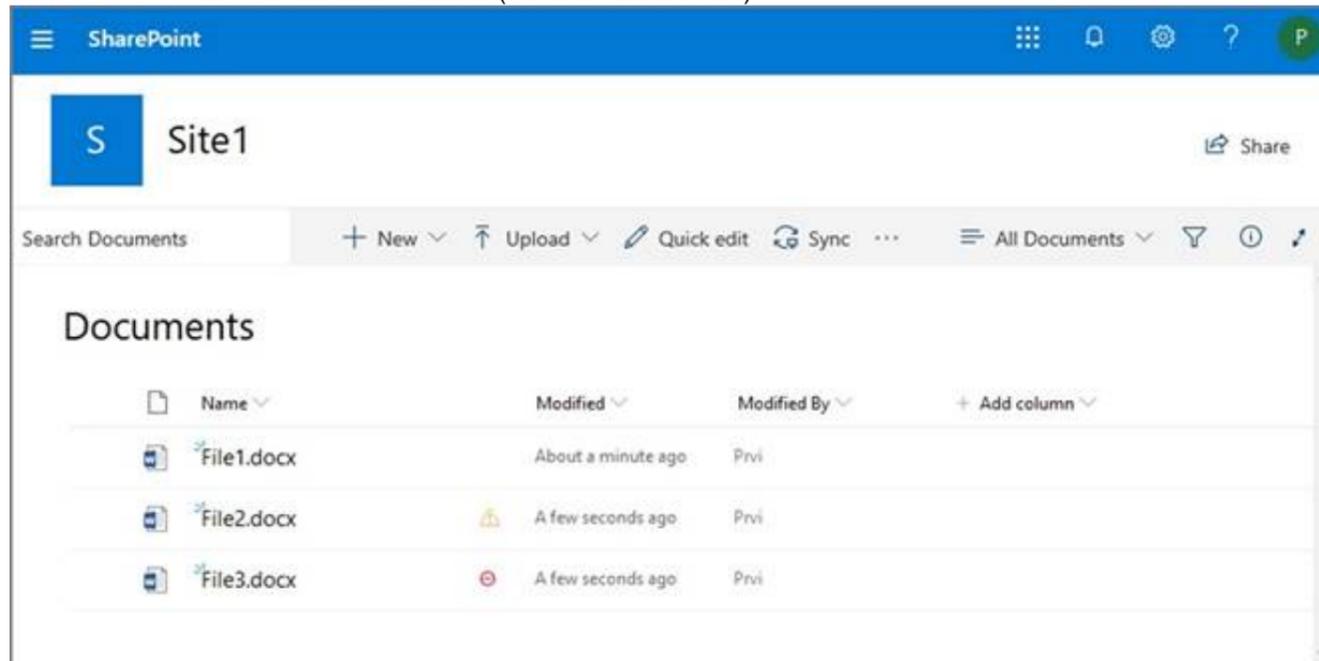
Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User1:

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

User2:

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

User1:

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

User2:

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

NEW QUESTION 98
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription that contains the devices shown in the following table.

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

You install Microsoft Word on all the devices.
You plan to configure policies to meet the following requirements:
• Word files created by using Windows devices must be encrypted automatically.
• If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
• For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.
Which type of polio/ should you configure for each device? To answer, drag the appropriate policy types to the correct devices. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Policy Types   Answer Area

| App configuration policy | Device1: [   ]

| App protection policy | Device2: [   ]

| Compliance policy | Device3: [   ]

| Conditional Access policy |

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 100
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.
You need to deploy the policy. What should you do first?

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

Answer: C

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

NEW QUESTION 101
- (Topic 6)
You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:
• Windows 10
• Android
• OS
On which devices can you configure the Endpoint DLP policies?

A. Windows 10 only
B. Windows 10 and Android only
C. Windows 10 and macO Sonly
D. Windows 10, Android, and iOS

Answer: D

Explanation:
Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide

NEW QUESTION 102
- (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 107
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

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

Name	Type
Label1	Sensitivity
Label2	Retention

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

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

You have labels In Microsoft 365 as shown in the following table.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	○	●
Admin2 can view the contents of File1 by using Content explorer.	○	●
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	○	●

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	○	○
Admin2 can view the contents of File1 by using Content explorer.	○	○
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	○	○

NEW QUESTION 110
HOTSPOT - (Topic 6)
HOTSPOT
Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

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

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

Settings > Endpoints > computer1

computer1

Device summary

Risk level ⓘ

▬▬ None

Device details

Domain

adatum.com

OS

Windows 10 64-bit
Version 21H2
Build 19044.2130

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

Answer Area

Computer1 will be a member of [answer choice].

▼
Group3 only
Group4 only
Group3 and Group4 only
Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

▼
Group1 only
Group1 and Group2 only
Group1, Group2, Group3, and Group4
Ungrouped devices

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Group3 and Group4 only Computer1 has no Demo Tag.
Computer1 is in the adatum domain and OS is Windows 10. Box 2: Group1, Group2, Group3 and Group4

NEW QUESTION 114
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. You need to perform the following tasks:
• Create a sensitive info type named SIT1 based on a regular expression.
• Add a watermark to all new documents that are matched by SIT1.
Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Microsoft Purview

- Home
- Compliance Manager
- Data classification
- Data connectors
- Reports

Solutions

- Catalog
- App governance
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery ⌄
- Data lifecycle management ⌄
- Information protection
- Information barriers ⌄
- Insider risk management
- Records management
- Privacy risk management ⌄
- Subject rights requests

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 119
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.
From Azure AD Identity Protection, you enable a sign-in risk policy.
Users report that when they use the VDI solution, they are regularly blocked when they attempt to access Microsoft 365.
What should you configure?

A. the Tenant restrictions settings in Azure AD
B. a trusted location
C. a Conditional Access policy exclusion
D. the Microsoft 365 network connectivity settings

Answer: B

Explanation:
There are two types of risk policies in Azure Active Directory (Azure AD) Conditional Access you can set up to automate the response to risks and allow users to self-remediate when risk is detected:
Sign-in risk policy User risk policy
Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.
Reference:

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity- protection-configure-risk-policies
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location- condition

NEW QUESTION 122
FILL IN THE BLANK - (Topic 6)
You have a Microsoft 365 tenant.
You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 127
- (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)
Your company has a Microsoft E5 tenant.
The company must meet the requirements of the ISO/IEC 27001:2013 standard. You need to assess the company's current state of compliance.
What should you use?

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

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

NEW QUESTION 133
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.
You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.
Solution: From the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group.
Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 137
- (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 141
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 145
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 subscription.
In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:
? Block emails that contain financial data.
? Display the following policy tip text: Message blocked.
From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:
? Use the following location: Exchange email.
? Display the following policy tip text: Message contains sensitive data.
? When a user sends an email, notify the user if the email contains health records.
What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Results

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

Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked. If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.
Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

NEW QUESTION 146
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Al users have Mac computers. ATl the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender for Endpoint.
You need to configure Microsoft Defender for Endpoint on the computers. What should you create from the Endpoint Management admin center?

A. a Microsoft Defender for Endpoint baseline profile
B. an update policy for iOS
C. a device configuration profile

D. a mobile device management (MDM) security baseline profile

Answer: D

NEW QUESTION 148
- (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 150
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 E5 tenant.
You need to implement compliance solutions that meet the following requirements:
• Use a file plan to manage retention labels.
• Identify, monitor, and automatically protect sensitive information.
• Capture employee communications for examination by designated reviewers.
Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 154
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 158
- (Topic 6)
You have a Microsoft 365 subscription.
You have a data loss prevention (DLP) policy that blocks sensitive data from being shared in email messages.
You need to modify the policy so that when an email message containing sensitive data is sent to both external and internal recipients, the message is only prevented from being delivered to the external recipients.
What should you modify?

A. the policy rule exceptions
B. the DLP policy locations
C. the policy rule conditions
D. the policy rule actions

Answer: C

NEW QUESTION 161
- (Topic 6)
You have a Microsoft 365 tenant.
Company policy requires that all Windows 10 devices meet the following minimum requirements:
? Require complex passwords.
? Require the encryption of data storage devices.
? Have Microsoft Defender Antivirus real-time protection enabled.
You need to prevent devices that do not meet the requirements from accessing resources in the tenant.
Which two components should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a configuration policy
B. a compliance policy
C. a security baseline profile
D. a conditional access policy
E. a configuration profile

Answer: BD

Explanation:
Reference:

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

NEW QUESTION 165
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.

Group1
Private group • 1 owner • 1 member

General   Members   **Settings**   Microsoft Teams

General settings

☐ Allow external senders to email this group

☑ Send copies of group conversations and events to group members

☐ Hide from my organization's global address list

Privacy

◉ Private

◯ Public
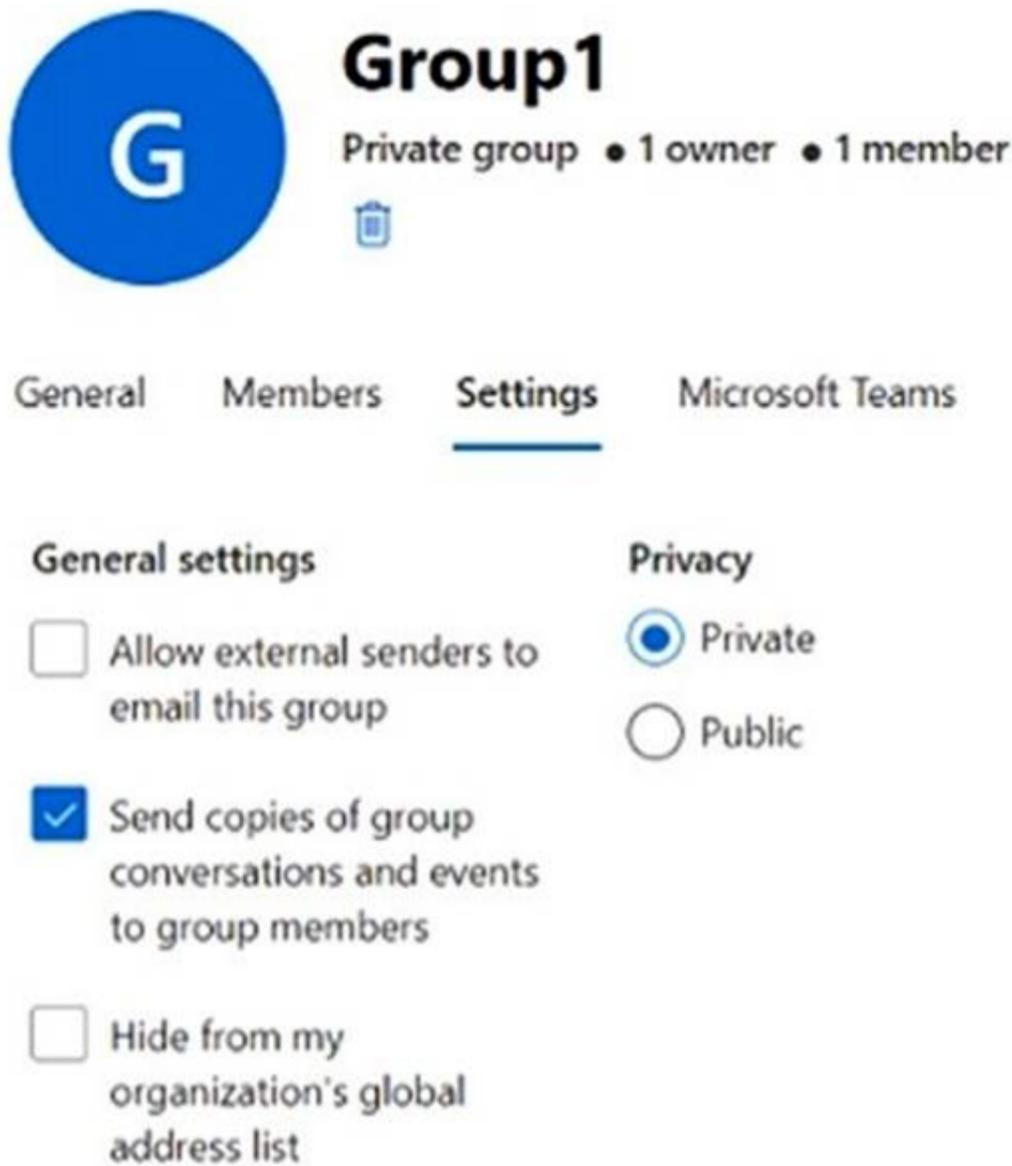
An external user named User1 has an email address of user1@outlook.com. You need to add User1 to Group1.
What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Action:
- Add User1 to the subscription as an active user.
- For Group1, change the Privacy setting to Public.
- For Group1, select Allow external senders to email this group.
- Invite User1 to collaborate with your organization as a guest.

Portal:
- The Microsoft Entra admin center
- The Exchange admin center
- The Microsoft 365 admin center
- The Microsoft Purview compliance portal

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Invite User1 to collaborate with your organization as a guest.
To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.
Navigate with your Web browser to https://admin.microsoft.com. On the left pane, click on "Users", then click "Guest Users".
On the "Guest Users" page, to create a new guest user, click on either the "Add a guest user" link on the top of the page or click on "Go to Azure Active Directory to add guest users" link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at https://aad.portal.azure.com.
On the "New user" page in the Microsoft Azure portal, you must choose to either "Create user" or "Invite user". If you choose the "Create user" option, this will create a new user in your organization, which will have a login address with format username@tenantdomain,dot,com. If you choose the "Invite user" option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating.

For the purpose of creating a guest user, you must choose the "Invite user" option.
Box 2: The Microsoft Entra admin center
Microsoft Entra admin center unites Azure AD with family of identity and access products
Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.
Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).

NEW QUESTION 169
- (Topic 6)
You have a Microsoft 365 subscription.
Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers
followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de- fghij.
You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.
D18912E1457D5D1DDCBD40AB3BF70D5D
What should you create to ensure that the DLP policy can detect the customer IDs?

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

Answer: A

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

NEW QUESTION 174
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft intune.
in the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices,
You enable device clean-up rules
What can you configure as the minimum number of days before a device a removed automatically?

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

Answer: D

NEW QUESTION 178
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to create a policy that will generate an email alert when a banned app is detected requesting permission to access user information or data in the subscription.
What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy type:

| Activity |
| App discovery | These are the selections for Policy type. |
| OAuth app |
| Session |

Filter type:

Filter type:

| App |
| App state | These are the selections for Filter type. |
| App tag |
| Permission level |
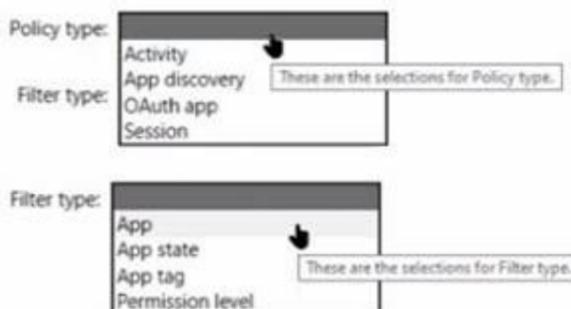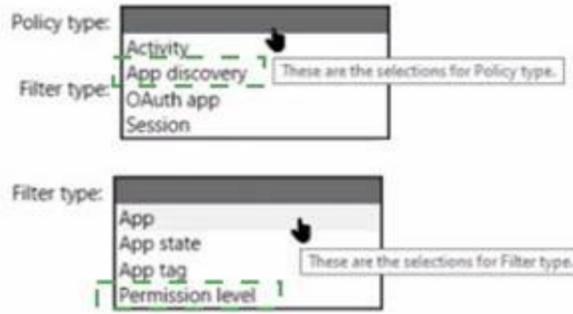
NEW QUESTION 180

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

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

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

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

NOTE: Each correct selection is worth one point.

Answer Area

User1: Phone number and email address ▼
- Email address only
- Phone number only
- Security questions only
- **Phone number and email address**

User2: Phone number and email address ▼
- Email address only
- Phone number only
- Security questions only
- **Phone number and email address**

User3: Security questions only ▼
- Email address only
- Phone number only
- **Security questions only**
- Phone number and email address

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

User1: Phone number and email address ▼
- Email address only
- Phone number only
- Security questions only
- **Phone number and email address**

User2: Phone number and email address ▼
- Email address only
- Phone number only
- Security questions only
- **Phone number and email address**

User3: Security questions only ▼
- Email address only
- Phone number only
- **Security questions only**
- Phone number and email address

NEW QUESTION 184

- (Topic 6)
You purchase a new computer that has Windows 10, version 21H1 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

A. Install all the feature updates released since version 21H1 and the latest quality update only.
B. Install the latest feature update and all the quality updates released since version 21H1.
C. Install the latest feature update and the latest quality update only.
D. Install all the feature updates released since version 21H1 and all the quality updates released since version 21H1 only.

Answer: C

NEW QUESTION 186
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You need to review reports to identify the following:
• The storage usage of files stored in Microsoft Teams
• The number of active users per team
Which report should you review for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 188
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E3 subscription.
You plan to launch Attack simulation training for all users.
Which social engineering technique and training experience will be available? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Credential Harvest
Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering.
Note: In Attack simulation training, multiple types of social engineering techniques are available:
Credential Harvest Malware Attachment Link to Malware
Etc.
Box 2: Mass Market Phishing

NEW QUESTION 193
HOTSPOT - (Topic 6)
You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

The device compliance policies in Endpoint Manager are configured as shown in the following table.

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group3
Policy2	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
Device1 is compliant.	○	○
Device2 is compliant.	○	○
Device3 is compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device1 is compliant.	○	◉
Device2 is compliant.	○	◉
Device3 is compliant.	◉	○

NEW QUESTION 198
- (Topic 6)
You have a Microsoft 365 subscription. You add a domain named contoso.com.
When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.com.
You need to change the email address used to verify the domain. What should you do?

A. From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription.
B. Add a TXT record to the DNS zone of the domain.
C. From the domain registrar, modify the contact information of the domain.
D. Modify the NS records for the domain.

Answer: C

NEW QUESTION 199
HOTSPOT - (Topic 6)
You have a Microsoft 365 ES 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 204
- (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 205
- (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 209
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 212
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 217
HOTSPOT - (Topic 5)
You need to configure the Office 365 service status notifications and limit access to the service and feature updates. The solution must meet the technical requirements.
What should you configure in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

To configure the notifications: Briefing email
- Briefing email
- Help desk information
- Organization information

To limit access: Release preferences
- Privileged Access
- Release preferences
- Office installation options

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 219
HOTSPOT - (Topic 5)
You need to ensure that Admin4 can use SSPR.
Which tool should you use. and which action should you perform? To answer, select the appropriate options m the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Action: Enable password writeback.
- Enable app registrations.
- Enable password writeback.
- Enable password hash synchronization.
- Disable password hash synchronization.

Tool: Azure AD Connect
- Azure AD Connect
- Synchronization Rules Editor
- Microsoft Entra admin center

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Action: Enable password writeback.
- Enable app registrations.
- **Enable password writeback.**
- Enable password hash synchronization.
- Disable password hash synchronization.

Tool: Azure AD Connect
- **Azure AD Connect**
- Synchronization Rules Editor
- Microsoft Entra admin center

NEW QUESTION 221
HOTSPOT - (Topic 5)
You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.
Which users can review the incidents and advisories, and which blade should the users use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Users: Admin1 and Admin3 only
- Admin1 only
- **Admin1 and Admin3 only**
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Blade: Service Health
- Reports
- **Service Health**
- Message center

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Users: Admin1 and Admin3 only
- Admin1 only
- **Admin1 and Admin3 only**
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Blade: Service Health
- Reports
- **Service Health**
- Message center

NEW QUESTION 224
- (Topic 5)
You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs.
What should you do?

A. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.
B. From PowerShell, run the Add-ADSyncConnectorAttrbuteinclusion cmdlet.
C. From PowerShell, run the start-ADSyncSyncCycle cmdlet.
D. From the Microsoft Azure AD Connect wizard, select Manage federation.

Answer: A

NEW QUESTION 229
- (Topic 4)
You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.
Which authentication strategy should you implement for the pilot projects?

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

Answer: C

Explanation:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
Fabrikam does NOT plan to implement identity federation.
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable SSO to enable all users to be signed in to on-premises and cloud- based applications automatically.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

NEW QUESTION 233
- (Topic 3)
You need to configure Office on the web to meet the technical requirements. What should you do?

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

Answer: B

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

NEW QUESTION 234
- (Topic 3)
You need to create the Safe Attachments policy to meet the technical requirements. Which option should you select?

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

Answer: D

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

NEW QUESTION 237
- (Topic 3)
You need to configure the compliance settings to meet the technical requirements. What should you do in the Microsoft Endpoint Manager admin center?

A. From Compliance policies, modify the Notifications settings.
B. From Locations, create a new location for noncompliant devices.
C. From Retire Noncompliant Devices, select Clear All Devices Retire State.
D. Modify the Compliance policy settings.

Answer: D

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

NEW QUESTION 241
HOTSPOT - (Topic 2)
You need to meet the technical requirement for log analysis.
What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Minimum number of data sources:

▼
1
3
6

Minimum number of log collectors:

▼
1
3
6

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

NEW QUESTION 242
- (Topic 2)
You need to protect the U.S. PII data to meet the technical requirements. What should you create?

A. a data loss prevention (DLP) policy that contains a domain exception
B. a Security & Compliance retention policy that detects content containing sensitive data
C. a Security & Compliance alert policy that contains an activity
D. a data loss prevention (DLP) policy that contains a user override

Answer: A

NEW QUESTION 246
- (Topic 1)
On which server should you install the Azure ATP sensor?

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

Answer: A

Explanation:
 References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning
However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

NEW QUESTION 247
HOTSPOT - (Topic 1)
You need to meet the technical requirements and planned changes for Intune. What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Settings to configure in Azure AD:
Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Settings to configure in Azure AD:
> Device settings _ _ _ _ _ _
> Mobility (MDM and MAM) _ |
> Organizational relationships
> User settings

Settings to configure in Intune:
> Device compliance
> Device configuration
> Device enrollment |
> Mobile Device Management Authority

NEW QUESTION 251
HOTSPOT - (Topic 1)
You need to meet the Intune requirements for the Windows 10 devices.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Settings to configure in Azure AD: ▼
> Device settings
> Mobility (MDM and MAM)
> Organizational relationships
> User settings

Settings to configure in Intune: ▼
> Device compliance
> Device configuration
> Device enrollment
> Mobile Device Management Authority

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/intune/windows-enroll

NEW QUESTION 256
- (Topic 1)
You need to meet the compliance requirements for the Windows 10 devices. What should you create from the Intune admin center?

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

Answer: C

NEW QUESTION 258
- (Topic 1)
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 named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.
Does this meet the goal?

A. Yes
B. NO

Answer: A

Explanation:
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune. Reference: https://docs.microsoft.com/en- us/configmgr/comanage/how-to-enable

NEW QUESTION 263
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to implement identity protection by configuring a sign-in risk policy and a user risk policy. Which type of risk is detected by each policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Sign-in risk policy: Leaked credentials
- Atypical travel
- Leaked credentials
- Possible attempt to access Primary Refresh Token (PRT)

User risk policy: Malicious IP address
- Leaked credentials
- Malicious IP address
- Suspicious browser

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Sign-in risk policy: Leaked credentials
- Atypical travel
- Leaked credentials
- Possible attempt to access Primary Refresh Token (PRT)

User risk policy: Malicious IP address
- Leaked credentials
- Malicious IP address
- Suspicious browser

NEW QUESTION 266
- (Topic 6)
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Microsoft 365 admin role	Microsoft Exchange Online admin role
User1	Global Administrator	None
User2	Exchange Administrator	None
User3	Service Support Administrator	None
User4	None	Organization Management

You plan to use Exchange Online to manage email for a DNS domain. An administrator adds the DNS domain to the subscription.
The DNS domain has a status of Incomplete setup.
You need to identify which user can complete the setup of the DNS domain. The solution must use the principle of least privilege.
Which user should you identify?

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

Answer: A

NEW QUESTION 271
DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune.
You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

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

Answer Area

| Create a Google account |
| Link the account to Intune |
| Add the app |
| Assign the app |

NEW QUESTION 272
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant.
You configure a device compliance policy as shown in the following exhibit.

Compliance settings Edit

Microsoft Defender ATP

Require the device to be at or under the machine risk score: Low

Device Health

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

System Security

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

Actions for noncompliance Edit

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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

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

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

Rooted devices will be ▼

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

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

Rooted devices will be ▼

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

NEW QUESTION 276
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You plan to deploy a monitoring solution that meets the following requirements:
? Captures Microsoft Teams channel messages that contain threatening or violent language.
? Alerts a reviewer when a threatening or violent message is identified.
What should you include in the solution?

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

Answer: C

NEW QUESTION 280
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

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

All the devices are onboarded To Microsoft Defender for Endpoint
You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:
• Detect operating system vulnerabilities.
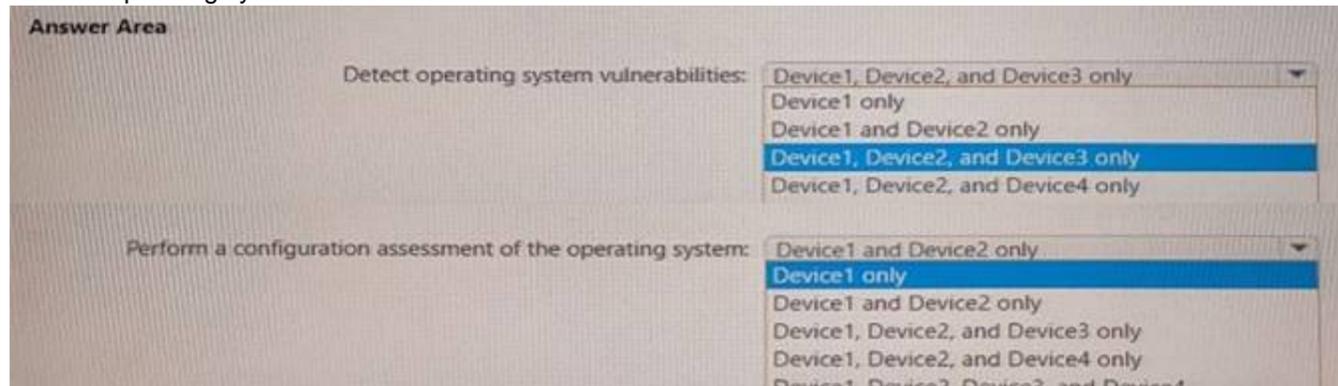
A. Mastered
B. Not Mastered

Answer: A

Explanation:
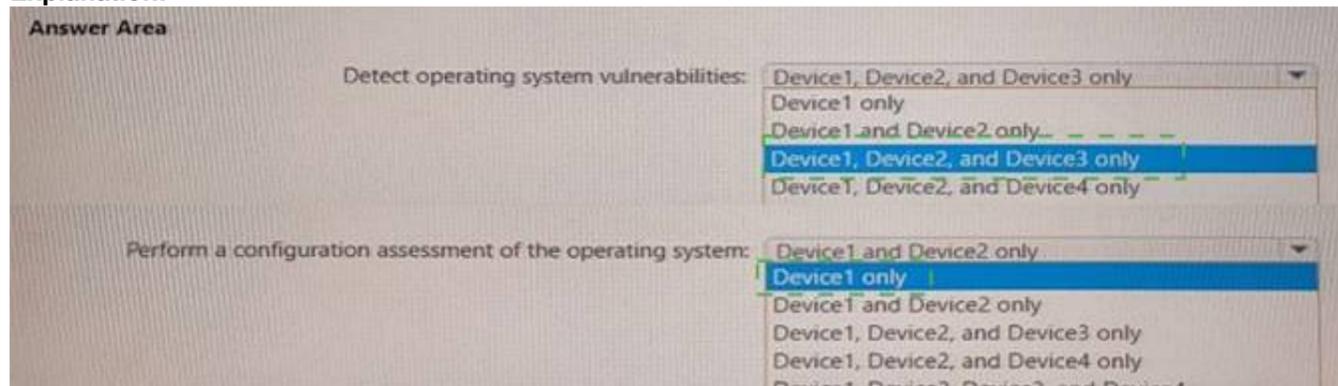
NEW QUESTION 282
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription.
From the Microsoft 365 admin center, you open the Microsoft 365 Apps usage report as shown in the following exhibit.

Username ⓘ	Last activation date (UTC)	Last activity date (UTC)	⊞ Choose columns
431B8D0D1D05D877FDC4416			
2F2747649D4150B686307383			
659213C0E1D99EA1A4AD56D		Wednesday, August 3, 2022	
FE185622F642B0381DB633EC			
988D39ED225FC80FF2A5684			

You need ensure that the report meets the following requirements:
• The Username column must display the actual name of each user.
• Usage of the Microsoft Teams mobile app must be displayed.
What should you modify for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

The Username column must display the actual name of each user: [Reports in Org settings ▼]
- Privacy profile in Org settings
- **Reports in Org settings**
- The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed: [Microsoft Teams in Org settings ▼]
- **Microsoft Teams in Org settings**
- The columns in the report
- The Teams license assignment

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

The Username column must display the actual name of each user: [Reports in Org settings ▼]
- Privacy profile in Org settings
- **Reports in Org settings**
- The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed: [Microsoft Teams in Org settings ▼]
- **Microsoft Teams in Org settings**
- The columns in the report
- The Teams license assignment

NEW QUESTION 286
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 287

- (Topic 6)

You have a Microsoft 365 E5 tenant.

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

What should you do in the Microsoft 365 compliance center?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 288

- (Topic 6)

Your company has an Azure AD tenant named contoso.com that includes the users shown in the following table.

Name	Usage location	Membership
User1	United States	Group1, Group2
User2	Not set	Group2
User3	Not set	Group1
User4	Canada	Group1

Group2isa member of Group1.

You assign an Office 365 Enterprise E3 license to Group1. How many Office 365 E3 licenses are assigned?

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

Answer: C

NEW QUESTION 293

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.

◯ **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.	◯	◯

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 295
- (Topic 6)
Your network contains an Active Directory domain named adatum.com that is synced to Azure AD.
The domain contains 100 user accounts.
The city attribute for all the users is set to the city where the user resides.
You need to modify the value of the city attribute to the three-letter airport code of each city.
What should you do?

A. From Windows PowerShell on a domain controller, run the Gec-ADUser and Sec- ADUser cmdlets.
B. From Azure Cloud Shell, run the Gec-ADUser and Sec-ADUser cmdlets.
C. From Windows PowerShell on a domain controller, run the Gec-MgUser and Updace- MgUser cmdlets.
D. From Azure Cloud Shell, run the Gec-MgUser and Update-MgUser cmdlets.

Answer: A

Explanation:
The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on- premise Active Directory.
You can use Windows PowerShell on a domain controller and run the Get-ADUser cmdlet to get the required users and pipe the results into Set-ADUser cmdlet to modify the city attribute.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
* 1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
* 2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.
Other incorrect answer options you may see on the exam include the following:
* 1. From the Azure portal, select all the Azure AD users, and then use the User settings blade.
* 2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set- AzureADUser cmdlets.
* 3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
* 4. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.
Reference:
https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser

NEW QUESTION 296
- (Topic 6)
You are reviewing alerts in the Microsoft 365 Defender portal. How long are the alerts retained in the portal?

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

Answer: C

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

Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data- retention
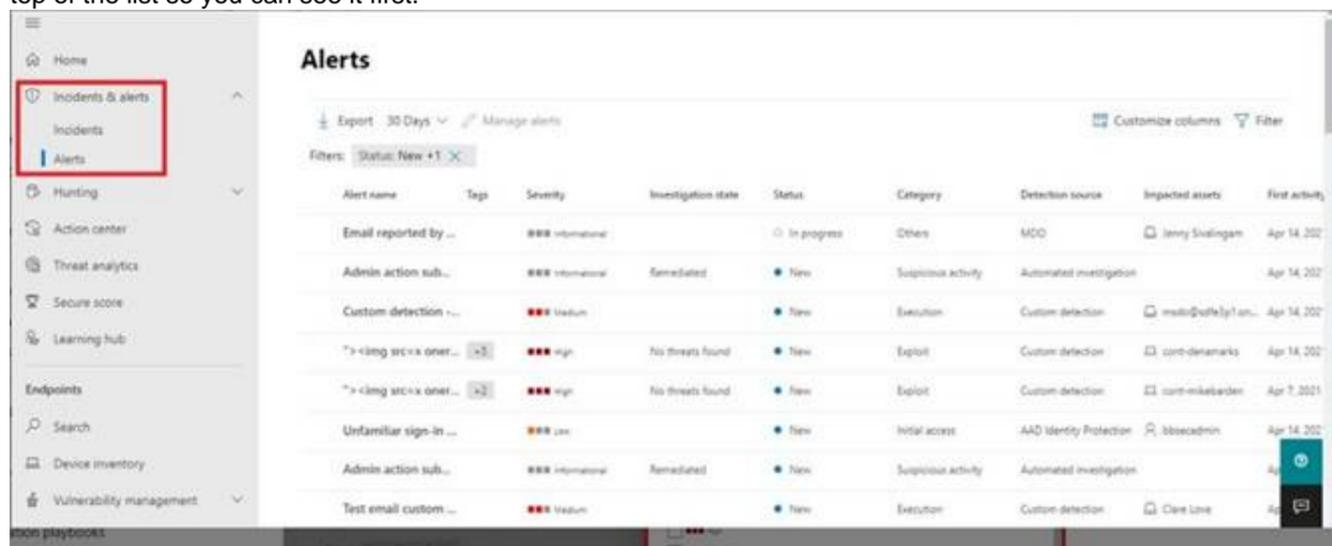
NEW QUESTION 297
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:
? Name: Case1
? Included content: Group1, User1, Site1
? Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders
The investigation for Case1 completes, and you close the case.
What occurs after you close Case1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 298
- (Topic 6)
Your network contains an Active Directory forest named contoso.local. You purchase a Microsoft 365 subscription.
You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months.
You need to prepare for the planned move to Microsoft 365.
What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

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

Answer: D

Explanation:
The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on- premise Active Directory if it's a routable domain name, for example, contoso.com.
If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active Directory.
Incorrect:
Not C: No need to rename the Active Directory forest. As we use a non-routable domain name contoso.local, we just need to add the routable domain name as a UPN suffix in Active Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization

NEW QUESTION 301
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) method registered
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1	None

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.

Enable and Target Configure

Enable

Include Exclude

Target ○ All users ⦿ Select groups

Add groups

Name	Type	Registration	Authentication mode
Group1	Group	Optional	Any
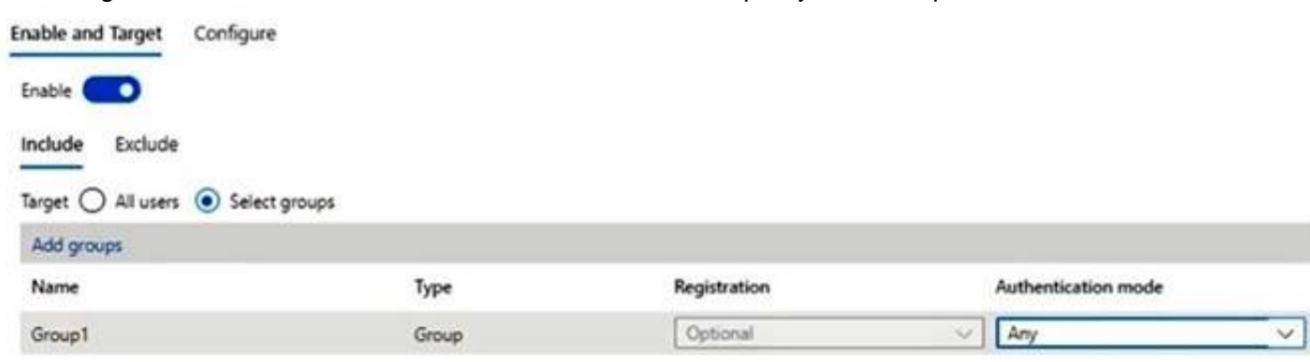
Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.	○	○
User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.	○	○
User3 can use passwordless authentication without further action.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
User1 is member of Group1.
User1 has MFA registered method of Microsoft Authenticater app (push notification) The Microsoft Authenticator authentication method policy is configured for Group1, registration is optional, authentication method is any.
Note: Microsoft Authenticator can be used to sign in to any Azure AD account without using a password. Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology.
This authentication technology can be used on any device platform, including mobile. This technology can also be used with any app or website that integrates with Microsoft Authentication Libraries.
Box 2: No
User2 is member of Group2.
The Microsoft Authenticator authentication method policy is configured for Group1, not for Group2.
Box 3: No
User3 is member of Group1.
User3 has no MFA method registered.
User3 must choose an authentication method.
Note: Enable passwordless phone sign-in authentication methods
Azure AD lets you choose which authentication methods can be used during the sign-in process. Users then register for the methods they'd like to use.

NEW QUESTION 306
- (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 308
- (Topic 6)
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.

Corporate policy states that user passwords must not include the word Contoso. What should you do to implement the corporate policy?

A. From Azure AD Identity Protection, configure a sign-in risk policy.
B. From the Microsoft Entra admin center, create a conditional access policy.
C. From the Microsoft 365 admin center, configure the Password policy settings.
D. From the Microsoft Entra admin center, configure the Password protection settings.

Answer: D

NEW QUESTION 312
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

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

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

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

Answer: C

NEW QUESTION 314
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the labels shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

You have the items shown in the following table.

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

Which items can you view in Content explorer?

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

Answer: C

NEW QUESTION 317
HOTSPOT - (Topic 6)
HOTSPOT
Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.
The domain contains the users shown in the following table.

Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

The domain contains the groups shown in the following table.

Name	Member of	In OU
Group1	*None*	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect.
You configure Domain and OU filtering as shown in the following exhibit.
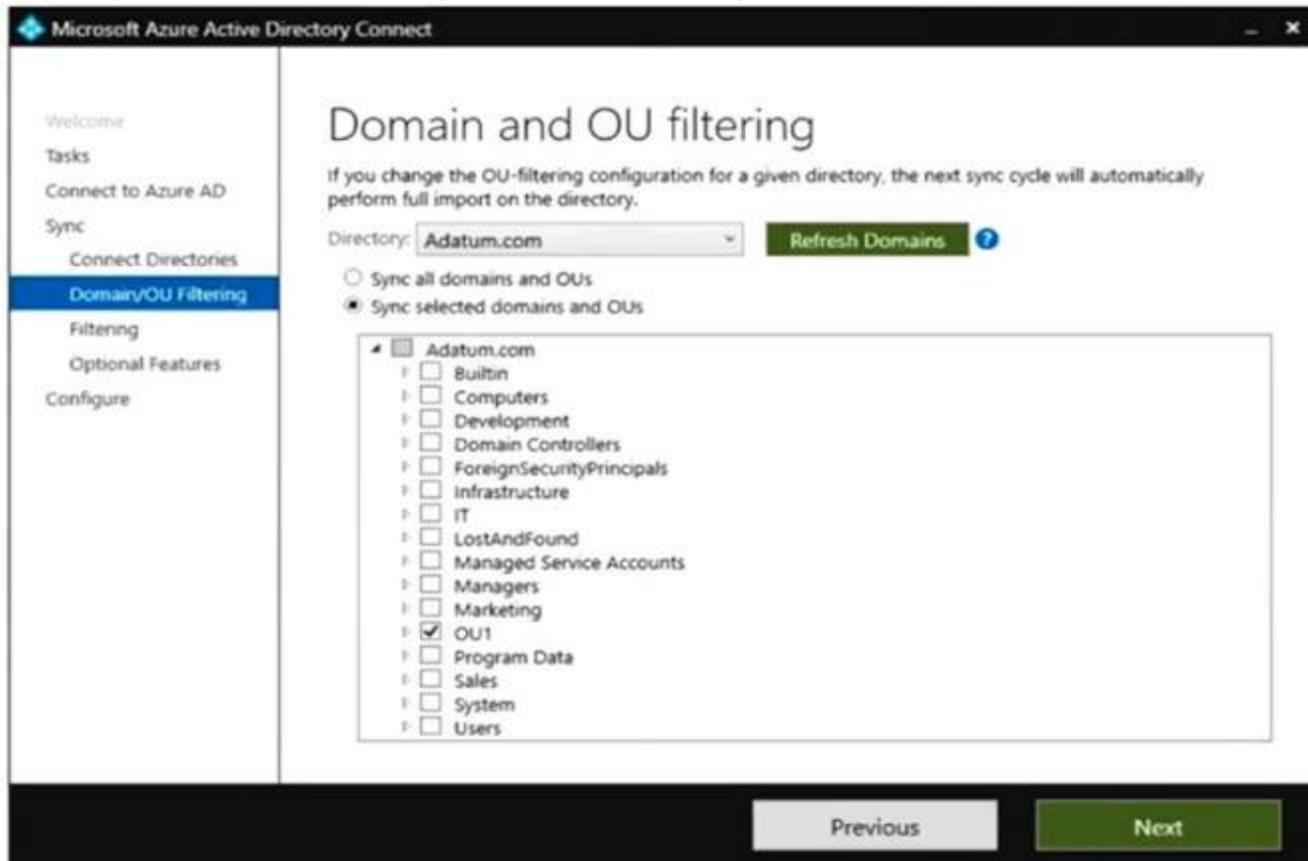
You configure Filter users and devices as shown in the following exhibit.

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 syncs to Azure AD.	⊙	⊙
User2 syncs to Azure AD.	⊙	⊙
Group2 syncs to Azure AD.	⊙	⊙

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	⊙	⊙
User2 syncs to Azure AD.	⊙	⊙
Group2 syncs to Azure AD.	⊙	⊙

NEW QUESTION 318
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

MS-102 Practice Exam Features:

* MS-102 Questions and Answers Updated Frequently

* MS-102 Practice Questions Verified by Expert Senior Certified Staff

* MS-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* MS-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The MS-102 Practice Test Here