

Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam



NEW QUESTION 1

HOTSPOT - (Topic 6)

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

Name	Require BitLocker	Require the device to be at or under the machine risk score
Policy1	Required	High
Policy2	Not configured	Medium
Policy3	Required	Low

The tenant contains the devices shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Microsoft Defender for Endpoint risk status	Policies applied
Device1	Configured	High	Policy1, Policy3
Device2	Not configured	Medium	Policy2, Policy3
Device3	Not configured	Low	Policy1, Policy2

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

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device1 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 2

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to implement identity protection. The solution must meet the following requirements:

- ? Identify when a user's credentials are compromised and shared on the dark web.
- ? Provide users that have compromised credentials with the ability to self-remediate.

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

NOTE: Each correct selection is worth one point.

Answer Area

To identify when users have compromised credentials, configure:

<input type="radio"/> A registration policy
<input type="radio"/> A sign-in risk policy
<input type="radio"/> A user risk policy
<input type="radio"/> A multifactor authentication registration policy

To enable self-remediation, select:

<input type="radio"/> Generate a temporary password
<input type="radio"/> Require multi-factor authentication
<input type="radio"/> Require password change

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: A user risk policy

Identify when a user's credentials are compromised and shared on the dark web.

User risk-based Conditional Access policy

Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:

Block access

Allow access but require a secure password change.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.

Box 2: Require password change

Provide users that have compromised credentials with the ability to self-remediate.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators

NEW QUESTION 3

- (Topic 6)

You have a Microsoft 365 tenant.

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

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

Answer: D

NEW QUESTION 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)

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 copy the Group Policy Administrative Templates from a Windows 10

computer to Server1. Does this meet the goal?

- A. yes
- B. No

Answer: A

NEW QUESTION 6

- (Topic 6)

You have a Microsoft 365 E5 subscription.

On Monday, you create a new user named User1.

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

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

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

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

Answer: C

NEW QUESTION 7

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to compare the current Safe Links configuration to the Microsoft recommended configurations.

What should you use?

- A. Microsoft Purview
- B. Azure AD Identity Protection
- C. Microsoft Secure Score
- D. the configuration analyzer

Answer: C

NEW QUESTION 8

HOTSPOT - (Topic 6)

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

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

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

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

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

You support the management tasks.

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

NOTE: Each correct selection is worth one point.

VPN device configuration profile:

▼

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2 and Device3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

VPN device configuration profile:

▼

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

NEW QUESTION 9

- (Topic 6)
 You have a Microsoft 365 subscription.
 You plan to use Adoption Score and need to ensure that it can obtain device and software metrics.
 What should you do?

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

Answer: A

NEW QUESTION 10

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

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

Answer: D

NEW QUESTION 10

- (Topic 6)
 You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

The policies are assigned to Device1.
 Which policy settings will be applied to Device1?

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

Answer: D

NEW QUESTION 13

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

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 17

- (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-AzureAdLabelSync
- D. Add-UnifiedGroupLinks

Answer: C

NEW QUESTION 21

- (Topic 6)

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.

You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for

10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.

You plan to onboard all the devices to Microsoft Defender for Endpoint. You need to store the Microsoft Defender for Endpoint data in Europe. What should you do first?

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

Answer: B

Explanation:

Storage locations

Understand where Defender for Cloud stores data and how you can work with your data:

* Machine information

- Stored in a Log Analytics workspace.

- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace>

NEW QUESTION 22

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You plan to perform device discovery and authenticated scans of network

devices. You install and register the network scanner on a device named Device1.

What should you do next?

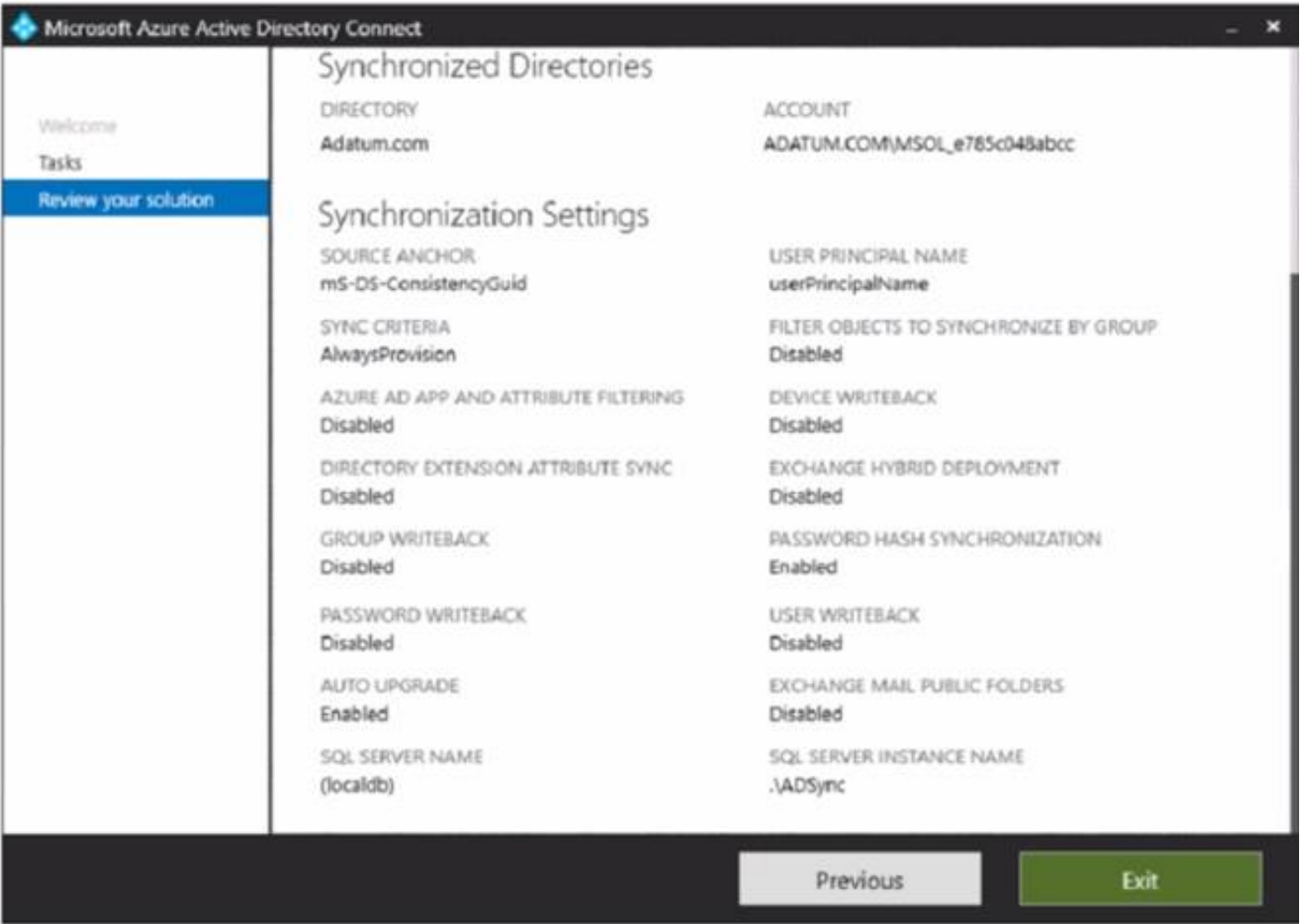
- A. Connect Defender for Endpoint to Microsoft Intune.
- B. Apply for Microsoft Threat Experts - Targeted Attack Notifications.
- C. Create an assessment job.
- D. Download and run an onboarding package.

Answer: C

NEW QUESTION 25

HOTSPOT - (Topic 6)

Your network contains an on-premises Active Directory domain that is synced to Azure AD as shown in the following exhibit.



An on-premises Active Directory user account named Allan Yoo is synchronized to Azure AD. You view Allan's account from Microsoft 365 and notice that his username is set to Allan @>ddatum.onmicrosoft.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
From the Azure portal, you can reset the password of Allan Yoo.	<input type="radio"/>	<input type="radio"/>
From the Azure portal, you can configure the job title of Allan Yoo.	<input type="radio"/>	<input type="radio"/>
From the Azure portal, you can configure the usage location of Allan Yoo.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From the Azure portal, you can reset the password of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>
From the Azure portal, you can configure the job title of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>
From the Azure portal, you can configure the usage location of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 26

- (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 a Microsoft Entra tenant.
Another administrator configures the domain to synchronize to the Microsoft Entra tenant.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.
You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.
Solution: From Microsoft Entra Connect, you modify the filtering settings. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 28

- (Topic 6)
 You have a Microsoft 365 E5 tenant.
 industry regulations require that the tenant comply with the ISO 27001 standard. You need to evaluate the tenant based on the standard

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

Answer: B

NEW QUESTION 32

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

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

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

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

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

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

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

Answer Area

Statements

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

Yes

☒

No

☐

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

☐
☐

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

☐
☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 35

- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it as a result these questions will not appear in the review screen.
Your network contains an Active Directory forest. You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

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

Solution: implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory. Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 36

- (Topic 6)
Your company has on-premises servers and an Azure AD tenant.
Several months ago, the Azure AD Connect Health agent was installed on all the servers. You review the health status of all the servers regularly.
Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect Servers list.
You suspect that another administrator removed Server1 from the list. You need to ensure that you can view the health status of Server1.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. From Azure Cloud shell, run the Connect-Azure AD cmdlet.
- B. From Server1, change the Azure AD Connect Health Services Startup type to Automatic (Delayed Start)
- C. From Server1, change the Azure AD Connect Health Services Startup type to Automatic
- D. From Windows PowerShell, run the Register-AzureADConnectHealthsyncAgent cmdlet.
- E. From Server1, reinstall the Azure AD Connect Health agent

Answer: DE

NEW QUESTION 38

HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:

- ? MDM user scope: Some
- ? uk.co.certification.simulator.questionpool.PList@184e72e0
- ? MAM user scope: Some
- ? uk.co.certification.simulator.questionpool.PList@184e7360

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	<input checked="" type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 42

- (Topic 6)

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

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

- Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources
- Supports the use of Azure AD Identity Protection

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

NOTE: Each correct selection is worth one point.

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

Answer: AB

NEW QUESTION 44

- (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 47

HOTSPOT - (Topic 6)

HOTSPOT

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

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

NEW QUESTION 48
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
Set-ComplianceTag
Set-HoldCompliancePolicy
Set-RetentionCompliancePolicy
Set-RetentionPolicy
Set-RetentionPolicyTag

-Identity "Policy1"

-RestrictiveRetention
-enabled
-Force
-RestrictiveRetention
-RetentionPolicyTagLinks
-SystemTag

\$true

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

Set-RetentionCompliancePolicy
Set-ComplianceTag
Set-HoldCompliancePolicy
Set-RetentionCompliancePolicy
Set-RetentionPolicy
Set-RetentionPolicyTag

-Identity "Policy1"

-RestrictiveRetention
-enabled
-Force
-RestrictiveRetention
-RetentionPolicyTagLinks
-SystemTag

\$true

NEW QUESTION 53
- (Topic 6)

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

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

You need to configure group-based licensing to meet the following requirements:
? To all users, deploy an Office 365 E3 license without the Power Automate license option.
? To all users, deploy an Enterprise Mobility + Security E5 license.
? To the users in the research department only, deploy a Power BI Pro license.
? To the users in the marketing department only, deploy a Visio Plan 2 license.
What is the minimum number of deployment groups required?

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

Answer: C

Explanation:
One for all users, one for the research department, and one for the marketing department.
Note: What are Deployment Groups?
With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers on-premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions

down to the server level.
 Reference:
<https://devblogs.microsoft.com/devops/deployment-groups-is-now-generally-available-sharing-of-targets-and-more>

NEW QUESTION 58

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 Computer1 and Computer2 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 62

HOTSPOT - (Topic 6)

HOTSPOT

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

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

Answer Area

Tool:

AccessChk
Azure AD Connect
Active Directory Explorer
IdFix

Required group membership:

Domain Admins
Domain Users
Server Operators
Enterprise Admins

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Box 1: IdFix

Query and fix invalid object attributes with the IdFix tool

Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft 365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization tools such as Azure AD Connect and Azure AD Connect cloud sync. The focus of IdFix is to enable you to accomplish this task in a simple, expedient fashion.

The IdFix tool provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Windows Server AD forests in preparation for deployment to Microsoft 365. The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow you to successfully synchronize users, contacts, and groups from on-premises Active Directory into Microsoft 365. Note: IdFix might identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be synchronized to the cloud, the product group recommends that these errors be corrected.

Incorrect:

* AccessChk

Box 2: Enterprise Admins

IdFix permissions requirements

The user account that you use to run IdFix must have read and write access to the AD DS domain.

If you aren't sure if your user account meets these requirements, and you're not sure how to check, you can still download and run IdFix. If your user account doesn't have the right permissions, IdFix will simply display an error when you try to run it.

* Enterprise Admins

The Enterprise Admins group exists only in the root domain of an Active Directory forest of domains. The group is a Universal group if the domain is in native mode. The group is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, like adding child domains.

Incorrect:

* Domain Admins

Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that's created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.

* Server Operator

Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer. Any service that accesses the system has the Service identity.

* Domain Users - too few permissions

The Domain Users group includes all user accounts in a domain. When you create a user account in a domain, it's automatically added to this group.

NEW QUESTION 64

- (Topic 6)

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.

Does this meet the goal?

- A. Yes
 B. No

Answer: A

NEW QUESTION 68

- (Topic 6)

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

You enable Azure AD Identity Protection.

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

To which role should you add User1?

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

Answer: A

NEW QUESTION 73

- (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 75

HOTSPOT - (Topic 6)

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

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

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

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

You apply DLP1 to Site1.

Which policy tip is displayed for each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

File1:

Tip2 only

Tip2 only

Tip3 only

Tip2 and Tip3

File2:

Tip1 and Tip2 only

Tip1 only

Tip3 only

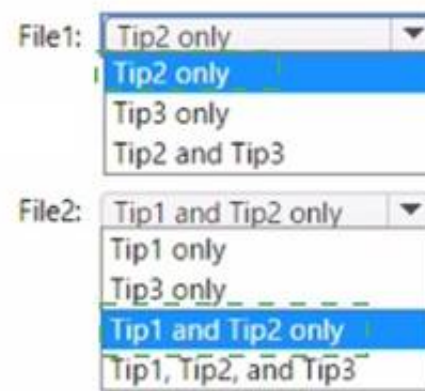
Tip1 and Tip2 only

Tip1, Tip2, and Tip3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 77

- (Topic 6)

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

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

Answer: C

NEW QUESTION 78

- (Topic 6)

You have a Microsoft 365 subscription.

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

Name	Role
User1	Security Administrator
User2	Global Administrator
User3	Service Support Administrator

You configure Tenant properties as shown in the following exhibit.

Technical contact

User1@contoso.com ✓

Global privacy contact

✓

Privacy statement URL

http://contoso.com/privacy ✓

Which users will be contacted by Microsoft if the tenant experiences a data breach?

- A. User1 only
- B. User2 only
- C. User3 only
- D. User1 and User2 only
- E. User2 and User3 only

Answer: B

Explanation:

Microsoft 365 is committed to notifying customers within 72 hours of breach declaration.

The customer's tenant administrator will be notified.

Reference:

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365>

NEW QUESTION 81

HOTSPOT - (Topic 6)

You have a Microsoft 365 Enterprise E5 subscription.

You add a cloud-based app named App1 to the Azure AD enterprise applications list.

You need to ensure that two-step verification is enforced for all user accounts the next time they connect to App1.

Which three settings should you configure from the policy? To answer, select the appropriate settings in the answer area.

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

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Name *

App1 policy

Assignments

Users or workload identities ⓘ
All users

Cloud apps or actions ⓘ
No cloud apps, actions, or authentication contexts selected

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 controls selected

Session ⓘ
0 controls selected

Enable policy

Report-only On Off

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.
[Learn more](#)

What does this policy apply to?

Users and groups

Include

Exclude

☐ None

☒ All users

☐ Select users and groups

⚠ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

App1 policy

Assignments

Users or workload identities

All users

Cloud apps or actions

No cloud apps, actions, or authentication contexts selected

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Enable policy

Report-only On Off

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

What does this policy apply to?

Users and groups

Include Exclude

☐ None

☒ All users

☐ Select users and groups

Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

NEW QUESTION 83

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription and an Azure AD tenant named contoso.com.

All users have computers that run Windows 11, are joined to contoso.com, and are protected by using BitLocker Drive Encryption (BitLocker).

You plan to create a user named Admin1 that will perform following tasks:

- View BitLocker recovery keys.
- Configure the usage location for the users in contoso.com.

You need to assign roles to Admin1 to meet the requirements. The solution must use the principle of least privilege. Which two roles should you assign? To answer, select the appropriate roles in the answer area.

NOTE: Each correct selection is worth one point

Answer Area

Devices

- ☐ Cloud Device Administrator ⓘ
- ☐ Desktop Analytics Administrator ⓘ
- ☐ Intune Administrator ⓘ
- ☐ Printer Administrator ⓘ
- ☐ Printer Technician ⓘ
- ☐ Windows 365 Administrator ⓘ

Global

- ☐ Global Administrator ⓘ

Identity

- ☐ Application Administrator ⓘ
- ☐ Application Developer ⓘ
- ☐ Authentication Administrator ⓘ
- ☐ Cloud Application Administrator ⓘ
- ☐ Conditional Access Administrator ⓘ
- ☐ Domain Name Administrator ⓘ
- ☐ External Identity Provider Administrator ⓘ
- ☐ Guest Inviter ⓘ
- ☐ Helpdesk Administrator ⓘ
- ☐ Hybrid Identity Administrator ⓘ
- ☐ License Administrator ⓘ
- ☐ Password Administrator ⓘ

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Devices

- ☐ Cloud Device Administrator ⓘ
- ☐ Desktop Analytics Administrator ⓘ
- ☐ Intune Administrator ⓘ
- ☐ Printer Administrator ⓘ
- ☐ Printer Technician ⓘ
- ☐ Windows 365 Administrator ⓘ

Global

- ☐ Global Administrator ⓘ

Identity

- ☐ Application Administrator ⓘ
- ☐ Application Developer ⓘ
- ☐ Authentication Administrator ⓘ
- ☐ Cloud Application Administrator ⓘ
- ☐ Conditional Access Administrator ⓘ
- ☐ Domain Name Administrator ⓘ
- ☐ External Identity Provider Administrator ⓘ
- ☐ Guest Inviter ⓘ
- ☐ Helpdesk Administrator ⓘ
- ☐ Hybrid Identity Administrator ⓘ
- ☐ License Administrator ⓘ
- ☐ Password Administrator ⓘ

NEW QUESTION 84

- (Topic 6)

You have a Microsoft 365 E5 subscription.

Conditional Access is configured to block high-risk sign-ins for all users.

All users are in France and are registered for multi-factor authentication (MFA). Users in the media department will travel to various countries during the next month.

You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention.

What should you configure?

- A. an exclusion group
- B. the MFA registration policy
- C. named locations
- D. self-service password reset (SSPR)

Answer: D

Explanation:

Self-remediation with self-service password reset

If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock>

NEW QUESTION 89

- (Topic 6)

You have a Microsoft 365 subscription that uses Security & Compliance retention policies.

You implement a preservation lock on a retention policy that is assigned to all executive users.

Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point?

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

Answer: AB

NEW QUESTION 90

DRAG DROP - (Topic 6)

Your company has an Azure AD tenant named contoso.onmicrosoft.com.
You purchase a domain named contoso.com from a registrar and add all the required DNS records.
You create a user account named User1. User1 is configured to sign in as user1@contoso.onmicrosoft.com.
You need to configure User1 to sign in as user1@contoso.com.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Run update-igDomain -DomainId contoso.com.

Modify the email address of User1.

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

Add a custom domain name.

Verify the custom domain.

Modify the username of User1.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Run update-igDomain -DomainId contoso.com.

Modify the email address of User1.

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

Add a custom domain name.

Verify the custom domain.

Modify the username of User1.

Answer Area

Add a custom domain name.

Verify the custom domain.

Modify the username of User1.

NEW QUESTION 92

- (Topic 6)

You have a Microsoft 365 E5 tenant.
You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.
Which two policies can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 93

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 subscription That contains the domains shown in the following exhibit.

Domains

+

Add domain

🛒

Buy domain

🔄

Refresh

Domain name ↑	Status	Choose columns
<input type="checkbox"/> contoso221018.onmicrosoft.com (Default)	🟢 Healthy	
<input type="checkbox"/> contoso.com	ⓘ Incomplete setup	
<input type="checkbox"/> east.contoso221018.onmicrosoft.com	ⓘ No services selected	

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

Answer Area

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

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

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

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

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

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

NEW QUESTION 94

HOTSPOT - (Topic 6)

Your company uses Microsoft Defender for Endpoint.
 The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

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

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

- Triggering IOC: Any IOC
- Action: Hide alert
- Suppression scope: Alerts on ATP1 device group

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

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 97

- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role.
Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to assign the Security Administrator role. Reference:
<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp>

NEW QUESTION 99

- (Topic 6)
You have a Microsoft 365 E5 tenant. You configure sensitivity labels.
Users report that the Sensitivity button is unavailability in Microsoft Word for the web. The sensitivity button is available in Word for Microsoft 365.
You need to ensure that the users can apply the sensitivity labels when they use Word for the web.
What should you do?

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

Answer: B

NEW QUESTION 101

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

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

Answer: D

NEW QUESTION 106

- (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 110

HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.
You deploy a third-party antivirus solution to the devices.
You need to ensure that the devices are marked as compliant.
Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Windows 10 compliance policy

Windows 10 and later

Encryption

Encryption of data storage on device

Require

Not configured

Device Security

Firewall

Require

Not configured

Trusted Platform Module (TPM)

Require

Not configured

Antivirus

Require

Not configured

Antispyware

Require

Not configured

Defender

Microsoft Defender Antimalware

Require

Not configured

Microsoft Defender Antimalware minimum version

Not configured

Microsoft Defender Antimalware security intelligence up-to-date

Require

Not configured

Real-time protection

Require

Not configured

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Windows 10 compliance policy

Windows 10 and later

Encryption

Encryption of data storage on device

Require

Not configured

Device Security

Firewall

Require

Not configured

Trusted Platform Module (TPM)

Require

Not configured

Antivirus

Require

Not configured

Antispyware

Require

Not configured

Defender

Microsoft Defender Antimalware

Require

Not configured

Microsoft Defender Antimalware minimum version

Not configured

Microsoft Defender Antimalware security intelligence up-to-date

Require

Not configured

Real-time protection

Require

Not configured

NEW QUESTION 114

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table. User1 reports that after sending 1,000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:

- Which administrators can unblock User1
- What to configure to allow User1 to send at least 2,000 emails per day without being blocked

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

Answer Area

Administrators:

Admin2 only

Admin1 only

Admin2 only

Admin1 and Admin2 only

Admin2 and Admin3 only

Admin1, Admin2, and Admin3

Settings:

Anti-spam

Anti-spam

Anti-phishing

Anti-malware

Advanced delivery

Enhanced filtering

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Administrators:

Admin2 only

Admin1 only

Admin2 only

Admin1 and Admin2 only

Admin2 and Admin3 only

Admin1, Admin2, and Admin3

Settings:

Anti-spam

Anti-spam

Anti-phishing

Anti-malware

Advanced delivery

Enhanced filtering

NEW QUESTION 118

HOTSPOT - (Topic 6)

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

You implement directory synchronization for all 10,000 users in the organization. You automate the creation of 100 new user accounts. You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible. Which command should you run? To answer, select the appropriate options in the answer area.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 122

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview policies to meet the following requirements: Identify documents that are stored in Microsoft Teams and SharePoint that contain

Personally Identifiable Information (PII). Report on shared documents that contain PII. What should you create?

- A. a data loss prevention (DLP) policy
- B. a retention policy
- C. an alert policy
- D. a Microsoft Defender for Cloud Apps policy

Answer: A

Explanation:

Demonstrate data protection

Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.

There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.

In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.

? From the Security & Compliance tab of your browser, click Home.

? Click Data loss prevention > Policy.

? Click + Create a policy.

? In Start with a template or create a custom policy, click Custom > Custom policy > Next.

? In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b. Description: Protect the personally identifiable information of European citizens

? Etc.

Reference:

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-test-environment>

NEW QUESTION 125

- (Topic 6)

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

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

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

What should you include in the recommendation?

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

Answer: D

NEW QUESTION 128

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 133

- (Topic 6)

You have a Microsoft 365 subscription.

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

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

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

Answer: C

Explanation:

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

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

Note: You can add the following types of groups:

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

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

Note:

Security groups

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

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

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

Security groups can be added to a team.

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

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

Reference:

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

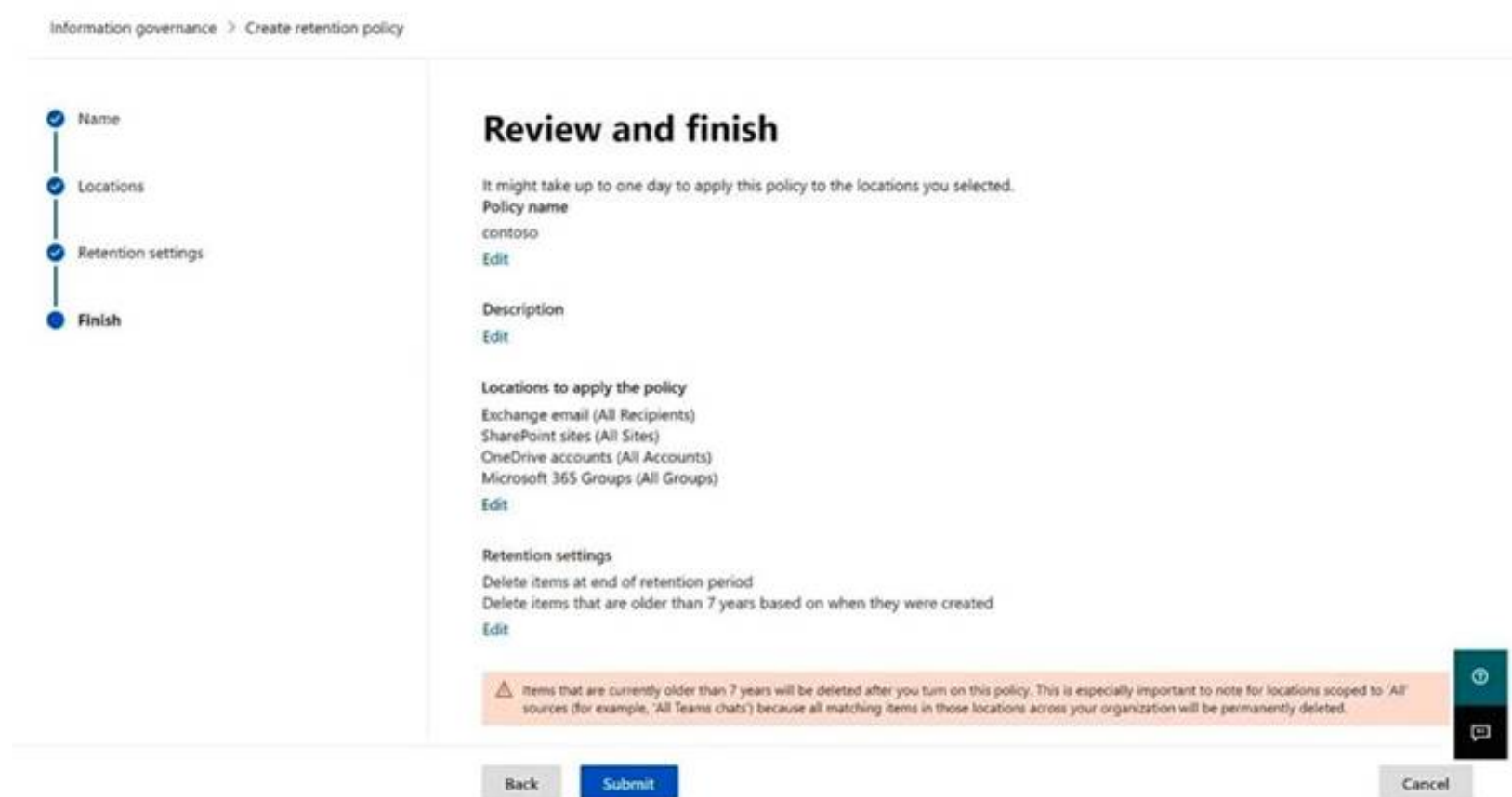
NEW QUESTION 134

HOTSPOT - (Topic 6)

HOTSPOT

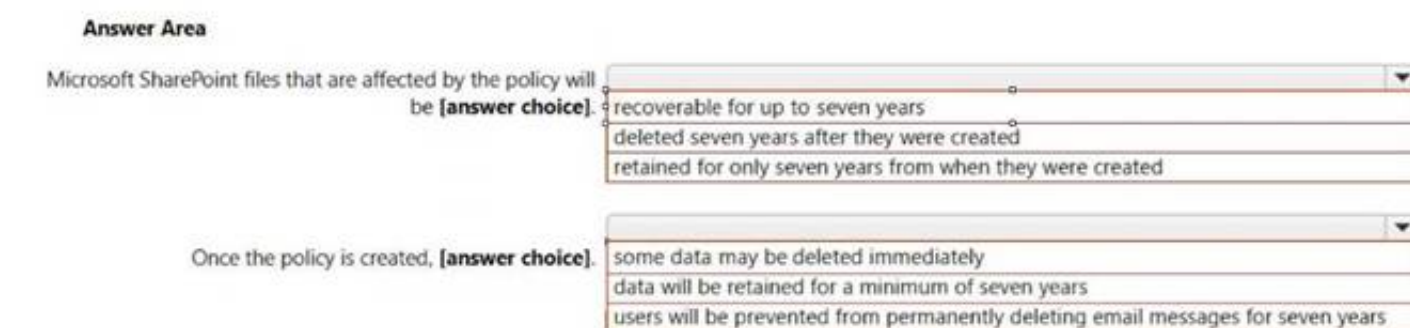
You have a Microsoft 365 tenant.

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



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

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

The retention policy applies to SharePoint sites.

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

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

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

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

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

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

NEW QUESTION 135

- (Topic 6)

Your company has a Microsoft 365 E5 subscription.
 Users in the research department work with sensitive data.
 You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents.
 Users in other departments must not be restricted.
 What should you do?

- A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
- B. Modify the safe links policy Global settings.
- C. Create a data loss prevention (DLP) policy that has a Content contains condition.
- D. Create a new safe links policy.

Answer: D

Explanation:

Use the Microsoft 365 Defender portal to create Safe Links policies
 In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies & Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use <https://security.microsoft.com/safelinksv2>.
 * 1. On the Safe Links page, select Create to start the new Safe Links policy wizard.
 * 2. On the Name your policy page, configure the following settings: Name: Enter a unique, descriptive name for the policy.
 Description: Enter an optional description for the policy.
 * 3. When you're finished on the Name your policy page, select Next.
 * 4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions):
 Users: The specified mailboxes, mail users, or mail contacts.
 *-> Groups:
 Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren't supported).
 The specified Microsoft 365 Groups.
 Domains: All recipients in the specified accepted domains in your organization. Etc.
 Reference:
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure>

NEW QUESTION 140

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.

Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 141

HOTSPOT - (Topic 6)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Devices that can onboarded to Microsoft Defender for Endpoint:

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

Endpoint security policies that must be configured:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, table Description automatically generated with medium confidence

NEW QUESTION 143

- (Topic 6)

You have a Microsoft 365 E5 subscription that contains the following user:

- ? Name: User1
- ? UPN: user1@contoso.com
- ? Email address: user1@marketing.contoso.com
- ? MFA enrollment status: Disabled

When User1 attempts to sign in to Outlook on the web by using the user1@marketing.contoso.com email address, the user cannot sign in.

You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com.
What should you do?

- A. Assign an MFA registration policy to User1.
- B. Reset the password of User1.
- C. Add an alternate email address for User1.
- D. Modify the UPN of User1.

Answer: D

Explanation:

Microsoft’s recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN’s to match.

Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user's email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only needs to remember a single name.

Configure the Azure AD multifactor authentication registration policy

Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.

Reference:

<https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname>

NEW QUESTION 146

HOTSPOT - (Topic 6)

You have a Microsoft 365 ES tenant.

You have the alerts shown in the following exhibit.

View alerts

Export

Filter

<div></div>	Severity	Alert name	Status	Tags	Category	Activity count	Last occurrence...
<div><div></div><div></div></div>	<div><div></div>Medium</div>	Alert1	Active	-	Threat management	2	3 minutes ago
<div><div></div><div></div></div>	<div><div></div>High</div>	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 149

HOTSPOT - (Topic 6)

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

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

You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email. You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2. Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Users who can assign Retention1:

▼

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

Users who can assign Retention2:

▼

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Users who can assign Retention1:

▼

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

Users who can assign Retention2:

▼

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

NEW QUESTION 150
 HOTSPOT - (Topic 6)
 HOTSPOT

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

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

You have the apps shown in the following table.

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

You plan to use Microsoft Endpoint Manager to manage the apps for the users.
 For each of the following statements, select Yes if the statement is true. Otherwise, select No.
 NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 152

- (Topic 6)
 You have an Azure AD tenant.
 You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD. You purchase a Microsoft 365 E3 subscription.
 You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort.
 What should you do?

- A. From the Microsoft Endpoint Manager admin center, create a Windows Autopilot deployment 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 156

HOTSPOT - (Topic 6)
 Your company has a Microsoft 365 E5 tenant.
 Users at the company use the following versions of Microsoft Office:
 • Microsoft 365 Apps for enterprise

- Office for the web
- Office 2016
- Office 2019

The company currently uses the following Office file types:

- .docx
- .xlsx
- .doc
- xls

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

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

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

Answer Area

Office versions that require an add-in to support the sensitivity labels:

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

Office file types that support the sensitivity labels:

- .docx and .xlsx
- .doc only
- .docx only
- .xls only
- .xlsx only
- .doc and .xls
- .docx and .xlsx

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Office versions that require an add-in to support the sensitivity labels:

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

Office file types that support the sensitivity labels:

- .docx and .xlsx
- .doc only
- .docx only
- .xls only
- .xlsx only
- .doc and .xls
- .docx and .xlsx

NEW QUESTION 161

- (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-ADSyncConnectorAttributeInclusion cmdlet.
- C. From PowerShell, run the start-ADSyncSyncCycle cmdlet.
- D. From the Microsoft Azure AD Connect wizard, select Manage federation.

Answer: A

NEW QUESTION 165

- (Topic 4)

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project.

Which DNS record should you recommend?

- A. host (A)
- B. host information
- C. text (TXT)
- D. alias (CNAME)

Answer: D

Explanation:

When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.

Note:

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

Text (TXT)

Mail exchanger (MX)

incorrect answer options you may see on the exam include the following: alias (CNAME)

Host (A) host (AAA)

Pointer (PTR) Name Server (NS)

host information (HINFO) pointer (PTR)

Reference:

<https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider>

NEW QUESTION 169

- (Topic 4)

Which role should you assign to User1?

Available Choices (select all choices that are correct)

A. Hygiene Management

B. Security Reader

C. Security Administrator

D. Records Management

Answer: C

Explanation:

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

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

Reference:

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

NEW QUESTION 173

- (Topic 3)

You create the planned DLP policies.

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

A. From the Microsoft 365 security center, configure an alert policy.

B. From the Microsoft Endpoint Manager admin center, configure a custom notification.

C. From the Microsoft 365 admin center, configure a Briefing email.

D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 175

HOTSPOT - (Topic 3)

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

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

NOTE: Each correct selection is worth one point.

Answer Area



The screenshot shows the 'Policy type' dropdown menu with 'Retention' selected. Below it, the 'Number of required policies' dropdown menu is set to '2'.

Policy type: Retention

Label

Retention

Auto-labeling

Number of required policies: 2

1

2

3

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy type:

Retention

Label

Retention

Auto-labeling

Number of required policies:

2

1

2

3

NEW QUESTION 178

- (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 180

HOTSPOT - (Topic 3)
You plan to implement the endpoint protection device configuration profiles to support the planned changes.
You need to identify which devices will be supported, and how many profiles you should implement.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Supported devices:

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2, and Device3

Device1, Device4, and Device5

Device1, Device2, Device3, Device4, and Device5

Number of required profiles:

1

2

3

4

5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Supported devices:

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

Number of required profiles:

1
2
3
4
5

NEW QUESTION 183

- (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 185

DRAG DROP - (Topic 2)

You need to meet the requirement for the legal department.

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

Actions	Answer Area
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References: <https://www.sherweb.com/blog/ediscovery-office-365/>

NEW QUESTION 190

- (Topic 2)

Which report should the New York office auditors view?

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

Answer: C

Explanation:

References:

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

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

NEW QUESTION 193

- (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 194

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that.

You need to identify whenever a sensitivity label is applied, changed, or removed within the subscription.

Which feature should you use, and how many days will the data be retained? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Answer Area

Feature:

Number of days the data will be retained:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Feature:

Number of days the data will be retained:

NEW QUESTION 197

- (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 201

- (Topic 6)

You have a Microsoft 365 E5 tenant.

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

You need to export the existing template.
Which file format should you use for the exported template?

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

Answer: B

Explanation:

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

NEW QUESTION 204

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

Policy1

Edit policyDelete 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 208

- (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 210

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

Name	Members
AU1	User1, User2
AU2	User3

You have the following users:
? A user named User1 that is assigned the Password Administrator for AU1 and AU2.
? A user named User2 that is assigned the User Administrator for AU1.
? A user named User3 that is assigned the User Administrator for the tenant.
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

User1 can reset the password of User3.

Yes

☐

No

☐

User2 can update the display name of User1.

☐☐

User1 can reset the password of User2.

☐☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

User1 is assigned the Password Administrator for AU1 and AU2. User3 is in AU2. User3 is User Administrator. Password administrators cannot reset User Administrators passwords.

Note: Password Administrator

Users with this role have limited ability to manage passwords. This role does not grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user's password depends on the role the user is assigned.

Role that password can be reset	Password Admin	Helpdesk Admin	Auth Admin	User Admin	Privileged Auth Admin	Global Admin
User Admin				✓	✓	✓
Usage Summary Reports Reader		✓	✓	✓	✓	✓

Box 2: Yes

Box 3: No

User1 is assigned the Password Administrator for AU1 and AU2. User2 is in AU1. User2 is User Administrator. Password administrators cannot reset User Administrators passwords.

Note: User Administrator

Can manage all aspects of users and groups, including resetting passwords for limited admins.

NEW QUESTION 214

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 tenant.

You need to create a custom Compliance Manager assessment template.

Which application should you use to create the template, and in which file format should the template be saved? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Application:

Microsoft Excel

Microsoft Forms

Microsoft Word

Visual Studio Code

File format:

csv

dbx

docx

dotx

json

xlsx

xltx

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Application:

Microsoft Excel

Microsoft Forms

Microsoft Word

Visual Studio Code

File format:

csv

dbx

docx

dotx

json

xlsx

xltx

NEW QUESTION 216

- (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.

Home

Incidents & alerts

Incidents

Alerts

Hunting

Action center

Threat analytics

Secure score

Learning hub

Endpoints

Search

Device inventory

Vulnerability management

Alerts

Export 30 Days

Manage alerts

Customize columns

Filter

Filters: Status: New +1

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity
Email reported by ...		Informational		In progress	Others	MDO	Jenny Sivalingam	Apr 14, 2021
Admin action sub...		Informational	Remediated	New	Suspicious activity	Automated investigation		Apr 14, 2021
Custom detection ...		Medium		New	Execution	Custom detection	madr@office365...	Apr 14, 2021
"> <img src=x oner...	5	High	No threats found	New	Exploit	Custom detection	cont-denemark	Apr 14, 2021
"> <img src=x oner...	2	High	No threats found	New	Exploit	Custom detection	cont-mikebarden	Apr 7, 2021
Unfamiliar sign-in ...		Low		New	Initial access	AAD Identity Protection	bbocadmin	Apr 14, 2021
Admin action sub...		Informational	Remediated	New	Suspicious activity	Automated investigation		Apr 14, 2021
Test email custom ...		Medium		New	Execution	Custom detection	Clare Lane	Apr 14, 2021

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

NEW QUESTION 221

HOTSPOT - (Topic 6)

HOTSPOT

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

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

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

Answer Area

(user.userType

-eq "Guest"

-in "Guest"

-ne "Guest"

-notmatch "Member"

) and (user.department

-contains "Support"

-in "Support"

-match "Support"

-startsWith "Sup"

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: -eq "Guest"
Dynamic membership rules for groups in Azure Active Directory
Supported expression operators
The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.

- * Equals
- eq
- * Contains
- contains
- * Etc.

Box 2: -contains "Support" Incorrect:

- * -in

If you want to compare the value of a user attribute against multiple values, you can use the -in or -notIn operators.

NEW QUESTION 226

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

Answer Area

Policy type:

Alert

Threat

Compliance

Role:

Quarantine

Security Administrator

Organization Configuration

Communication Compliance Admin

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy type:

Alert

Threat

Compliance

Role:

Quarantine

Security Administrator

Organization Configuration

Communication Compliance Admin

NEW QUESTION 229

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

Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.

Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress.

Yes

No

Show time limit error when installation takes longer than specified number of minutes.

60

Show custom message when time limit error occurs.

Yes

No

Allow users to collect logs about instalattion errors.

Yes

No

Only show page to devices provisioned by out-of-box experience (OOBE)

Yes

No

Block device use until all apps and profiles are installed

Yes

No

You assign the policy to Group1.
 You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input checked="" type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 234
 HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

All corporate Windows 11 devices are managed by using Microsoft Intune and onboarded to Microsoft Defender for Endpoint.

You need to meet the following requirements:

- * View an assessment of the device configurations against the Center for Internet Security (CIS) v1.0.0 benchmark.
- Protect a folder named C:\Folder1 from being accessed by untrusted applications on the devices.

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

Answer Area

To view the device configuration assessment:

- Create a baseline assessment profile.
- Add a connected application.
- Create a baseline assessment profile.
- Filter the Vulnerable devices report.

To protect C:\Folder1, enable:

- Controlled folder access.
- Controlled folder access
- Exploit protection
- Removable storage protection

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

To view the device configuration assessment:

- Create a baseline assessment profile.
- Add a connected application.
- Create a baseline assessment profile.
- Filter the Vulnerable devices report.

To protect C:\Folder1, enable:

- Controlled folder access.
- Controlled folder access
- Exploit protection
- Removable storage protection

NEW QUESTION 238

- (Topic 6)

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

You need to ensure that User1 can search the Microsoft 365 audit logs from the Security & Compliance admin center.

Which role should you assign to User1?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 240

- (Topic 6)

Your company has a Microsoft 365 subscription.

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

What should you use?

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

Answer: D

Explanation:

Microsoft 365 Reports in the admin center

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

Which activity reports are available in the admin center

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

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

Reference:

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

NEW QUESTION 242

- (Topic 6)

You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.

You have the devices shown in the following table.

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

You plan to enable co-management.

You need to identify which devices support co-management without requiring the installation of additional software.

Which devices should you identify?

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

Answer: D

NEW QUESTION 247

- (Topic 6)

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

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

Answer: C

NEW QUESTION 248

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

MS-102 Practice Exam Features:

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

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