

Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator



NEW QUESTION 1

HOTSPOT

You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.

Which other settings should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Set the frequency to:

| | |
|----------|---|
| One time | v |
| Weekly | |
| Monthly | |

To ensure that access is removed if an administrator fails to respond, configure the:

| | |
|--------------------------|---|
| Upon completion settings | v |
| Advanced settings | |
| Programs | |
| Reviewers | |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Set the frequency to:

| | |
|----------|---|
| One time | v |
| Weekly | |
| Monthly | |

To ensure that access is removed if an administrator fails to respond, configure the:

| | |
|--------------------------|---|
| Upon completion settings | v |
| Advanced settings | |
| Programs | |
| Reviewers | |

NEW QUESTION 2

HOTSPOT

You install Azure ATP sensors on domain controllers.

You add a member to the Domain Admins group. You view the timeline in Azure ATP and discover that information regarding the membership change is missing.

You need to meet the security requirements for Azure ATP reporting.

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

Policy to edit:

| | |
|---|---|
| | ▼ |
| Default Domain Controllers Policy | |
| Default Domain Policy | |
| A local policy on one domain controller | |

Audit setting to configure:

| | |
|---------------------------------------|---|
| | ▼ |
| Audit User Account Management | |
| Audit Computer Account Management | |
| Audit Other Account Management Events | |
| Audit Security Group Management | |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-advanced-audit-policy>

NEW QUESTION 3

You need to create Group2.

What are two possible ways to create the group?

- A. an Office 365 group in the Microsoft 365 admin center
- B. a mail-enabled security group in the Microsoft 365 admin center
- C. a security group in the Microsoft 365 admin center
- D. a distribution list in the Microsoft 365 admin center
- E. a security group in the Azure AD admin center

Answer: CE

NEW QUESTION 4

You need to implement Windows Defender ATP to meet the security requirements. What should you do?

- A. Configure port mirroring
- B. Create the ForceDefenderPassiveMode registry setting
- C. Download and install the Microsoft Monitoring Agent
- D. Run WindowsDefenderATPOnboardingScript.cmd

Answer: C

Explanation:

Case Study: 3 Contoso, Ltd Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, and New York.

The company has the offices shown in the following table.

| Location | Employees | Laptops | Desktops computers | Mobile devices |
|----------|-----------|---------|--------------------|----------------|
| Montreal | 2,500 | 2,800 | 300 | 3,100 |
| Seattle | 1,000 | 1,100 | 200 | 1,500 |
| New York | 300 | 320 | 30 | 400 |

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise. Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

| Location | IP address space | Public NAT segment |
|----------|------------------|--------------------|
| Montreal | 10.10.0.0/16 | 190.15.1.0/24 |
| Seattle | 172.16.0.0/16 | 194.25.2.0/24 |
| New York | 192.168.0.0/16 | 198.35.3.0/24 |

Named locations are defined in Azure AD as shown in the following table.

| Name | IP address range | Trusted |
|----------|------------------|---------|
| Montreal | 10.10.0.0/16 | Yes |
| New York | 192.168.0.0/16 | No |

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department. The tenant contains the users shown in the following table.

| Name | User type | City | Role |
|-------|-----------|----------|----------------------------------|
| User1 | Member | Seattle | None |
| User2 | Member | Sea | Password administrator |
| User3 | Member | SEATTLE | None |
| User4 | Guest | SEA | None |
| User5 | Member | London | None |
| User6 | Member | London | Customer LockBox Access Approver |
| User7 | Member | Sydney | Reports reader |
| User8 | Member | Sydney | User administrator |
| User9 | Member | Montreal | None |

The tenant contains the groups shown in the following table.

| Name | Group type | Dynamic membership rule |
|----------|------------|--------------------------|
| ADGroup1 | Security | User.city-contains "SEA" |
| ADGroup2 | Office 365 | User.city-match "Sea" |

Customer Lockbox is enabled in Microsoft 365. Microsoft Intune Configuration

The devices enrolled in Intune are configured as shown in the following table.

| Name | Platform | Encryption | Member of |
|---------|------------|----------------|----------------|
| Device1 | Android | Disabled | GroupA, GroupC |
| Device2 | Windows 10 | Enabled | GroupB, GroupC |
| Device3 | Android | Disabled | GroupB, GroupC |
| Device4 | Windows 10 | Disabled | GroupB |
| Device5 | iOS | Not applicable | GroupA |
| Device6 | Windows 10 | Enabled | None |

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

| Name | Platform | Encryption | Assigned |
|---------------|------------|----------------|----------|
| DevicePolicy1 | Android | Not configured | Yes |
| DevicePolicy2 | Windows 10 | Required | Yes |
| DevicePolicy3 | Android | Required | Yes |

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

| Name | Include | Exclude |
|---------------|---------|---------|
| DevicePolicy1 | GroupC | None |
| DevicePolicy2 | GroupB | GroupC |
| DevicePolicy3 | GroupA | None |

The Mark devices with no compliance policy assigned as setting is set to Compliant.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

- Use the principle of least privilege
- Enable User1 to assign the Reports reader role to users
- Ensure that User6 approves Customer Lockbox requests as quickly as possible
- Ensure that User9 can implement Azure AD Privileged Identity Management

NEW QUESTION 5

Which user passwords will User2 be prevented from resetting?

- A. User6 and User7
- B. User4 and User6
- C. User4 only
- D. User7 and User8
- E. User8 only

Answer: C

NEW QUESTION 6

Which role should you assign to User1?

- A. Global administrator
- B. User administrator
- C. Privileged role administrator
- D. Security administrator

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access-to-pim>

NEW QUESTION 7

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

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

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

| Name | Role |
|-------|----------------------------------|
| User1 | Compliance Manager Contributor |
| User2 | Compliance Manager Assessor |
| User3 | Compliance Manager Administrator |
| User4 | Portal Admin |

You discover that all the users in the subscription can access Compliance Manager reports. The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend assigning the Compliance Manager Reader role to User1. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 8

Note: This question is part of 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 is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution: You modify the Password Hash Synchronization settings.

Does that meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps>

NEW QUESTION 9

Note: This question is part of 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 is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution: You modify the Source Anchor settings.

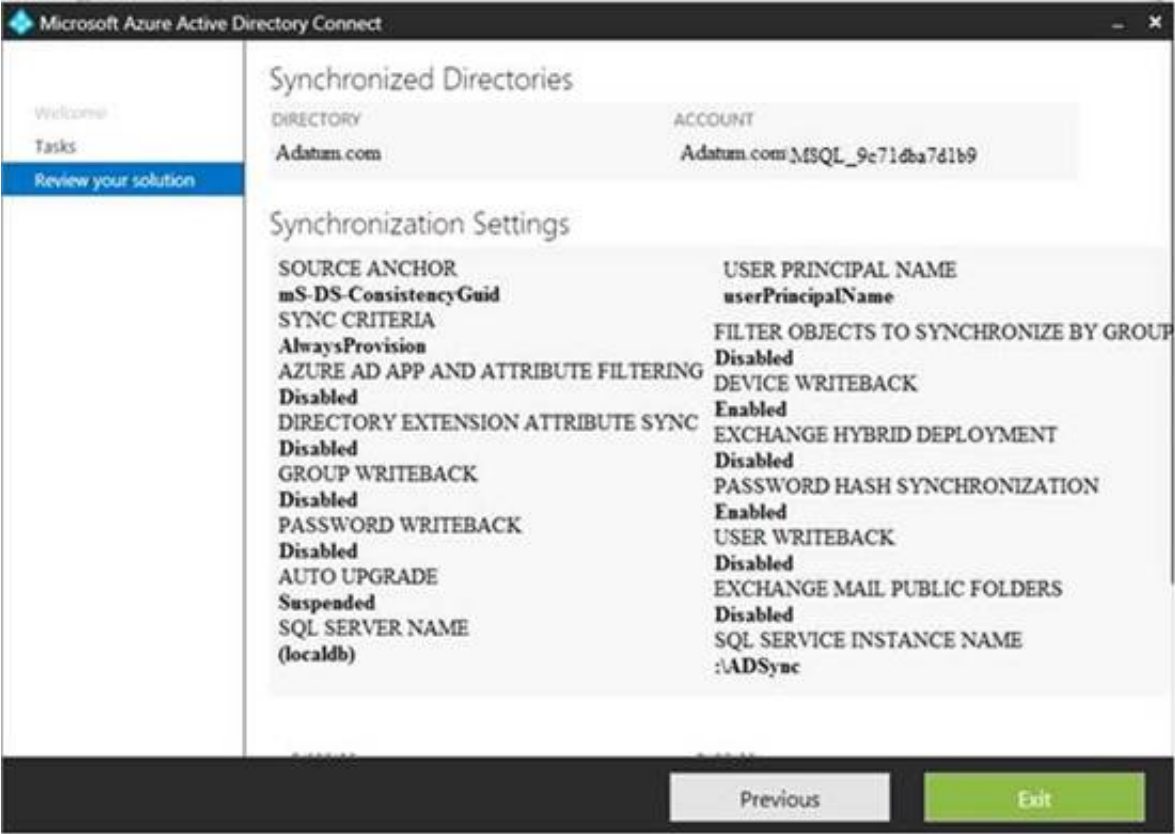
Does that meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 10

HOTSPOT
You configure Microsoft Azure Active Directory (Azure AD) Connect 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.

If you reset a password in Azure AD, the password will [answer choice].

| | |
|--|---|
| be overwritten | V |
| be synced to Active Directory | |
| be subject to the Active Directory password policy | |

If you join a computer to Azure AD,[answer choice].

| | |
|---|---|
| an object will be provisioned in the Computers container | V |
| an object will be provisioned in the RegisteredDevices container | |
| the device object in Azure will be deleted during synchronization | |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

NEW QUESTION 10

You have a Microsoft 365 Enterprise E5 subscription.

You use Windows Defender Advanced Threat Protection (Windows Defender ATP). You plan to use Microsoft Office 365 Attack simulator.

What is a prerequisite for running Attack simulator?

- A. Enable multi-factor authentication (MFA)
- B. Configure Advanced Threat Protection (ATP)
- C. Create a Conditional Access App Control policy for accessing Office 365
- D. Integrate Office 365 Threat Intelligence and Windows Defender ATP

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator>

NEW QUESTION 12

You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.

Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.

You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members.

The email address that you intend to spoof belongs to the Executive group members. What should you do first?

- A. From Azure ATP admin center, configure the primary workspace settings
- B. From the Microsoft Azure portal, configure the user risk settings in Azure AD Identity Protection
- C. Enable MFA for the Research group members
- D. Migrate the Executive group members to Exchange Online

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator>

NEW QUESTION 16

Your company uses Microsoft Azure Advanced Threat Protection (ATP).

You enable the delayed deployment of updates for an Azure ATP sensor named Sensor1. How long after the Azure ATP cloud service is updated will Sensor1 be updated?

- A. 7 days
- B. 24 hours
- C. 1 hour
- D. 48 hours
- E. 12 hours

Answer: B

Explanation:

Note: The delay period was 24 hours. In ATP release 2.62, the 24 hour delay period has been increased to 72 hours.

NEW QUESTION 17

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy to quarantine malware. You need to configure the retention duration for the attachments in quarantine.

Which type of threat management policy should you create from the Security&Compliance admin center?

- A. ATP anti-phishing
- B. DKIM
- C. Anti-spam
- D. Anti-malware

Answer: D

NEW QUESTION 22

Note: This question is part of 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 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.

You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them. Solution: You modify the encryption settings of the label.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 27

Note: This question is part of 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 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.

You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them. Solution: You modify the content expiration settings of the label.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 28

HOTSPOT

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.

| Name | Type | Email address |
|--------|--------------------------------|---------------------------|
| Group1 | Security Group – Domain Local | <u>Group1@contoso.com</u> |
| Group2 | Security Group – Universal | None |
| Group3 | Distribution Group – Global | None |
| Group4 | Distribution Group – Universal | <u>Group4@contoso.com</u> |

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

| Name | Type | Membership type |
|---------|-----------------------------|-----------------|
| Group11 | Security group | Assigned |
| Group12 | Security group | Dynamic |
| Group13 | Office | Assigned |
| Group14 | Mail-enabled security group | Assigned |

You create an Azure Information Protection policy named Policy1. You need to apply Policy1.

To which groups can you apply Policy1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

On-premises Active Directory groups:

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

Azure AD groups:

| | |
|---|---|
| Group13 only | V |
| Group13 and Group14 only | |
| Group11 and Group12 only | |
| Group11, Group13, and Group14 only | |
| Group11, Group12,Group13,and Group14 only | |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/information-protection/prepare>

NEW QUESTION 33

HOTSPOT

Your company has a Microsoft 365 subscription, a Microsoft Azure subscription, and an Azure Active Directory (Azure AD) tenant named contoso.com. The company has the offices shown in the following table.

| Location | IP address space | Public NAT segment |
|----------|------------------|--------------------|
| Montreal | 10.10.0.0/16 | 190.15.1.0/24 |
| Seattle | 172.16.0.0/16 | 194.25.2.0/24 |
| New York | 192.168.0.0/16 | 198.35.3.0/24 |

The tenant contains the users shown in the following table.

| Name | Email address |
|-------|-------------------|
| User1 | User1@contoso.com |
| User2 | User2@contoso.com |

You create the Microsoft Cloud App Security policy shown in the following exhibit.

Create filters for the policy

Act on:

Single activity:
Every activity that matches the filters

Repeated activity:
Repeated activity by a single user

Minimum repeated activities:

Within timeframe: minutes

☐ In a single app

☐ Count only unique target files or folders per user

[Edit and preview results](#)

ACTIVITIES MATCHING ALL OF THE FOLLOWING

equals

OR

equals

From group equals as

[+](#)

Alerts

☒ Create alert Use your organization's default settings

Daily alert limit

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 |
|---|-----------------------|-----------------------|
| In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created. | <input type="radio"/> | <input type="radio"/> |
| In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created. | <input type="radio"/> | <input type="radio"/> |
| In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created. | <input checked="" type="radio"/> | <input type="radio"/> |
| In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created. | <input checked="" type="radio"/> | <input type="radio"/> |
| In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created. | <input type="radio"/> | <input checked="" type="radio"/> |

NEW QUESTION 36

You have a Microsoft 365 subscription.
 Some users access Microsoft SharePoint Online from unmanaged devices.
 You need to prevent the users from downloading, printing, and synching files. What should you do?

- A. Run the Set-SPODataConnectionSetting cmdlet and specify the AssignmentCollection parameter
 B. From the SharePoint admin center, configure the Access control settings
 C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
 D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy

Answer: B

NEW QUESTION 40

DRAG DROP

You have a Microsoft 365 subscription.

A customer requests that you provide her with all documents that reference her by name. You need to provide the customer with a copy of the content.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

| Actions | Answer Area |
|---|-------------|
| Close the case. | |
| Regenerate a report. | |
| View the results. | |
| Export the results. | |
| Create a Data Subject Request (DSR) case. | |
| Save the search. | |
| Download the results. | |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365>

NEW QUESTION 42

You recently created and published several labels policies in a Microsoft 365 subscription.

You need to view which labels were applied by users manually and which labels were applied automatically.

What should you do from the Security & Compliance admin center?

- A. From Search & investigation, select Content search
- B. From Data governance, select Events
- C. From Search & investigation, select eDiscovery
- D. From Reports, select Dashboard

Answer: B

NEW QUESTION 43

You have a Microsoft 365 subscription.

The Global administrator role is assigned to your user account. You have a user named Admin1. You create an eDiscovery case named Case1.

You need to ensure that Admin1 can view the results of Case1. What should you do first?

- A. From the Azure Active Directory admin center, assign a role group to Admin1.
- B. From the Microsoft 365 admin center, assign a role to Admin1.
- C. From Security & Compliance admin center, assign a role group to Admin1.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions>

NEW QUESTION 45

You have a Microsoft 365 subscription.

You need to enable auditing for all Microsoft Exchange Online users. What should you do?

- A. From the Exchange admin center, create a journal rule
- B. Run the Set-MailboxDatabase cmdlet
- C. Run the Set-Mailbox cmdlet
- D. From the Exchange admin center, create a mail flow message trace rule.

Answer: C

Explanation:
Reference:
<https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing>

NEW QUESTION 49
HOTSPOT
You view Compliance Manager 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.

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

| | |
|---|---|
| assign action items | V |
| review actions | |
| perform an assessment | |
| create a service request with Microsoft | |

The current GDPR Compliance Score [answer choice].

| | |
|--|---|
| proves that the organization is non-compliant | V |
| proves that the organization is compliant | |
| shows that actions are required to evaluate compliance | |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Reference:
<https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud>

NEW QUESTION 54
You have a Microsoft 365 subscription that includes a user named Admin1.
You need to ensure that Admin1 can preserve all the mailbox content of users, including their deleted items.
The solution must use the principle of least privilege. What should you do?

- A. From the Microsoft 365 admin center, assign the Exchange administrator role to Admin1.
- B. From the Exchange admin center, assign the Discovery Management admin role to Admin1.
- C. From the Azure Active Directory admin center, assign the Service administrator role to Admin1.
- D. From the Exchange admin center, assign the Recipient Management admin role to Admin1.

Answer: B

NEW QUESTION 57
You have a Microsoft 365 subscription.
Yesterday, you created retention labels and published the labels to Microsoft Exchange Online mailboxes.
You need to ensure that the labels will be available for manual assignment as soon as possible. What should you do?

- A. From the Security & Compliance admin center, create a label policy
- B. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning
- C. From Exchange Online PowerShell, run Start-ManagedFolderAssistant
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

Answer: C

NEW QUESTION 62
HOTSPOT
You have a Microsoft 365 E5 subscription.
Users and device objects are added and removed daily. Users in the sales department frequently change their device.
You need to create three following groups:

| Group | Requirement |
|-------|--|
| 1 | All the devices of users where the Department attributes is set to Sales |
| 2 | All the devices where the Department attribute is set to Sales |
| 3 | All the devices where the deviceOwnership attribute is set to Company |

The solution must minimize administrative effort.
What is the minimum number of groups you should create for each type of membership? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Groups that have assigned membership:

▼

0

1

2

3

Groups that have dynamic membership:

▼

0

1

2

3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
References:
<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dynamic-membership.md>

NEW QUESTION 63
HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

| Name | Member | Multi-factor authentication (MFA) status |
|-------|----------------|--|
| User1 | Group1 | Disabled |
| User2 | Group1, Group2 | Enabled |

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

- Assignments: Include Group1, Exclude Group2
- Conditions: Sign in risk of Low and above
- Access: Allow access, Require password change

You need to identify how the policy affects User1 and User2.
What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Must change their password:

▼

User1 only

User2 only

Both User1 and User2

Neither User1 not User2

Prompted for MFA:

▼

User1 only

User2 only

Both User1 and User2

Neither User1 not User2

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Must change their password:

User1 only
User2 only
Both User1 and User2
Neither User1 not User2

Prompted for MFA:

User1 only
User2 only
Both User1 and User2
Neither User1 not User2

NEW QUESTION 65

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

| Name | Member of | Multi-factor authentication (MFA) status |
|-------|----------------|--|
| User1 | Group1, Group2 | Disabled |
| User2 | Group1 | Disabled |

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

- Assignments: Include Group1, Exclude Group2
 - Conditions: Sign in risk of Low and above
 - Access: Allow access, Require password multi-factor authentication
- You need to identify how the policy affects User1 and User2. What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.
- NOTE: Each correct selection is worth one point.

User1:

Blocked
Can sign in without MFA
Prompted for MFA

User2:

Blocked
Can sign in without MFA
Prompted for MFA

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1:

Blocked
Can sign in without MFA
Prompted for MFA

User2:

Blocked
Can sign in without MFA
Prompted for MFA

NEW QUESTION 67

You have a Microsoft 365 Enterprise E5 subscription.
You use Windows Defender Advanced Threat Protection (Windows Defender ATP).
You need to integrate Microsoft Office 365 Threat Intelligence and Windows Defender ATP. Where should you configure the integration?

- A. From the Microsoft 365 admin center, select Settings, and then select Services & add-ins.
- B. From the Security & Compliance admin center, select Threat management, and then select Explorer.
- C. From the Microsoft 365 admin center, select Reports, and then select Security & Compliance.
- D. From the Security & Compliance admin center, select Threat management and then select Threat tracker.

Answer: B

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-office-365-ti-with-wdatp>

NEW QUESTION 69

HOTSPOT
You have a Microsoft 365 subscription that uses a default name of litwareinc.com.
You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.

Links

Choose the kind of link that's selected by default when users share items.

Default link type

☒ Shareable: Anyone with the link

☐ Internal: Only people in your organization

☐ Direct: Specific people

External sharing

Users can share with:

SharePoint

Most permissive

Least permissive

OneDrive

Anyone

New and existing external users

Existing external users

Only people in your organization

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

☒ Allow or block sharing with people on specific domains

Allow only these domains: Contoso.com, Adatum.com

Add domains

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 user who has an email address of user1@fabrikam.com [answer choice]

cannot access OneDrive content

can access OneDrive content after a link is created

must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

the user cannot access OneDrive content

the user can access OneDrive content after a link is created

must be added to a group before the user can access shared files

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

NEW QUESTION 71

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 questions sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1. You run the Set-AuditConfig -Workload Exchange command.
Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:
<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps>

NEW QUESTION 73

You have a Microsoft 365 subscription.
You need to be notified by email whenever an administrator starts an eDiscovery search. What should you do from the Security & Compliance admin center?

- A. From Search & investigation, create a guided search.
- B. From Events, create an event.
- C. From Alerts, create an alert policy.
- D. From Search & Investigation, create an eDiscovery case.

Answer: C

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies>

NEW QUESTION 78

HOTSPOT
You have a Microsoft 365 subscription. Auditing is enabled.
A user named User1 is a member of a dynamic security group named Group1. You discover that User1 is no longer a member of Group1.
You need to search the audit log to identify why User1 was removed from Group1.
Which two actions should you use in the search? To answer, select the appropriate activities in the answer area.
NOTE: Each correct selection is worth one point.

Search

Clear

Results

Activities

Show results for all activities

Date

IP address

User

Activity

Item

Clear all to show results for all activities

Search

User administration activities

Added user

Deleted user

Set license properties

Reset user password

Changed user password

Changed user license

Updated user

Set property that forces user to change password

Azure AD group administration activities

Added group

Updated group

Deleted group

Added member to group

Removed member from group

Application administration activities

Added service principal

Removed a service principal from the directory

Set delegation entry

Removed credentials from a service principal

Added delegation entity

Added credentials to a service principal

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

NEW QUESTION 82

You have a Microsoft 365 subscription.
 You create and run a content search from the Security & Compliance admin center. You need to download the results of the content search.
 What should you obtain first?

- A. an export key
- B. a password
- C. a certificate
- D. a pin

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results>

NEW QUESTION 84

HOTSPOT
 You have a Microsoft 365 subscription.
 You create a retention label named Label1 as shown in the following exhibit.

The screenshot shows the 'Review your settings' page for a retention label named 'Label1'. On the left, there are three tabs: 'Name your label', 'Label settings', and 'Review your settings', with the last one being active. The main area displays the following settings:

- Name:** Label1 (with an 'Edit' link)
- Descriptions for admins:** (with an 'Edit' link)
- Description for users:** (with an 'Edit' link)
- Retention:**
 - 2 years
 - Retain and Delete
 - Based on when it was created
 - Use Label to classify content as a "Record"

At the bottom, there are three buttons: 'Back', 'Create this label', and 'Cancel'.

You publish Label1 to SharePoint sites.
 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.

| | |
|--|--|
| If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice]. | <div>▼</div> <div> never delete the file. delete the file before January 1, 2021. delete the file after January 1, 2021. </div> |
| If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice]. | <div>▼</div> <div> always remain in the library. remain in the library until you delete the file. be deleted automatically on March 15, 2021. </div> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/labels>

NEW QUESTION 87

HOTSPOT
 You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. OneDrive stores files that are shared with external users. The files are configured as shown in the following table.

| Name | Applied label |
|-------|----------------|
| File1 | Label1 |
| File2 | Label1, Label2 |
| File3 | Label2 |

You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:
 •Rule:

- Conditions: Label 1, Detect content that's shared with people outside my organization
- Actions: Restrict access to the content for external users
- User notifications: Notify the user who last modified the content
- User overrides: On
- Priority: 0
- Rule2:
- Conditions: Label 1 or Label2
- Actions: Restrict access to the content
- Priority: 1
- Rule3:
- Conditions: Label2, Detect content that's shared with people outside my organization
- Actions: Restrict access to the content for external users
- User notifications: Notify the user who last modified the content
- User overrides: On
- Priority: 2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.
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 |
|--|-----------------------|-----------------------|
| External users can access File1. | <input type="radio"/> | <input type="radio"/> |
| The users in contoso.com can access File2. | <input type="radio"/> | <input type="radio"/> |
| External users can access File3. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

| Statements | Yes | No |
|--|----------------------------------|-----------------------|
| External users can access File1. | <input checked="" type="radio"/> | <input type="radio"/> |
| The users in contoso.com can access File2. | <input checked="" type="radio"/> | <input type="radio"/> |
| External users can access File3. | <input checked="" type="radio"/> | <input type="radio"/> |

NEW QUESTION 91

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 questions 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 an on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events.
You use the Directory Service event log on Server1. Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:
<https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

NEW QUESTION 96

.....

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-500 Practice Exam Features:

- * MS-500 Questions and Answers Updated Frequently
- * MS-500 Practice Questions Verified by Expert Senior Certified Staff
- * MS-500 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * MS-500 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The MS-500 Practice Test Here](#)