

## Exam Questions MS-500

Microsoft 365 Security Administrator

<https://www.2passeasy.com/dumps/MS-500/>



### NEW QUESTION 1

An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.

#### Exchange Administrator - Members

+ Add member
X Remove member
Access reviews
Export
Refresh

Assignment type  
All

Search  
Search by members name

Member	Email	ASSIGNMENT TYPE	EXPIRATION
Admin1	Admin1@M365x901434.onmicrosoft.com	Permanent	-
Admin2	Admin2@M365x901434.onmicrosoft.com	Eligible	-

What should you do to meet the security requirements?

- A. Change the Assignment Type for Admin2 to Permanent
- B. From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
- C. From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
- D. Change the Assignment Type for Admin1 to Eligible

**Answer:** D

### 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

DRAG DROP

You need to configure threat detection for Active Directory. The solution must meet the security requirements.

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	Answer Area
Configure the Directory services setting in Azure ATP	
Download and install the ATA Gateway on DC1, DC2, and DC3	
Download and install the Azure ATP sensor package on DC1, DC2, and DC3	
Configure a site-to-site VPN	
Create a workspace in Azure ATP	
Download and install the ATA Center on Server1	

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Create a workspace in Azure ATP

Download and install the Azure ATP sensor package on DC1, DC2, and DC3

Configure the Directory services setting in Azure ATP

#### NEW QUESTION 4

##### HOTSPOT

You are evaluating which finance department users will be prompted for Azure MFA credentials. 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
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input checked="" type="radio"/>
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	<input checked="" type="radio"/>	<input type="radio"/>
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	<input checked="" type="radio"/>	<input type="radio"/>

#### NEW QUESTION 5

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 6**

What should User6 use to meet the technical requirements?

- A. Supervision in the Security & Compliance admin center
- B. Service requests in the Microsoft 365 admin center
- C. Security & privacy in the Microsoft 365 admin center
- D. Data subject requests in the Security & Compliance admin center

**Answer:** B

**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 User5. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 8**

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 9**

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 modifying the licenses assigned to User5. Does this meet the goal?

- A. Yes
- B. No

Answer: A

#### Explanation:

Case Study: 4 Mix Questions

#### NEW QUESTION 10

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 have a Microsoft 365 subscription that uses a default domain name of contoso.com.

The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

**multi-factor authentication**

users   service settings

app passwords (earn more)

☒ Allow users to create app passwords to sign in to non-browser apps

☐ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips(earn more)

☐ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

verification options (earn more)

Methods available to users:

☐ Call to phone

☒ Text message to phone

☒ Notification through mobile app

☒ Verification code from mobile app or hardware token

remember multi-factor authentication (earn more)

☐ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60)

In contoso.com, you create the users shown in the following table.

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

What is the effect of the configuration? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

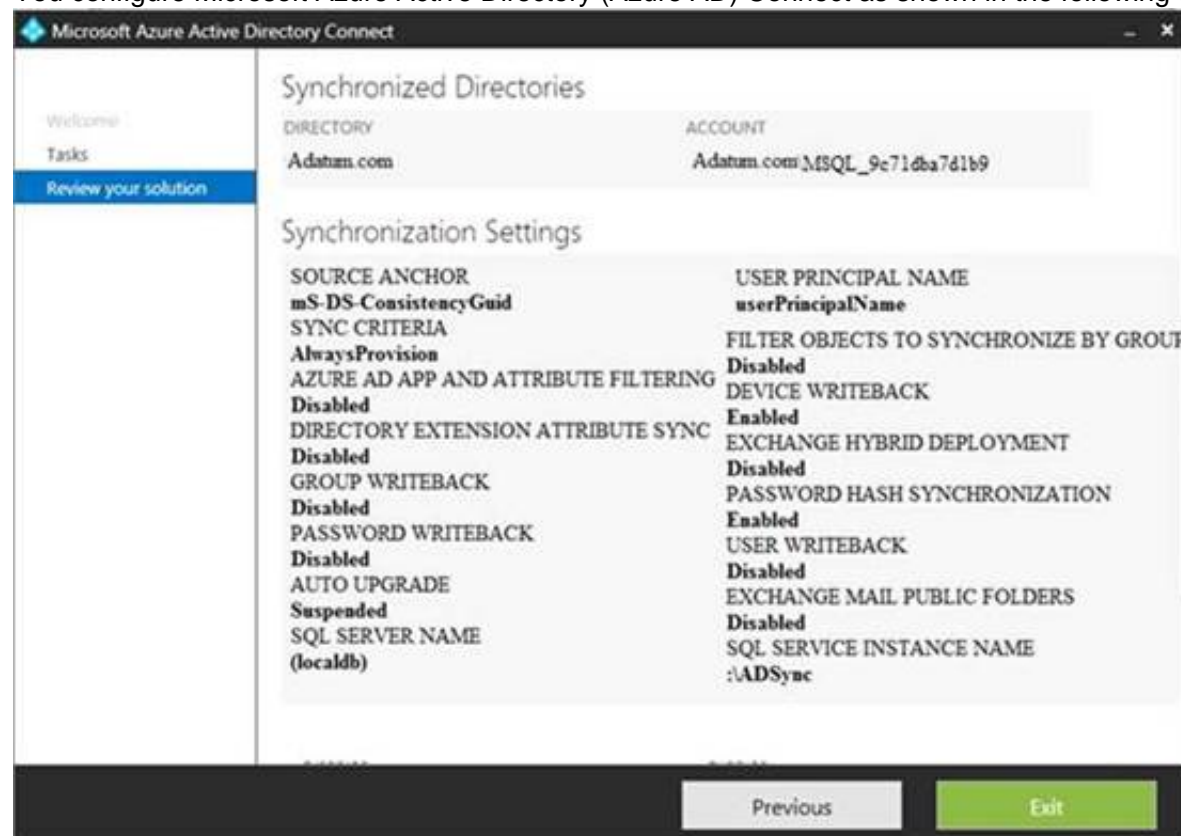
User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

## NEW QUESTION 12

### 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 17

You have a Microsoft 365 subscription.

You need to ensure that all users who are assigned the Exchange administrator role have multi-factor authentication (MFA) enabled by default.

What should you use to achieve the goal?

- A. Security & Compliance permissions
- B. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- C. Microsoft Azure AD group management
- D. Microsoft Office 365 user management

**Answer:** B

#### NEW QUESTION 21

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 24

You have a Microsoft 365 E5 subscription.

You implement Advanced Threat Protection (ATP) safe attachments policies for all users.

User reports that email messages containing attachments take longer than expected to be received. You need to reduce the amount of time it takes to receive email messages that contain attachments. The solution must ensure that all attachments are scanned for malware. Attachments that have malware must be blocked.

What should you do from ATP?

- A. Set the action to Block
- B. Add an exception
- C. Add a condition
- D. Set the action to Dynamic Delivery

**Answer:** D

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-previewing>

#### NEW QUESTION 26

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain name of contoso.com. Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Intune has two devices enrolled as shown in the following table:

Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.

You create an app protection policy named ProtectionPolicy1 that has the following settings:

- Protected apps: App1
- Exempt apps: App2
- Windows Information Protection mode: Block

You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1. 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

Yes No

From Device1, User1 can copy data from App1 to App3.

☐
☐

From Device2, User1 can copy data from App1 to App2.

☐
☐

From Device2, User1 can copy data from App1 to App3.

☐
☐

A. Mastered

B. Not Mastered

Answer: A

Explanation:

### Answer Area

Yes No

From Device1, User1 can copy data from App1 to App3.

☐
☒

From Device2, User1 can copy data from App1 to App2.

☒
☐

From Device2, User1 can copy data from App1 to App3.

☒
☐

### NEW QUESTION 29

HOTSPOT

Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The company implements Windows Defender Advanced Threat Protection (Windows Defender ATP). Windows Defender ATP includes the roles shown in the following table:

Name	Permission	Assigned user group
Role1	View data, Active remediation actions, Alerts investigation	Group1
Role2	View data, Active remediation actions	Group2
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Windows Defender ATP contains the machine groups shown in the following table:

Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

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



Statements	Yes	No
User1 can run an antivirus scan on Device1.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can run an antivirus scan on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 32

DRAG DROP

You have a Microsoft 365 subscription. All users use Microsoft Exchange Online. Microsoft 365 is configured to use the default policy settings without any custom rules. You manage message hygiene.

Where are suspicious email messages placed by default? To answer, drag the appropriate location to the correct message types. Each location may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Locations

ATP quarantine

The Junk Email folder of a user's mailbox

The Chutter folder a user's mailbox

Messages that contain word-filtered content:

Messages that are classified as phishing:

Answer Area

Location

Location

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

Messages that contain word-filtered content:

Messages that are classified as phishing:

The Junk Email folder of a user's mailbox

The Junk Email folder of a user's mailbox

NEW QUESTION 33

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 create a new label in the global policy and instruct the user to resend the email message.

Does this meet the goal?

- A. Yes  
B. No

Answer: A

#### NEW QUESTION 38

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 40

HOTSPOT

You have a Microsoft 365 subscription.

You identify the following data loss prevention (DLP) requirements:

- Send notifications to users if they attempt to send attachments that contain EU social security numbers
- Prevent any email messages that contain credit card numbers from being sent outside your organization
- Block the external sharing of Microsoft OneDrive content that contains EU passport numbers
- Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Policies:

1	V
2	
3	

Rules:

1	V
2	
3	
4	

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Policies:

1	V
2	
3	

Rules:

1	V
2	
3	
4	

#### NEW QUESTION 43

You have a Microsoft 365 subscription.

You need to create data loss prevention (DLP) queries in Microsoft SharePoint Online to find sensitive data stored in sites.

Which type of site collection should you create first?

A. Records Center

B. Compliance Policy Center

C. eDiscovery Center

D. Enterprise Search Center

E. Document Center

Answer: C

**Explanation:**

Reference:

<https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bbb944-448d-b83d-8fec4abcc24c>

**NEW QUESTION 44**

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 48**

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 52**

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 57**

HOTSPOT

You have a Microsoft 365 subscription. From the Security & Compliance admin center, you create the retention policies shown in the following table.

Name	Location
Policy1	OneDrive accounts
Polciy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

Policy1 if configured as showing in the following exhibit.

Decide if you want to retain content, delete it, or both

Do you want to retain content?

☒ Yes, I want to retain it

For this long... 1 years

☐ No, just delete content that's older than

1 years

Delete the content based on when it was created

Need more options?

☐ Use advanced retention settings

Back

Next

Cancel

Policy2 is configured as shown in the following exhibit.

Decide if you want to retain content, delete it, or both

Do you want to retain content?

☒ Yes, I want to retain it

For this long... 3 years

Retain the content based on when it was created

Do you want us to delete it after this time?

☐ Yes ☒ No

☐ No, just delete content that's older than

1 years

Need more options?

☐ Use advanced retention settings

Back

Next

Cancel

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

Answer Area	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the-principles-of-retention-or-what-takes-precedence>

#### NEW QUESTION 61

##### 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 65

You have a Microsoft 365 subscription.  
All computers run Windows 10 Enterprise and are managed by using Microsoft Intune. You plan to view only security-related Windows telemetry data.  
You need to ensure that only Windows security data is sent to Microsoft. What should you create from the Intune admin center?

- A. a device configuration profile that has device restrictions configured
- B. a device configuration profile that has the Endpoint Protection settings configured
- C. a device configuration policy that has the System Security settings configured
- D. a device compliance policy that has the Device Health settings configured

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10#reporting-and-telemetry>

NEW QUESTION 67

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 70

You have a hybrid Microsoft 365 environment.  
All computers run Windows 10 Enterprise and have Microsoft Office 365 ProPlus installed. All the computers are joined to Active Directory.  
You have a server named Server1 that runs Windows Server 2016. Server1 hosts the telemetry database. You need to prevent private details in the telemetry data from being transmitted to Microsoft.  
What should you do?

- A. On Server1, run readinessreportcreator.exe
- B. Configure a registry on Server1
- C. Configure a registry on the computers
- D. On the computers, run tdadm.exe

Answer: C

## NEW QUESTION 72

### 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 73

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 76

Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled. The security logs of the servers are collected by using a third-party SIEM solution. You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors. You need to ensure that you can detect when sensitive groups are modified and when malicious services are created. What should you do?

- A. Configure auditing in the Office 365 Security & Compliance center.
- B. Turn off Delayed updates for the Azure ATP sensors.
- C. Modify the Domain synchronizer candidate's settings on the Azure ATP sensors.
- D. Integrate SIEM and Azure ATP.

**Answer: C**

#### Explanation:

References:  
<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5>

#### NEW QUESTION 81

You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com. You create a safe links policy, as shown in the following exhibit.

Safe links policy for your organization

#### Settings that apply to content across Office 365

When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.  
 Block the following URLs:

-

Enter a valid URL

+

\*.phishing.\*.\*

malware.\*com

\*.contoso.com

#### Settings that apply to content except email

These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

- ☒ Office 356 ProPlus, Office for iOS and Android
- ☒ Office Online of above applications

For the locations selected above:

- ☒ Do not track when users click safe links:
- ☒ Do not let users click through safe links to original URL:

Which URL can a user safely access from Microsoft Word Online?

- A. fabrikam.phishing.fabrikam.com
- B. malware.fabrikam.com
- C. fabrikam.contoso.com
- D. www.malware.fabrikam.com

**Answer: D**

#### Explanation:

References:  
<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-a-custom-blocked-urls-list- wtih-atp>

#### NEW QUESTION 86

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 89**

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-AdminAuditLogConfig -AdminAuditLogEnabled \$true-AdminAuditLogCmdlets \*Mailbox\* 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/setadmindauditlogconfig?view=exchange-ps>

**NEW QUESTION 93**

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. The files in Site1 are protected by using Microsoft Azure Information Protection.

From the Security & Compliance admin center, you create a label that designates personal data. You need to auto-apply the new label to all the content in Site1.

What should you do first?

A. From PowerShell, run Set-ManagedContentSettings.

B. From PowerShell, run Set-ComplianceTag.

C. From the Security & Compliance admin center, create a Data Subject Request (DSR).

D. Remove Azure Information Protection from the Site1 files.

Answer: D

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/apply-labels-to-personal-data-in-office-365>

**NEW QUESTION 98**

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

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 103**

HOTSPOT

You have a Microsoft 365 subscription that include three users named User1, User2, and User3.

A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute.

You create an alert policy named Policy1 as shown in the following exhibit.

Policy1	
<div>Edit policy Delete policy</div>	
Status	<div>On</div>
Description	<div>Policy1 description</div> <div>Edit</div>
Severity	<div>Low</div>
Category	<div>Threat management</div>
Conditions	<div>Activity is Copied file and File name is Like any of File1.docx</div>
Aggregation	<div>Aggregated</div> <div>Edit</div>
Threshold	<div>10 activities</div>
Window	<div>60 minutes</div>
Scope	<div>All users</div>
Email recipients	<div>prvi@sk180920.onmicrosoft.com</div>
Daily notifications limit	<div>Do not send email notifications</div> <div>Edit</div>

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 User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

	▼
<div>Policy1 will not be triggered</div> <div>Policy1 will be triggered after 45 minutes</div> <div>Policy1 will be triggered after 60 minutes</div>	

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

	▼
<div>Policy1 will not be triggered</div> <div>Policy1 will be triggered within 20 minutes</div> <div>Policy1 will be triggered within 45 minutes</div> <div>Policy1 will be triggered after 60 minutes</div>	

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

References:

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

**NEW QUESTION 108**

You have a Microsoft 365 subscription.

You create a retention policy and apply the policy to Exchange Online mailboxes.

You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible.

What should you do?

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

Answer: D

**Explanation:**

References:

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

#### NEW QUESTION 110

You have a Microsoft 365 subscription.

You have a team named Team1 in Microsoft Teams. You plan to place all the content in Team1 on hold.

You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.

Which cmdlet should you use?

- A. Get-UnifiedGroup
- B. Get-MailUser
- C. Get-TeamMessagingSettings
- D. Get-TeamChannel

**Answer:** A

#### NEW QUESTION 115

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:

- Rule1:
- 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 118

Several users in your Microsoft 365 subscription report that they received an email message without the attachment. You need to review the attachments that were removed from the messages. Which two tools can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. the Exchange admin center
- B. the Azure ATP admin center
- C. Microsoft Azure Security Center
- D. the Security & Compliance admin center
- E. Outlook on the web

**Answer:** AD

#### Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages-and-files>

#### NEW QUESTION 123

DRAG DROP

You have a Microsoft 365 E5 subscription.

All computers run Windows 10 and are onboarded to Windows Defender Advanced Threat Protection (Windows Defender ATP).

You create a Windows Defender machine group named MachineGroup1.

You need to enable delegation for the security settings of the computers in MachineGroup1.

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	Answer Area
From Windows Defender Security Center, create a role.	
From Windows Defender Security Center, configure the permissions for MachineGroup1.	
From the Azure portal, create an RBAC role.	
From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.	
From Azure Cloud Shell, run the Add-IsolRoleMember cmdlet.	

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Actions	Answer Area
From Windows Defender Security Center, create a role.	
From Windows Defender Security Center, configure the permissions for MachineGroup1.	
From the Azure portal, create an RBAC role.	
From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.	
From Azure Cloud Shell, run the Add-IsolRoleMember cmdlet.	

#### NEW QUESTION 125

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy.

You need to configure the retention duration for the attachments in quarantine. Which type of threat management policy should you create?

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

**Answer:** A

#### NEW QUESTION 127

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 Security 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 128**

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 System 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 130**

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-MailboxFolderPermission –Identity "User1"

-User User1@contoso.com –AccessRights Owner command. Does that meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps>

**NEW QUESTION 133**

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MS-500 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MS-500 Product From:

<https://www.2passeasy.com/dumps/MS-500/>

## Money Back Guarantee

### 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 FirstTry
- \* MS-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year