

## MS-500 Dumps

### Microsoft 365 Security Administrator

<https://www.certleader.com/MS-500-dumps.html>



## 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 need to recommend an email malware solution that meets the security requirements.

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

NOTE: Each correct selection is worth one point.

Policy to create:

ATP safe attachments	V
ATP Safe Links	
Anti-spam	
Anti-malware	

Option to configure:

Block	V
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

- A. Mastered
- B. Not Mastered

**Answer: A**

### Explanation:

Policy to create:

ATP safe attachments	V
ATP Safe Links	
Anti-spam	
Anti-malware	

Option to configure:

Block	V
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

### NEW QUESTION 3

You need to recommend a solution that meets the technical and security requirements for sharing data with the partners. What should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Create an access review.
- B. Assign the Global administrator role to User1.
- C. Assign the Guest inviter role to User1.
- D. Modify the External collaboration settings in the Azure Active Directory admin center.

**Answer:** AC

### NEW QUESTION 4

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 5

HOTSPOT

Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

ADGroup1:	None	V
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

ADGroup2:	None	V
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values>

**NEW QUESTION 6**

**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 7**

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 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 Azure AD app and attribute filtering settings.

Does that meet the goal?

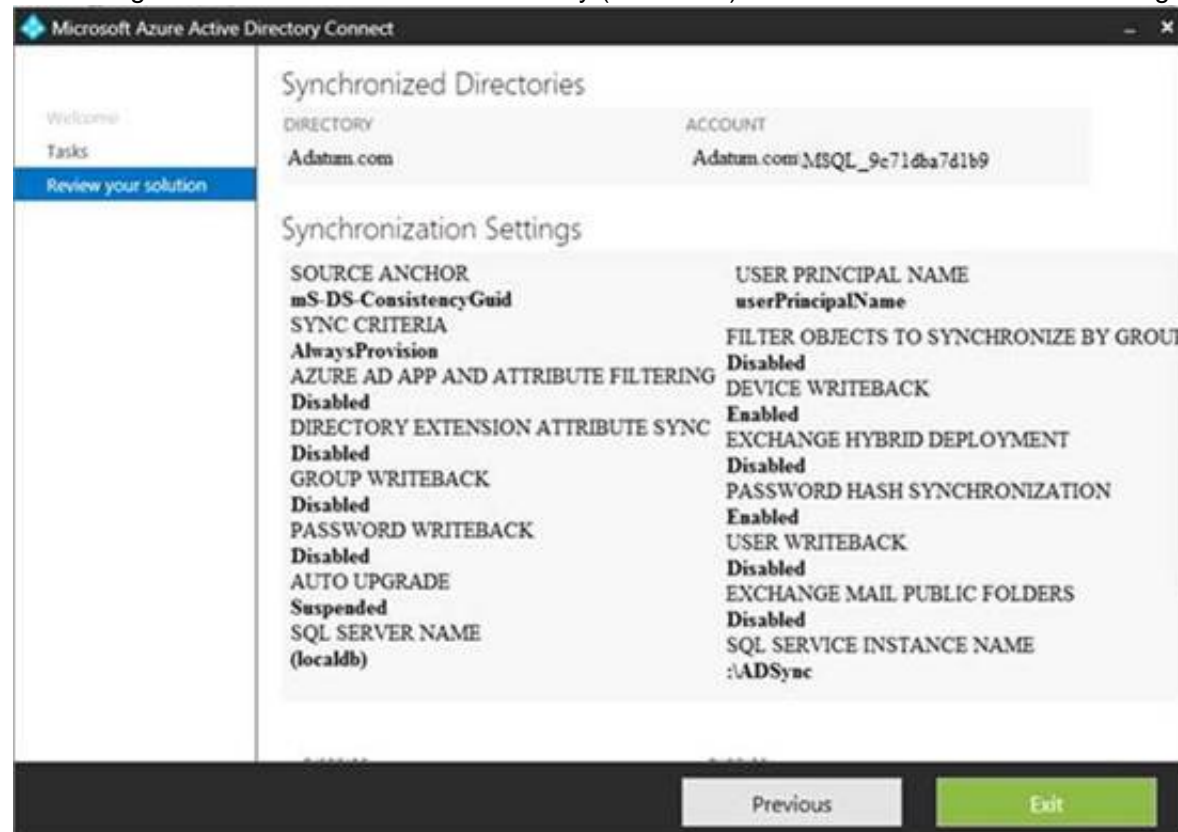
- A. Yes
- B. No

**Answer: B**

## NEW QUESTION 9

### 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	▼
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	▼
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 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 10

You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription. You need to allow a user named User1 to view ATP reports in the Threat management dashboard. Which role provides User1 with the required role permissions?

- A. Security reader
- B. Message center reader
- C. Compliance administrator
- D. Information Protection administrator

**Answer:** A

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-areneeded-to-view-the-atp-reports>

#### NEW QUESTION 11

You have a Microsoft 365 tenant.

You have 500 computers that run Windows 10.

You plan to monitor the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP) after the computers are enrolled in Microsoft Intune.

You need to ensure that the computers connect to Windows Defender ATP. How should you prepare Intune for Windows Defender ATP?

- A. Configure an enrollment restriction
- B. Create a device configuration profile
- C. Create a conditional access policy
- D. Create a Windows Autopilot deployment profile

**Answer:** B

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/intune/advanced-threat-protection>

#### NEW QUESTION 14

##### 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 18

##### 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		Answer Area
ATP quarantine	Messages that contain word-filtered content:	Location
The Junk Email folder of a user's mailbox	Messages that are classified as phishing:	Location
The Chutter folder a user's mailbox		

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

	Answer Area
Messages that contain word-filtered content:	The Junk Email folder of a user's mailbox
Messages that are classified as phishing:	The Junk Email folder of a user's mailbox

#### 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 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 25

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.

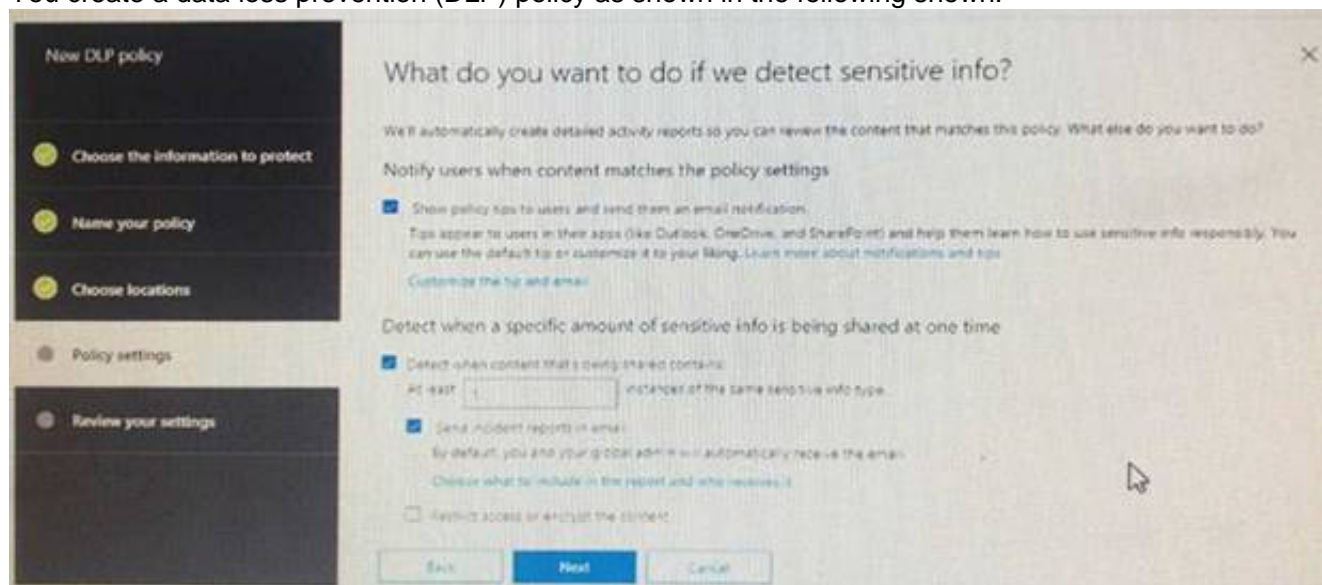
Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

### NEW QUESTION 30

You create a data loss prevention (DLP) policy as shown in the following shown:



What is the effect of the policy when a user attempts to send an email messages that contains sensitive information?

- A. The user receives a notification and can send the email message
- B. The user receives a notification and cannot send the email message
- C. The email message is sent without a notification
- D. The email message is blocked silently

**Answer:** A

#### Explanation:

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

### NEW QUESTION 33

You have a Microsoft 365 subscription.

A user reports that changes were made to several files in Microsoft OneDrive.

You need to identify which files were modified by which users in the user's OneDrive. What should you do?

- A. From the Azure Active Directory admin center, open the audit log
- B. From the OneDrive admin center, select Device access
- C. From Security & Compliance, perform an eDiscovery search
- D. From Microsoft Cloud App Security, open the activity log

**Answer:** D

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/activity-filters>

### NEW QUESTION 34

You have a Microsoft 365 subscription. You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. From the Cloud App Security admin center, create a file policy.
- B. From the SharePoint admin center, modify the Site Settings.
- C. From the SharePoint & Compliance admin center, create a label.
- D. From the SharePoint admin center, modify the records management settings.
- E. From the Security & Compliance admin center, publish a label.

**Answer:** CE

#### Explanation:

Reference:



<https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-office-365-labels-and-dlp>

### NEW QUESTION 35

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 40

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 42**

**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 45**

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 46**

Your company has a Microsoft 365 subscription that includes a user named User1.  
You suspect that User1 sent email messages to a competitor detailing company secrets.  
You need to recommend a solution to ensure that you can review any email messages sent by User1 to the competitor, including sent items that were deleted.  
What should you include in the recommendation?

- A. Enable In-Place Archiving for the mailbox of User1
- B. From the Security & Compliance, perform a content search of the mailbox of User1
- C. Place a Litigation Hold on the mailbox of User1
- D. Configure message delivery restrictions for the mailbox of User1

**Answer: C**

#### NEW QUESTION 51

Your company has a main office and a Microsoft 365 subscription.  
You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.  
What should you include in the configuration?

- A. a user risk policy
- B. a sign-in risk policy
- C. a named location in Azure Active Directory (Azure AD)
- D. an Azure MFA Server

**Answer: C**

#### Explanation:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

#### NEW QUESTION 56

##### 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 59

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 61

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 62


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 65

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

Date	IP address	User	Activity	Item
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 66

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 68

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 73

You have a Microsoft 365 subscription.

You need to ensure that users can manually designate which content will be subject to data loss prevention (DLP) policies.

What should you create first?

- A. A retention label in Microsoft Office 365
- B. A custom sensitive information type
- C. A Data Subject Request (DSR)
- D. A safe attachments policy in Microsoft Office 365

**Answer:** C

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/manage-gdpr-data-subject-requests-with-thedsr-case-tool#more-information-about-using-the-dsr-case-tool>

#### NEW QUESTION 75

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 76**

You have a Microsoft 365 subscription. You enable auditing for the subscription.  
You plan to provide a user named Auditor with the ability to review audit logs. You add Auditor to the Global administrator role group.  
Several days later, you discover that Auditor disabled auditing.  
You remove Auditor from the Global administrator role group and enable auditing.

- A. Security operator  
B. Security reader  
C. Security administrator  
D. Compliance administrator

**Answer:** D

**NEW QUESTION 81**

You have a hybrid Microsoft Exchange Server organization. All users have Microsoft 365 E5 licenses. You plan to implement an Advanced Threat Protection (ATP) anti-phishing policy. You need to enable mailbox intelligence for all users. What should you do first?

- A. Configure attribute filtering in Microsoft Azure Active Directory Connect (Azure AD Connect).  
B. Purchase the ATP add-on.  
C. Select Directory extension attribute sync in Microsoft Azure Active Directory Connect (Azure AD Connect).  
D. Migrate the on-premises mailboxes to Exchange Online.

**Answer:** B

**NEW QUESTION 85**

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 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 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 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 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 96**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your MS-500 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/MS-500-dumps.html>