

# Exam Questions MS-500

Microsoft 365 Security Administrator

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



#### NEW QUESTION 1

You need to recommend a solution for the user administrators that meets the security requirements for auditing. Which blade should you recommend using from the Azure Active Directory admin center?

- A. Sign-ins
- B. Azure AD Identity Protection
- C. Authentication methods
- D. Access review

**Answer:** A

#### Explanation:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>

#### NEW QUESTION 2

You need to resolve the issue that targets the automated email messages to the IT team. Which tool should you run first?

- A. Synchronization Service Manager
- B. Azure AD Connect wizard
- C. Synchronization Rules Editor
- D. IdFix

**Answer:** B

#### Explanation:

References:

<https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization>

Case Study: 2 Litware, Inc Overview

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment

Internal Network Infrastructure

The network contains a single domain forest. The forest functional level is Windows Server 2016. Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address range shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

- Windows Server 2016
- Windows 10 Enterprise
- Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group 1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Planned Changes

Litware plans to implement the following changes: Migrate the email system to Microsoft Exchange Online Implement Azure AD Privileged Identity Management Security Requirements

Litware identifies the following security requirements:

- Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
- Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
- Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
- Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory

- Implement a permanent eligible assignment of the Compliance administrator role for User1
- Integrate Windows Defender and Windows Defender ATP on domain-joined servers
- Prevent access to Azure resources for the guest user accounts by default
- Ensure that all domain-joined computers are registered to Azure AD

#### Multi-factor authentication (MFA) Requirements

Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts. You identify the following requirements for testing MFA. Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.

If an authentication attempt is suspicious, MFA must be used, regardless of the user location Any disruption of legitimate authentication attempts must be minimized

#### General Requirements

Litware want to minimize the deployment of additional servers and services in the Active Directory forest.

### 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

You need to meet the technical requirements for User9. What should you do?

- A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9
- B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9
- C. Assign the Security administrator role to User9
- D. Assign the Global administrator role to User9

**Answer:** A

#### Explanation:

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

### NEW QUESTION 5

#### HOTSPOT

Which policies apply to which devices? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

DevicePolicy1: 

None  
Device1 only  
Device3 only  
Device2 and Device3 only  
Device1 and Device3 only  
Device1, Device2, and Device3

DevicePolicy2: 

None  
Device4 only  
Device2 and Device4 only  
Device2, Device3, and Device 4 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

DevicePolicy1: 

None  
Device1 only  
Device3 only  
Device2 and Device3 only  
Device1 and Device3 only  
Device1, Device2, and Device3

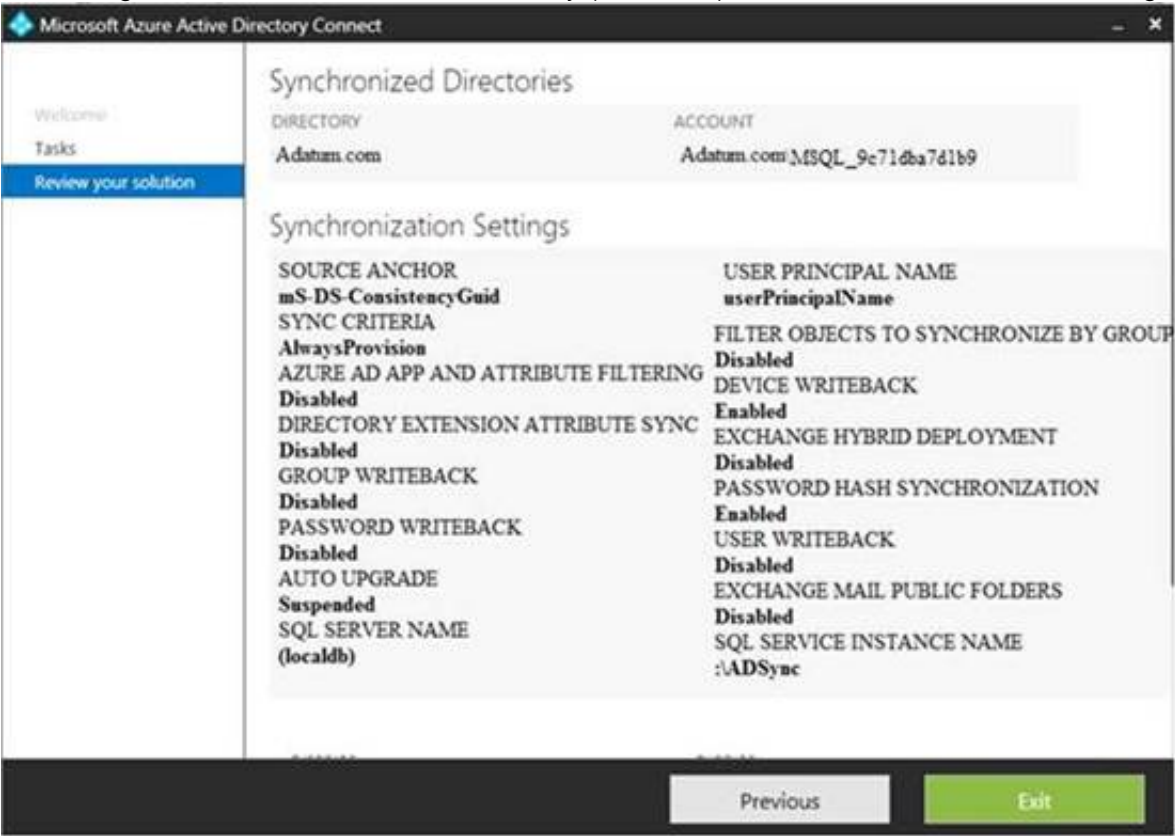
DevicePolicy2: 

None  
Device4 only  
Device2 and Device4 only  
Device2, Device3, and Device 4 only

NEW QUESTION 6

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 7

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 8

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 9

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 10

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Microsoft Azure Active Directory (Azure AD), you create a security group named Group1. You add 10 users to Group1.

You need to apply app enforced restrictions to the members of Group1 when they connect to Microsoft Exchange Online from non-compliant devices, regardless of their location.

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

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	V
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	V
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	V
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailboxPolicy and Set-OwaMailboxPolicy	V
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

#### NEW QUESTION 10

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 15

HOTSPOT

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 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... v 2 years v

Retain the content based on when it was last modified v ⓘ

Do you want us to delete it after this time? ⓘ

☒ Yes ☐ No

☐ No, just delete content that's older than ⓘ

1 years v

Need more options?

☐ Use advanced retention settings ⓘ

Back

Next

Cancel

You apply Retention1 to SharePoint sites and OneDrive accounts.

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 a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be [answer choice].

retained	v
deleted on January 1, 2021	
deleted on July 1, 2021	

If a user creates a file in Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file	v
can recover the file until January 1, 2020	
can recover the file until March 1, 2020	
can recover the file until May 1, 2020	



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be [answer choice].

retained

deleted on January 1, 2021

deleted on July 1, 2021

If a user creates a file in Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file

can recover the file until January 1, 2020

can recover the file until March 1, 2020

can recover the file until May 1, 2020

**NEW QUESTION 19**

**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 is 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 21

You create a label that encrypts email data. Users report that they cannot use the label in Outlook on the web to protect the email messages they send. You need to ensure that the users can use the new label to protect their email. What should you do?

- A. Modify the priority order of label policies
- B. Wait six hours and ask the users to try again
- C. Create a label policy
- D. Create a new sensitive information type

Answer: B

#### NEW QUESTION 22

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 24

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 28

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:



+

\*.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 33

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 38

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 39

You have a Microsoft 365 subscription.

A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.

You need to limit alert notifications to actionable DLP events.

What should you do?

- A. From the Security & Compliance admin center, modify the Policy Tips of a DLP policy.
- B. From the Cloud App Security admin center, apply a filter to the alerts.
- C. From the Security & Compliance admin center, modify the User overrides settings of a DLP policy.
- D. From the Security & Compliance admin center, modify the matched activities threshold of an alert policy.

**Answer: D**

### Explanation:

References:

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

### NEW QUESTION 43

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, a sidebar indicates that 'Name your label' and 'Label settings' are completed, while 'Review your settings' is the current step. The main area shows 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" (with an 'Edit' link)

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].

	▼
never delete the file.	
delete the file before January 1, 2021.	
delete the file after January 1, 2021.	

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

	▼
always remain in the library.	
remain in the library until you delete the file.	
be deleted automatically on March 15, 2021.	

- A. Mastered
- B. Not Mastered

**Answer: A**

### Explanation:

References:

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

### NEW QUESTION 44

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 46

.....

## 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