

## MS-500 Dumps

### Microsoft 365 Security Administrator

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



### 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 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	▼
Weekly	
Monthly	

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

Upon completion settings	▼
Advanced settings	
Programs	
Reviewers	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Set the frequency to:

One time	▼
Weekly	
Monthly	

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

Upon completion settings	▼
Advanced settings	
Programs	
Reviewers	

### NEW QUESTION 3

Which IP address space should you include in the MFA configuration?

- A. 131.107.83.0/28
- B. 192.168.16.0/20
- C. 172.16.0.0/24

D. 192.168.0.0/20

**Answer:** B

#### NEW QUESTION 4

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

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

**Answer:** C

#### Explanation:

Case Study: 3 Contoso, Ltd Overview

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

The company has the offices shown in the following table.

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

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

Existing Environment Infrastructure

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

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

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

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

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

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

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

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

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

The tenant contains the groups shown in the following table.

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

Customer Lockbox is enabled in Microsoft 365. Microsoft Intune Configuration

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

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

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

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

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

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

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

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

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

## NEW QUESTION 5

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	✓
User1 and User2 only	
User2 and User4 only	
User3 and User4 only	
User1, User2, User3, and User4	

**ADGroup2:**

None	✓
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

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 9

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 10

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 10

You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune.

You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on- premises network.

What should you do first?

- A. From the Azure Active Directory admin center, create a new certificate
- B. Enable Application Proxy in Azure AD
- C. From Active Directory Administrative Center, create a Dynamic Access Control policy
- D. From the Azure Active Directory admin center, configure authentication methods

**Answer:** A

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn- connectivitywindows10>

### NEW QUESTION 13

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 14

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

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

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

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

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

**Answer:** C

#### Explanation:

Reference:

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

### NEW QUESTION 18

#### HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed. You have a Microsoft Azure subscription.

You are deploying Azure Advanced Threat Protection (ATP)

You install an Azure ATP standalone sensor on a server named Server1 that runs Windows Server 2016.

You need to integrate the VPN and Azure ATP.

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

On VPN1:

Configure an authentication provider.	✓
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:

443	✓
1723	
1813	
8080	
8531	

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn>

### NEW QUESTION 19

#### 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 23

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 28

##### 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 30

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 31

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 33

You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

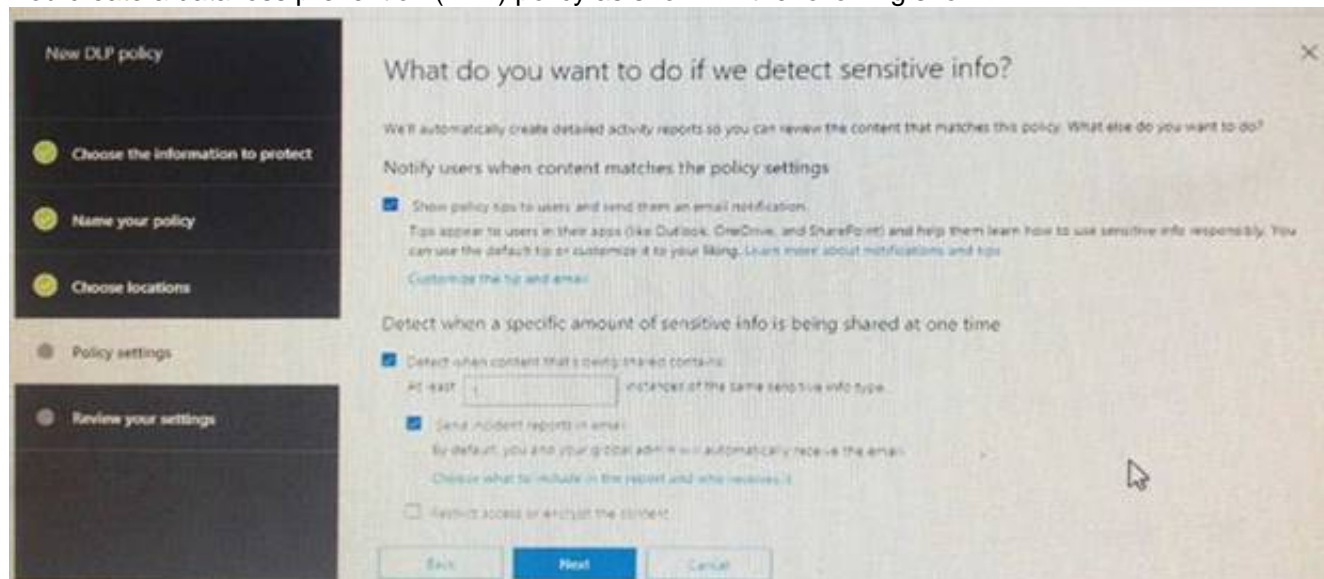
You need to prevent the users from downloading, printing, and synching files. What should you do?

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

**Answer:** B

### NEW QUESTION 37

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 38

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

#### NEW QUESTION 41

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 45

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 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 53

#### 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 contet, 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
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019

If a user deletes a Microsoft OneDrive file created on January 1,2018, an administrator can recover the file on April 15, 2019

If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022

- 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 55**

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 59**

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 60**

DRAG DROP

You have a Microsoft 365 subscription.

You have a site collection named SiteCollection1 that contains a site named Site2. Site2 contains a document library named Customers.

Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.

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 PowerShell, run Remove-SPOUserProfile	
Delete Litware.docx from the Recycle Bin of Site2.	
From PowerShell, run Set-SPOSite.	
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run Remove-SPOUserInfo	
Delete Litware.docx from Customers.	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area
Delete Litware.docx from Customers.
Delete Litware.docx from the Recycle Bin of Site2.
Delete Litware.docx from the Recycle Bin of SiteCollection1.

**NEW QUESTION 64**

HOTSPOT



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

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

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

Groups that have assigned membership:

	▼
0	
1	
2	
3	

Groups that have dynamic membership:

	▼
0	
1	
2	
3	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

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

#### NEW QUESTION 67

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 71

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 72

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 74

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 77

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

You have a conditional access policy that applies to Microsoft Exchange Online. The conditional access policy is configured to use Conditional Access App Control.

You need to create a Microsoft Cloud App Security policy that blocks User1 from printing from Exchange Online.

Which type of Cloud App Security policy should you create?

- A. an app permission policy
- B. an activity policy
- C. a Cloud Discovery anomaly detection policy
- D. a session policy

**Answer: D**

**NEW QUESTION 81**

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 84**

You have a Microsoft 365 subscription.

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

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

**Answer:** C

**Explanation:**

References:

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

**NEW QUESTION 89**

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 94**

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 97

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 98

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

Create a label to help users classify their content.

✓ Name your label

✓ Label settings

● Review your settings

Review your settings

Name

Label1

Edit

Descriptions for admins

Edit

Description for users

Edit

Retention

2 years

Retain and Delete

Based on when it was created

Use Label to classify content as a "Record"

Edit

Back

Create this label

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 100**

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 103**

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 107**

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 112**

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-Hso1RoleMember 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 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 the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.	From the Azure portal, create an RBAC role.
From Azure Cloud Shell, run the Add-Hso1RoleMember cmdlet.	

**NEW QUESTION 117**

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 121**

.....

## 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>