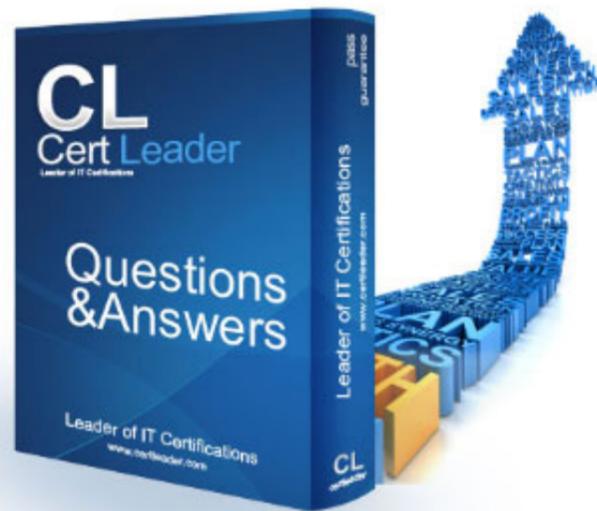


## MS-500 Dumps

### 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	<input type="checkbox"/>
Weekly	<input checked="" type="checkbox"/>
Monthly	<input type="checkbox"/>

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

Upon completion settings	<input checked="" type="checkbox"/>
Advanced settings	<input type="checkbox"/>
Programs	<input type="checkbox"/>
Reviewers	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Set the frequency to:

One time	<input type="checkbox"/>
Weekly	<input checked="" type="checkbox"/>
Monthly	<input type="checkbox"/>

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

Upon completion settings	<input checked="" type="checkbox"/>
Advanced settings	<input type="checkbox"/>
Programs	<input type="checkbox"/>
Reviewers	<input type="checkbox"/>

**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	<input checked="" type="checkbox"/>
ATP Safe Links	<input checked="" type="checkbox"/>
Anti-spam	<input type="checkbox"/>
Anti-malware	<input type="checkbox"/>

Option to configure:

Block	<input checked="" type="checkbox"/>
Replace	<input type="checkbox"/>
Dynamic Delivery	<input type="checkbox"/>
Monitor	<input type="checkbox"/>
Quarantine message	<input type="checkbox"/>

- 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**

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 5**

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 6**

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 7**

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 8**

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 9**

HOTSPOT

You are evaluating which devices are compliant in Intune.

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
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input type="radio"/>
Device6 is compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Statements	Yes	No
Device2 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device6 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 10**

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

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

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

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

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

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Source Anchor settings.

Does that meet the goal?

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 10**

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 15**

You have a Microsoft 365 subscription. From the Microsoft 365 admin center, you create a new user. You plan to assign the Reports reader role to the user. You need to see the permissions of the Reports reader role. Which admin center should you use?

- A. Azure Active Directory
- B. Cloud App Security
- C. Security & Compliance
- D. Microsoft 365

**Answer:** A

**NEW QUESTION 16**

Your company has a Microsoft 365 subscription. The company forbids users to enroll personal devices in mobile device management (MDM). Users in the sales department have personal iOS devices. You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant. The users must be prevented from backing up the app's data to iCloud. What should you create?

- A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
- B. an app protection policy in Microsoft Intune
- C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
- D. a device compliance policy in Microsoft Intune

**Answer:** B

**NEW QUESTION 17**

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 22**

**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.

<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

- 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.

<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 26**

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 27**

Your company has 500 computers.

You plan to protect the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP). Twenty of the computers belong to company executives.

You need to recommend a remediation solution that meets the following requirements: Windows Defender ATP administrators must manually approve all remediation for the executives

Remediation must occur automatically for all other users

What should you recommend doing from Windows Defender Security Center?

- A. Configure 20 system exclusions on automation allowed/block lists
- B. Configure two alert notification rules
- C. Download an offboarding package for the computers of the 20 executives
- D. Create two machine groups

**Answer:** D

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/machine-groups/windows-defender-advanced-threat-protection>

**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 34**

HOTSPOT

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

Name	Type	Email address
Group1	Security Group – Domain Local	<a href="mailto:Group1@contoso.com">Group1@contoso.com</a>
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	<a href="mailto:Group4@contoso.com">Group4@contoso.com</a>

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

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

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

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

On-premises Active Directory groups:

Group4 only	<input checked="" type="checkbox"/>
Group1 and Group4 only	<input type="checkbox"/>
Group3 and Group4 only	<input type="checkbox"/>
Group1, Group3, and Group4 only	<input type="checkbox"/>
Group1, Group2, Group3, and Group4	<input type="checkbox"/>

Azure AD groups:

Group13 only	<input checked="" type="checkbox"/>
Group13 and Group14 only	<input type="checkbox"/>
Group11 and Group12 only	<input type="checkbox"/>
Group11, Group13, and Group14 only	<input type="checkbox"/>
Group11, Group12, Group13, and Group14 only	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 35**

HOTSPOT

You have the Microsoft conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	Product1	Off
Condition2	Product2	On

You have the Azure Information Protection labels shown in the following table.

Name	Use condition	Label is applied
Label1	Condition1	Automatically
Label2	Condition2	Automatically

You have the Azure Information Protection policies shown in the following table.

Name	Applies to	Use label	Set the default label
Global	<i>Not applicable</i>	<i>None</i>	None
Policy1	User1	Label1	None
Policy2	User2	Label2	None

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

Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	<input type="radio"/>	<input type="radio"/>
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	<input type="radio"/>	<input type="radio"/>
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 39**

**HOTSPOT**

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

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

The tenant contains the users shown in the following table.

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

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

**Create filters for the policy**

**Act on:**

**Single activity:**  
Every activity that matches the filters

**Repeated activity:**  
Repeated activity by a single user

Minimum repeated activities:

Within timeframe:  minutes

In a single app

Count only unique target files or folders per user

[Edit and preview results](#)

ACTIVITIES MATCHING ALL OF THE FOLLOWING

equals

OR

equals

From group  equals

as

**Alerts**

Create alert Use your organization's default settings  
Daily alert limit 5

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

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

- A. Mastered
- B. Not Mastered

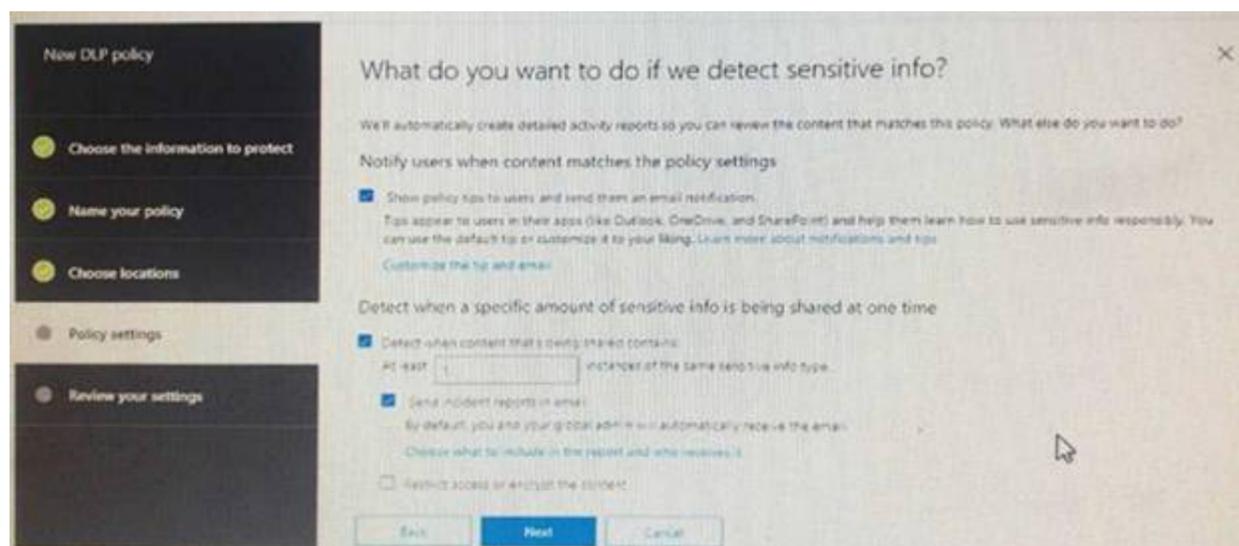
Answer: A

Explanation:

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

**NEW QUESTION 40**

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 41**

**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 43**

**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
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 46**

You have a Microsoft 365 subscription.  
You need to enable auditing for all Microsoft Exchange Online users. What should you do?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 47**

**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 49**

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 51**

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

- A. From the Security & Compliance admin center, create a label policy
- B. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning

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

**Answer:** C

**NEW QUESTION 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 of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group1	Disabled

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

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

User1:  ▼

Blocked
Can sign in without MFA
Prompted for MFA

User2:  ▼

Blocked
Can sign in without MFA
Prompted for MFA

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

User1:  ▼

Blocked
Can sign in without MFA
Prompted for MFA

User2:  ▼

Blocked
Can sign in without MFA
Prompted for MFA

**NEW QUESTION 60**

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 63

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:

The screenshot shows a configuration window for a safe links policy. At the top, there is a text input field with the placeholder text "Enter a valid URL" and a plus sign to its right. Below this field, a list of blocked URLs is displayed: \*.phishing.\*, malware.\*com, and \*.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 365 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 68

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 71

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 73**

**HOTSPOT**

You have a Microsoft 365 subscription that include three users named User1, User2, and User3. A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute. You create an alert policy named Policy1 as shown in the following exhibit.

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

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

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

▼
Policy1 will not be triggered
Policy1 will be triggered after 45 minutes
Policy1 will be triggered after 60 minutes

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

▼
Policy1 will not be triggered
Policy1 will be triggered within 20 minutes
Policy1 will be triggered within 45 minutes
Policy1 will be triggered after 60 minutes

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 78**

You have a Microsoft 365 subscription. All users are assigned a Microsoft 365 E5 license. How long will auditing data be retained?

- A. 30 days
- B. 90 days
- C. 365 days
- D. 5 years

**Answer:** B

**Explanation:**

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

**NEW QUESTION 79**

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 80**

HOTSPOT

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

Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

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

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

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

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

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

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

**NEW QUESTION 85**

**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 Azure Cloud Shell, run the Add-Hso1RoleMember cmdlet.	From the Azure portal, create an RBAC role.

**NEW QUESTION 86**

You have a Microsoft 365 subscription.

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

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

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

**Answer:** A

**NEW QUESTION 89**

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 91**

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

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

You have an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events.

You use the Directory Service event log on Server1. Does that meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

References:

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

**NEW QUESTION 94**

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 99**

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 Event Forwarding on the domain controllers

B. Configure auditing in the Office 365 Security & Compliance center.

C. Turn on Delayed updates for the Azure ATP sensors.

D. Enable the Audit account management Group Policy setting for the servers.

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding>

**NEW QUESTION 100**

.....

## 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>