

➤ **Vendor: Microsoft**

➤ **Exam Code: MS-500**

➤ **Exam Name: Microsoft 365 Security Administration**

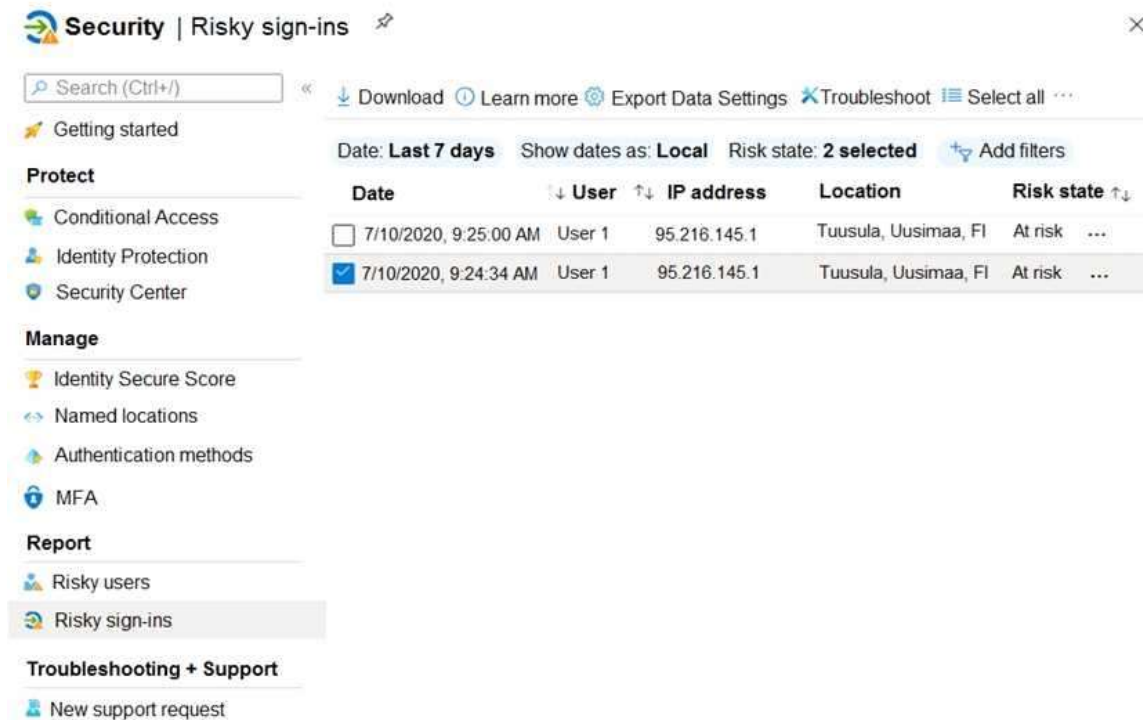
➤ **New Updated Questions from [Braindump2go](#) (Updated in [October/2020](#))**

### **Visit Braindump2go and Download Full Version MS-500 Exam Dumps**

#### **QUESTION 211**

You have a Microsoft 365 tenant.

From the Azure Active Directory admin center, you review the Risky sign-ins report as shown in the following exhibit.



Security | Risky sign-ins

Search (Ctrl+/) Download Learn more Export Data Settings Troubleshoot Select all

Getting started

**Protect**

- Conditional Access
- Identity Protection
- Security Center

**Manage**

- Identity Secure Score
- Named locations
- Authentication methods
- MFA

**Report**

- Risky users
- Risky sign-ins

**Troubleshooting + Support**

- New support request

Date: Last 7 days Show dates as: Local Risk state: 2 selected Add filters

Date	User	IP address	Location	Risk state
<input type="checkbox"/> 7/10/2020, 9:25:00 AM	User 1	95.216.145.1	Tuusula, Uusimaa, FI	At risk ...
<input checked="" type="checkbox"/> 7/10/2020, 9:24:34 AM	User 1	95.216.145.1	Tuusula, Uusimaa, FI	At risk ...

You need to ensure that you can see additional details including the risk level and the risk detection type. What should you do?

- A. Purchase Microsoft 365 Enterprise E5 licenses.
- B. Activate an instance of Microsoft Defender for Identity.
- C. Configure Diagnostic settings in Azure Active Directory (Azure AD).
- D. Deploy Azure Sentinel and add a Microsoft Office 365 connector.

**Answer: A**

#### **QUESTION 212**

You have a Microsoft 365 E5 subscription.

You plan to create a conditional access policy named Policy1.

You need to be able to use the sign-in risk level condition in Policy1.

What should you do first?

[MS-500 Exam Dumps](#) [MS-500 Exam Questions](#) [MS-500 PDF Dumps](#) [MS-500 VCE Dumps](#)

<https://www.braindump2go.com/ms-500.html>

- A. Connect Microsoft Endpoint Manager and Microsoft Defender for Endpoint.
- B. From the Azure Active Directory admin center, configure the Diagnostics settings.
- C. From the Endpoint Management admin center, create a device compliance policy.
- D. Onboard Azure Active Directory (Azure AD) Identity Protection.

**Answer:** D

**Explanation:**

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk>

**QUESTION 213**

You have a hybrid Microsoft 365 deployment that contains the Windows 10 devices shown in the following table.

Name	Trusted Platform Module (TPM) version	Joined to	Microsoft Intune enrolled
Device1	v2.0	Active Directory	Yes
Device2	v2.0	Azure Active Directory (Azure AD)	Yes
Device3	v1.3	Azure Active Directory (Azure AD)	Yes

You assign a Microsoft Endpoint Manager disk encryption policy that automatically and silently enables BitLocker Drive Encryption (BitLocker) on all the devices.

Which devices will have BitLocker enabled?

- A. Device 1, Device2, and Device3
- B. Device2 only
- C. Device1 and Device2 only
- D. Device2 and Device3 only

**Answer:** B

**Explanation:**

To silently enable BitLocker, the device must be Azure AD Joined or Hybrid Azure AD Joined and the device must contain TPM (Trusted Platform Module) 2.0.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices>

**QUESTION 214**

You have a Microsoft 165 E5 subscription.

You need to enable support for sensitivity labels in Microsoft SharePoint Online.

What should you use?

- A. the SharePoint admin center
- B. the Microsoft J65 admin center
- C. the Microsoft 365 compliance center
- D. the Azure Active Directory admin

**Answer:** D

**QUESTION 215**

You have a Microsoft 165 ES subscription that contains users named User 1 and User2.

You have the audit log retention requirements shown in the following table.

User	Action	Retention period
User1	Rename a Microsoft SharePoint Online site.	12 months
User1	Perform all actions in Microsoft Dynamics 365.	6 months
User2	Create a Microsoft SharePoint Online site collection.	12 months
User2	Perform all Microsoft Exchange Online administrative actions.	10 years

You need to create audit retention policies to meet the requirements.

The solution must minimize cost and the number of policies.

What is the minimum number of audit retention policies that you should create?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: C**

#### QUESTION 216

You have a Microsoft 365 subscription named contofco.com.

You need to configure Microsoft OneDrive for Business external sharing to meet the following requirements:

- Enable file sharing for users that have a Microsoft account
- Block file sharing for anonymous users.

What should you do?

- A. From Advanced settings for external sharing, select Allow or Block sharing with people on specific domains and add contoso.com.
- B. From the External sharing settings for OneDrive, select Existing external users.
- C. From the External sharing settings for OneDrive, select New and existing external users.
- D. From the External sharing settings for OneDrive, select Only people in your organization.

**Answer: B**

#### QUESTION 217

You have 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 Alerts, create an alert policy.
- B. From Search & investigation, create a guided search.
- C. From ediscovery create an eDiscovery case
- D. From Reports, create a managed schedule

**Answer: A**

#### QUESTION 218

You have a Microsoft 365 subscription.

You receive a General Data Protection Regulation (GDPR) request for the custom dictionary of a user.

From the Compliance admin center you need to create a content search.

How should you configure the content search?

- A. Condition: Type Operator Equals any of Value Documents
- B. Condition: Type Operator Equals any of Value Office Roaming Service
- C. Condition: Title Operator Equals any of Value. Normal. dot
- D. Condition: file type Operator Equals any of Value: doc

**Answer: D**

**QUESTION 219**

You have a Microsoft 365 subscription.

You receive a General Data Protection Regulation (GDPR) request for the custom dictionary of a user.

From The Compliance admin center you need to create a content search, should you configure the content search?

- A. Condition: Type Operator Equals any of Value Documents
- B. Condition; Type Operator Equals any of Value Office Roaming Service
- C. Condition: Title Operator Equals any of Value Normal. dot
- D. Condition: We type Operator Equals any of Value dic

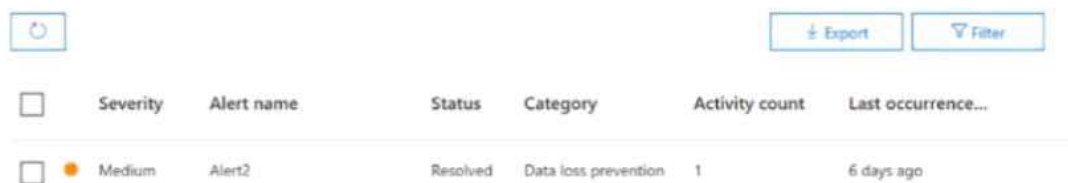
**Answer: A**

**QUESTION 220**

You have a Microsoft 365 alert named Alert?

as shown in the following exhibit.

View alerts



	Severity	Alert name	Status	Category	Activity count	Last occurrence...
<input type="checkbox"/>	Medium	Alert2	Resolved	Data loss prevention	1	6 days ago

You need to manage the status of Alert. To which status can you change Alert2?

- A. The status cannot be changed.
- B. investigating only
- C. Active or investigating only
- D. Investigating, Active, or Dismissed
- E. Dismissed only

**Answer: E**

**QUESTION 221**

You have a Microsoft 365 subscription linked to an Azure Active Directory (Azure AD) tenant that contains a user named User1.

You need to grant User1 permission to search Microsoft 365 audit logs. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. the View-Only Audit Logs role in the Security & Compliance admin
- B. the Security reader role in the Azure Active Directory admin center
- C. the View-Only Audit Logs role in the Exchange admin center
- D. the Compliance Management role in the Exchange admin center

**Answer: B**

**QUESTION 222**

You have a Microsoft 365 tenant that uses Azure Information Protection to encrypt sensitive content.

You plan to implement Microsoft Cloud App Security to inspect protected files that are uploaded to Microsoft OneDrive for Business.

You need to ensure that at Azure Information Protection-protected files can be scanned by using Cloud App Security. 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, enable file monitoring of software as a service (SaaS) apps.

- B. From the Cloud App Security admin center, create an OAuth app policy for apps that have the Have full access to user files permission
- C. From the Microsoft 365 compliance admin center create a data loss prevention (EXP) policy that contains an exception for content that contains a sensitive information type.
- D. From the Azure Active Directory admin center, grant Cloud App Security permission to read all the protected content of the tenant

**Answer:** BD

#### QUESTION 223

You have an Azure Acme Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Group	Role
User1	Microsoft Defender for Identity Contoso Users	None
User2	Microsoft Defender for Identity Contoso Viewers	None
User3	Not applicable	Security administrator
User4	Not applicable	Security operator

You discover several security alerts are visible from the Microsoft Defender for Identity portal. You need to identify which users in contoso.com can close the security Alerts. Which users should you identify?

- A. User1 only
- B. User1 and User3 only
- C. User1 and User2 only
- D. User4 only
- E. User3 and User4 only

**Answer:** E

#### QUESTION 224

You have an Azure Active Directory (Azure AD) tenant that has a Microsoft 365 subscription. You recently configured the tenant to require multi factor authentication (MFA) for risky sign ins. You need to review the users who required MFA. What should you do?

- A. From the Microsoft 365 admin center, review a Security & Compliance report.
- B. From the Azure Active Directory admin center, download the sign-ins to a CSV file
- C. From the Microsoft 365 Compliance admin center, run an audit log search and download the results to a CSV file
- D. From the Azure Active Directory admin center, review the Authentication methods activities.

**Answer:** D

#### QUESTION 225

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not

[MS-500 Exam Dumps](#) [MS-500 Exam Questions](#) [MS-500 PDF Dumps](#) [MS-500 VCE Dumps](#)

<https://www.braindump2go.com/ms-500.html>

affect User 4.

Solution: You enable SSPR for Group1.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**QUESTION 226**

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User 4.

Solution: You create a conditional access policy for User1, User2, and User3.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**QUESTION 227**

You have a hybrid Azure Active Directory (Azure AD) tenant that has pass-through authentication enabled.

You plan to implement Azure AD identity Protection and enable the user risk policy.

You need to configure the environment to support the user risk policy.

- A. Enable password hash synchronization.
- B. Configure a conditional access policy.
- C. Enforce the multi-factor authentication (MFA) registration policy.
- D. Enable the sign-in risk policy.

**Answer: C**

**QUESTION 228**

You have a Microsoft 365 E5 subscription and an Sentinel workspace named Sentinel1.

You need to launch the Guided investigation ?Process Alerts notebooks= in Sentinel.

What should you create first?

- A. a Log Analytic workspace
- B. a Kusto query
- C. an Azure Machine learning workspace
- D. an Azure logic app

**Answer: B**

**QUESTION 229**

You have a Microsoft 365 E5 subscription

You need to ensure that users who are assigned the Exchange administrator role have time-limited permissions and



must use multi factor authentication (MFA) to request the permissions.  
What should you use to achieve the goal?

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

**Answer: D**

#### **QUESTION 230**

You have a Microsoft 365 subscription that contains several Windows 10 devices.  
The devices are managed by using Microsoft Endpoint Manager.  
You need to enable Microsoft Defender Exploit Guard (Microsoft Defender EG) on the devices.  
Which type of device configuration profile should you use?

- A. Endpoint protection
- B. Device restrictions
- C. Microsoft Defender for Endpoint
- D. identity protection

**Answer: A**

#### **QUESTION 231**

You have a Microsoft 365 subscription.  
You have a Microsoft SharePoint Online site named Site1.  
You have a Data Subject Request X>SR1 case named Case1 that searches Site1.  
You create a new sensitive information type.  
You need to ensure that Case1 returns all the documents that contain the new sensitive information type.  
What should you do?

- A. From the Compliance admin center, create a new Content search.
- B. From Site1, modify the search dictionary.
- C. From Site1, initiate a re-indexing of Site1.
- D. From the Compliance admin center, create a new Search by ID List.

**Answer: C**

#### **QUESTION 232**

You have a Microsoft 365 E5 subscription that contains a user named User1.  
The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1.  
For User1, you select Confirm user compromised.  
User1 can still sign in.  
You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.  
Solution: You configure the user risk policy to block access when the user risk level is high.  
Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

#### **QUESTION 233**

You have a Microsoft 365 E5 subscription that contains a user named User1.  
The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1.  
For User1, you select Confirm user compromised.  
User1 can still sign in.

You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.

Solution: You configure the user risk policy to block access when the user risk level is medium and higher.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### **QUESTION 234**

You have a Microsoft 365 E5 subscription that contains a user named User1.

The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1.

For User1, you select Confirm user compromised.

User1 can still sign in.

You need to prevent User1 from signing in. The solution must minimize the impact on users at a tower risk level.

Solution: From the Access settings, you select Block access for User1.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### **QUESTION 235**

You have a Microsoft 365 E5 subscription

You need to use Microsoft Cloud App Security to identify documents stored in Microsoft SharePoint Online that contain proprietary information.

What should you create in Cloud App Security?

- A. a data source and a file policy
- B. a data source and an app discovery policy
- C. an app connector and an app discovery policy
- D. an app connector and a We policy

**Answer: B**

#### **QUESTION 236**

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Configuration
DC1	Domain controller
Server1	Member server

You plan to implement Microsoft Defender for Identity for the domain.

You install a Microsoft Defender for Identity standalone sensor on Server 1.

You need to monitor the domain by using Microsoft Defender for Identity.

What should you do?

- A. Configure port mirroring for DO.
- B. Install the Microsoft Monitoring Agent on DC1.
- C. Configure port mirroring for Server1.
- D. Install the Microsoft Monitoring Agent on Server 1.

**Answer: B**

#### **QUESTION 237**

Hotspot Question

[MS-500 Exam Dumps](#) [MS-500 Exam Questions](#) [MS-500 PDF Dumps](#) [MS-500 VCE Dumps](#)

<https://www.braindump2go.com/ms-500.html>



You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Type	Member of
User1	Member	Group1
User2	Member	Group2
User3	Guest	Group1

You assign an enterprise application named App1 to Group1 and User2.

You configure an Azure AD access review of App1. The review has the following settings:

Review name: Review1

Start date: 01-15-2020

Frequency: One time

End date: 02-14-2020

Users to review: Assigned to an application

Scope: Everyone

Applications: App1

Reviewers: Members (self)

Auto apply results to resource: Enable

Should reviewer not respond: Take recommendations

On February 15, 2020, you review the access review report and see the entries shown in the following table:

Name	User requires access to App1	Last sign in
User1	Yes	February 14, 2020
User2	No response	February 1, 2020
User3	No response	January 3, 2020

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
On February 20, 2020, User1 can access App1.	<input type="radio"/>	<input type="radio"/>
On February 20, 2020, User2 can access App1.	<input type="radio"/>	<input type="radio"/>
On February 20, 2020, User3 can access App1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
On February 20, 2020, User1 can access App1.	<input checked="" type="radio"/>	<input type="radio"/>
On February 20, 2020, User2 can access App1.	<input checked="" type="radio"/>	<input type="radio"/>
On February 20, 2020, User3 can access App1.	<input type="radio"/>	<input checked="" type="radio"/>

**QUESTION 238**

Hotspot Question

You have an Azure Sentinel workspace.

You configure a rule to generate Azure Sentinel alerts when Azure Active Directory (Azure AD) Identity Protection detects risky sign-ins. You develop an Azure Logic Apps solution to contact users and verify whether reported risky sign-ins are legitimate.

You need to configure the workspace to meet the following requirements:

- Call the Azure logic app when an alert is triggered for a risky sign-in.
- To the Azure Sentinel portal, add a custom dashboard that displays statistics for risky sign-ins that are detected and resolved.

What should you configure in Azure Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Call the logic app:

	▼
An entity mapping	
A hunting query	
A notebook	
A playbook	
A workbook	

Displays statistics for risky sign-ins:

	▼
An entity mapping	
A hunting query	
A notebook	
A playbook	
A workbook	

**Answer:**

Call the logic app:

	▼
An entity mapping	
A hunting query	
A notebook	
A playbook	
A workbook	

Displays statistics for risky sign-ins:

	▼
An entity mapping	
A hunting query	
A notebook	
A playbook	
A workbook	

**Explanation:**

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>