



MS-500^{Q&As}

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

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

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to create a conditional access policy named Policy1 that meets the following requirements:

1.

Enforces multi-factor authentication (MFA)

2.

Requires that users reauthenticate after eight hours

Which settings should you configure in Policy1 for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Enforces MFA:

	▼
Grant	
Session	
Conditions	
Cloud apps or actions	

Requires that users reauthenticate after eight hours:

	▼
Grant	
Session	
Conditions	
Cloud apps or actions	

Correct Answer:



Answer Area

Enforces MFA:

	▼
Grant	
Session	
Conditions	
Cloud apps or actions	

Requires that uses reauthenticate after eight hours:

	▼
Grant	
Session	
Conditions	
Cloud apps or actions	

QUESTION 2

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions sets might have more than one correct solution,

while others might not have a correct solution.

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

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

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.



Solution: You recommend assigning the Compliance Manager Reader role to User5.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

QUESTION 3

You have a Microsoft 365 tenant that is linked to a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

You need to enable Azure AD Seamless Single Sign-On (Azure AD SSO) for contoso.com.

What should you use?

A. Azure AD Connect

B. the Azure Active Directory admin center

C. the Microsoft 365 Security admin center

D. the Microsoft 365 admin center

Correct Answer: A

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ssso-quick-start>

QUESTION 4

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 contains 100 users and has dynamic user membership.

All users have Windows 10 devices and use Microsoft SharePoint Online and Exchange Online.

You create a sensitivity label named Label and publish Label 1 as the default label for Group1.

You need to ensure that the users in Group1 must apply Label1 to their email and documents.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Install the Azure Information Protection unified labeling client on the Windows 10 devices.

B. From the Microsoft 365 Compliance center, modify the settings of the Label1 policy.

C. Install the Active Directory Rights Management Services (AD RMS) client on the Windows 10 devices.



- D. From the Microsoft 365 Compliance center, create an auto-labeling policy.
- E. From the Azure Active Directory admin center, set Membership type for Group1 to Assigned.

Correct Answer: AB

D is wrong. Auto-Labeling policy will not achieve the requirement “You need to ensure that the users in Group1 must apply Label1 to their email and documents”

This requirement is a setting in the sensitivity label policy that can be selected.

Auto-Labeling is an admin activity.

Auto-Labeling policy:

When you create a sensitivity label, you can automatically assign that label to files and emails when it matches conditions that you specify.

This ability to apply sensitivity labels to content automatically is important because:

1.

You don't need to train your users when to use each of your classifications.

2.

You don't need to rely on users to classify all content correctly.

3.

Users no longer need to know about your policies—they can instead focus on their work.

E is wrong. It is not a must to Membership type for Group1 to be Assigned. Label can be applied to both Assigned and Dynamic.

QUESTION 5

HOTSPOT

You company has a Microsoft 365 E5 subscription and a hybrid Azure active Directory named contoso.com.

Contoso.com includes the following users:

Name	Password	Source
User1	CoNtOsO.Password	Azure Active Directory
User2	P1AiNPWD	Azure Active Directory
User3	MyV3rrYC0mplexPWD	Windows Server Active Directory (AD)

You configure Password protection for Contoso.com as shown in the following exhibit.



Custom smart lockout

Lockout threshold ⓘ

 ✓

Lockout duration in seconds ⓘ

 ✓

Custom banned passwords

Enforce custom list ⓘ

 Yes No

Custom banned password list ⓘ

 ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

 Yes No

Mode ⓘ

 Enforced Audit

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

Hot Area:



- | | Yes | No |
|---|-----------------------|-----------------------|
| User1 must change his password next time he authenticates to Azure Active Directory | <input type="radio"/> | <input type="radio"/> |
| User2 can change his password to C0NT0\$0C0NT0\$0 | <input type="radio"/> | <input type="radio"/> |
| User3 can change his password to myC0NT0\$0c0mp1exPwD | <input type="radio"/> | <input type="radio"/> |

Correct Answer:

- | | Yes | No |
|---|----------------------------------|----------------------------------|
| User1 must change his password next time he authenticates to Azure Active Directory | <input type="radio"/> | <input checked="" type="radio"/> |
| User2 can change his password to C0NT0\$0C0NT0\$0 | <input checked="" type="radio"/> | <input type="radio"/> |
| User3 can change his password to myC0NT0\$0c0mp1exPwD | <input checked="" type="radio"/> | <input type="radio"/> |

Audit mode is the default initial setting, where passwords can continue to be set. Passwords that would be blocked are recorded in the event log. After you deploy the proxy servers and DC agents in audit mode, monitor the impact that the password policy will have on users when the policy is enforced.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

[Latest MS-500 Dumps](#)

[MS-500 Study Guide](#)

[MS-500 Exam Questions](#)