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.pass4itsure.com/ms-500.html

100% Passing Guarantee
100% Money Back Assurance

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

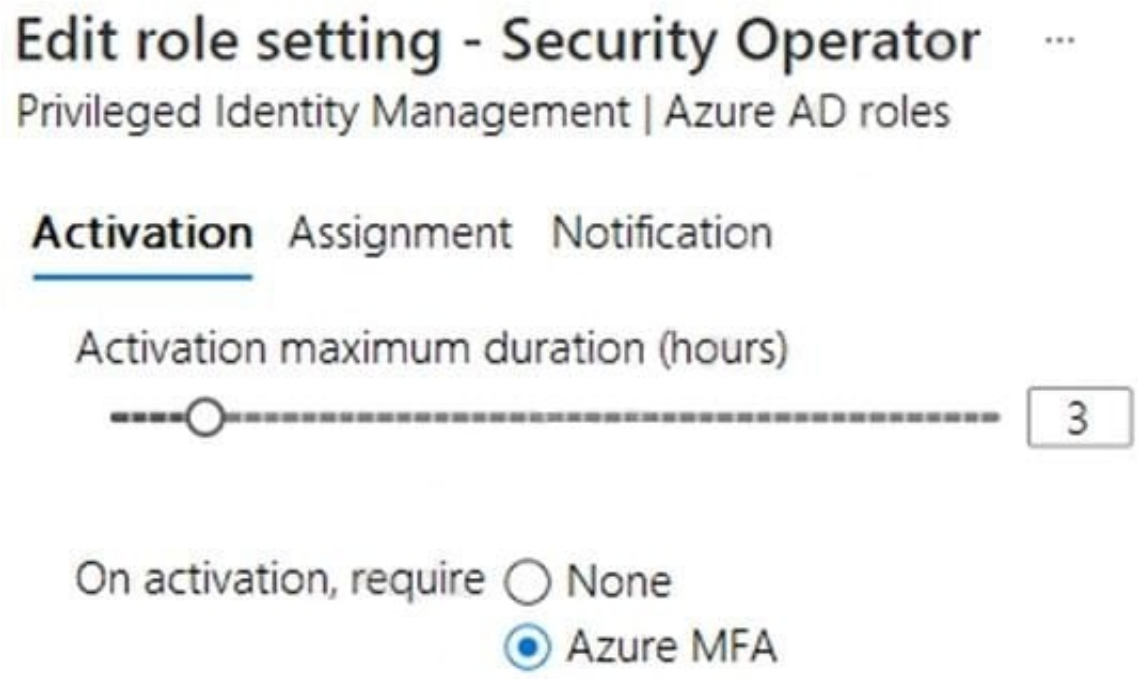
- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

You configure the Security Operator role in Azure AD Privileged Identity Management (PIM) as shown in the following exhibit.



You add assignments to the Security Operator role as shown in the following table.

Name	Assignment type
User1	Eligible
User2	Eligible
User3	Active

Which users can activate the Security Operator role?

A. User2 only

B. User3 only

C. User1 and User2 only

D. User2 and User3 only

E. User1, User2, and User3

Correct Answer: D

QUESTION 2

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

Correct Answer: D

Enforce read-only mode for external users in real time

Prevent company data from being exfiltrated by external users, by blocking print and copy/paste activities in real-time, utilizing Cloud App Security\\'s session controls.

References:

https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad

QUESTION 3

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 and Compliance admin center

B. the View-Only Audit Logs role in the Exchange admin center

C. the Compliance Management role in the Exchange admin center

D. the Security reader role in the Azure Active Directory admin center

Correct Answer: B

There is no View-Only Audit logs role in Exchange Admin Center. The documentation for the View-Only Logs role also state that it applies to Exchange Server 2013 Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide https://learn.microsoft.com/en-us/exchange/view-only-audit-logs-role-exchange-2013-help

QUESTION 4

DRAG DROP

Your company has two departments named department1 and department2 and a Microsoft 365 E5 subscription.

You need to prevent communication between the users in department1 and the users in department2.

How should you complete the PowerShell script?

To answer, drag the appropriate values to the correct targets. Each value 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.

NOTE: Each correct selection is worth one point.

Select and Place:

Values

New-InformationBarrierPolicy	Set-InformationBarrierPolicy
New-OrganizationSegment	Set-OrganizationSegment

Answer Area

```
[ ]
-Name "Department1" -UserGroupFilter "Department -eq 'department1'"
...
[ ]
-Name "Department1and2" -AssignedSegment "Department1"
-SegmentsBlocked "Department2" -State Active
```

Correct Answer:

Box 1: New-OrganizationSegment Use the New-OrganizationSegment cmdlet to create organization segments for use with information barrier policies in the Microsoft Purview compliance portal.

Organization Segments are not in effect until you apply information barrier policies.

Syntax:

New-OrganizationSegment [-Name]

-UserGroupFilter

[-Confirm]

[-WhatIf]

[]

Box 2: New-InformationBarrierPolicy

To define your first blocking policy, use the New-InformationBarrierPolicy cmdlet with the SegmentsBlocked parameter.

Reference:

https://docs.microsoft.com/en-us/powershell/module/exchange/new-organizationsegment

https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies

QUESTION 5

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:

1.

Source Anchor: objectGUID

2.

Password Hash Synchronization: Disabled

3.

Password writeback: Disabled

4.

Directory extension attribute sync: Disabled

5.

Azure AD app and attribute filtering: Disabled

6.

Exchange hybrid deployment: Disabled

7.

User writeback: Disabled

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

Solution: You modify the Password Hash Synchronization settings.

Does that meet the goal?

A. Yes

B. No

Correct Answer: A

Enabling PHS will meet the requirement.

Leaked credential detection is done by trying a list of known-exposed credentials against your users\\' password hashes to discover one being used in your directory. It\\'s done in Azure, so unless you sync password hashes into Azure AD, the service has nothing to check against. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#password-hash-synchronization