

## MS-500<sup>Q&As</sup>

Microsoft 365 Security Administration

**Pass Microsoft MS-500 Exam with 100% Guarantee**

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

<https://www.leads4pass.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 Sentinel workspace that has an Azure Active Directory (Azure AD) connector and a Microsoft Office 365 connector. You need to assign built-in role-based access control (RBAC) roles to achieve the following tasks:

1.

Create and run playbooks.

2.

Manage incidents.

The solution must use the principle of least privilege.

Which two roles should you assign? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Automation Operator
- B. Azure Sentinel responder
- C. Automation Runbook Operator
- D. Azure Sentinel contributor
- E. Logic App contributor

Correct Answer: DE

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

Refer to the table

Microsoft Sentinel Contributor + Logic App Contributor

Create and run playbooks

Manage incidents (dismiss, assign, etc.)

Microsoft Sentinel roles and allowed actions

The following table summarizes the Microsoft Sentinel roles and their allowed actions in Microsoft Sentinel.

---

**QUESTION 2****HOTSPOT**

You have a Microsoft 365 E5 subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains three groups named Group1, Group2, and Group3 and the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You create a new access package as shown in the following exhibit.

## New access package ...

\* Basics   Resource roles   \* Requests   Requestor information

\* Lifecycle   Review + Create

Summary of access package configuration

### Basics

Name Package1  
Description Package1 description  
Catalog name General

### Resource roles

Resource	Type	Sub Type	Role
Group1	Group and Team	Security Group	Member
Group3	Group and Team	Security Group	Member
Site1	SharePoint Site	SharePoint Online Site	Site1 Members

### Requests

Users who can request access For users in your directory(Group2)  
Require approval No  
Enabled Yes

### Requestor information

#### Questions

Question	Answer format	Required
----------	---------------	----------

### Lifecycle

Access package assignments expire After 10 days  
Require access reviews No

You assign Package1 on June 1, 2021, by using die following configurations:

1.

Select users: User1, User2, User3

2.

Select policy: Initial policy

3.

Assignment starts: June 1, 2021

4.

Assignment ends: July 1, 2021

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:

Statements	Yes	No
On June 5, 2021, User1 can access Package1.	<input type="radio"/>	<input type="radio"/>
On June 15, 2021, User2 can access Package1.	<input type="radio"/>	<input type="radio"/>
On June 5, 2021, User1, User2, and User3 are members of Group3.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
On June 5, 2021, User1 can access Package1.	<input checked="" type="radio"/>	<input type="radio"/>
On June 15, 2021, User2 can access Package1.	<input type="radio"/>	<input checked="" type="radio"/>
On June 5, 2021, User1, User2, and User3 are members of Group3.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes

Box 2: No Lifecycle, Access package assignments expires: After 10 days

Box 3: Yes The access package resource roles includes: Group3 Member Note: Entitlement management introduces to Azure AD the concept of an access package. An access package is a bundle of all the resources with the access a user needs to work on a project or perform their task. Access packages are used to govern access for your internal employees, and also users outside your organization. Here are the types of resources you can manage user's access to, with entitlement management:

1.

Membership of Azure AD security groups

2.

Membership of Microsoft 365 Groups and Teams

3.

Assignment to Azure AD enterprise applications, including SaaS applications and custom-integrated applications that support federation/single sign-on and/or provisioning

4.

Membership of SharePoint Online sites

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview>

---

### QUESTION 3

#### HOTSPOT

You have a Microsoft Sentinel workspace that has an Azure Active Directory (Azure AD) connector and an Office 365 connector.

From the workspace, you plan to create an analytics rule that will be based on a custom query and will run a security play.

You need to ensure that you can add the security playbook and the custom query to the rule.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Set the template type of the analytics rule to: ▼
Fusion
Scheduled
Microsoft security
Machine learning behavioral analytics

Configure the security playbook to include: ▼
A trigger
Diagnostic settings
A user-assigned managed identity
A system-assigned managed identity

Correct Answer:

Set the template type of the analytics rule to: ▼
Fusion
<b>Scheduled</b>
Microsoft security
Machine learning behavioral analytics

Configure the security playbook to include: ▼
<b>A trigger</b>
Diagnostic settings
A user-assigned managed identity
A system-assigned managed identity

Box 1: Scheduled Create a custom analytics rule with a scheduled query

1.  
From the Microsoft Sentinel navigation menu, select Analytics.
2.  
In the action bar at the top, select +Create and select Scheduled query rule. This opens the Analytics rule wizard.
3.  
Etc.

Box 2: A trigger

Use triggers and actions in Microsoft Sentinel playbooks.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom> <https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions#microsoft-sentinel-triggers-summary>

#### QUESTION 4



HOTSPOT

You have a Microsoft 365 Tenant.

A conditional access policy is configured for the tenant as shown in the Policy exhibit. (Click the Policy tab.)

... > Security > Conditional Access >

## Require MFA for all users

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

**Name \***

Require MFA for all users

**Assignments**

- Users and groups** > All users included and specific use...
- Cloud apps or actions** > All cloud apps
- Conditions** > 1 condition selected

### Grant

Control user access enforcement to block or grant access. [Learn more](#)

- Block access
- Grant access
  - Require multi-factor authentication
  - Require device to be marked as compliant
  - Require Hybrid Azure AD joined device
  - Require approved client app [See list of approved client apps](#)
  - Require app protection policy (Preview) [See list of policy protected client apps](#)
  - Require password change (Preview)

For multiple controls

The User Administrator role is configured as shown in the Role setting exhibit (Click the Role setting tab.)



# User Administrator | Role settings

Privileged Identity Management | Azure AD roles



Edit

## Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	<a href="#">1 Member(s)</a> , <a href="#">0 Group(s)</a>

## Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication o...	Yes
Require justification on active assignment	Yes

The User Administrator role has the assignments shown in the Assignments exhibit (Click the Assignments tab.)

Name	Principal name	Type	Scope	Membership	Start time	End time	Action
Admin2	Admin2@sk200510outlc	User	Directory	Direct	8/27/2020, 8:37:06 AM	Permanent	Remove   Update   Extend
Admin3	Admin3@sk200510outlc	User	Directory	Direct	8/27/2020, 8:37:08 AM	Permanent	Remove   Update   Extend
Admin1	Admin1@sk200510outlc	User	Directory	Direct	8/27/2020, 8:37:01 AM	Permanent	Remove   Update   Extend

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
Before Admin1 can perform a task that requires the User Administrator role, the approver must approve the activation request	<input type="radio"/>	<input type="radio"/>
Admin2 can request that the User Administrator role be activated for a period of two hours	<input type="radio"/>	<input type="radio"/>
Admin3 will be prompted to authenticate by using Azure Multi-Factor Authentication(MFA) when the user signs in to the Azure Active Directory admin center, and again when the user activates the User Administrator role	<input type="radio"/>	<input type="radio"/>

Correct Answer:

	Yes	No
Before Admin1 can perform a task that requires the User Administrator role, the approver must approve the activation request	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can request that the User Administrator role be activated for a period of two hours	<input checked="" type="radio"/>	<input type="radio"/>
Admin3 will be prompted to authenticate by using Azure Multi-Factor Authentication(MFA) when the user signs in to the Azure Active Directory admin center, and again when the user activates the User Administrator role	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes

In this scenario the User Administrator role is require justification on active assignment.

Require justification

You can require that users enter a business justification when they activate. To require justification, check the Require justification on active assignment box or the

Require justification on activation box.

Box 2: Yes

Activation maximum duration is 8 hours.

Box 3: Yes

Require multifactor authentication

Privileged Identity Management provides enforcement of Azure AD Multi-Factor Authentication on activation and on active assignment.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>

---

## QUESTION 5

You have a Microsoft 365 subscription.

You create a supervision policy named Policy1, and you designate a user named User1 as the reviewer.

What should User1 use to view supervised communications?

- A. a team in Microsoft Teams
- B. the Security and Compliance admin center / the Microsoft 365 Compliance center
- C. Outlook on the web
- D. the Exchange admin center

Correct Answer: B

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/supervision-policies?view=o365-worldwide>

[MS-500 PDF Dumps](#)

[MS-500 Practice Test](#)

[MS-500 Exam Questions](#)