Vendor: Microsoft

Exam Code:MS-500

Exam Name: Microsoft 365 Security Administration

Version: Demo

QUESTION 1

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Microsoft 365 role
User1	Global Administrator
User2	Security Administrator
User3	Security Operator
User4	Security Reader
User5	Application Administrator

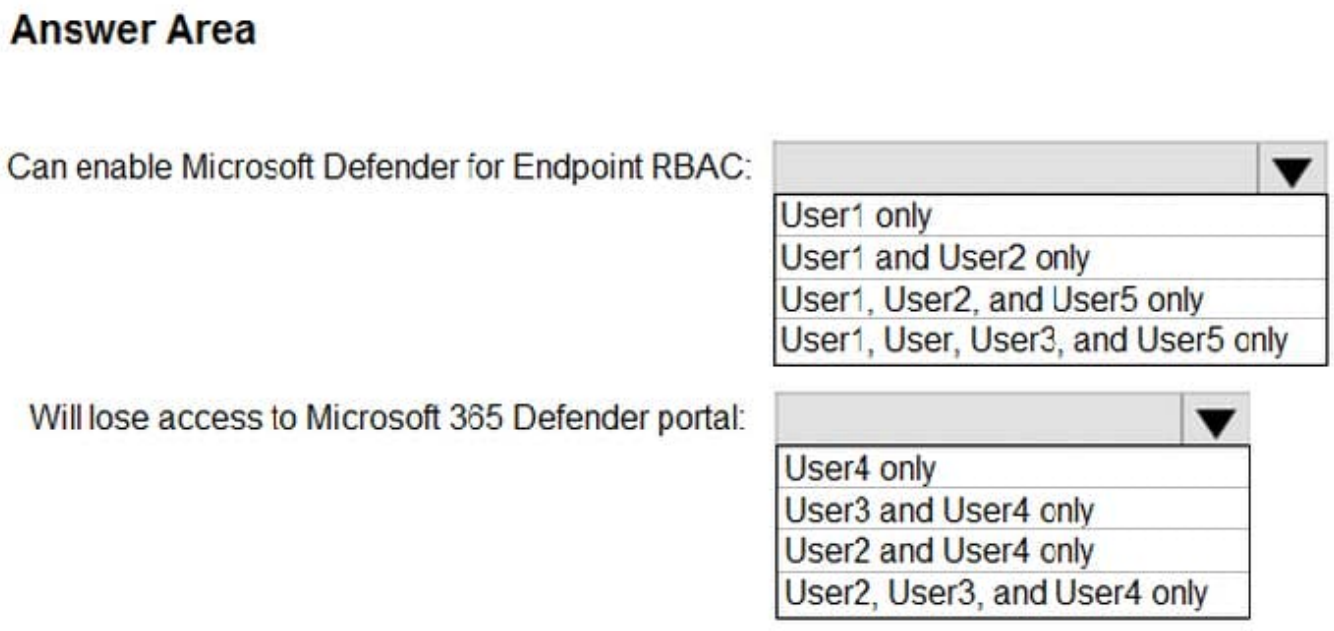
You plan to enable Microsoft Defender for Endpoint role-based access control (RBAC).

You need to identify which users can enable RBAC in Microsoft Defender for Endpoint, and which users will lose access to Microsoft 365 Defender portal after RBAC in enabled.

Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area

Can enable Microsoft Defender for Endpoint RBAC:

- User1 only
- User1 and User2 only
- User1, User2, and User5 only
- User1, User, User3, and User5 only

Will lose access to Microsoft 365 Defender portal:

- User4 only
- User3 and User4 only
- User2 and User4 only
- User2, User3, and User4 only

QUESTION 2

HOTSPOT

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:

1.

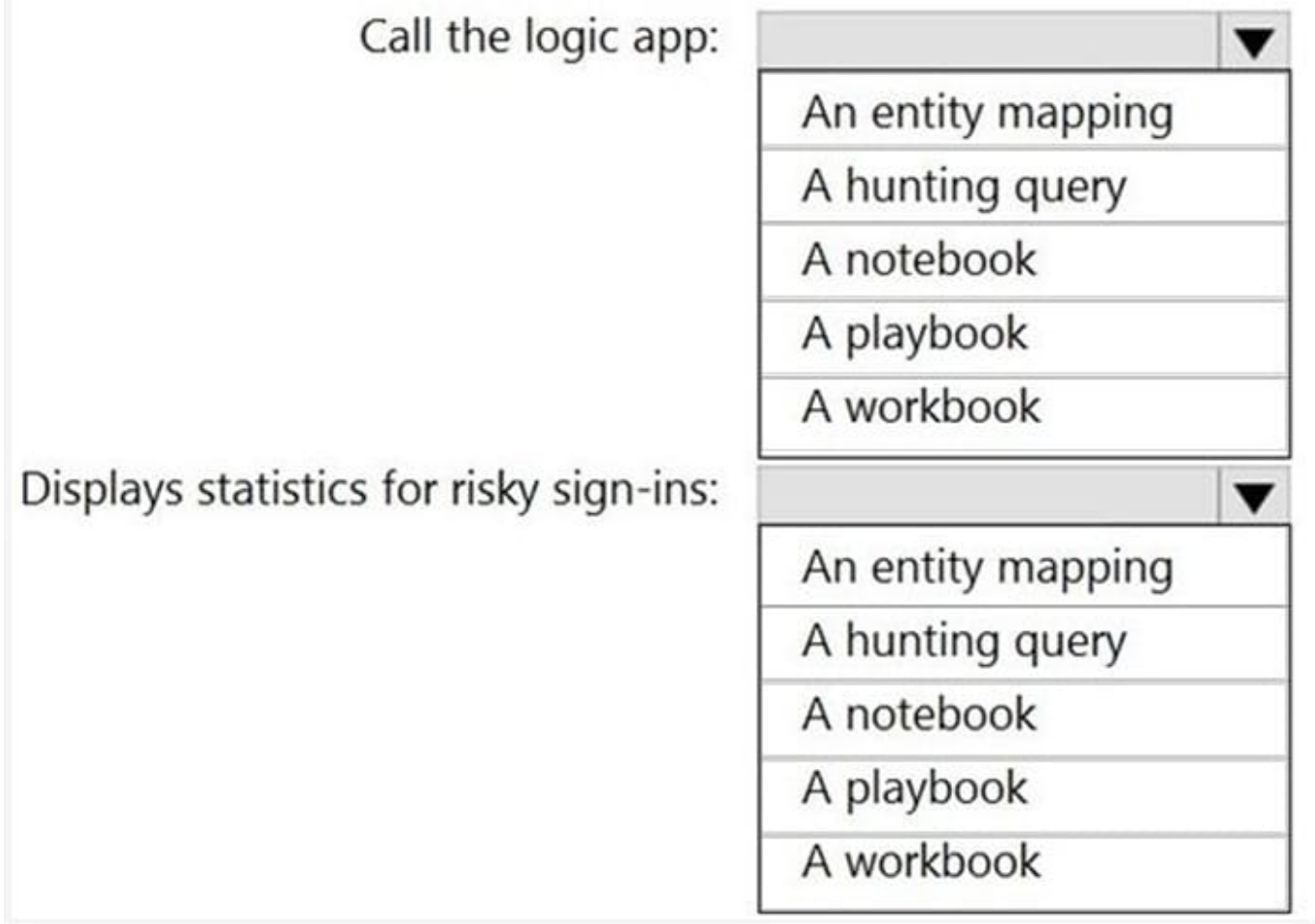
Call the Azure logic app when an alert is triggered for a risky sign-in.

2.

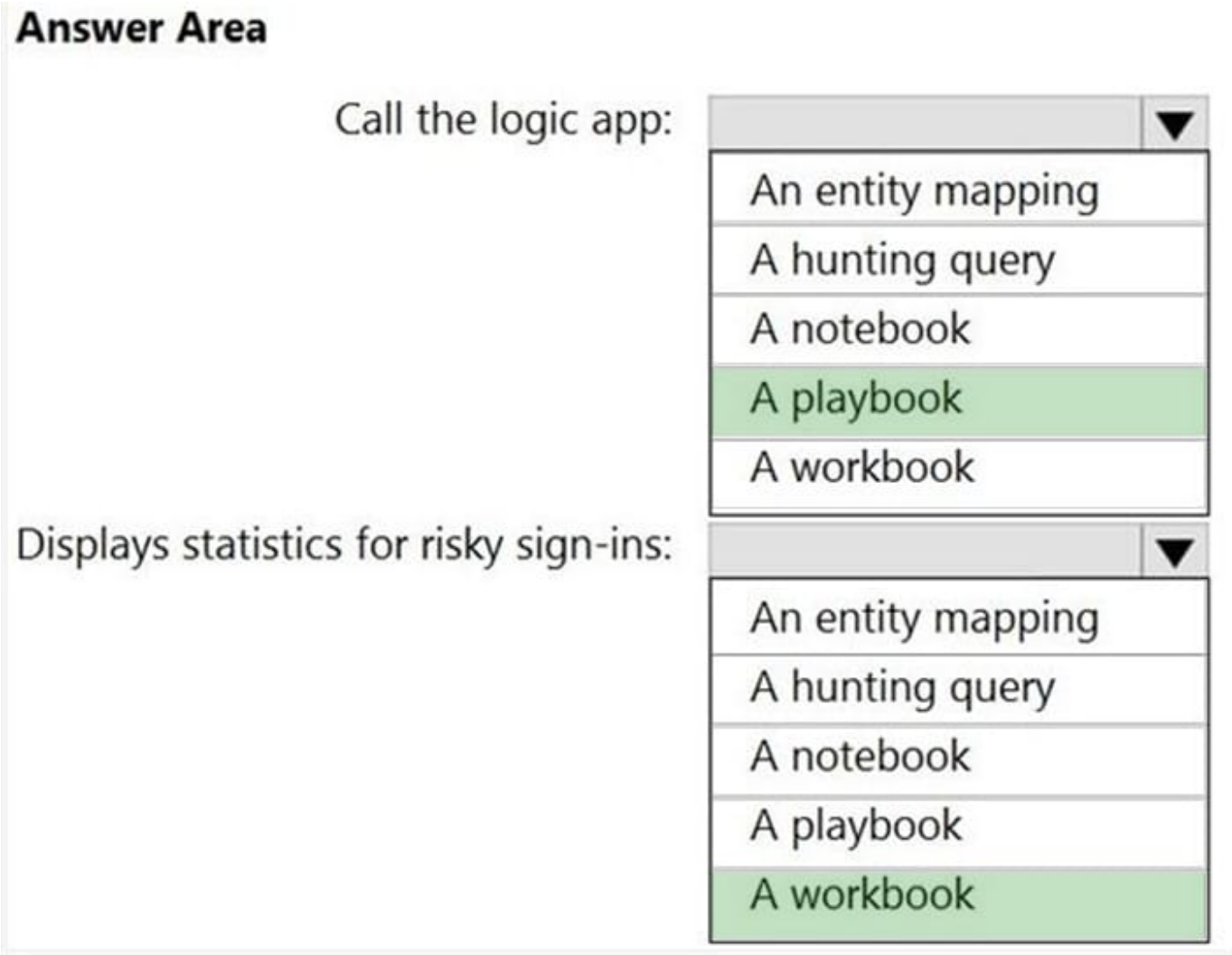
To the Azure Sentinel portal, add a custom dashboard that displays statistics for risky sign-ins that are detected and resolved. What should you configure in Azure Sentinel to meet each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Correct Answer:



Call the Azure logic app when an alert is triggered for a risky sign-in > a playbook https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

displays statistics for risky sign-ins that are detected and resolved > a workbook https://docs.microsoft.com/en-gb/azure/azure-monitor/visualize/workbooks-overview

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

---

QUESTION 3

DRAG DROP

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Identity. You receive the following alerts:

1.

Suspected Netlogon privilege elevation attempt

2.

Suspected Kerberos SPN exposure

3.

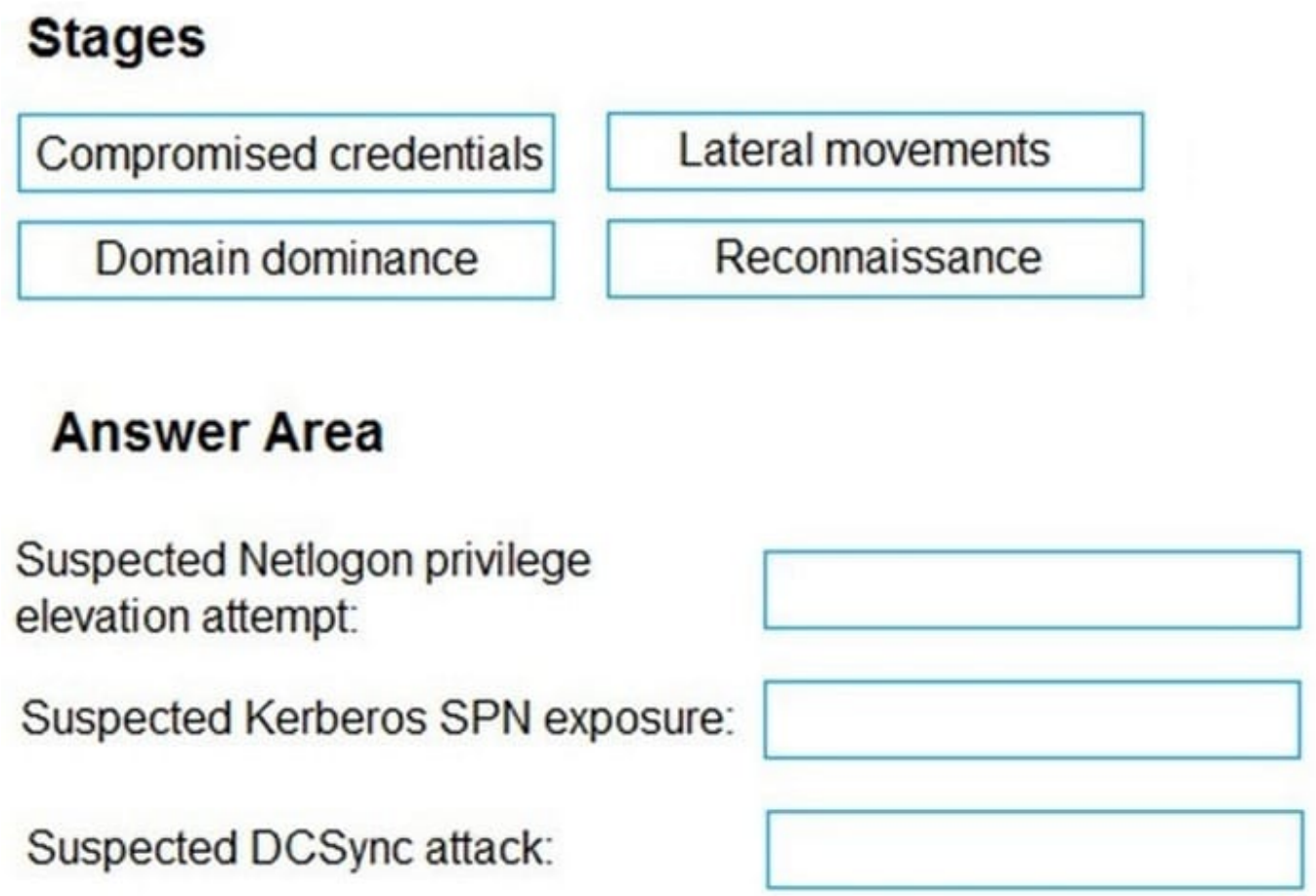
Suspected DCSync attack

To which stage of the cyber-attack kill chain does each alert map? To answer, drag the appropriate alerts to the correct stages. Each alert may be used once, more than once, or not at all. You may need to drag the split bar between panes or

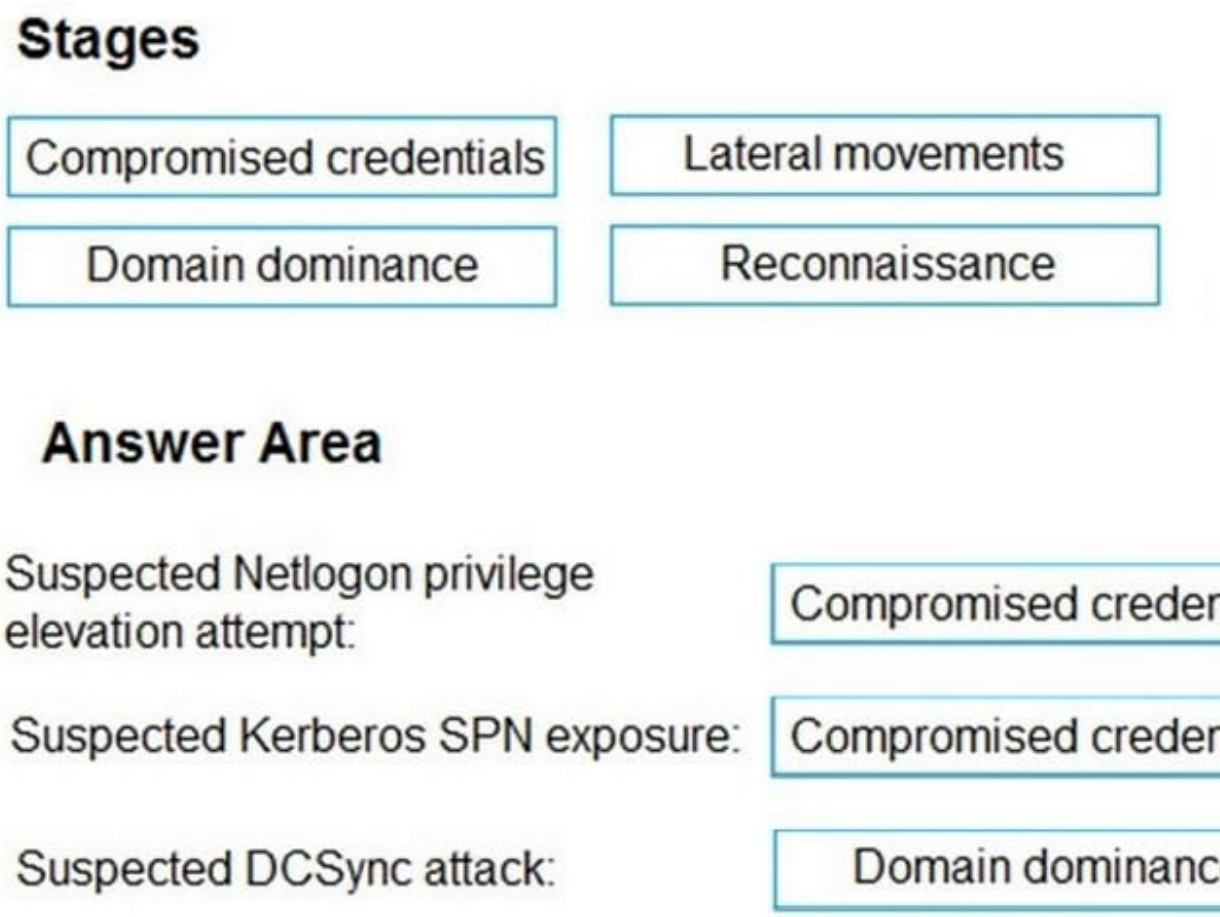
scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: Compromised credential

The following security alerts help you identify and remediate Compromised credential phase suspicious activities detected by Defender for Identity in your network.

In this tutorial, you\\'ll learn how to understand, classify, remediate and prevent the following types of attacks:

Suspected Netlogon privilege elevation attempt (CVE-2020-1472 exploitation) (external ID 2411)

Suspected Kerberos SPN exposure (external ID 2410)

Etc.

Box 2: Compromised credential

Box 3: Domain dominance

The following security alerts help you identify and remediate Domain dominance phase suspicious activities detected by Defender for Identity in your network. In this tutorial, learn how to understand, classify, prevent, and remediate the

following attacks:

Suspected DCSync attack (replication of directory services) (external ID 2006)

Etc.

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/compromised-credentials-alerts https://docs.microsoft.com/en-us/defender-for-identity/domain-dominance-alerts

---

QUESTION 4

You have a Microsoft 365 subscription.

You need to create data loss prevention (DLP) queries in Microsoft SharePoint Online to find sensitive data stored in sites.

Which type of site collection should you create first?

A. Records Center

B. eDiscovery Center

C. Enterprise Search Center

D. Document Center

Correct Answer: B

Reference: https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bb-b944-448d-b83d-8fec4abcc24c

---

QUESTION 5

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Application administrator
User2	Security administrator
User3	Security operator
User4	User administrator

You need to identify which user can enable Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) roles. Which user should you identify?

A. User1

B. User2

C. User3

D. User4

Correct Answer: B

The Security Administrator and the Global Administrator can enable roles in the Microsoft Defender portal. Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/rbac

---

QUESTION 6

You need to recommend a solution to protect the sign-ins of Admin1 and Admin2. What should you include in the recommendation?

A. a device compliance policy

B. an access review

C. a user risk policy

D. a sign-in risk policy

Correct Answer: D

Signing in from an unfamiliar location or anonymous IP will cause the level of sign-in risk to increase. With a conditional access policy based on higher sign-in risk, you can force MFA for the sign-in and meet the requirement. https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy

---

QUESTION 7

You have a Microsoft 365 subscription.

You need to recommend a passwordless authentication solution that uses biometric authentication.

What should you include in the recommendation?

A. Windows Hello for Business

B. a smart card

C. the Microsoft Authenticator app

D. a PIN

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

---

QUESTION 8

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.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security and Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the Set-AdminAuditLogConfig -AdminAuditLogEnabled $true

-AdminAuditLogCmdlets *Mailbox*command.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-adminauditlogconfig?view=exchange-ps

---

QUESTION 9

You have a Microsoft 365 subscription.

Your company uses Jamf Pro to manage macOS devices.

You plan to create device compliance policies for the macOS devices based on the Jamf Pro data.

You need to connect Microsoft Endpoint Manager to Jamf Pro.

What should you do first?

A. From the Azure Active Directory admin center, add a Mobility (MDM and MAM) application.

B. From the Endpoint Management admin center, add the Mobile Threat Defense connector.

C. From the Endpoint Management admin center, configure Partner device management.

D. From the Azure Active Directory admin center, register an application.

Correct Answer: D

Connect Intune to Jamf Pro (To connect Intune with Jamf Pro steps are):

1.

Create a new application in Azure. (In the Azure portal, go to Azure Active Directory > App Registrations, and then select New registration.)

2.

Enable Intune to integrate with Jamf Pro. (From MEM admin center, Select Tenant administration > Connectors and tokens > Partner device management... Enable the Compliance Connector for Jamf by pasting the Application ID you

saved during the previous procedure into the Specify the Azure Active Directory App ID for Jamf field).

3.

Configure Conditional Access in Jamf Pro.

Step a. Activate the connection in the Jamf Pro console: Open the Jamf Pro console and navigate to Global Management > Conditional Access. Click the Edit button on the macOS Intune Integration tab.

Step b. In Intune, go to the Partner device management page. Under Connector Settings configure groups for assignment

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-integrate-jamf

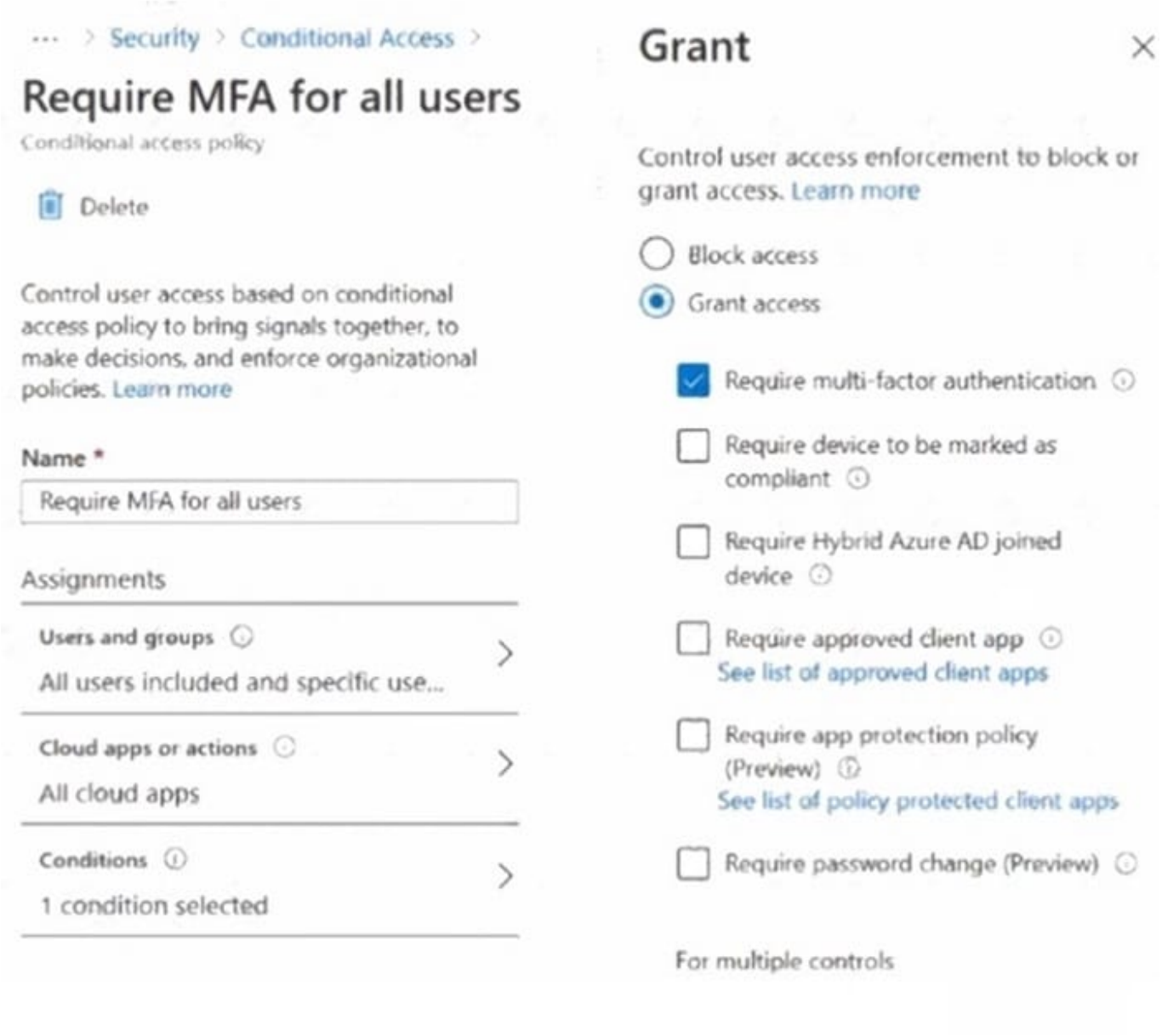
---

QUESTION 10

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.)



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

User Administrator | Role settings

Privileged Identity Management | Azure AD roles

Edit

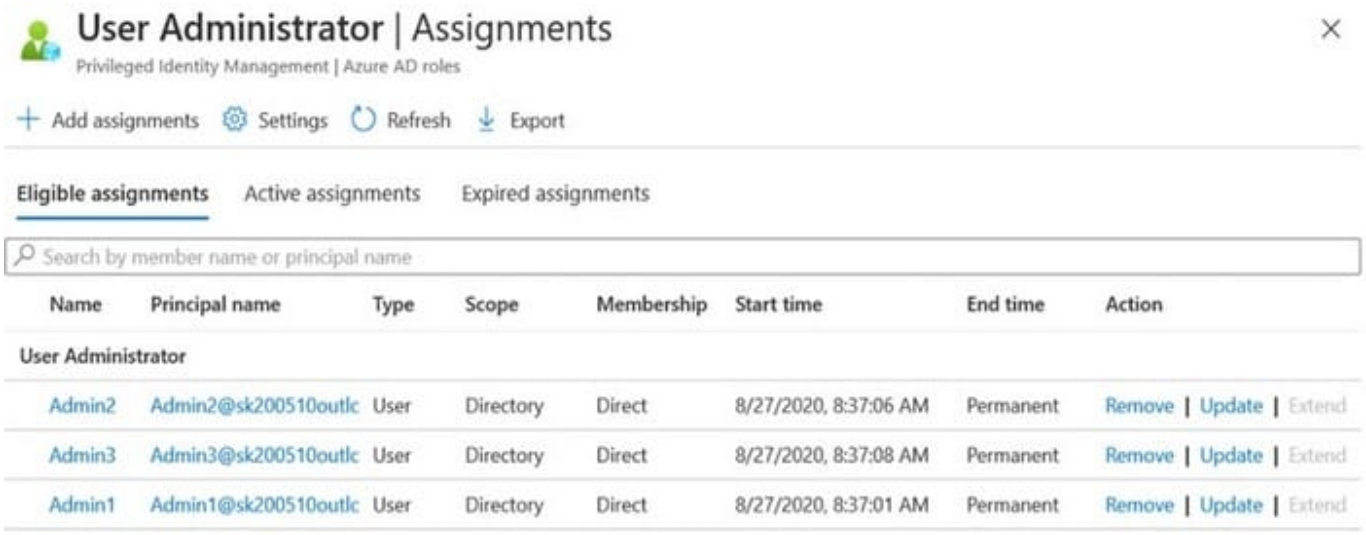
Activation

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	1 Member(s), 0 Group(

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.)



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	○	○
Admin2 can request that the User Administrator role be activated for a period of two hours	○	○
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	○	○

Correct Answer:

	Yes	No
Before Admin1 can perform a task that requires the User Administrator role, the approver must approve the activation request	○	○
Admin2 can request that the User Administrator role be activated for a period of two hours	○	○
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	○	○

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 11

Which role should you assign to User1?

A. Global administrator

B. User administrator

C. Privileged role administrator

D. Security administrator

Correct Answer: C

This role grants the ability to manage assignments for all Azure AD roles including the Global Administrator role. This role does not include any other privileged abilities in Azure AD like creating or updating users. However, users assigned to this role can grant themselves or others additional privilege by assigning additional roles.
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access

---

QUESTION 12

You have a Microsoft 365 E5 subscription and 5,000 users.

You create several alert policies that are triggered every time activities match rules.

You need to create an alert policy that is triggered when the volume of matched activities becomes unusual.

What should you do first?

A. Enable Microsoft Office 365 auditing.

B. Enable Microsoft Office 365 analytics.

C. Enable Microsoft Office 365 Cloud App Security.

D. Deploy a Microsoft Office 365 add-in to all the users.

Correct Answer: B