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.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

QUESTION 1

Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled. The security logs of the servers are collected by using a third-party SIEM solution.

You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors. You need to ensure that you can detect when sensitive groups are modified and when malicious services

are created.

What should you do?

A. Configure Azure ATP notifications

B. Configure Event Forwarding on the domain controllers

C. Configure auditing in the Office 365 Security and Compliance center

D. Modify the Domain synchronizer candidate settings on the Azure ATP sensors

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

QUESTION 2

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 3

You have a Microsoft 365 subscription.

You enable auditing for the subscription.

You plan to provide a user named Auditor with the ability to review audit logs.

You add Auditor to the Global administrator role group.

Several days later, you discover that Auditor disabled auditing.

You remove Auditor from the Global administrator role group and enable auditing.

You need to modify Auditor to meet the following requirements:

1.

Be prevented from disabling auditing

2.

Use the principle of least privilege

3.

Be able to review the audit log

To which role group should you add Auditor?

A. Security reader

B. Compliance administrator

C. Security operator

D. Security administrator

Correct Answer: C

Roles with "View Only Audit Logs" are (there is no security reader):

*

Compliance Administrator

*

Compliance Data Administrator

*

Global Reader

*

Organization Management

*

Security Administrator

*

Security Operator https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?

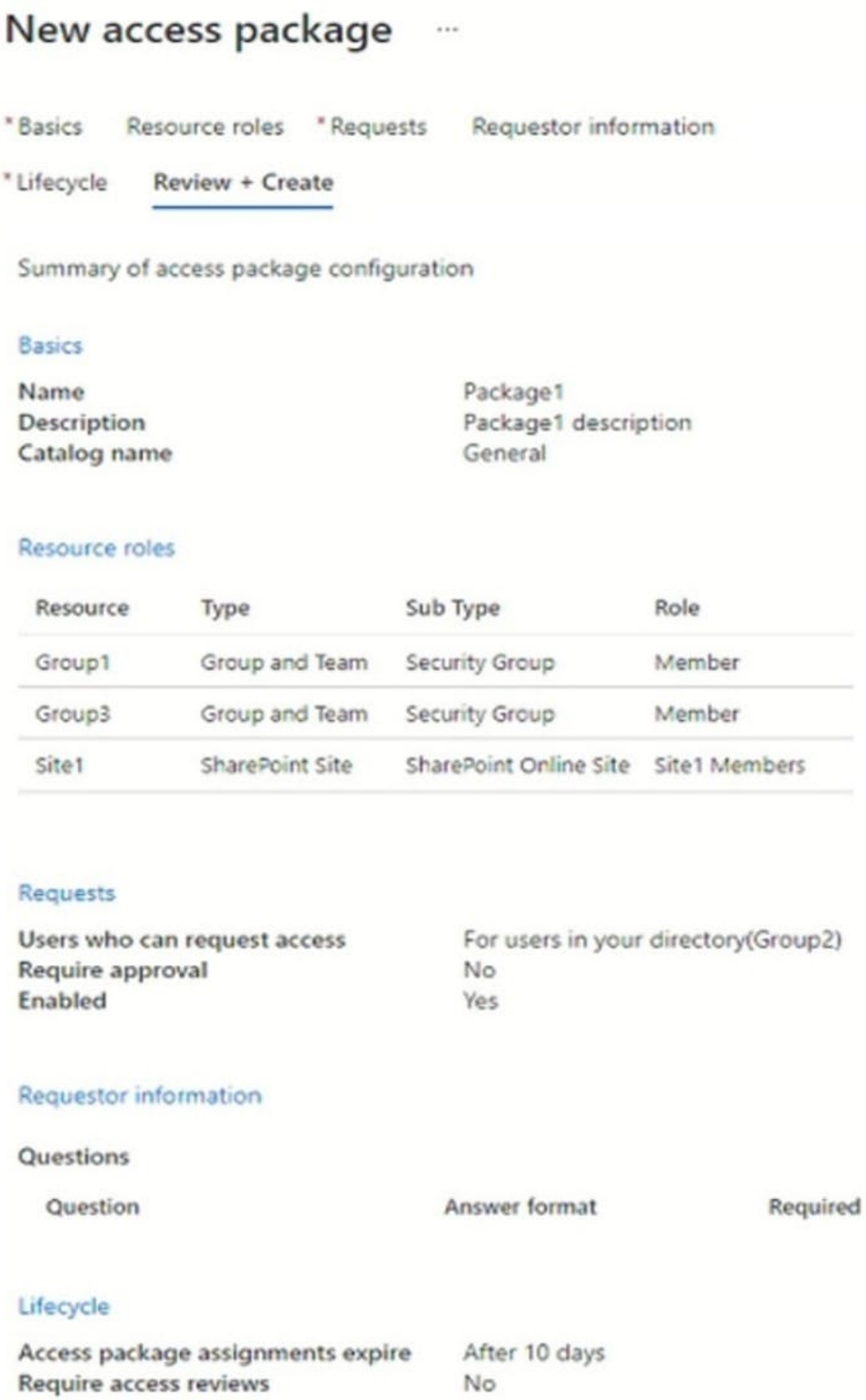
QUESTION 4

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.	○	○
On June 15, 2021, User2 can access Package1.	○	○
On June 5, 2021, User1, User2, and User3 are members of Group3.	○	○

Correct Answer:

Statements	Yes	No
On June 5, 2021, User1 can access Package1.	○	○
On June 15, 2021, User2 can access Package1.	○	○
On June 5, 2021, User1, User2, and User3 are members of Group3.	○	○

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 5

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 6

You plan to deploy a new Microsoft 365 Subscription that will contain 500 users.

You need to ensure that the following actions are performed the users sign in to the subscription

Evaluate the users\\' risk level based on their location and travel. Require high-risk users to sign in by using Azure Multi-Factor Authentication (Azure MFA).

The solution must minimize cost.

Which license should you assign to each user?

A. Microsoft 365 Business Premium

B. Microsoft 365 E3

C. Enterprise Mobility + Security E3

D. Microsoft 365 ES

Correct Answer: A

QUESTION 7

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

Correct Answer: BD

QUESTION 8

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 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.

Your on-premises network contains a server that runs Windows Server 2019, computers that run Windows 10, macOS, or Linux, and a firewall that utilizes syslog.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. All the computers are onboarded to Microsoft Defender for Endpoint.

You are implementing Microsoft Defender for Cloud Apps.

You need to discover which cloud apps are accessed from the computers.

Solution: You install a Microsoft Defender for Cloud Apps log collector and collect logs from the firewall.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

https://www.youtube.com/watch?v=MsHkTOoqSQo

QUESTION 9

You need to create an Azure Information Protection label to meet the following requirements:

1.

Content must expire after 21 days.

2.

Offline access must be allowed for 21 days only.

3.

Documents must be protected by using a cloud key.

4.

Authenticated users must be able to view content only.

To complete this task, sign in to the Microsoft 365 admin center.

Correct Answer: See explanation below.

1.

If you haven\\'t already done so, open a new browser window and sign in to the Azure portal. Then navigate to the Azure Information Protection pane. For example, in the search box for resources, services, and docs: Start typing Information and select Azure Information Protection.

2.

From the Classifications > Labels menu option: On the Azure Information Protection - Labels pane, select the label you want to change. On the Label pane, locate Set permissions for documents and emails containing this label, and select Protect.

3.

Select Protection.

4.

On the Protection pane, select Azure (cloud key).

5.

Select Set permissions to define new protection settings in this portal.

6.

If you selected Set permissions for Azure (cloud key), this option lets you select users and usage rights.

To specify the users that you want to be able to open protected documents and emails, select Add permissions. Then on the Add permissions pane, select the first set of users and groups who will have rights to use the content that will be

protected by the selected label:

Choose Select from the list where you can then add all users from your organization by selecting Add - All members. This setting excludes guest accounts. Or, you can select Add any authenticated users, or

browse the directory.

When you choose all members or browse the directory, the users or groups must have an email address. In a production environment, users and groups nearly always have an email address, but in a simple testing environment, you might

need to add email addresses to user accounts or groups.

Change the File Content Expiration setting to 21 days.

Change the Allow offline access setting to 21 days.

When you have finished configuring the permissions and settings, click OK.

This grouping of settings creates a custom template for the Azure Rights Management service. These templates can be used with applications and services that integrate with Azure Rights Management.

7.

Click OK to close the Protection pane and see your choice of User defined or your chosen template display for the Protection option in the Label pane.

8.

On the Label pane, click Save.

9.

On the Azure Information Protection pane, use the PROTECTION column to confirm that your label now displays the protection setting that you want:

A check mark if you have configured protection.

An x mark to denote cancellation if you have configured a label to remove protection.

A blank field when protection is not set.

When you clicked Save, your changes are automatically available to users and services. There\\'s no longer a separate publish option.

Reference: https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection

QUESTION 10

A company named Contoso, Ltd. acquires a company named Fabrikam, Inc.

Users at each company continue to use their company\\'s Microsoft 365 tenant. Both companies have hybrid Azure Active Directory (Azure AD) tenants configured as shown in the following table.

Company	Azure AD domain	Azure AD Connect server	Authentication
Contoso	Contoso.com	Yes	Password hash synchronization
Fabrikam	Fabrikam.com	Yes	Pass-through authentication

In the Contoso tenant, you create a new Microsoft 365 group named FabrikamUsers, and you add FabrikamUsers as a member of a Microsoft Teams team named Corporate.

You need to add Fabrikam users to the FabrikamUsers group.

What should you do first?

A. Configure the Contoso tenant to use pass-through authentication as the authentication method.

B. In the Contoso tenant, create a new conditional access policy.

C. In the Contoso tenant, create guest accounts for all the Fabrikam users.

D. Configure the Fabrikam tenant to use federation as the authentication method.

Correct Answer: C

Since both companies have hybrid Azure AD tenants, creating guest accounts for Fabrikam users in the Contoso tenant would allow them to access the FabrikamUsers group in the Corporate Teams team. Option A is not necessary for this task. Option B is not relevant to adding Fabrikam users to a group. Option D is also not necessary as both companies already have hybrid Azure AD tenants.

QUESTION 11

DRAG DROP

You have a Microsoft 365 E5 subscription.

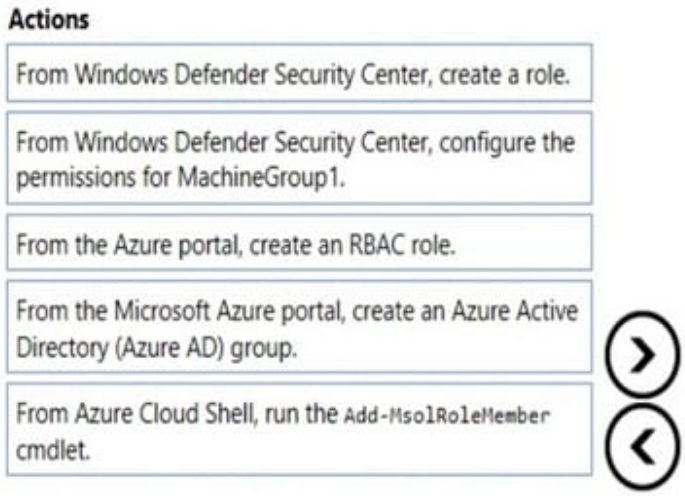
All computers run Windows 10 and are onboarded to Windows Defender Advanced Threat Protection (Windows Defender ATP).

You create a Windows Defender machine group named MachineGroup1.

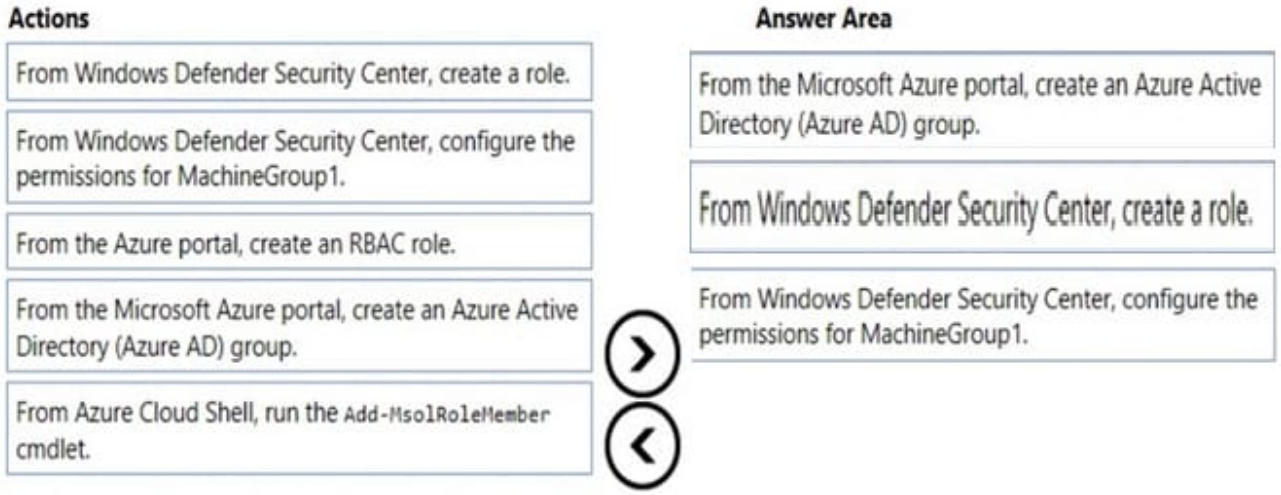
You need to enable delegation for the security settings of the computers in MachineGroup1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



QUESTION 12

You have a Microsoft 365 subscription.

You need to ensure that users can manually designate which content will be subject to data loss prevention (DLP) policies.

What should you create first?

A. A retention label in Microsoft Office 365

B. A custom sensitive information type

C. A Data Subject Request (DSR)

D. A safe attachments policy in Microsoft Office 365

Correct Answer: A

A retention label in Microsoft Office 365

Using a retention label as a condition in a DLP policy

Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

Support for sensitivity labels is coming

You can currently use only a retention label as a condition, not a sensitivity label. We\\'re currently working on support for using a sensitivity label in this condition.

Types of sensitive information

A DLP policy can help protect sensitive information, which is defined as a sensitive information type. Microsoft 365 includes definitions for many common sensitive information types across many different regions that are ready for you to use,

such as a credit card number, bank account numbers, national ID numbers, and passport numbers.

Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

QUESTION 13

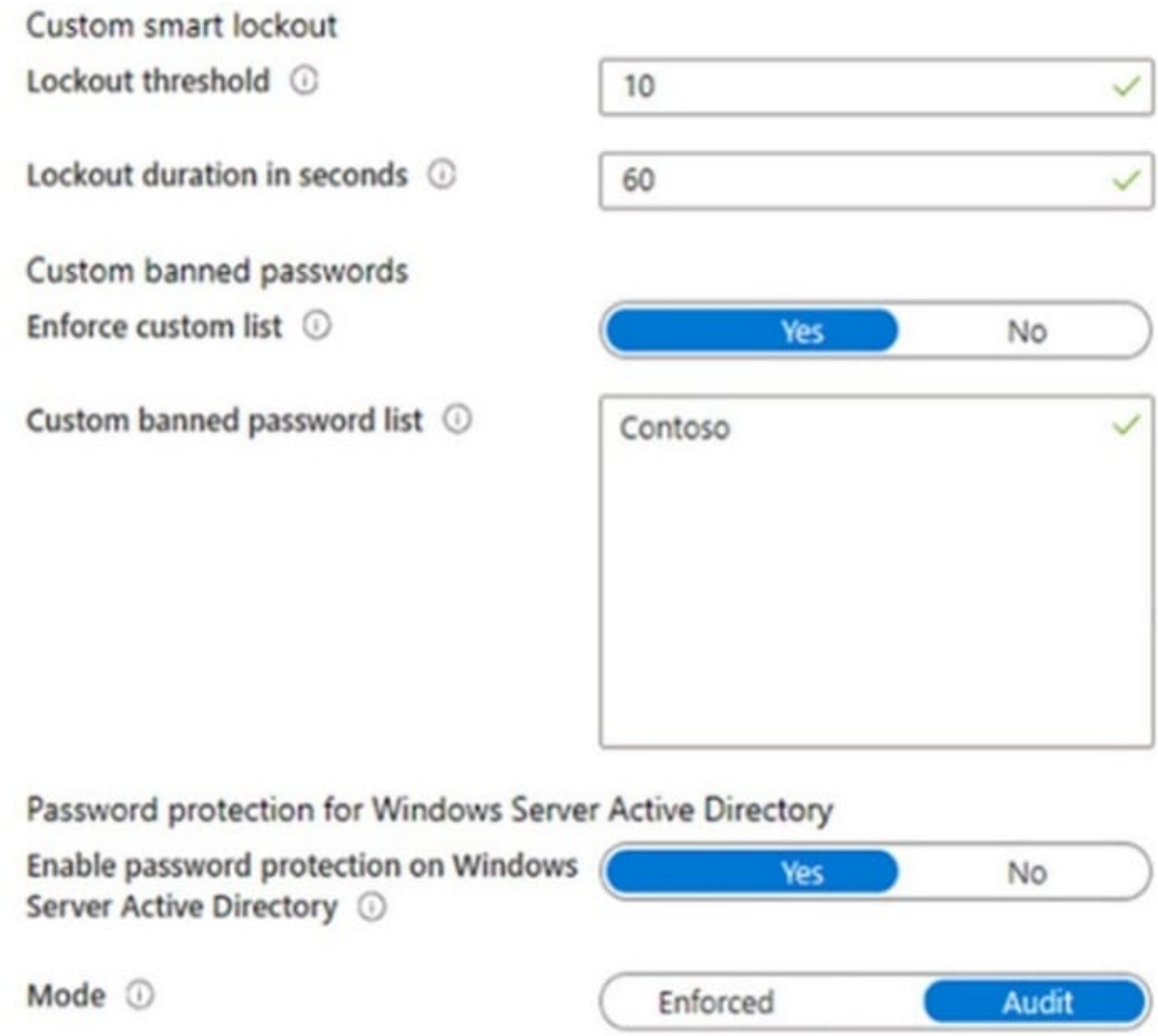
HOTSPOT

You company has a Microsoft 36S 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.



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	○	○
User2 can change his password to C0NT0$0C0NT0$0	○	○
User3 can change his password to myCONTOSOc0mp1exPWD	○	○

Correct Answer:

	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory	○	◉
User2 can change his password to C0NT0$0C0NT0$0	◉	○
User3 can change his password to myCONTOSOc0mp1exPWD	◉	○

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

QUESTION 14

You have a Microsoft 365 E5 subscription that contains a user named User1. You need to ensure that User1 can review Conditional Access policies.

Solution: You assign User1 the Security Administrator role.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 15

HOTSPOT

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

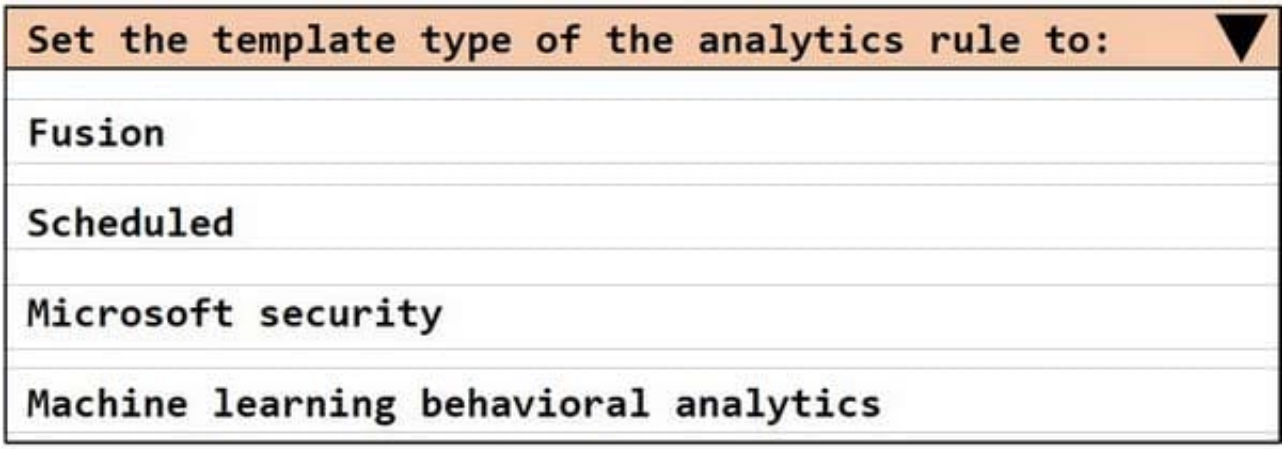
From the workspace, you plan to create an analytics rule that will be based on a custom query and will run a security play.

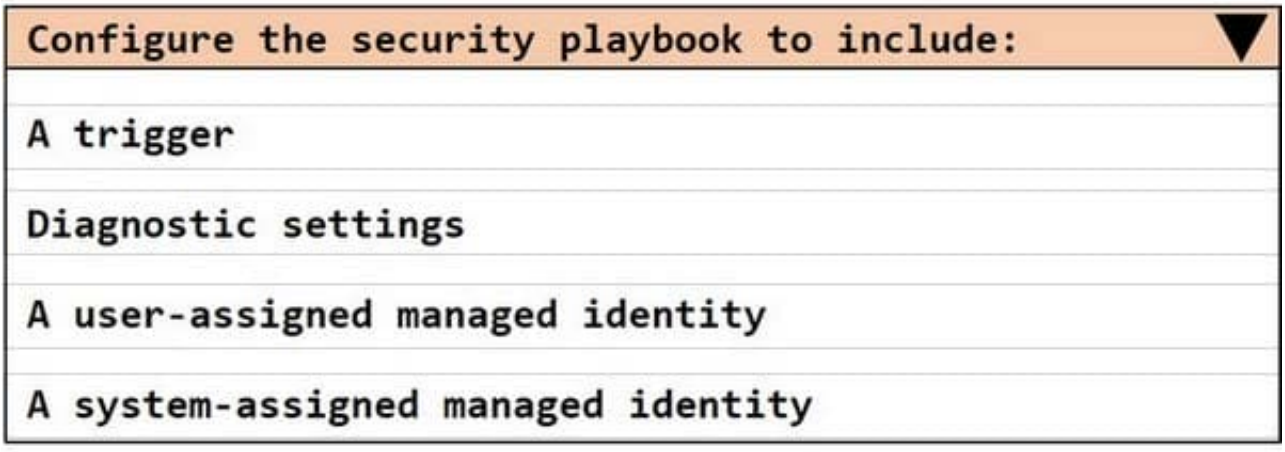
You need to ensure that you can add the security playbook and the custom query to the rule.

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

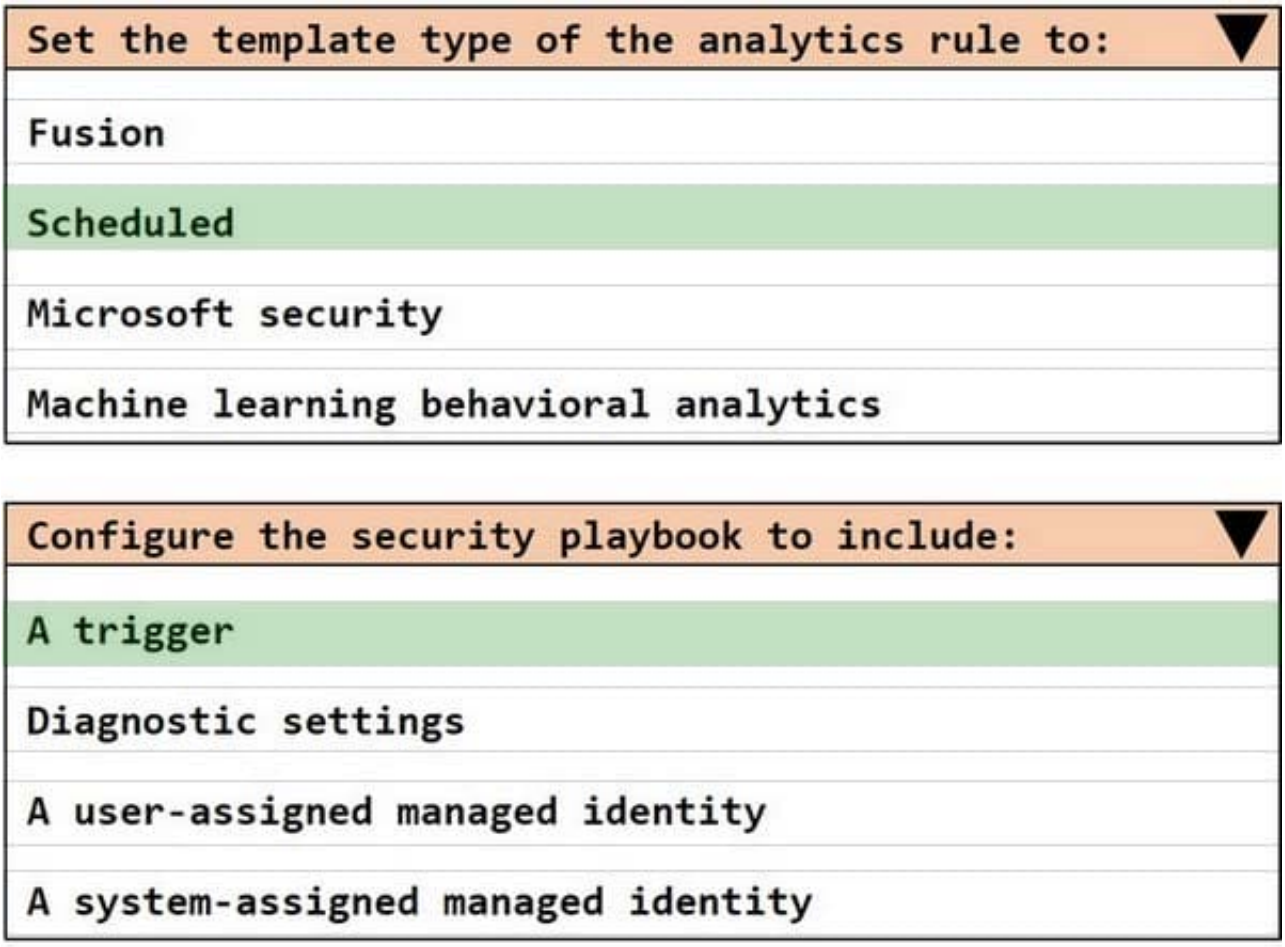
NOTE: Each correct selection is worth one point.

Hot Area:





Correct Answer:



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