MS-102 Q&As

Microsoft 365 Certified: Enterprise Administrator Expert

Pass Microsoft MS-102 Exam with 100% Guarantee

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

https://www.pass4itsure.com/ms-102.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com.

You create a Microsoft Defender for identity instance Contoso.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	**None**
User2	Defender for Identity Contoso Users	**None**
User3	**None**	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.

Solutions: You instruct User1 to modify the Defender for identity sensor configuration.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 2

HOTSPOT

You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1	Enforced

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs. The tenant contains the named locations shown in the following table.

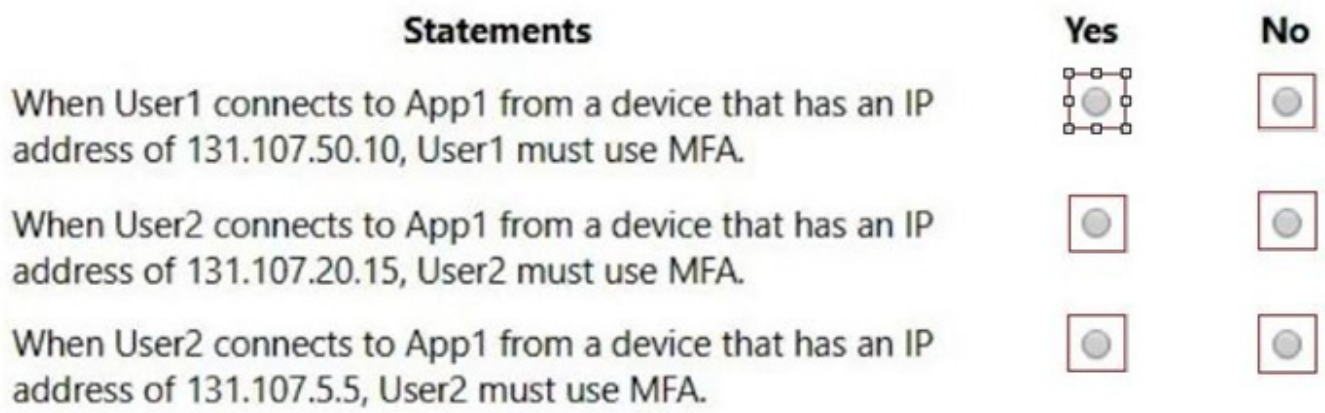
Name	IP address range	Trusted location
Location1	131.107.20.0/24	Yes
Location2	131.107.50.0/24	Yes

You create a conditional access policy that has the following configurations:

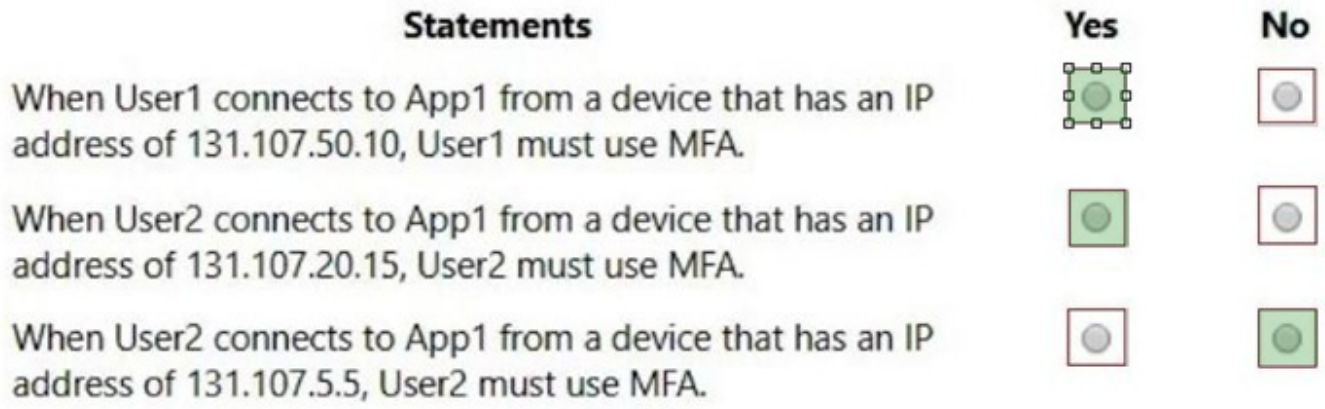
Users or workload identities assignments: All users Cloud apps or actions assignment: App1 Conditions: Include all trusted locations Grant access: Require multi-factor authentication For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 3

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

You need to enable user access to the partner company\\'s portal. Which Microsoft Defender for Endpoint setting should you modify?

A. Alert notifications

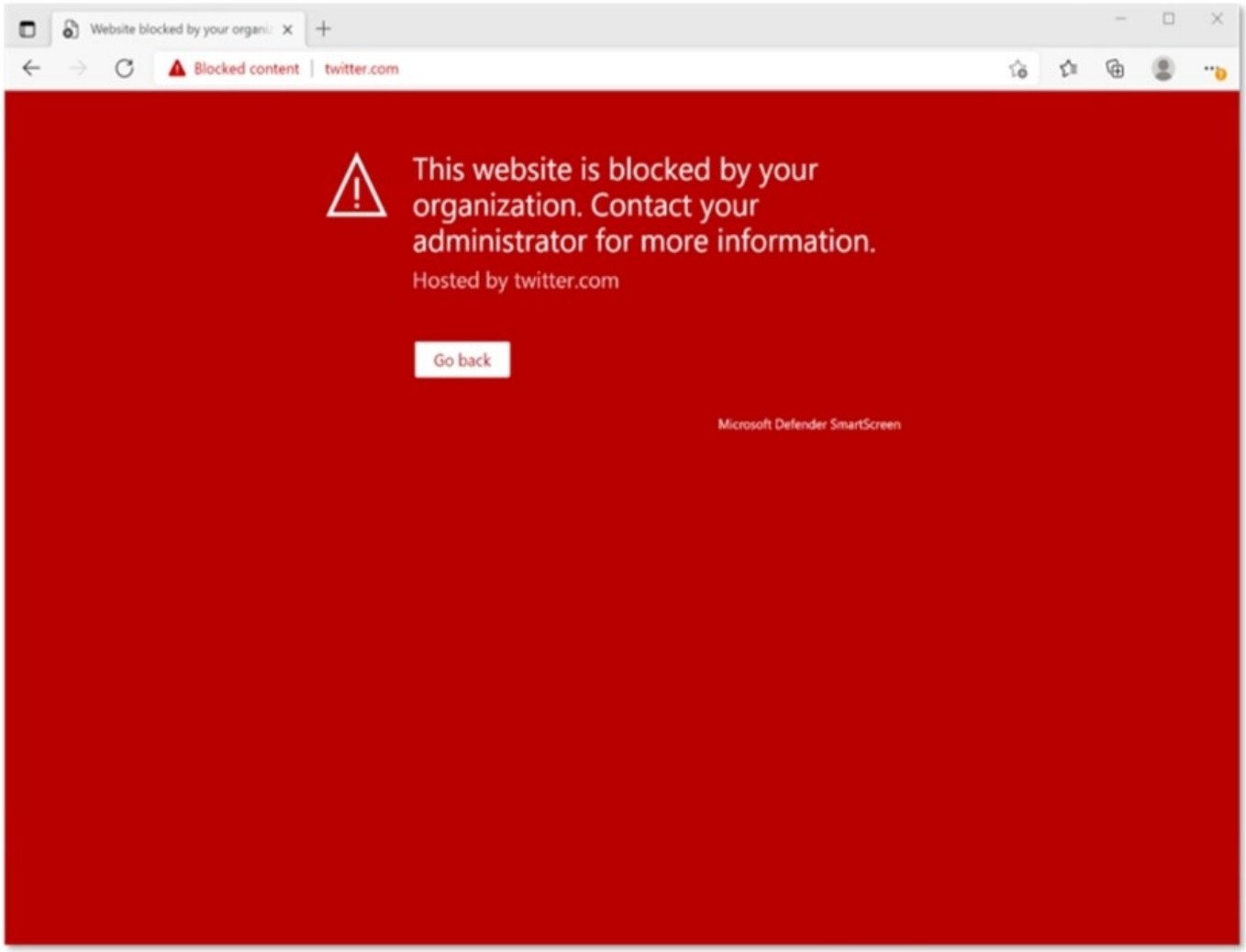
B. Alert suppression

C. Custom detections

D. Advanced hunting

E. Indicators

Correct Answer: E



This Website Is Blocked By Your Organization

Custom indicators will block malicious IPs, URLs, and domains. Then, they will display the above message for the user.

Reference:

https://jadexstrategic.com/web-protection/

QUESTION 4

You have a Microsoft 365 subscription that contains a user named User1.

You need to ensure that User1 can search the Microsoft 365 audit logs from the Security and Compliance admin center.

Which role should you assign to User1?

A. View-Only Audit Logs in the Security and Compliance admin center

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

C. Security reader in the Azure Active Directory admin center

D. Security Reader in the Security and Compliance admin center

Correct Answer: B

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in- security-and-compliance?view=o365-worldwide

QUESTION 5

You have a Microsoft 365 E5 subscription.

You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.

Which conditions can you use in the DLP rules of the policy?

A. sensitive info types

B. content search queries

C. keywords

D. sensitivity labels

Correct Answer: A

The correct answer is A. sensitive info types.

Sensitive info types are predefined patterns that can help you identify and protect sensitive data, such as credit card numbers, social security numbers, bank account numbers, and so on1. You can use sensitive info types as conditions in your DLP rules to detect and protect data that matches these patterns. For example, you can create a DLP rule that blocks the external sharing of documents that contain credit card numbers2. B, C, and D are incorrect because they are not valid conditions for DLP rules in Office

QUESTION 6

Your company has three main offices and one branch office. The branch office is used for research.

The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.

You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.

What should you include in the recommendation?

A. Azure AD password protection

B. a Microsoft Intune device configuration profile

C. a Microsoft Intune device compliance policy

D. Azure AD conditional access

Correct Answer: D

QUESTION 7

You have a Microsoft 365 E5 tenant.

You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.

Which two policies can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. a data loss prevention (DLP) policy

B. a sensitivity label policy

C. a Microsoft Cloud App Security file policy

D. a communication compliance policy

E. a retention label policy

Correct Answer: AD

QUESTION 8

You have a Microsoft 365 subscription.

You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.

Which type of group should you use to assign the Reports Reader role and to access App1?

A. a Microsoft 365 group that has assigned membership

B. a Microsoft 365 group that has dynamic user membership

C. a security group that has assigned membership

D. a security group that has dynamic user membership

Correct Answer: C

To grant permissions to assignees to manage users and group access for a specific enterprise app, go to that app in Azure AD and open in the Roles and Administrators list for that app. Select the new custom role and complete the user or

group assignment. The assignees can manage users and group access only for the specific app.

Note: You can add the following types of groups:

Assigned groups - Manually add users or devices into a static group.

Dynamic groups (Requires Azure AD Premium) - Automatically add users or devices to user groups or device groups based on an expression you create.

Note:

Security groups

Security groups are used for granting access to Microsoft 365 resources, such as SharePoint. They can make administration easier because you need only administer the group rather than adding users to each resource individually.

Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.

Security groups can be configured for dynamic membership in Azure Active Directory, allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device

attributes such as operating system version.

Security groups can be added to a team.

Microsoft 365 Groups can\\'t be members of security groups.

Microsoft 365 Groups

Microsoft 365 Groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 Group, members get a group email and shared workspace for conversations, files, and calendar events, Stream,

and a Planner.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups? https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy

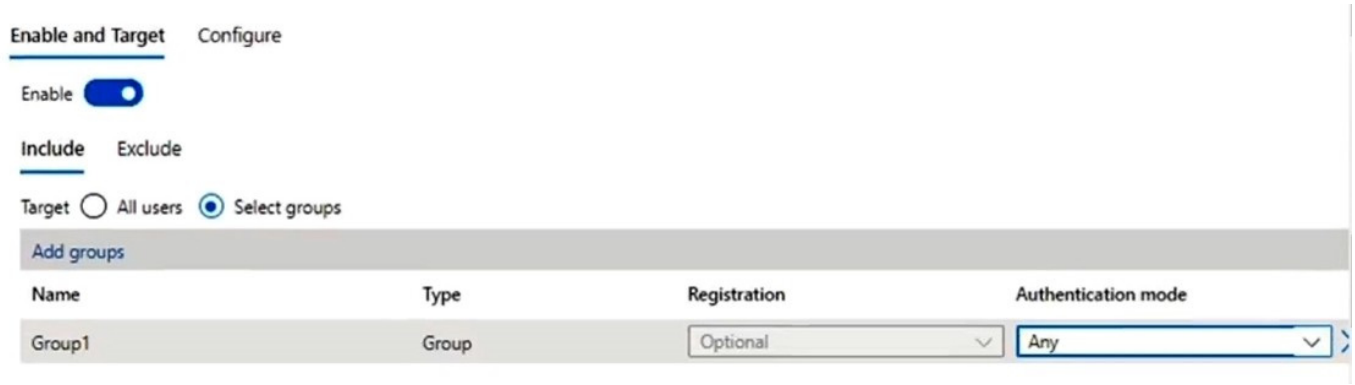
QUESTION 9

HOTSPOT

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

Name	Member of	Multi-factor authentication (MFA) method registered
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1	*None*

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.

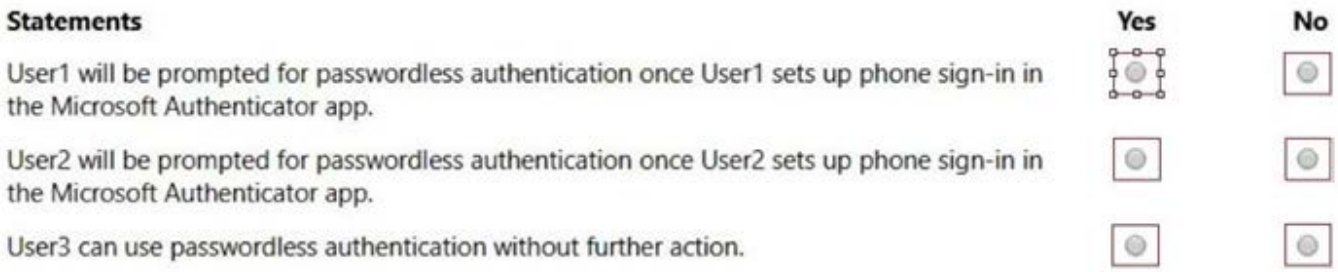


Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.

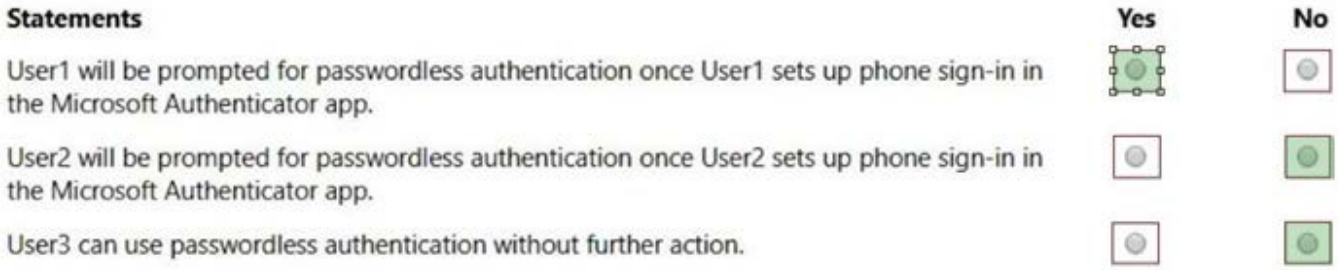
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 10

You have a Microsoft 365 tenant.

You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.

What should you use?

A. an attack surface reduction (ASR) policy

B. an app configuration policy

C. a device compliance policy

D. a device configuration profile

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

QUESTION 11

Your network contains an Active Directory domain.

You deploy a Microsoft Entra tenant.

Another administrator configures the domain to synchronize to the Microsoft Entra tenant. You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts

synchronized successfully.

You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.

Solution: From Microsoft Entra Connect, you modify the filtering settings.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 12

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

Retention period 7 years

Start the retention period bated on: When items were created

You need to prevent the removal of the label once the label K applied to a lie What should you select in the retention label settings?

A. Retain items even If users delete

B. Mark items as a record

C. Mark items as a regulatory record

D. Retain items forever

Correct Answer: C

QUESTION 13

HOTSPOT

You have a Microsoft 365 E5 subscription.

All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.

You need to configure Defender for Endpoint to meet the following requirements:

Block a vulnerable app until the app is updated.

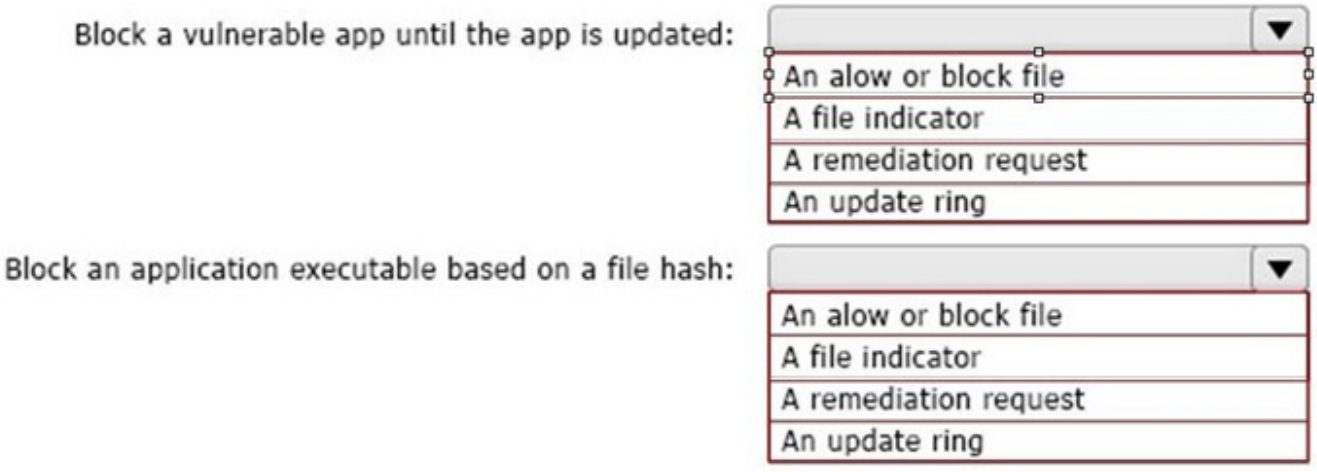
Block an application executable based on a file hash.

The solution must minimize administrative effort.

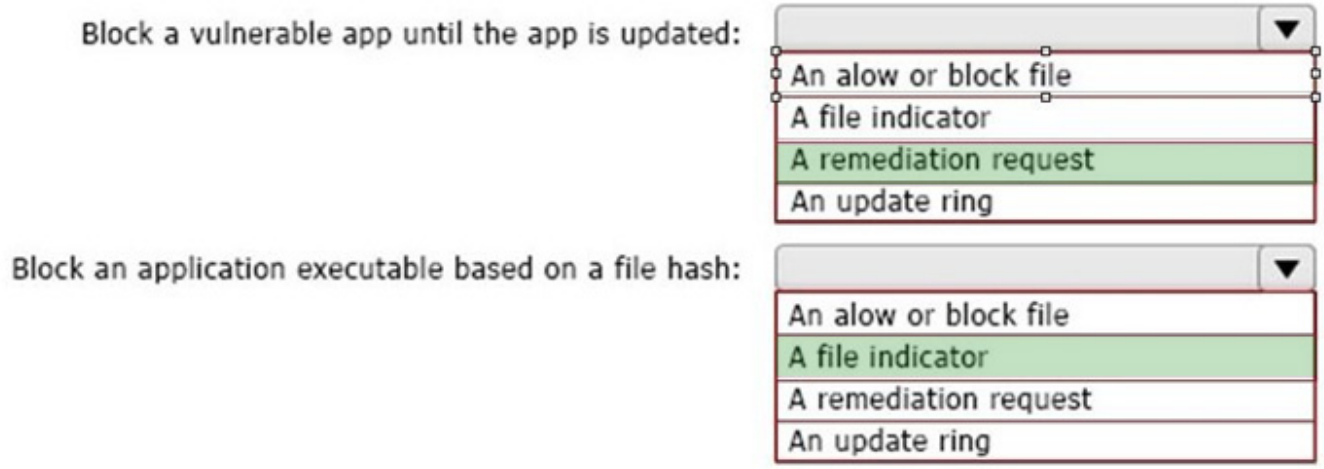
What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



MS-102 Practice Test MS-102 Study Guide MS-102 Braindumps