PassQueen
a.k.a dumpsqueen.com

McAfee Certified Product Specialist - ENS

McAfee MA0-107

Version Demo

Total Demo Questions: 9

Total Premium Questions: 92

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

An ePO administrator assigns a new Threat Prevention policy to a subgroup. The subgroup currently inherits its policy from the parent group, but it requires different on-access scanning settings than the parent. Which of the following should the administrator do?

A. Break inheritance and assign the new policy to the subgroup.

B. Assign the policy to the parent group and retain inheritance.

C. Create an on-demand scan task for the subgroup.

D. Move the systems to the Lost&Found group.

ANSWER: A

Explanation:

Break inheritance and assign the new policy to the subgroup. This allows the subgroup to retain its membership in the existing System Tree structure while receiving a policy assignment that differs from its parent. Systems in the subgroup then enforce the newly assigned Threat Prevention policy, while systems remaining in the parent group continue to inherit the parent policy.

Breaking inheritance is appropriate when a subset of systems has a legitimate, distinct operational requirement, such as a server workload that needs different scanning settings. The administrator should scope the exception only to the required subgroup and document the reason for the separate assignment. See the Trellix Product Documentation portal for Endpoint Security policy-assignment guidance.

QUESTION NO: 2

The network operations team has configured the company's VPN connector to deny connectivity if virus scan definitions are older than seven days. In order for a user to immediately meet the VPN connector's policy, which of the following should the administrator enable?

A. Managed custom tasks

B. "Update now" button

C. Default client update task schedule

D. Proxy server

ANSWER: B

Explanation:

The *"Update now" button* should be enabled because it gives the endpoint user a direct way to initiate an immediate update of the security content, including the virus scan definitions used to determine compliance. Once the update completes successfully, the endpoint reports current definition information through its management and security components, allowing the device to satisfy a VPN posture rule that requires definitions no older than seven days. This is appropriate when access is needed immediately: the user does not have to wait for the next scheduled update interval or for an administrator to create and distribute a task. The administrator enables this client-interface capability in the applicable Endpoint Security policy, while the endpoint still uses its configured update repositories and credentials to retrieve the current content. The update must be allowed to complete before the VPN connector reevaluates the device’s posture. McAfee Endpoint Security documentation describes client update behavior and policy-controlled update settings in the Endpoint Security Product Guide. Additional product documentation is available through the Trellix Documentation Portal.

QUESTION NO: 3

A trusted business application reads a large number of unchanged files throughout the day. The administrator wants to reduce on-access scanning overhead for that application while retaining scanning when files are created or modified. Which of the following process settings should be used?

A. Low-Risk Processes

B. High-Risk Processes

C. Potentially Unwanted Program Detections

D. Exploit Prevention process exclusions

ANSWER: A

Explanation:

Low-Risk Processes is correct. Threat Prevention applies reduced on-access scanning to processes configured as low risk. In particular, files accessed by a low-risk process are scanned on write, which helps reduce the repeated scanning overhead associated with frequent reads of unchanged files.

The process should be added only after it has been verified as trusted and its operational behavior has been reviewed. Low-risk process settings are intended to improve performance for approved workloads while maintaining inspection when files are introduced or changed. See the Trellix Product Documentation portal for Endpoint Security Threat Prevention on-access scanning configuration.

QUESTION NO: 4

The ePO administrators have already tuned and configured dynamic application containment rules within the policy. In which of the following ways will dynamic application containment protect against malware once enforcement is enabled?

A. The scan engine will learn the behavior of the application and send up to GT1 for analysis, and then receive an action to block all actions from the application's process.

B. If an application's reputation is below the threshold while triggering a block rule and is not an excluded application, malicious behavior of the application will be contained.

C. The ENS client will receive the reputation as "highly suspicious" from either the McAfee GTI or TIE server, and then immediately uninstall the application on the system.

D. The adaptive threat protection scanner will send the file automatically to a preconfigured "Sandbox" folder and analyze the application for malicious features before use.

ANSWER: B

Explanation:

Dynamic application containment protects endpoints by restricting the behavior of an application when its reputation falls below the configured threshold and the application attempts an action that matches a configured containment block rule. The rule is therefore reputation-aware and behavior-aware: reputation information identifies software that warrants reduced trust, while the containment rule determines which potentially harmful behaviors must be prevented. Provided the application has not been explicitly excluded, Endpoint Security applies the configured containment response to stop the malicious behavior from proceeding. This enables administrators to limit the damage that unknown, suspicious, or low-reputation applications can cause without necessarily relying on a traditional signature-based detection alone.

The policy tuning mentioned in the question is important because administrators define the reputation thresholds, exclusions, and behavior rules appropriate for their environment before enabling enforcement. Reputation can be supplied through McAfee Global Threat Intelligence and, where deployed, Threat Intelligence Exchange. Dynamic application containment is a Threat Prevention capability intended to control risky application actions at the endpoint. Trellix provides Endpoint Security product information at Trellix Endpoint Security and documentation resources at Trellix Product Documentation.

QUESTION NO: 5

The security team has requested that adaptive threat protection be integrated with a TIE server. Which of the following is required?

A. Data Exchange Layer

B. Advanced Threat Defense

C. Event Security Manager

D. Active Response

ANSWER: A

Explanation:

Data Exchange Layer is required because Endpoint Security Adaptive Threat Protection communicates with the Threat Intelligence Exchange server through the DXL fabric. DXL provides the message-bus infrastructure that lets the endpoint request a file's reputation and receive enterprise reputation information from TIE. This connection enables ATP to use locally established reputation data when making threat-prevention decisions, rather than relying only on the endpoint's local intelligence or cloud lookups. In a deployment, the endpoint must be able to connect to the DXL brokers and the policy must enable the TIE-related ATP capability so that the endpoint can publish and consume the relevant reputation messages. TIE itself is designed to distribute reputation intelligence among connected security products, while DXL is the transport and integration layer that makes this real-time exchange possible. Therefore, a functioning Data Exchange Layer environment, including appropriate broker connectivity, is the prerequisite for integrating Adaptive Threat Protection with a TIE server. See the official Trellix Threat Intelligence Exchange overview and the OpenDXL documentation for the architecture and messaging role of DXL.

QUESTION NO: 6

In which of the following ways does Dynamic App Containment protect against malware?

A. It checks for spyware, unwanted programs, and viruses based on known patterns.

B. It monitors communication between the computer and the network.

C. It detects malicious files and activities using machine-learning techniques.

D. It limits the actions unknown applications can take on the end system.

ANSWER: D

Explanation:

Dynamic App Containment protects endpoints by limiting the actions that unknown applications can perform on the endpoint while their trustworthiness has not been established. This containment-based approach reduces the opportunity for a newly encountered or suspicious program to make harmful system changes, alter protected files, access sensitive resources, or otherwise carry out malware-like behavior. Rather than immediately treating every unknown executable as definitively malicious, the feature applies restrictions appropriate to the application's reputation and risk state. This gives Endpoint Security time to evaluate the application and helps preserve normal endpoint protection even when a threat has not yet been identified by a traditional signature. Dynamic App Containment is part of the adaptive, behavior-focused protection capabilities associated with Endpoint Security and is intended to reduce exposure to zero-day and unknown threats. Trellix's Endpoint Security information describes its layered endpoint defenses and adaptive protection capabilities at Trellix Endpoint Security. Product documentation and administration guidance are available through the Trellix Documentation portal.

QUESTION NO: 7

A trusted database process causes high disk activity because many data files are opened repeatedly. The security team wants to reduce on-access scanning overhead for this process while continuing to scan files when they are modified. Which of the following Threat Prevention settings should be configured?

A. Add the process to High-Risk Processes.

B. Add the process to Low-Risk Processes.

C. Disable AMCore content updates.

D. Configure the process as a trusted network.

ANSWER: B

Explanation:

Add the process to Low-Risk Processes. Low-Risk Processes settings allow administrators to identify trusted processes that do not require scanning every file when it is read. Files accessed by a configured low-risk process can still be scanned when they are written or modified, reducing repeated scan activity and improving performance for high-I/O applications.

This setting should be used only after the process has been verified as trusted and the operational requirement has been validated. It is more targeted than disabling on-access scanning or excluding the entire database directory from scanning. See the Trellix Product Documentation portal for Endpoint Security Threat Prevention configuration guidance.

QUESTION NO: 8

An administrator has assigned an updated Endpoint Security policy to a managed system and needs the system to receive the change immediately rather than waiting for the next agent-to-server communication interval. Which of the following should the administrator use?

A. Send an agent wake-up call.

B. Restart the ePO server.

C. Run an on-demand scan.

D. Create a new repository branch.

ANSWER: A

Explanation:

Send an agent wake-up call. An agent wake-up call prompts the McAfee Agent on the managed system to communicate with ePO immediately. During that communication, the agent can retrieve and enforce the latest assigned policies and receive applicable tasks or content updates.

This is useful after an urgent policy assignment, during troubleshooting, or when validating a configuration change on a specific endpoint. It does not replace the normal scheduled agent-to-server communication interval, which should remain configured for routine policy enforcement. See the Trellix Product Documentation portal for ePolicy Orchestrator and Endpoint Security management guidance.

QUESTION NO: 9

A user navigates to a website and notices a small blue square around an "M" in the upper-right corner of the Chrome browser. Which of the following does the blue color indicate within the toolbar?

A. It is an internal website.

B. Web Control is disabled.

C. No rating is available.

D. It is a phishing website.

ANSWER: C

Explanation:

No rating is available. is correct. The small McAfee “M” icon displayed in a supported browser is the Endpoint Security Web Control browser-toolbar indicator. Its color communicates the current website’s reputation or rating status as determined by McAfee/Trellix web-reputation services and the installed Web Control components. A blue toolbar icon means that Web Control does not have a reputation rating available for the site currently being viewed. This can occur when a URL has not yet been categorized or rated, when it is new or uncommon, or when reputation information cannot be obtained for that address at the time of access. The blue state is therefore an informational status: it tells the user that a safety classification is unavailable, rather than assigning a known safe, suspicious, malicious, or policy-defined classification to the website. Administrators can configure Web Control policy responses for unrated websites, but the toolbar’s blue color itself specifically represents the absence of an available rating. See the Trellix Endpoint Security Web Control Product Guide and the Trellix Endpoint Security product information.