



250-428^{Q&As}

Administration of Symantec Endpoint Protection 14

Pass Symantec 250-428 Exam with 100% Guarantee

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

<https://www.geekcert.com/250-428.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Which option is unavailable in the Symantec Endpoint Protection console to run a command on the group menu item?

- A. Disable SONAR
- B. Scan
- C. Disable Network Threat Protection
- D. Update content and scan

Correct Answer: A

QUESTION 2

What happens when the license expires in Symantec Endpoint Protection 14 enterprise Edition?

- A. LiveUpdate stops.
- B. Group Update Providers (GUP) stop.
- C. Symantec Insight is disabled.
- D. Content updates continue.

Correct Answer: D

QUESTION 3

An organization needs to ensure that SEP detects a malicious or potentially malicious file when downloaded via a text messaging client. What feature can an organization enable in the Virus and Spyware Protection policy and modify its sensitivity settings?

- A. Global Scan Options
- B. SONAR
- C. Internet Email Auto Protect
- D. Download Protection

Correct Answer: D

Reference: <https://sway.office.com/uK6GBTakzHS7HoIL?accessible=true>

QUESTION 4

An administrator is using the SylinkDrop tool to update a Symantec Endpoint Protection client install on a system. The



client fails to migrate to the new Symantec Endpoint Protection Manager (SEPM), which is defined correctly in the Sylink.xml file that was exported from the SEPM.

Which settings must be provided with SylinkDrop to ensure the successful migration to a new Symantec Endpoint Protection environment with additional Group Level Security Settings?

- A. -s "silent"
- B. -t "Tamper Protect"
- C. -r "reboot"
- D. -p "password"

Correct Answer: D

QUESTION 5

An organization created a rule in the Application and Device Control policy to block peer-to-peer applications. What two other protection technologies can block and log such unauthorized application? (Choose two.)

- A. Memory Exploit Mitigation
- B. Virus and Spyware Protection
- C. Custom IPS Signatures
- D. Host Integrity
- E. Firewall

Correct Answer: CE

Reference: <https://support.symantec.com/us/en/article.tech122597.html>

[Latest 250-428 Dumps](#)

[250-428 VCE Dumps](#)

[250-428 Practice Test](#)