

DUMPSQUEEN

PSE: Endpoint Associate training for Traps 4.0

Palo Alto Networks PSE-Endpoint-Associate

Version Demo

Total Demo Questions: 5

Total Premium Questions: 24

Buy Premium PDF

<https://dumpsqueen.com>

support@dumpsqueen.com

dumpsqueen.com

QUESTION NO: 1

What is the maximum supported number of endpoints per ESM Server in a Traps 3.4 deployment?

- A. 350
- B. 16,000
- C. 10,000
- D. 80,000

ANSWER: D

QUESTION NO: 2

In the Traps product, what does the term “Service Protection” mean?

- A. the protection of a specified process
- B. the ability of one ESM Server to take over for another
- C. the protection of a process running on a Windows Server system
- D. the ability of the Traps agent to make itself tamper-proof

ANSWER: A

QUESTION NO: 3

Which two statements about troubleshooting installation and upgrade problems are true? (Choose two.)

- A. A common cause of ESM Server installation problems is the failure to confirm connectivity to WildFire before running the installer.
- B. A common cause of Traps endpoint agent installation problems is the failure to configure the SSL option correctly.
- C. ESM Server services will shut down if they are not licensed within 24 hours of being started.
- D. Use MSIEXEC with appropriate flags to get more logging detail at installation time.

ANSWER: A B

QUESTION NO: 4

Which three statements about the trusted publisher mechanism are true? (Choose three.)

- A.** The trusted-publisher mechanism blocks executables from running unless they are signed by a trusted publisher.
- B.** The list of trusted publishers is maintained through content updates.
- C.** The trusted-publisher mechanism takes precedence over verdict overrides by administrators.
- D.** The trusted-publisher mechanism is called whenever an executable file would otherwise get an Unknown or No Connection verdict.
- E.** The trusted-publisher mechanism allows trusted signed executables to run without seeking a WildFire verdict.
- F.** No executable will be affected by the trusted-publisher mechanism unless it is signed by a publisher on a list maintained by Palo Alto Networks.

ANSWER: B C D

QUESTION NO: 5

Which statement about Malware verdicts is true?

- A.** If WildFire is not available when the active ESM server tries to reach it for a verdict on a file, the endpoint will get a verdict from local analysis.
- B.** If the ESM server is not available when the Traps agent tries to reach it for a verdict on a file, the file status is marked as Benign.
- C.** The end user can use the Traps console to override a verdict of Malicious.
- D.** Local analysis verdicts take precedence over WildFire verdicts.

ANSWER: A