



250-438^{Q&As}

Administration of Symantec Data Loss Prevention 15

Pass Symantec 250-438 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/250-438.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 two technologies should an organization utilize for integration with the Network Prevent products? (choose two.)

- A. Network Tap
- B. Network Firewall
- C. Proxy Server
- D. Mail Transfer Agent
- E. Encryption Appliance

Correct Answer: CD

Reference: <https://www.symantec.com/connect/articles/network-prevent>

QUESTION 2

How should a DLP administrator change a policy so that it retains the original file when an endpoint incident has detected a "copy to USB device" operation?

- A. Add a "Limit Incident Data Retention" response rule with "Retain Original Message" option selected.
- B. Modify the agent config.db to include the file
- C. Modify the "Endpoint_Retain_Files.int" setting in the Endpoint server configuration
- D. Modify the agent configuration and select the option "Retain Original Files"

Correct Answer: A

QUESTION 3

A DLP administrator determines that the \SymantecDLP\Protect\Incidents folder on the Enforce server contains .BAD files dated today, while other .IDC files are flowing in and out of the \Incidents directory. Only .IDC files larger than 1MB are

turning to .BAD files.

What could be causing only incident data smaller than 1MB to persist while incidents larger than 1MB change to .BAD files?

- A. A corrupted policy was deployed.
- B. The Enforce server's hard drive is out of space.
- C. A detection server has excessive filereader restarts.
- D. Tablespace is almost full.



Correct Answer: D

QUESTION 4

Under the "System Overview" in the Enforce management console, the status of a Network Monitor detection server is shown as "Running Selected." The Network Monitor server's event logs indicate that the packet capture and filereader processes are crashing.

What is a possible cause for the Network Monitor server being in this state?

- A. There is insufficient disk space on the Network Monitor server.
- B. The Network Monitor server's certificate is corrupt or missing.
- C. The Network Monitor server's license file has expired.
- D. The Enforce and Network Monitor servers are running different versions of DLP.

Correct Answer: D

QUESTION 5

Which detection server is available from Symantec as a hardware appliance?

- A. Network Prevent for Email
- B. Network Discover
- C. Network Monitor
- D. Network Prevent for Web

Correct Answer: D

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v122938258_v120691346/Setting-up-the-DLP-S500-Appliance?locale=EN_US

[250-438 VCE Dumps](#)

[250-438 Exam Questions](#)

[250-438 Brindumps](#)