

ST0-134^{Q&As}

Symantec EndPoint Protection 12.1 Technical Assessment

Pass Symantec ST0-134 Exam with 100% Guarantee

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

<https://www.leads4pass.com/st0-134.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

An administrator is in the process of recovering from a disaster and needs the keystore password to update the certificate on the Symantec Endpoint Protection Manager (SEPM). From which two locations can the administrator obtain this information? (Select two.)

- A. SEPM replication partners
- B. original installation log
- C. disaster recovery file
- D. settings.properties file
- E. Sylink.xml file from the SEPM

Correct Answer: CD

QUESTION 2

A client is unable to communicate with the Symantec Endpoint Protection Manager (SEPM) Server. The administrator decides to replace the Sylink.xml file on the client using the ylinkDrop tool. Which two additional tasks can be accomplished by replacing the Sylink.xml file? (Select two.)

- A. Convert an unmanaged client to a managed client.
- B. Migrate the SEPM servers to a new domain.
- C. Enable remote troubleshooting for administrators.
- D. Update Symantec Endpoint Protection client to the latest eraser engine.
- E. Migrate or move clients to a new domain or management server.

Correct Answer: AE

QUESTION 3

Which client log shows that a client is downloading content from its designated source?

- A. Risk Log
- B. System Log
- C. SesmLu.log
- D. Log.LiveUpdate

Correct Answer: B

QUESTION 4

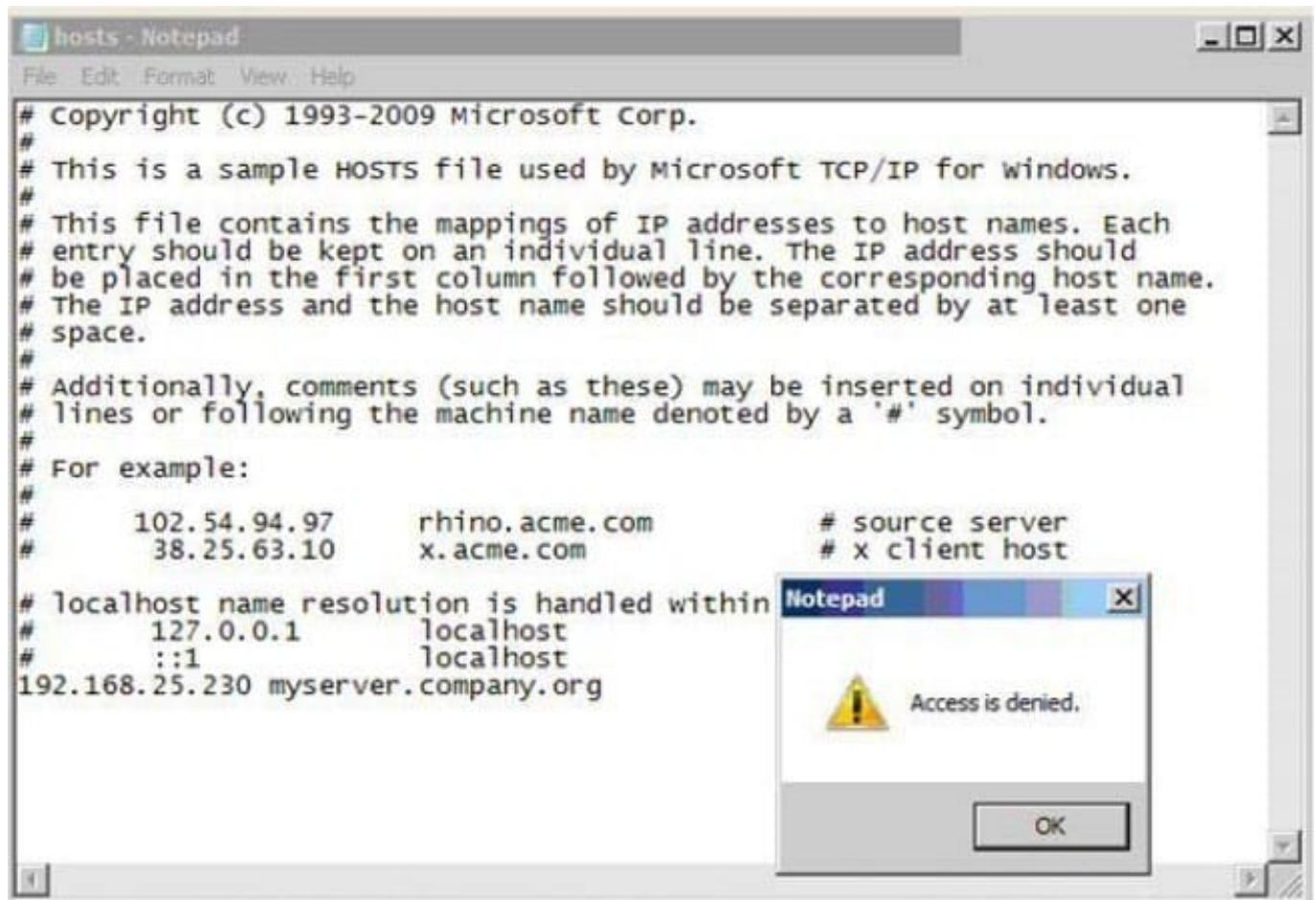
Administrators at a company share a single terminal for configuring Symantec Endpoint Protection. The administrators want to ensure that each administrator using the console is forced to authenticate using their individual credentials. They are concerned that administrators may forget to log off the terminal, which would easily allow others to gain access to the Symantec Endpoint Protection Manager (SEPM) console. Which setting should the administrator disable to minimize the risk of non-authorized users logging into the SEPM console?

- A. allow users to save credentials when logging on
- B. delete clients that have not connected for specified time
- C. lock account after the specified number of unsuccessful logon attempts
- D. allow administrators to reset the passwords

Correct Answer: A

QUESTION 5

Refer to the exhibit.



A user runs a full scan on a system and is confused by the "Files trusted" count. Which option will result in the files being left unscanned?

- A. Enabling the "Only when files are executed" setting in the Virus and Spyware Protection policy.
- B. Enabling the "Do not scan files when trusted processes access the files" setting in the Virus and Spyware Protection policy.
- C. Enabling Insight in the Virus and Spyware Protection policy.
- D. Enabling the file cache settings in the Virus and Spyware Protection policy.

Correct Answer: C

[ST0-134 PDF Dumps](#)

[ST0-134 Study Guide](#)

[ST0-134 Braindumps](#)