



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.passapply.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

Drive-by downloads are a common vector of infections. Some of these attacks use encryption to bypass traditional defense mechanisms. Which Symantec Endpoint Protection 12.1 protection technology blocks such obfuscated attacks?

- A. SONAR
- B. Bloodhound heuristic virus detection
- C. Client Firewall
- D. Browser Intrusion Prevention

Correct Answer: D

QUESTION 2

An administrator tests a new Application and Device Control policy. One of the rule sets being tested blocks the notepad.exe application from running. After pushing the policy to a test client, the administrator finds that notepad.exe is still able to run. The administrator verifies that the rule set is enabled in the Application and Device Control policy. Which two reasons may be preventing the policy from performing the application blocking? (Select two.)

- A. The System Lockdown policy includes notepad.exe in the whitelist.
- B. System Lockdown has been removed from the client.
- C. The Client User Interface Control is set to Client control.
- D. The rule set is in Production mode.
- E. A rule set with conflicting rules exists higher up in the policy.

Correct Answer: AE

QUESTION 3

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. Symlink.xml file from the SEPM



Correct Answer: CD

QUESTION 4

A computer is configured in Mixed Control mode. The administrator creates and applies a Firewall policy to the computer that has a rule that allows FTP traffic above the blue line and another rule that blocks LDAP traffic below the blue line. On the computer, local rules are created to allow LDAP traffic and block FTP traffic. Which traffic flow behavior should be expected on the local computer?

- A. Both FTP and LDAP traffic are allowed.
- B. Both FTP and LDAP traffic are blocked.
- C. FTP is blocked and LDAP is allowed.
- D. FTP is allowed and LDAP is blocked.

Correct Answer: A

QUESTION 5

An administrator wants to deploy the Symantec Endpoint Protection 12.1 (SEP) client to computers that are lacking the Symantec Endpoint Protection client. Which tool should the administrator use to discover and deploy the SEP client to the computers?

- A. Unmanaged Detector
- B. Client Deployment Wizard
- C. Symantec Endpoint Recovery Tool
- D. Symantec Endpoint Discovery Tool

Correct Answer: B

[Latest ST0-134 Dumps](#)

[ST0-134 PDF Dumps](#)

[ST0-134 Study Guide](#)