
Question: 1

After several failed logon attempts, the Symantec Endpoint Protection Manager (SEPM) has locked the default admin account. An administrator needs to make system changes as soon as possible to address an outbreak, but the admin account is the only account.

Which action should the administrator take to correct the problem with minimal impact to the existing environment?

- A. Wait 15 minutes and attempt to log on again
- B. Restore the SEPM from a backup
- C. Run the Management Server and Configuration Wizard to reconfigure the server
- D. Reinstall the SEPM

Answer: A

https://support.symantec.com/en_US/article.HOWTO80757.html

Question: 2

In which two areas can host groups be used? (Select two.)

- A. Locations
- B. Download Insight
- C. IPS
- D. Application and Device Control
- E. Firewall

Answer: CE

Question: 3

Which Symantec Endpoint Protection technology blocks a downloaded program from installing browser plugins?

- A. Intrusion Prevention
- B. SONAR
- C. Tamper Protection
- D. Application and Device Control

Answer: D

Question: 4

Which Symantec End point Protection defense mechanism provides protection against threats that propagate from system to system through the use of autotun.inf files?

- A. Host Integrity
- B. SONAR
- C. Application and Device Control
- D. Emulator

Answer: C

Question: 5

An administrator uses the search criteria displayed in the image below. Which results are returned from the query?

Search Field	Comparison Operator	Value
Operating System	=	Windows Server 2012 Standard Edit...
Virtualization Platform	=	VMware

- A. Only VMware Servers in the Default Group
- B. All Windows 2012 Servers in the Default Group
- C. Only Windows 2012 Servers that are Virtualized in the Default Group
- D. All Windows 2012 Servers and all Virtualized Servers in the Default Group

Answer: D

Question: 6

Which action should an administrator take to prevent users from using Windows Security Center?

- A. Set Disable antivirus alert within Windows Security Center to Disable
- B. Set Disable Windows Security Center to Always

- C. Set Disable Windows Security Center to Disable
- D. Set Disable antivirus alert within Windows Security Center to Never

Answer: B

Question: 7

Which two options are supported Symantec End point Manager authentication types? (Select two.)

- A. Microsoft Active Directory
- B. MS-CHAP
- C. RSA SecurID
- D. Biometrics
- E. Network Access Control

Answer: A, C

Question: 8

A Symantec Endpoint Protection (SEP) client uses a management server list with three management servers in the priority 1 list.

Which mechanism does the SEP client use to select an alternate management server if the currently selected management server is unavailable?

- A. The client chooses another server in the list randomly.
- B. The client chooses a server based on the lowest server load.
- C. The client chooses a server with the next highest IP address.
- D. The client chooses the next server alphabetically by server name.

Answer: A

Question: 9

A Symantec Endpoint Protection (SEP) administrator creates a firewall policy to block FTP traffic and assigns the policy to all of the SEP clients. The network monitoring team informs the administrator that a client system is making an FTP connection to a server. While investigating the problem from the SEP client GUI, the administrator notices that there are zero entries pertaining to FTP traffic in the SEP Traffic log or Packet log. While viewing the Network Activity dialog, there is zero inbound/outbound traffic for the FTP process.

What is the most likely reason?

-
- A. The block rule is below the blue line.
 - B. The server has an IPS exception for that traffic.
 - C. Peer-to-peer authentication is allowing the traffic.
 - D. The server is in the IPS policy excluded hosts list.

Answer: D