

Checkpoint

Exam 156-708.70

Check Point Endpoint Specialist - Media Encryption(CPEPS-ME)

Version: 6.0

[Total Questions: 58]

Question No : 1

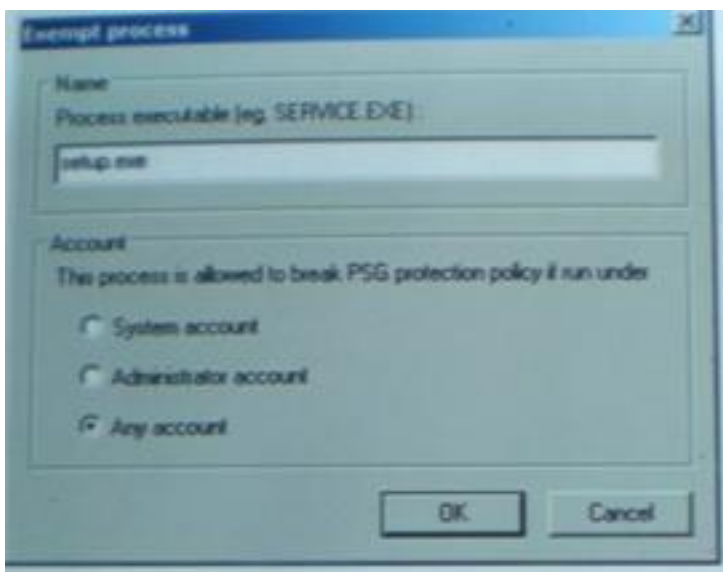
True or False. The EPM Explorer offline access to encrypted data on third party matches without the need to install any software.

- A. True, if offline access is permitted in the Removable Media manager tab of the profile.
- B. True, if offline access is permitted in Encryption tab of the profile, and correct password is entered.
- C. False, third party matches without Endpoint Security Media Encryption client or the EPM client software installed cannot access Encrypted Media.
- D. False, access is granted only via a password

Answer: B

Question No : 2

Consider the following Graphic. As a result of exempting this application, PSG will



- A. Block the file setup.exe
- B. Be disabled
- C. Still block the file setup.exe when running under a domain account.
- D. Not block the file setup.exe

Answer: D

Question No : 3

What are three file types that Endpoint Security Media Encryption exempts by default?

- A. .BAT .MP3 .EXE
- B. .CMD .EXE .MP3
- C. .EXE .VBS .BAT
- D. .CAB .MSI .DLL

Answer: D

Question No : 4

What port number is the default value used by Endpoint Security Media Encryption Clients to communicate with the server?

- A. 22
- B. 942
- C. 9738
- D. 25

Answer: C

Question No : 5

Which Endpoint Security Media Encryption component digitally signs and approves devices attached to a workstation?

- A. Removable Media Manager
- B. Auditor
- C. Device manager
- D. Encryption Policy Manager

Answer: A

Question No : 6

During the installation of Endpoint SecurityServer a default profiletemplate is created. Which of the following statements about default profile is FALSE?

- A. The default profile is usedwhen a user connectsfrom an endpointSecuritymedia EncryptionClient Machinethat is not in the endpoint SecurityMedia Encryption user database.
- B. It is recommended thatyou modifythe default profileto reflect organization policies.
- C. It is used if the serverconnection fails and as a fail-safemechanism.
- D. The default profile is usedas the base profilefor all other profiles.

Answer: A

Question No : 7

Which EndpointSecurityMedia Encryptioncommand controls deviceaccess an all availableports includingUSB andFirewall?

- A. Encryption Policy Manager
- B. Removable Media Manager
- C. Program Security Guard
- D. Device Manager

Answer: D

Question No : 8

What setup commandwould you useto create a recorded ME Client installation?

- A. setup.exe -r
- B. setup.exe -s
- C. setup.exe -r
- D. setup.exe -capture

Answer: C

Question No : 9

Assume you configure a profile template named Standard users that contained the Device manager setting as depicted in the following graphic.

Device	Define	Auth	Plan Text	Encrypted
Apple iPod	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Read only, Encrypt	Access
CD/DVD-ROM Drives	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Read only	Access
External Hard Drives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	Access, Create
Floppy disks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Tape Drives	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Modems	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Modem (USB)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Bluetooth Radio	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Bluetooth Devices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	
Bluetooth	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Bluetooth USB	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Cell image devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Infrared Devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Smart Card Readers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access, Encrypt	
POCMA Memory	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
USB Controllers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	
BlackBerry Devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Palm OS Devices (USB)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	
Windows CE Portable D...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Ports (COM & LPT)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	
Ports COM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	
Ports LPT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	
Network Adapters	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	
Windows Network A...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	
Windows Portable Dev...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No access	
Keyboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	
PS/2 Keyboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full access	

Specifically, what permissions are configured for users using external Hard Devices?

- A. The users may not only read data from device, and are permitted the ability to encrypt the device.
- B. The users may not only read data from device, but are required to encrypt the device before accessing the data.
- C. The users may not only read data from device, and can access as well as create encrypted media.
- D. The users may not only read data from device, but are required to encrypt the device when protector client machine.

Answer: C

Question No : 10