Checkpoint 156-708-70

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

Practice Test

Version: 4.0

QUESTION NO: 1

Under whatcircumstancesthis command line procedure wouldbe used?

1)osq 1. Exe –z

2)use disknet

3)updates global configuration set

4)go

A. To connect to a local MSDEdatabaseinstalled on a machine usinga Microsoft trusted application
B. To unlock andaccess the EndpointSecurity Media Encryption Server service.
C. To address a blue screenissue when usingEndpoint Security media Encryptionand McAfee 8.5i on a windows vista enterprise machine.
D. To connect to a remote SQL instance using trusted authentication

Answer: A
Explanation:

QUESTION NO: 2

Can Endpoint Security Media Encryptionimport Novell groups?

A. No, Endpoint Security Media Encryption only works with active Directory.
B. Yes
C. Yes. If the Novell Server is usingRADIUS with LDAP
D. No, Endpoint Security Media Encryption only USERS RADIUS

Answer: B
Explanation:

QUESTION NO: 3

When you created your client install package, you entered the incorrectME server name and now your clients cannot download their profiles. How can you update your clients to point the correct server?

A. Change the server name in the defaultprofile;export the profile in.dnp format, import.dnp on the

attached clients.
B. On each client edit the registrykeyHELM\software checkpoint\Encryption\Servername\with the correct ME server name.
C. Update the server infile on each clientwith the correct server name
D. On each client, edit the registry key HKIM\software\Reflex\disknet\servername with the correct ME server name.

Answer: D
Explanation:

QUESTION NO: 4

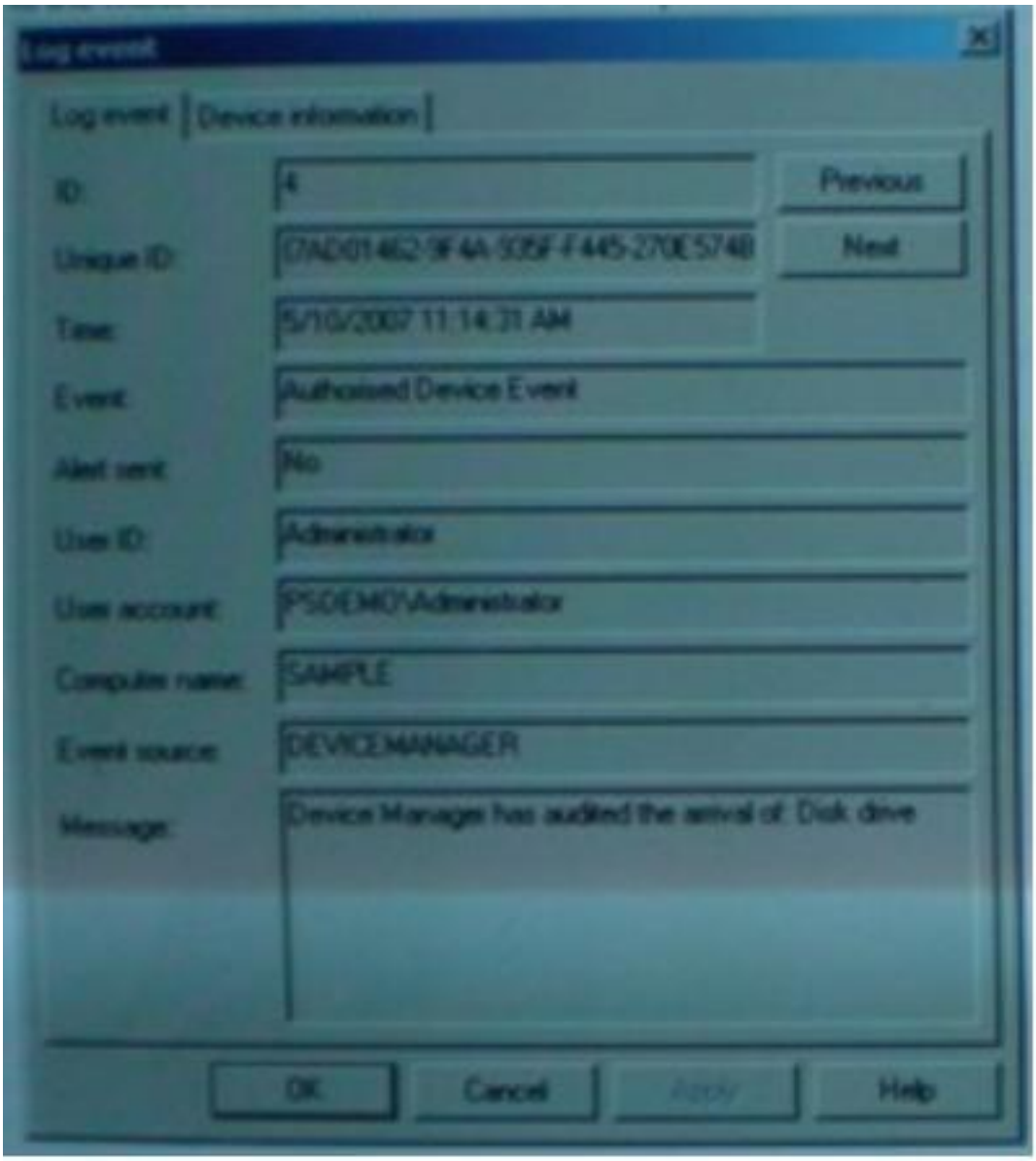
Find in the blank if no Ant-Virus Scanner or PointSec DataScan is detected on theclient machine, thanaromaticauthentication_____.

A. Will be possible under certain restrictions.
B. Will be possibleand access will not begranted.
C. Is initiated with administrative approval
D. Will permit the user to authorize the device anyway

Answer: B
Explanation:

QUESTION NO: 5

Consider the following imageof log event. Assume the device is frequentlyused, but you cannot control its use to theextent that isrequired. What is the most reliable solution to this dilemma?



A. Add the device to the desktop Device Manager
B. Create email alerts any time the device is accessed
C. Create a media audit rule
D. Require that thedevice be passwordencrypted

Answer: A

Explanation:

QUESTION NO: 6

There have been a securitybreach of your company’snetwork and you must blockclients from downloadingall fields with an–instextension. What isthe correct approachto resolve the issue?

A. Create the extension in PSG, save the profile, and update all groups.
B. Load the default profileto groups in the organizationuntil steps are taken to remove the threat.
C. PSG does notsupport executing fileshaving other than three character extension and willtherefore block the file.
D. Select the extension in PSG, and reload the profile appropriately.

Answer: C
Explanation:

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
Explanation:

QUESTION NO: 8

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
Explanation:

QUESTION NO: 9

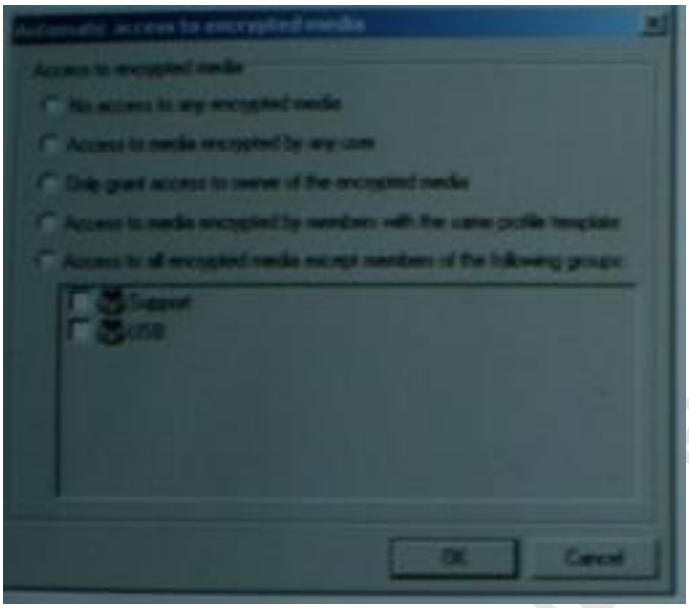
Before endpoint Securitymedia Encryption Serverversion4.93 can run on windows 2003Machine, what must be installed?

A. Endpoint Security Media Encryptionver.4.91 HFA 1
B. Windows 2003 server pack 1
C. Windows 2003 server pack 2
D. The Endpoint Security Media Encryption administration console

Answer: A
Explanation:

QUESTION NO: 10

Assuming you wantspecific users to haveaccess t theirencryptedmedia from anycomputer on the network, regardless ofwhoislogged in. Which of the following screen options would you use?

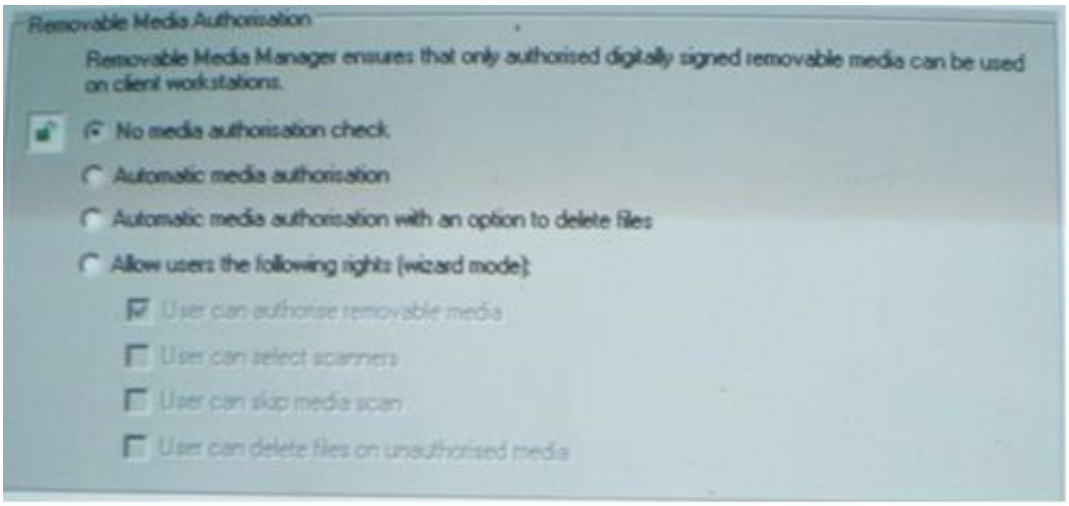


A. Access to all encrypted media exceptmembers of the following groups.
B. Access to media encrypted by any user
C. Only grant accessto owner of the encrypted media
D. Access to media encryptedby members with the sameprofile template.

Answer: A
Explanation:

QUESTION NO: 11

According to the following graphic, what is the result of the setting?



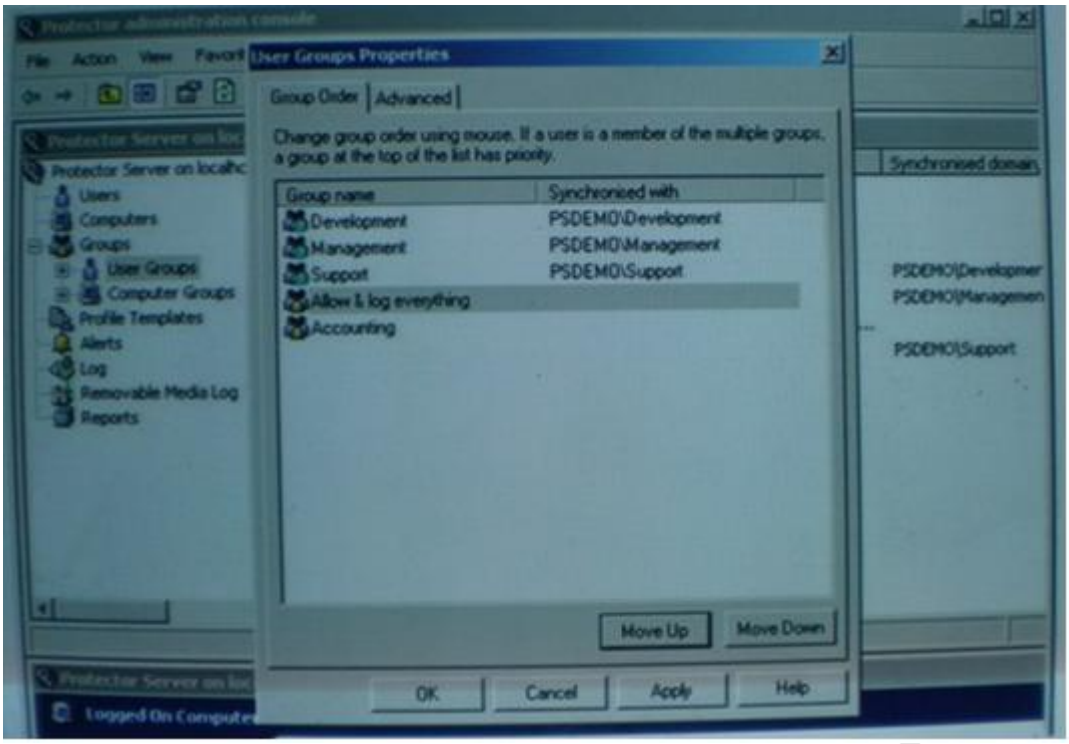
A. Disables removableMedia Manager.
B. Bypass userauthentication butvirus and data scanning still occurs
C. BypassRemovable media manager in the current profile.
D. Users will not be able to access certain devices listed in Device Manager

Answer: A

Explanation:

QUESTION NO: 12

Considerthe following image.Inthis situation, the groups listed here areindividually pointed todifferent EndpointSecurity Media Encryption. You have allowed usersto be members of multiple groupsand userX is member of all 4 media Encryption groups. After synchronization with the AD server, which endpoint Security media Encryptiongroup(s) inherits the user?



A. Support
B. Development
C. Group_All
D. accounting

Answer: C

Explanation:

QUESTION NO: 13

You areEndpoint Security media encryptionadministrator,you observed that clients are successfully pullingtheir profiles, but are not being pushed fromuser. What is the likeliest cause?

A. If running a windows firewall on theclient machine, disable it.
B. Server initiated trafficsent over UDP might be gettingblocked by firewallrules on the client
C. All communication betweenserver and client must beallowed to occur overTCP
D. The client must be addedto the trusted zone list

Answer: B

Explanation:

QUESTION NO: 14
You are an administratorwho, after examining stored log events, must set specificrestrictionson a

commonly used deviceby a group of clients. Which command or operation must you invoke to beginsetting proper restrictions?

A. Add the device from theDevice information tab.
B. Edit the express .int file
C. Perform a Media Revocation
D. Click Edit in the Device Manager Configuration Editor

Answer: A
Explanation:

QUESTION NO: 15

On a new server installationof Endpoint Security mediaEncryption, Who has access to theadministrationconsole?

A. All Domain Users
B. Members of the Domain Admin group
C. Members of the local Administrators group
D. Only the built in administrator group
E. Only the built in administrator account

Answer: D
Explanation:

QUESTION NO: 16

Which Endpoint Securitymedia Encryptioncomponentdigitallysigns and approvesdevices attached toa workstation?

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

Answer: A
Explanation:

QUESTION NO: 17

In your Endpoint Security Media Encryptionnetworkcertain computers needs to haveaccess to local printersand scanners. Select thebest approach tomeet this requirement?

A. Create a new profile modifying Device manager for Specific users
B. Apply profile changesto user groups permitting specific machine setting
C. Create a Group with specificconfiguration in device manager
D. Customize profile to the appropriate users.

Answer: C
Explanation:

QUESTION NO: 18

What are the minimum requirementsfor installing endpoint securitymedia Encryption Server?

A. 1 GB RAM/4GB + hard-Disk space for MySQL database storage/windows NT/MS Windows NT Service Pack 7a\MS windows2000/3 server/Advanced-Server or Professional/MS windows 2000/3 Service Pack 3+/ MS Windows XP Home/ red hat link Kernel Version 6.14.
B. 512MB+ RAM/2GB + hard-Disk space for MSSQL database storage/windows NT/MS Windows NT Service Pack 7a\MS windows 2000/3 server/Advanced-Server or Professional/MS windows 2000/3 Service Pack 3+/ MS Windows XPprofessional.
C. 512 MB+RAM/4GB + hard-Disk space for MySQL database storage/windows NT/MS Windows NT Service Pack 7a\MS windows 2000/3 server/Advanced-Server or Professional/MS windows 2000/3 Service Pack 3+/ MS Windows XPProfessional.
D. 2GB+RAM/4GB + hard-Disk space for MySQL database storage/windows NT/MS Windows NT Service Pack 7a\MS windows 2000/3 server/Advanced-Server or Professional/MS windows 2000/3 Service Pack 3+/ MS Windows XPProfessional.

Answer: B
Explanation:

QUESTION NO: 19

Client anti-tamper protection prevents_____.

A. Unauthorized client profile reloads without a password.
B. End users from modifying or deletingEndpoint Securitymedia Encryptionregistry keys or system files.
C. The ability to debug client software effectively
D. A client's profile from being modified or deleted.

Answer: B
Explanation:

QUESTION NO: 20

What server(s) must be accepted by an internalfirewall to permite-mail alertsto administrators?

A. SMTP
B. DHCP
C. TCP and UDP
D. SNMP

Answer: A
Explanation:

QUESTION NO: 21

Mega picture Corp, wants to create interactive photo kiosks, where customers canupload picture datafrom their digital cameras any where in the worldto a central server and down load data to photo-printer CD near theirhome. Which Endpoint Security Media Encryptioncomponent wouldthis bymanaging knownand unknown devicesby type, brand, model, or individual device?

A. Author
B. Removable media manager
C. Program Security Guard
D. Device Manager

Answer: D
Explanation:

QUESTION NO: 22

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

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

Answer: D
Explanation:

QUESTION NO: 23

What is a function of Endpoint Security Media Encryptiondatabase server?

A. Handle the server connections
B. Provide communicationbetween the management console and the database
C. Register Endpoint Security media Encryption clients
D. Store client profiled

Answer: D
Explanation:

QUESTION NO: 24

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
Explanation:

QUESTION NO: 25

Which of the following is a feature of Endpoint Security Media Encryption'sDevice Manager?

A. Complete audit of applications used
B. Integrated data authorization
C. Encryptsusing a 128-bit AESalgorithm
D. Devices controlled by type, brand, or model/this is the right answer

Answer: D
Explanation:

QUESTION NO: 26

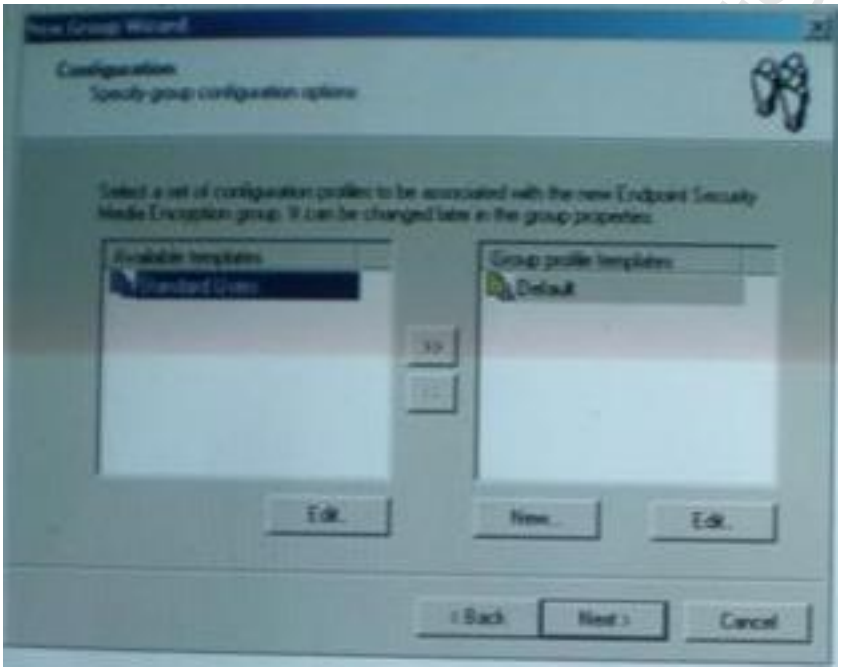
Can a device be addedto deviceManager directly froma report?

A. No. There is no direct link to the device properties.
B. No, but by nothingthe log ID, it is possibleto accessthe Log event, thereby accessing the device information tab
C. No, but it is possibleto click the device ID which directs you to theLog Events tab
D. Yes by clickingthe device ID which directs youto the device Propertiespage where there is an optionto add the device.

Answer: C
Explanation:

QUESTION NO: 27

Whencreating a new group, the following image will appear. Which of the statement aboutthe new groupscreen is true?



A. When the edit button on the right is selected(under Group profiles Templates) any changes will affect the groupusing the offline usersprofile template.
B. Change the New buttoncreates the customprofiletemplate for the selected groupand will not be availablefor other groups of users.
C. Selecting nextwithout selectinga profile template fromthe availabletemplates list willcreate the groupbut without an assigned profile.
D. When the Edit button on the rightis selected(under Group profile template) any changes will

affect only the selected group.

Answer: D

Explanation:

QUESTION NO: 28

An _____ can be copiedto the Endpoint securitymedia EncryptionClientinstallation folder and can be usedfor future installation when a Endpoint Security Media EncryptionServer is not Present.

A. Installation template
B. .msi file
C. Exported profile
D. .iss file

Answer: B

Explanation:

QUESTION NO: 29

Can one user experience different assigned profiles whenlogging into different machines?

A. Not unless the user is assigned to a group using a custom profile
B. No
C. Yes, by assigning profiles to specific computers
D. Yes,by defining permitted sites with different access permissions.

Answer: C

Explanation:

QUESTION NO: 30

True or False. The EPM Explorer offline access to encrypted data on third partymatcheswithout the need to installany software.

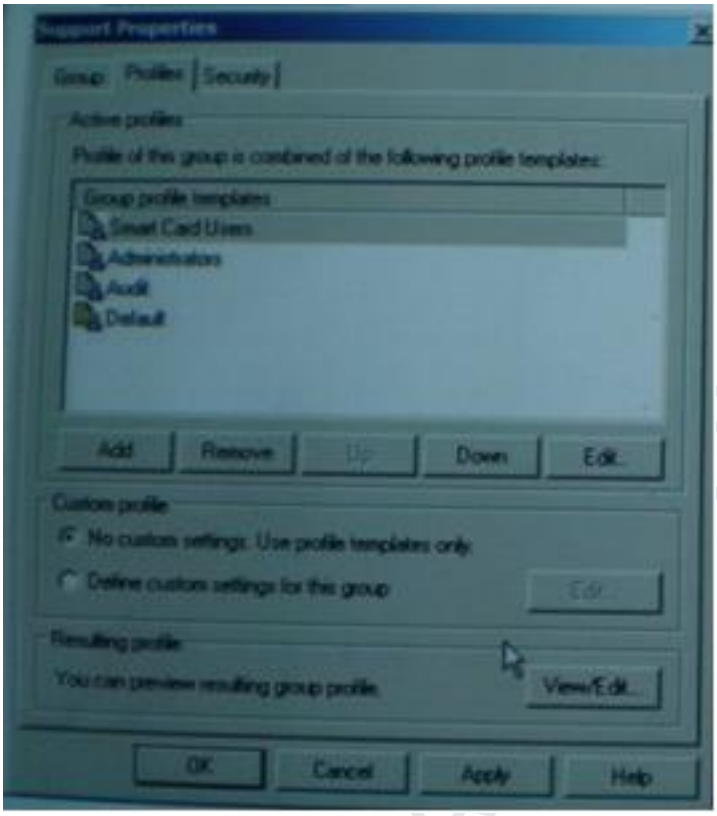
A. True, if offline access is permittedin the Removable Media manager tab of the profile.
B. True, if offline access is permittedinEncryption tab oftheprofile, and correct password is entered.

C. False,third party matches withoutEndpoint Security Media Encryptionclient or the EPM client software installedcannot access Encrypted Media.
D. False, access is granted only via a password

Answer: B
Explanation:

QUESTION NO: 31

Fill in the blank. Consider the following imageof the support groups propertiesscreen. Selecting the optiondisplays the resulting profile that is _____?



A. The default profile and theSmart Card user's profile.
B. Cumulative, based on profile order
C. The Smart card Users profile
D. Cumulative, but only the most restrictive

Answer: B
Explanation:

QUESTION NO: 32
Multibank faces new information assurance requirementsto prevent the installation ofunknown

removable mediadeviceson internal workstations, and monitor device usage. Which Endpoint Security Media Encryption component shouldMultibank's SecurityAdministrator as a solution?

A. Removable Media Manager
B. Device Manager and Auditing
C. Device Manager
D. Program Security Guard

Answer: B

Explanation:

QUESTION NO: 33

You have developed the clientsoftware to an endpointcomputer and you wantto check the profilethat is active on theclient, the best way to do this isusing the profilethe profile view and checking theparameter templateinfoname.Howdo you accessthe profile view Screen?

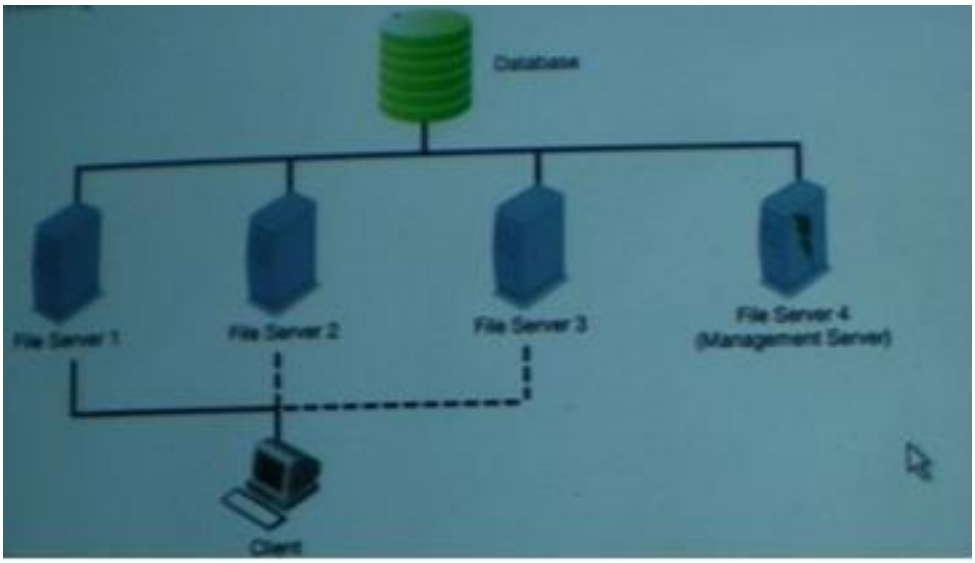
A. Right click on the Media encryptionsystray icon and selectviewprofile.
B. Right click on the Media encryption systray icon and select settings than press Ctrl+Shift+F8
C. Open a command promptand enter the commandpointsec.exe / view:profile
D. Right click on the Media encryption systray icon and selectsettings than click on the view profile button.

Answer: C

Explanation:

QUESTION NO: 34

Considering the followinggraphic, which one of the following statements is NOT TRUE?



A. Random server selection can be usedfor load balancingacross multiple servers.
B. When theclient software first starts, it registers itselfwith the Endpoint SecurityMediaEncryptionthe Server.
C. The EndpointSecurity MediaEncryptionClients havethe ability to connect multipleEndpoint Securitymedia encryptionfileservers toaprofile.
D. Endpoint Security Media Encryption Clients must connectedto an Endpoint SecurityMedia Encryptionfile servers that is managed sequential with other file servers.

Answer: D
Explanation:

QUESTION NO: 35

An Endpoint SecurityEncryptionR70 user is attemptingto open LotusNotes 6.55, but experiences a blue screenerror withPSG, sys. Which of thesestepswould you take to solvethis issue?

a)Retrieve to cash dump and contact support

b)Read the release Notes for this version

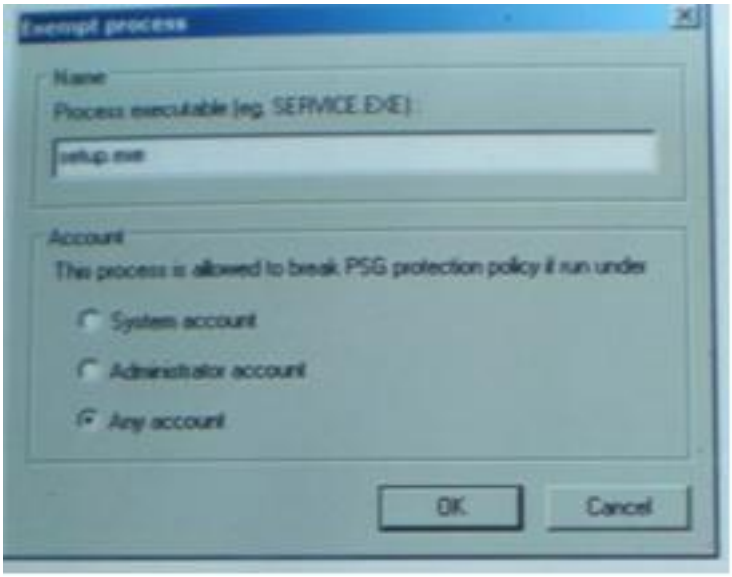
c)Modify the PSG.sys file

A. B, C
B. A, C
C. A, B, C
D. A, B

Answer: C
Explanation:

QUESTION NO: 36

Consider the following Graphic. As a resultof exemptingthis application, PSG will



A. Block the file setup.exe
B. Be disabled
C. Still blockthe filesetup.exe when running under a domainaccount.
D. Not block the file setup.exe

Answer: D
Explanation:

QUESTION NO: 37

What mustbe a requirementtoreceive EndpointSecurity Media Encryption e-mailalerts?

A. An MS SQL Server must beinstalled on the Endpoint Security Media EncryptionServer machine
B. Network port number 9738 must be specified
C. Only TCP must be accepted when using an internal firewall
D. SMTP server information including hostname and port number

Answer: D
Explanation:

QUESTION NO: 38

Which of the following would be aneffective use ofthe Events List fromthe profile Auditingtab?

A. To record authorizedprogram execution.
B. To record device password recovery
C. To record fixed hard disk configuration change
D. To detectpotential viruses or malware

Answer: C
Explanation:

QUESTION NO: 39

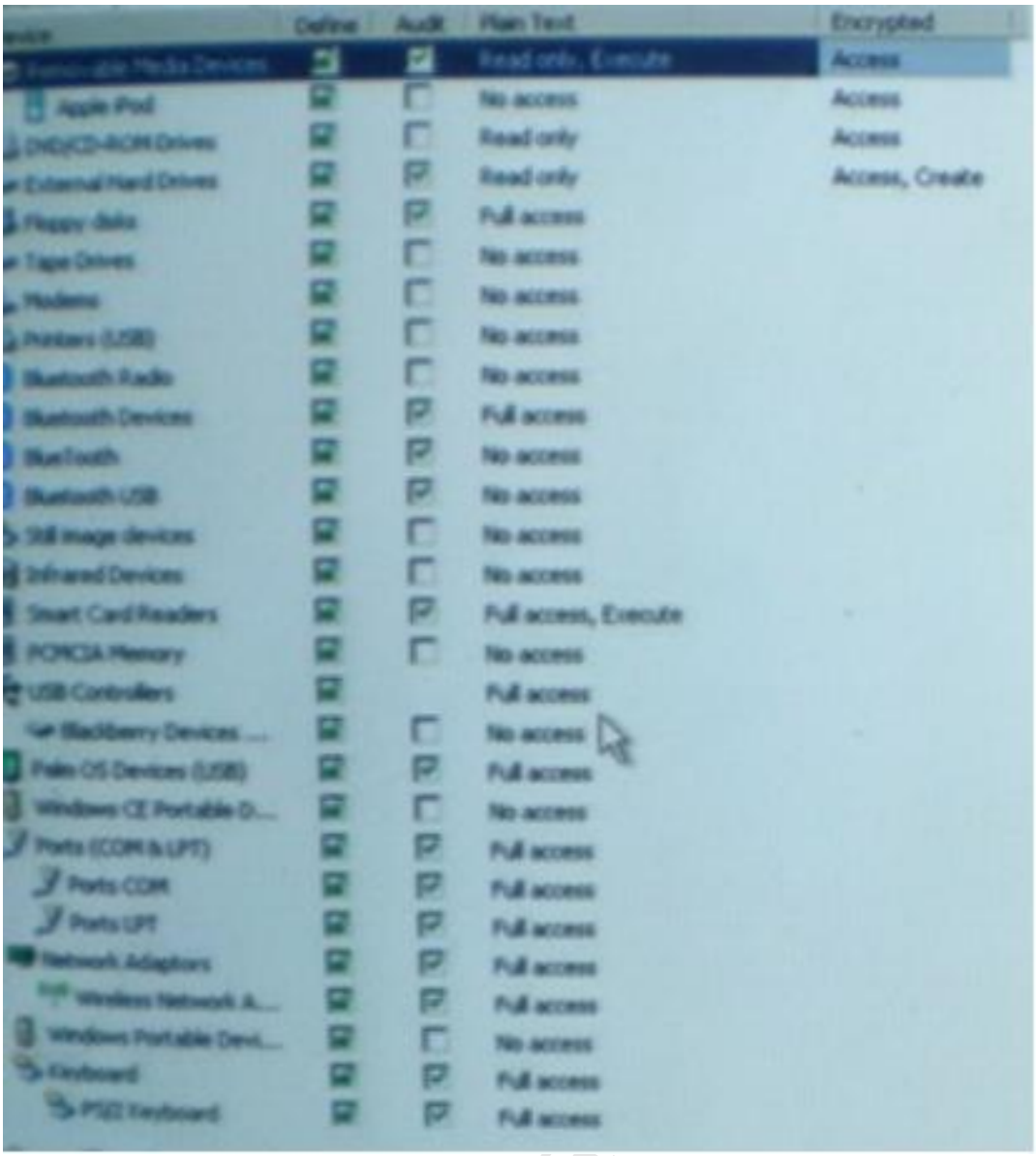
What port number is the default value used by EndpointSecurityMedia EncryptionClients to communicate with the server?

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

Answer: C
Explanation:

QUESTION NO: 40

Assume you configure a profile templatenamed standard usersthat contained theDevice managersettings as shown here.



A. The user is permitted read only access to executefiles.
B. The user is permittedto read and copy datafrom the devices as well asto execute files fromthedevice.
C. The user is permitted to read and execute data from approved devices.
D. The user is permitted to read and copy data from the devices, butonly to executeencryptedfiles.

Answer: D

Explanation:

QUESTION NO: 41

How does a client who is offlineand has been grantedoff-line access to mediaknown that is removablemedia is encrypted?

A. When he is promptedto supplya passwordto access the removable media.
B. A PSG alert message informsthe user when attempted access is made.
C. He doesn't know
D. When he is automatically granted access to encrypted media.

Answer: A
Explanation:

QUESTION NO: 42

A removable media device isencryptedon a PC runningEndpointMedia Encryption. On which of the following willthis device be accessible requiring a password?

A. A standard PCwith a standard-alone EndpointSecurity Full Disk Encryptionadministrativeinstall,even throughEndpoint Security Media Encryption is not installed.
B. A standard PC withoutany EndpointSecurity Full Disk Encryptionproducts installed.
C. Every PC not connected to the corporate network.
D. A standard PC without any endpointSecurity Products installed, if only a portion of a drive wasencrypted,the encrypted would beaccessible.

Answer: B
Explanation:

QUESTION NO: 43

Endpoint Security Media Encryption alerts are createdto apply to :

A. User groups
B. Computer groups
C. Specific users
D. Logged-on computers

Answer: A
Explanation:

QUESTION NO: 44

Pushing a profileappears to fail froma windows 2003 server. What could be the problem?

A. UDP 9738 is being blocked from the server to client.
B. TCP9738 is being blocked from the server to client.
C. TCP must be permittedif using a local Firewall
D. TCP and UDP must be permitted if usingWindows Firewall.

Answer: A
Explanation:

QUESTION NO: 45

Where does the Endpoint Security media EncryptionServer Store the profileand user information?

A. On the file Server.
B. In a MS SQL Engine.
C. Locally on the client machine.
D. The database is installed separately by the administrator.

Answer: B
Explanation:

QUESTION NO: 46

Auser inyour organizationwishes to upload customer evaluationsoftware from the USB drive to their laptop to provide feedbackabout system compatibility issues. However, the users endpoint SecurityMedia Encryptionclientprofile willnot permitexecutables of that type. What would be the best solution?

A. Modify the user'sprofileright toallowthe application type, but requirethe user todeletethe unauthorized files.
B. Modify the user'sprofile rightsto allow the applicationtype.
C. Create a computergroupallowing themto skip the mediascanwhen authorizing the device.
D. Permit the user to authorize the removable media.

Answer: B
Explanation:

QUESTION NO: 47

Which encryptionalgorithm andbit strengthdoes endpoint Securitymedia Encryption's encryptionuse?

A. 128 and 256 AES
B. 3DES
C. Blowfish
D. 64 and 192 AES

Answer: A
Explanation:

QUESTION NO: 48

Your encryption policyis set allow accessto media encryptedby anyuser. A clientinforms the administratorthat he/she cannotaccess data ontheir removablemedia, what is themost likely cause?

A. Themedia is encrypted, and the userhas attemptedaccess on a computerwithouttheendpoint security MediaEncryption Client.
B. The encrypted Media is notpassword protected.
C. The mediawas notencrypted onthat computer.
D. The user must reset their password

Answer: A
Explanation:

QUESTION NO: 49

Which Endpoint Security Media Encryptioncomponent controlsremovablemedia on all connection parts?

A. Device Manager
B. Program Security Guard
C. Encryption Policy Manager
D. Auditor

Answer: A
Explanation:

QUESTION NO: 50

Multibank facesnew information Assurancerequirements todetect changesperformed on removablemediawhen outside theCompany.Which Endpoint SecurityMedia Encryption

componentshould Multibank's SecurityAdministrator recommendedas a solution?

A. Removable MediaManager
B. Program Security Guard
C. Device Manager
D. Removable Media manager

Answer: B
Explanation:

QUESTION NO: 51

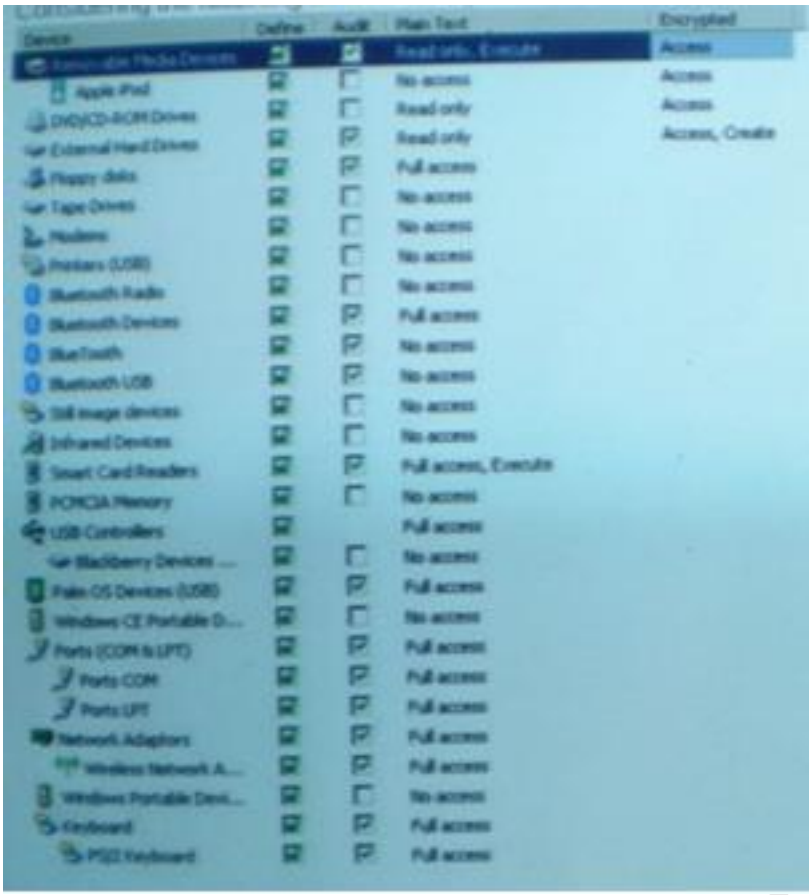
Which of the following statementregardingEndpoint SecurityMedia Encryptionreport Generation is TRUE?

A. Report types are fullyconfigurablepermitting the administratorto customizeall aspectsof theinformation required.
B. Device can be selected by typeand classification duringreport creation.
C. Onlarge sites, report generation requiresthe administrationconsole to remain open.
D. Reports can be configuredto run at regular intervals.

Answer: A
Explanation:

QUESTION NO: 52

Considering thefollowing Device Manager settings, what does auditinga devicewithout permittingaccessaccomplish foran administrator?



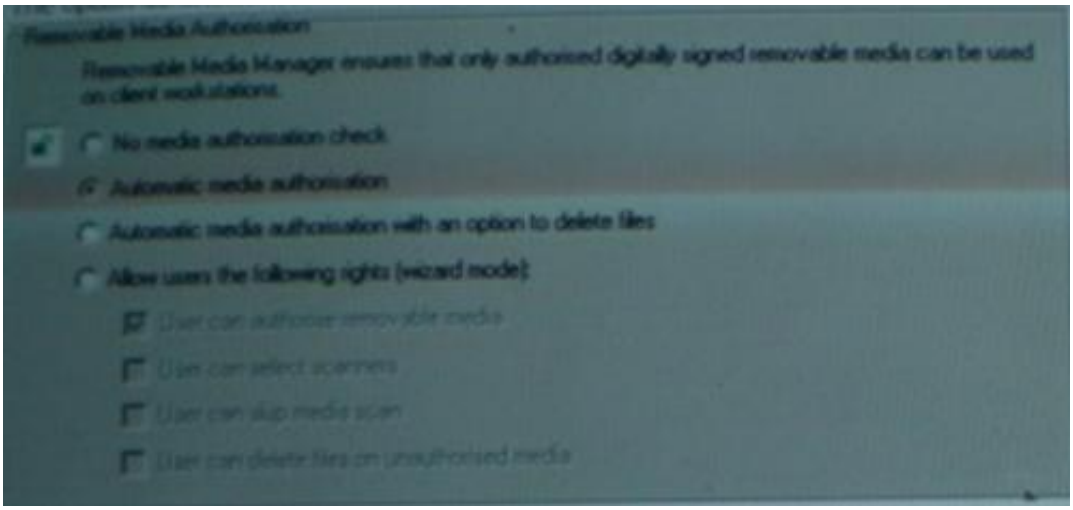
A. To alert users of failed accessto unauthorized media.
B. To alert the administratorwhenever a device isbeing accessed.
C. To monitor failed attemptsfor accessinga deviceto establishguidelinesof actual media use.
D. To monitor user's attempts,then permitaccess on a case-by-case basis.

Answer: B

Explanation:

QUESTION NO: 53

The option as shownin the following graphic,automaticmedia authorization, makes what specificrequirement of the user?



A. Data accessis not blockedto the user, but user cannotoverridevirusanddata scans.
B. Theuser is permitted to select the typeof checks made to the media.
C. Data access is blockedif themediacontainsunauthorizedfilesor a virus is detected.The user cannotoverrideresultingvirus and data checks.
D. Dependingon the file typespecifiedin the PSG tab, the user is blocked full access to the data, but is permitted limitedread onlyrights.

Answer: C
Explanation:

QUESTION NO: 54

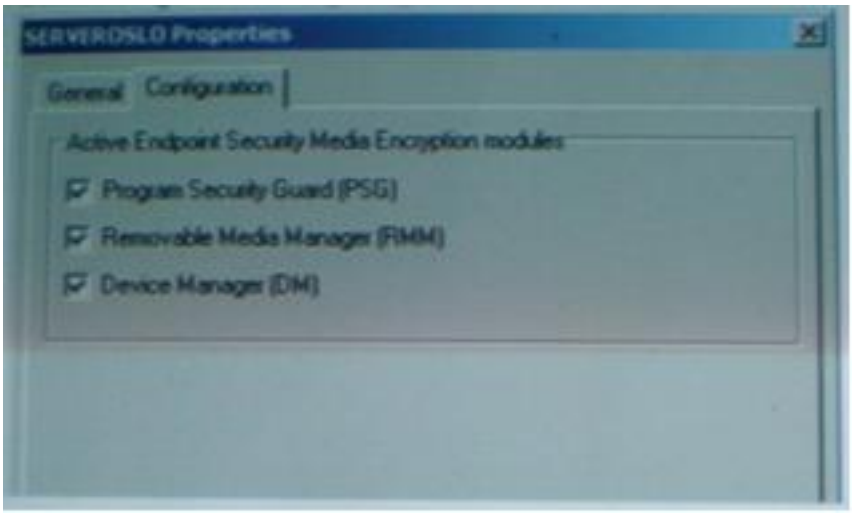
For the Endpoint SecurityMedia Encryptionclient to have the abilityto decrypt removablemedia, what other options besidesuser can remove EPM Encryption from media must beenabled in the administration console?

A. Product with a password for full accessin offline mode.
B. Icon and full menu
C. Only grant access to owner of the encrypted media
D. Users can recovertheir passwordusingchallenge/response

Answer: A
Explanation:

QUESTION NO: 55

Considering thefollowing image, what could be apotentialusefor these options?



A. Enable client menu access to these features instantly
B. Updating clientin real-time.
C. Restrictingclient access to these permissions.
D. Disablecomponents to troubleshoot client issues.

Answer: A
Explanation:

QUESTION NO: 56

Which of the following statementregardingEndpoint SecurityMedia EncryptionAudit Events is TRUE?

A. Unless the computer generatingthe event is trustedsite, the machine cannot be identified in the log.
B. A device's unique ID relates to manufacturer.
C. It is possible to use the contents of a CD from the logged data.
D. It is not possibleto know whena particulardevice has been encrypted.

Answer: B
Explanation:

QUESTION NO: 57

Endpoint Security Media EncryptionClient ver R70 is deployedsilently either by using Active Directoryand Group policyObjects(GPOs) or by

A. Using MS SMS v2 0/2003
B. Creating an installation.iss file
C. Using manual installations
D. Using the Endpoint Security Media EncryptionDeployment utility

Answer: C
Explanation:

QUESTION NO: 58

Assume you configurea profile templatenamed Standardusers thatcontainedthe Device manager setting asdepicted in the following graphic.

Specifically, what permissions are configured forusers usingexternal Hard Devices?

A. The users may not only read data from device, and are permittedthe ability to encrypt the device.
B. The users may not only read data from device, but are required to encryptthe device before accessingthe data.
C. The users may not only read data from device, and can accessas well as create encryptedmedia.
D. The users may not only read data from device, but are required to encrypt the device

whenprotector client machine.

Answer: C