

QUESTION NO: 1

Under what circumstances this command line procedure would be used?

- 1) osq 1. Exe -z
- 2) use disknet
- 3) updates global configuration set
- 4) go

- A. To connect to a local MSDE database installed on a machine using a Microsoft trusted application
- B. To unlock and access the Endpoint Security Media Encryption Server service.
- C. To address a blue screen issue when using Endpoint Security media Encryption and 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 Encryption import Novell groups?

- A. No, Endpoint Security Media Encryption only works with Active Directory.
- B. Yes
- C. Yes. If the Novell Server is using RADIUS with LDAP
- D. No, Endpoint Security Media Encryption only uses RADIUS

Answer: B

Explanation:

QUESTION NO: 3

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

- A. Change the server name in the default profile; 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

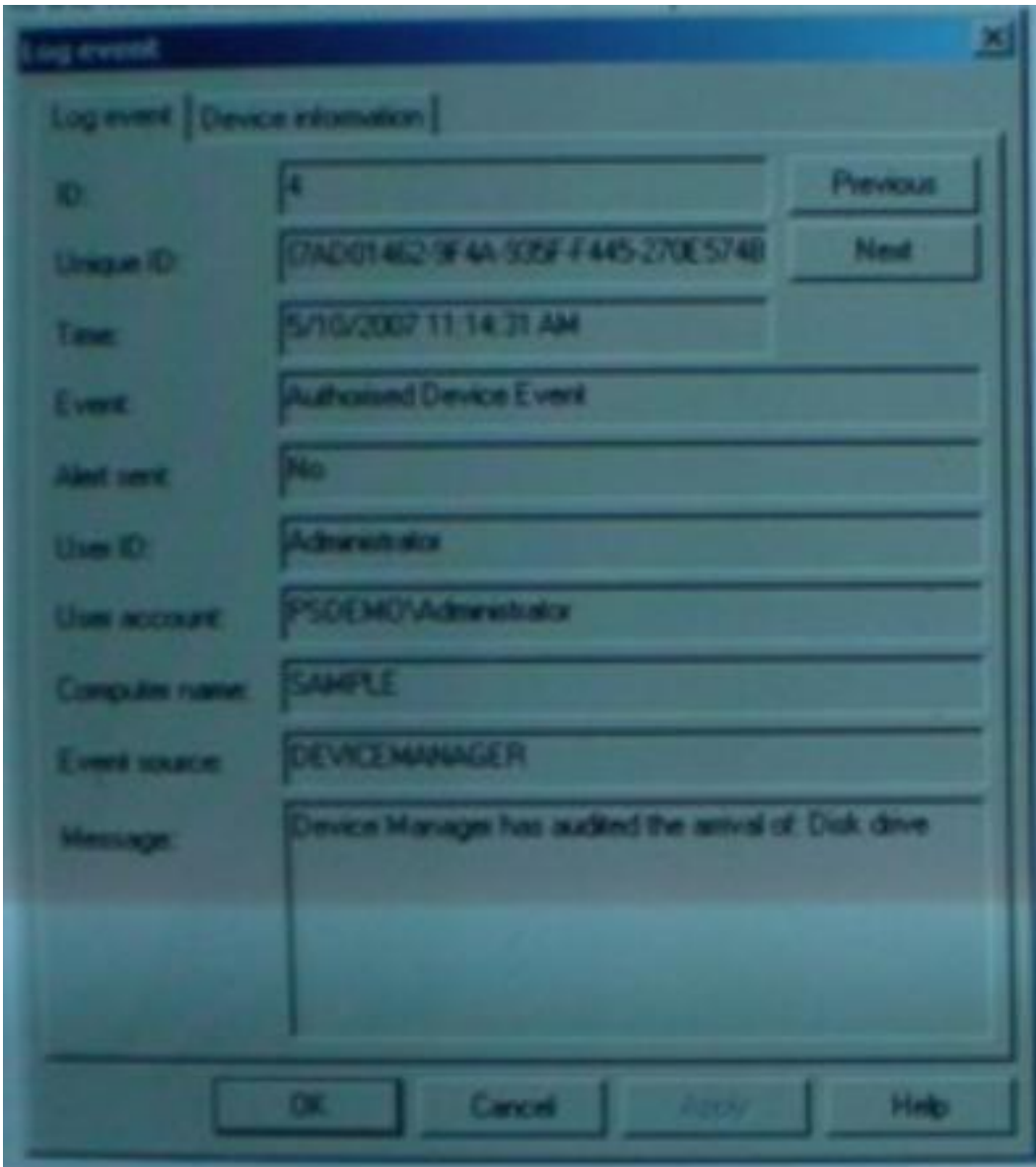
D. Will permit the user to authorize the device anyway

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 the device be password encrypted

Answer: A

Explanation:

QUESTION NO: 6

There have been a security breach of your company's network and you must block clients from downloading all files with an .exe extension. What is the correct approach to resolve the issue?

- A. Create the extension in PSG, save the profile, and update all groups.
- B. Load the default profile to groups in the organization until steps are taken to remove the threat.
- C. PSG does not support executing files having other than three character extension and will therefore block the file.
- D. Select the extension in PSG, and reload the profile appropriately.

Answer: C

Explanation:

QUESTION NO: 7

Which Endpoint Security Media Encryption command controls device access on all available ports including USB and Firewall?

- 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 Security Server a default profile template is created. Which of the following statements about default profile is FALSE?

- A. The default profile is used when a user connects from an endpoint Security Media Encryption Client Machine that is not in the endpoint Security Media Encryption user database.
- B. It is recommended that you modify the default profile to reflect organization policies.
- C. It is used if the server connection fails and as a fail-safe mechanism.
- D. The default profile is used as the base profile for all other profiles.

Answer: A

Explanation:

QUESTION NO: 9

Before endpoint Security Media Encryption Server version 4.93 can run on Windows 2003 Machine, what must be installed?