100% Money Back Guarantee

Vendor: Symantec

Exam Code:250-315

Exam Name: Administration of Symantec Endpoint Protection 12.1

Version: Demo

QUESTION 1

What are two supported Symantec Endpoint Protection Manager authentication types? (Select two.)

A. Microsoft Active Directory

B. MS-CHAP

C. RSA SecurID

D. Biometrics

E. Network Access Control

Correct Answer: AC

QUESTION 2

A company needs to configure an Application and Device Control policy to block read/write access to all USB removable media on its Symantec Endpoint Protection (SEP) systems.

Which tool should an administrator use to format the GUID and device IDs as required by SEP?

A. CheckSum.exe

B. DeviceTree.exe

C. TaskMgr.exe

D. DevViewer.exe

Correct Answer: D

QUESTION 3

An administrator is using the SylinkDrop tool to update a Symantec Endpoint Protection client install on a system. The client fails to migrate to the new Symantec Endpoint Protection Manager (SEPM), which is defined correctly in the Sylink.xml file that was exported from the SEPM. Which settings must be provided with SylinkDrop to ensure the successful migration to a new Symantec Endpoint Protection environment with additional Group Level Security Settings?

A. -s "silent"

B. -t "Tamper Protect"

C. -r "reboot"

D. -p "password"

Correct Answer: D

QUESTION 4

Administrators at a company share a single terminal for configuring Symantec Endpoint Protection. The administrators want to ensure that each administrator using the console is forced to authenticate using their individual credentials. They are concerned that administrators may forget to log off the terminal, which would easily allow others to gain access to the Symantec Endpoint Protection Manager (SEPM) console.

Which setting should the administrator disable to minimize the risk of non-authorized users logging into the SEPM console?

A. allow users to save credentials when logging on

B. delete clients that have not connected for specified time

C. lock account after the specified number of unsuccessful logon attempts

D. allow administrators to reset the passwords

Correct Answer: A

QUESTION 5

Which protection engine should be enabled to drop malicious vulnerability scans against a client system?

A. SONAR

B. Intrusion Prevention

C. Tamper Protection

D. Application and Device Control

Correct Answer: B

QUESTION 6

A company has an application that requires network traffic in both directions to multiple systems at a specific external domain. A firewall rule was created to allow traffic to and from the external domain, but the rule is blocking incoming traffic.

What should an administrator enable in the firewall policy to allow this traffic?

A. TCP resequencing

B. Smart DHCP

C. Reverse DNS Lookup

D. Smart WINS

Correct Answer: C

QUESTION 7

Which technology can prevent an unknown executable from being downloaded through a browser session?

A. Browser Intrusion Prevention

B. Download Insight

C. Application Control

D. SONAR

Correct Answer: B

QUESTION 8

A Symantec Endpoint Protection administrator needs to comply with a service level agreement stipulating that all definitions must be internally quality assurance tested before being deployed to customers.

Which step should the administrator take?

A. install a LiveUpdate Administrator Server

B. install a Shared Insight Cache Server

C. install a Group Update Provider (GUP) to the existing site

D. install a Symantec Protection Center

Correct Answer: D

QUESTION 9

A managed service provider (MSP) is managing Symantec Endpoint Protection for a number of independent companies. Each company has administrators who will log in from time to time to add new clients. Administrators must be prevented from seeing the existence of other companies in the console.

What should an administrator create for each independent company?

A. Domain

B. Location

C. Group

D. Site

Correct Answer: A

QUESTION 10

The LiveUpdate Download Schedule is set to the default on the Symantec Endpoint Protection Manager (SEPM).

How many content revisions must the SEPM keep to ensure clients that check in to the SEPM every 10 days receive xdelta content packages instead of full content packages?

A. 10

B. 20

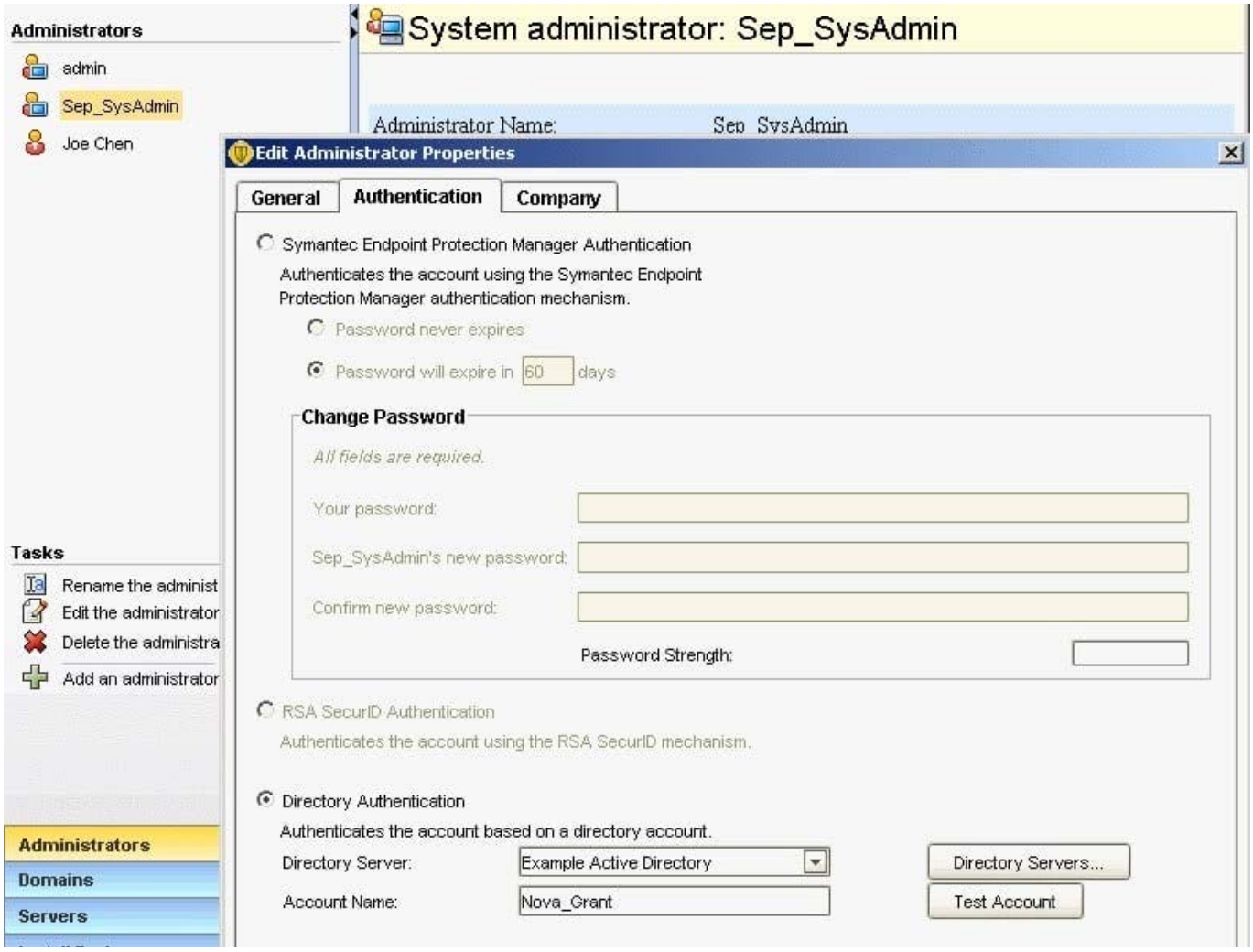
C. 30

D. 60

Correct Answer: C

QUESTION 11

Refer to the exhibit.



An administrator has configured the Symantec Endpoint Protection Manager (SEPM) to use Active Directory authentication. The administrator defines a new Symantec Endpoint Protection administrator named Sep_SysAdmin, configured to use Directory Authentication.

Which password needs to be entered when the administrator logs in to the SEPM console as Sep_SysAdmin?

A. The password for the Active Directory account Nova_Grant

B. The password for the SEPM account Nova_Grant

C. The password for the Active Directory account Sep_SysAdmin

D. The password for the SEPM account Sep_SysAdmin

Correct Answer: A

QUESTION 12

Which ports on the company firewall must an administrator open to avoid problems when connecting to Symantec Public LiveUpdate servers?

A. 25, 80, and 2967

B. 2967, 8014, and 8443

C. 21, 443, and 2967

D. 21, 80, and 443

Correct Answer: D