

ST0-029

ST0-029

**Symantec Endpoint Protection 11
(STS)**

Version 3.5

ST0-029

QUESTION NO: 1

Which Symantec Network Access Control method supports basic and transparent mode for 802.1x?

- A. Gateway Enforcer
- B. Self Enforcement
- C. DHCP Enforcer
- D. LAN Enforcer

Answer: D

QUESTION NO: 2

When using the Push Deployment wizard, which two methods can you use to identify the target machines to which you want to install the Symantec Endpoint Protection client? (Select two.)

- A. browse through Windows Networking
- B. import a file containing IP addresses
- C. specify a UNC path
- D. import a file containing MAC addresses
- E. import hostnames from an LDAP server

Answer: A, C

QUESTION NO: 3

From where does the Migration and Deployment wizard collect settings?

- A. configuration file

ST0-029

- B. Symantec Client Firewall Administrator
- C. Symantec AntiVirus server
- D. Active Directory server

Answer: C

QUESTION NO: 4

In which group can you NOT create new subgroups?

- A. Global
- B. Subgroup
- C. Temporary
- D. Administrator-created

Answer: C

QUESTION NO: 5

Which four events trigger an Auto-Protect scan? (Select four.)

- A. create
- B. open
- C. archive
- D. move
- E. rename
- F. run

ST0-029

Answer: A, C, D, F

QUESTION NO: 6

Upon which convention are custom Symantec Endpoint Protection Intrusion Prevention signatures based?

- A. Generic Exploit Blocking
- B. Cisco IDS
- C. SNORT
- D. Tripwire

Answer: C

QUESTION NO: 7

Symantec released a new version of Symantec Endpoint Protection client software. An administrator needs to find out what versions of Symantec Endpoint Protection are currently in the network. Which report provides this information?

- A. Application and Device Control Report
- B. System Report
- C. Compliance Report
- D. Computer Status Report

Answer: D

QUESTION NO: 8

ST0-029

Where can you determine what content updates are available on the Symantec Endpoint Protection Manager?

- A. Home page
- B. Monitors page
- C. Clients page
- D. Admin page

Answer: D

QUESTION NO: 9

How does Symantec Endpoint Protection use Unmanaged Detector to find unmanaged devices on the network?

- A. It compares MAC addresses to a list of known hosts.
- B. It receives logon failures notifications from an LDAP server.
- C. It pings clients on port 80 to trigger a response from managed clients.
- D. It attempts to make http connections with clients in an address range.

Answer: A

QUESTION NO: 10

What are three features of Symantec Endpoint Protection 11.0? (Select three.)

- A. Application Performance Management
- B. Client Firewall

ST0-029

- C. Application and Device Control
- D. Endpoint Change Control
- E. Intrusion Prevention

Answer: B, C, E

QUESTION NO: 11

How many client installation packages are required to install Symantec Endpoint Protection 11.0 with all available components?

- A. one
- B. two
- C. three
- D. four

Answer: A

QUESTION NO: 12

What is a benefit of Symantec Endpoint Protection 11.0?

- A. A single client provides all functions, which reduces the resource usage footprint.
- B. Solaris is a supported platform for the client.
- C. The number of required management consoles is reduced from five to three, which simplifies administration compared to previous versions.
- D. Proactive Threat Protection runs in real-time.

ST0-029

Answer: A

QUESTION NO: 13

Which two roles can Symantec Endpoint Protection Manager assign to managed clients? (Select two.)

- A. LAN Enforcer
- B. Group Update Provider
- C. Unmanaged Detector
- D. Database Replicator

Answer: B, C

QUESTION NO: 14

Which two statements describe the interactions between Symantec Endpoint Protection 11.0 and Quarantine Server? (Select two.)

- A. Clients upload log data and quarantined files to Symantec Endpoint Protection Manager, which forwards the files to the Quarantine Server.
- B. Clients upload log data to Symantec Endpoint Protection Manager and upload quarantined files to Quarantine Server.
- C. Clients upload log data and quarantined files to the Quarantine Server, which forwards the log data to the Symantec Endpoint Protection Manager.
- D. Symantec Endpoint Protection Manager sends quarantine policies, which define the location of the Quarantine Server, to managed clients.
- E. The Quarantine Server sends its location and quarantine policies and rules to all clients.

Answer: B, D

ST0-029

QUESTION NO: 15

Which parameter is unique to each Symantec Endpoint Protection client?

- A. CUID
- B. GUID
- C. SUID
- D. RUID

Answer: B

QUESTION NO: 16

Which two are characteristics of Proactive Threat Protection? (Select two.)

- A. detects unknown threats
- B. inspects encrypted network traffic
- C. evaluates process behavior
- D. blocks attacker's IP address

Answer: A, C

QUESTION NO: 17

Which two high-level components make up the Symantec Endpoint Protection solution? (Select two.)

- A. Symantec Endpoint Protection

ST0-029

- B. Symantec Critical System Protection
- C. Symantec Security Information Manager
- D. Symantec Network Access Control

Answer: A, D

QUESTION NO: 18

Which two do you need in order to add a Replication Partner? (Select two.)

- A. local domain user and password
- B. administrator name and password
- C. local domain administrator name and password
- D. replication server name and port

Answer: B, D

QUESTION NO: 19

Which failover option is available in Symantec Endpoint Protection?

- A. One manager can fail over between two databases in a single site.
- B. One client can fail over between two managers in a single site.
- C. One manager can fail over to another Group Update Provider.
- D. One client can fail over between two databases in separate sites.

Answer: B

ST0-029

QUESTION NO: 20

What is the relationship of Symantec Network Access Control to Symantec Endpoint Protection 11.0?

- A. Symantec Network Access Control is completely integrated with Symantec Endpoint Protection 11.0 and cannot be installed alone.
- B. Symantec Network Access Control is a part of Symantec Endpoint Protection 11.0, but is not enabled unless a separate license is purchased.
- C. Symantec Network Access Control is not part of Symantec Endpoint Protection 11.0, but does not interfere with Symantec Endpoint Protection 11.0 components.
- D. Symantec Network Access Control works with Symantec Endpoint Protection 11.0, but uses a different management console and installation process.

Answer: B

QUESTION NO: 21

How do requirements for installing Symantec Network Access Control relate to installing various components of Symantec Endpoint Protection 11.0?

- A. It does NOT install on any host that is used as either the Symantec Endpoint Protection Manager or a Group Update Provider.
- B. It installs in the same client package as all of the Symantec Endpoint Protection 11.0 components.
- C. It does NOT install on any client unless Symantec Endpoint Protection 11.0 is installed.
- D. It installs and is automatically enabled when the Network Threat Protection component of Symantec Endpoint Protection 11.0 is installed on any client.

Answer: B