

500-275^{Q&As}

Securing Cisco Networks with Sourcefire FireAMP Endpoints
(SSFAMP)

Pass Cisco 500-275 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/500-275.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

The FireAMP Mobile endpoint connector currently supports which mobile OS device?

- A. Firefox
- B. HTML5
- C. Android
- D. iPhone

Correct Answer: C

QUESTION 2

If a file's SHA-256 hash is sent to the cloud, but the cloud has never seen the hash before, which disposition is returned?

- A. Clean
- B. Neutral
- C. Malware
- D. Unavailable

Correct Answer: B

QUESTION 3

Which question should be in your predeployment checklist?

- A. How often are backup jobs run?
- B. Are any Linux servers being deployed?
- C. Who are the users of the hosts on which you will deploy?
- D. Which applications are installed on the hosts on which you will deploy?

Correct Answer: D

QUESTION 4

What is the default clean disposition cache setting?

- A. 3600

- B. 604800
- C. 10080
- D. 1 hour

Correct Answer: B

QUESTION 5

Which option describes a requirement for using Remote File Fetch?

- A. It must be done from a private cloud console.
- B. It can be done only over port 32137.
- C. The administrator must have two-step authentication enabled.
- D. The feature is integrated into the product, so no specific requirements must be fulfilled.

Correct Answer: C

QUESTION 6

Which action can you take from the Detections/Quarantine screen?

- A. Create a policy.
- B. Restore the detected file.
- C. Run a report.
- D. Change computer group membership.

Correct Answer: B

QUESTION 7

When you are viewing information about a computer, what is displayed?

- A. the type of antivirus software that is installed
- B. the internal IP address
- C. when the operating system was installed
- D. the console settings

Correct Answer: B

QUESTION 8

Which statement about two-step authentication is true?

- A. It is the ability to use two separate passwords.
- B. It is the ability to enable biometric authentication.
- C. It is the ability to have a passphrase sent to a mobile device.
- D. It is the ability to use a verification code in conjunction with the correct username and password.

Correct Answer: D

QUESTION 9

How many days\ ' worth of data do the widgets on the dashboard page display?

- A. the previous 5 days of data
- B. the previous 6 days of data
- C. the previous 7 days of data
- D. the number of days you set in the dashboard configuration

Correct Answer: C

QUESTION 10

The FireAMP connector supports which proxy type?

- A. SOCKS6
- B. HTTP_proxy
- C. SOCKS5_filename
- D. SOCKS7

Correct Answer: B

QUESTION 11

Which statement is true about the Device Trajectory feature?

- A. It shows where the endpoint devices have moved in your environment by displaying each IP address that a device has had over time.
- B. A "plus" sign on the File Trajectory map indicates that you can execute the file inside FireAMP.

- C. In the File Trajectory map, you can view the parent process for a file by selecting the infected system.
- D. It shows hosts that display Indications of Compromise.

Correct Answer: C

QUESTION 12

When discussing the FireAMP product, which term does the acronym DFC represent?

- A. It means Detected Forensic Cause.
- B. It means Duplicate File Contents.
- C. It means Device Flow Correlation.
- D. It is not an acronym that is associated with the FireAMP product.

Correct Answer: C

QUESTION 13

The FireAMP connector monitors the system for which type of activity?

- A. Vulnerabilities
- B. Enforcement of usage policies
- C. File operations
- D. Authentication activity

Correct Answer: C

QUESTION 14

A default FireAMP Private Cloud installation can accommodate how many connectors over which period of time?

- A. 100 connectors over a 15-day period
- B. 1000 connectors over a 45-day period
- C. 5000 connectors over a 10-day period
- D. 500 connectors over a 30-day period

Correct Answer: D

QUESTION 15

Which pair represents equivalent processes whose names differ, depending on the connector version that you are running?

- A. immunet_protect and iptray
- B. agent.exe and sfc.exe
- C. TETRA and SPERO
- D. ETHOS and SPERO

Correct Answer: B

[Latest 500-275 Dumps](#)

[500-275 VCE Dumps](#)

[500-275 Exam Questions](#)