

# Actual4Labs

Pass Your Next Certification Exam Fast!

Everything you need to prepare, learn & pass your certification exam easily.

Login / Register

Shopping Cart (0)

Search...



### Online Test Engine

Instant Online Access, Test History and Performance Review, Supports Windows / Mac / Android / iOS, etc. →

### Desktop Test Engine

Installable Software Application, Simulates Real Exam Environment, Supports MS Operating System, Practice Offline Anytime. →

### PDF Format

Printable PDF Format, Prepared by IT Experts, Study Anywhere, Anytime, Free PDF Demo Available. →

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarantee in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

<http://www.actual4labs.com>

Excellent Quality Exam Dumps Questions Never Let You down -  
Actual4Labs

**Exam :** MSC-131

**Title :** Design and Deploy AirDefense Solutions

**Vendors :** Motorola Solutions

**Version :** DEMO

NO.1 There was a rogue AP on your network as detected by ADSP. The rogue was displayed in your Alarms.

When you run a wireless security posture details report for the same time range, the rogue does not

appear in the report. What is the most likely cause for the rogue not being in the report?

- A. The report was run for a different scope than the one that detected the rogue.
- B. Your account was not created in the scope level where the rogue was detected.
- C. You are logged into ADSP as a guest account which lacks the permission to run the report.
- D. The rogue device has been removed from the network and the corresponding alarm is now inactive.

Answer: A

NO.2 Broadcasting the SSID and allowing the access point to respond to clients with no SSID makes it easier

for the clients, but some consider it a security loophole. The theory for disallowing these two practices is

that it helps ° h i d ± t h e n e t w o r k

What is the problem with this theory?

- A. Hiding the SSID turns off the beacons thus disabling passive scanning
- B. Not responding to null SSIDs causes the EAP process to break down
- C. These values must be present in order for intrusion detection systems to function
- D. The SSID will still be present in probe request frames and can be seen with a protocol analyzer

Answer: D

NO.3 Spectrum Analysis can be performed using different modes of operation. Which of following modes

would be the most appropriate to use if you need to perform a Spectrum Analysis and capture information

about the data link layer (Layer 2 of OSI model)?

- A. Dual Layer Scan Mode
- B. Continuous Scan Mode
- C. Background Scan Mode
- D. Interference Scan Mode

Answer: C

NO.4 Your company processes and stores credit card information in a corporate database.

You must be able

to determine the status of the company's compliance to the Payment Card Industry (PCI) standard with

regard to wireless device use. How can this be accomplished using ADSP?

- A. By running a PCI compliance report at each of the retail store levels of your ADSP tree.
- B. By running a PCI compliance report at the accounting department level of your ADSP tree,
- C. By running a PCI compliance report at the system level of your ADSP tree.
- D. By running a PCI compliance report at network operations center level of your ADSP tree.

Answer: C

NO.5 A new coffee shop opens in your building offering hot-spot internet access. Several of your users are

connecting to the hot-spot while at their desks to bypass your firewall rules. What is the best thing that can

be done using the ADSP system to prevent this?

- A. Integrate with the firewall using SNMP and import the same firewall rules.
- B. Create a termination policy to prevent accidental associations of authorized AP's.
- C. Create a termination policy to prevent authorized stations from using ad-hoc networks.
- D. Create a termination policy to prevent accidental associations of your work stations to unauthorized networks.

Answer: D

NO.6 Which of the following appropriately characterizes a rogue access point (AP)?

- A. An AP that is causing Co-Channel interference with your APs.
- B. An AP that is not the same brand as your customers APs.
- C. An AP that is on your wired network without proper authorization.
- D. An AP that is not using the security required by corporate policy.

Answer: C

NO.7 What is the purpose of the Bonding command in the ADSP CLI.?

- A. The Bonding command is used to link sensors to the correct container in the ADSP tree.
- B. The Bonding command is used to enable the Primary and Secondary ADSP appliances to synchronize.
- C. The Bonding command is used to enable both of the NIC's on ADSP's system board to act as one for high availability.
- D. The Bonding command is used to ensure that both the Primary and Secondary ADSP

appliances are configured to use the same IP address.

Answer: C

NO.8 You used the Report Builder to create a custom template to support your PCI compliance initiative.

Two weeks later you decide to use the report but you're not quite sure where to locate it. How would you access this template?

- A. By selecting it in the Custom Reports found in the reporting feature
- B. By using the search feature in the Web reporting interface
- C. By selecting it under the Inactive category on the Reports page
- D. By using the Templates drop down box in the Report Builder application

Answer: A

NO.9 How can the Wireless Intrusion Protection System (WIPS) feature of the Motorola Solutions

AirDefense Services Platform (ADSP) be used to protect your Wi-Fi network?

- A. The WIPS system can remove rogue access points from neighboring networks
- B. The WIPS system can utilize RF Jamming to keep your channels clear.
- C. The WIPS system can identify wired leakage and other network vulnerabilities
- D. The WIPS system can stop neighboring devices from using your channels

Answer: C

NO.10 You are the administrator of a very large ADSP installation protecting an international WLAN

deployment. Running a compliance report each day for your boss takes a great deal of your time in the mornings. What can you do using ADSP to reduce the amount of your time it takes to render this information and deliver it to your boss?

- A. Create a Guest account for your boss. Teach them to run their own each day, leaving you free for other tasks.
- B. Create an Admin account for your boss. Teach them to run their own each day, leaving you free for other tasks.
- C. Add the desired report to the Data Collection Polling interval with a daily schedule to be

emailed to your boss.

D. Add the report to your favorites list. Then schedule it to run at an off peak time and to automatically be emailed to your boss each day.

Answer: D

NO.11 A requirement for seamless roaming in a Robust Security network is that the access points receive the Pairwise Master Key (PMK) identifier from the station in the reassociation frame. What other information must be included in that frame?

- A. Any 802.1g VLAN tags.
- B. The IP address and subnet mask.
- C. The randomly generated shared secret.
- D. The MAC address of the old access point.

Answer: D

NO.12 Which of the following best defines a "security risk"?

- A. The likelihood of being targeted by a given attack, of an attack being successful, and general exposure to a given threat.
- B. The source and means of a particular type of attack.
- C. The security flaws in a system that allow an attack to be successful.
- D. Reduced Instruction Set Kernel.

Answer: A

NO.13 You have configured your ADSP appliance to use a RADIUS server to validate user credentials upon GUI logon. However, users continue to be validated directly by ADSP. What additional step must be taken to ensure GUI users are authenticated via the RADIUS server you configured when they are logging into ADSP?

- A. The ADSP appliance must be rebooted to ensure the settings are recorded properly
- B. Each user account must be configured to use the correct RADIUS server for authentication
- C. You must log into the CLI using the SMXMGR account and run the Enforce Credentials

command

D. Log into the GUI with your admin account and click on the Synchronize RADIUS Accounts button in

Appliance Manager

Answer: B

NO.14 What security exists for the communication between sensors and the ADSP appliance?

A. EAP-TTLS and SSL

B. PEAP and SSL

C. PKI and SSL

D. EAP-TLS and SSL

Answer: C

NO.15 When would the configuration of ADSP include the use of a RADIUS server?

A. When LDAP is not available

B. When sensor validation is required

C. When sensors require a VPN connection

D. When centralized authentication is required

Answer: D