Vendor: Motorola Solutions

Exam Code: MSC-131

Exam Name: Design and Deploy AirDefense Solutions

Version: Demo

QUESTION: 1
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

QUESTION: 2
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

QUESTION: 3
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

QUESTION: 4
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

QUESTION: 5
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 "hide" the network. 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

QUESTION: 6
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

QUESTION: 7
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

QUESTION: 8
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

QUESTION: 9
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

QUESTION: 10
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

QUESTION: 11
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

QUESTION: 12
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

QUESTION: 13
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

QUESTION: 14
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.

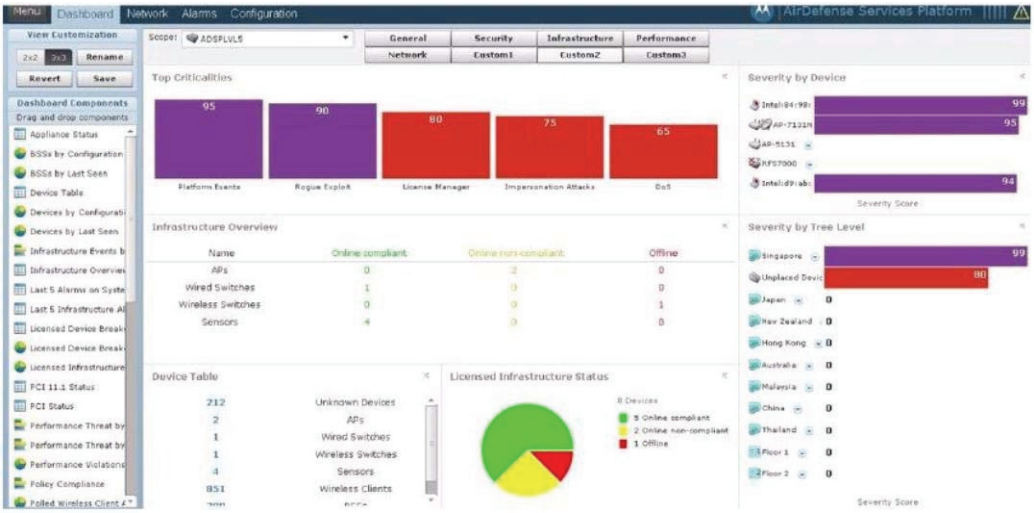
Answer: D

QUESTION: 15
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

QUESTION: 16
The dashboard shows that 2 APs are non-compliant and 1 Wired switch and 4 sensors are compliant. Based solely on the information contained in the exhibit below, can you confirm that there is a wireless security risk?



A. Yes, the security implemented on the WLAN will not protect the wireless environment.
B. No, because security risks are only tracked at the wireless switch level which is compliant.
C. Yes, there is a wireless security risk, because the APs are non-compliant which is a securitybreach of the security policy.
D. No, the reason the APs are not compliant can be either that they have not been audited or the configurations have not been retrieved in the ADSP

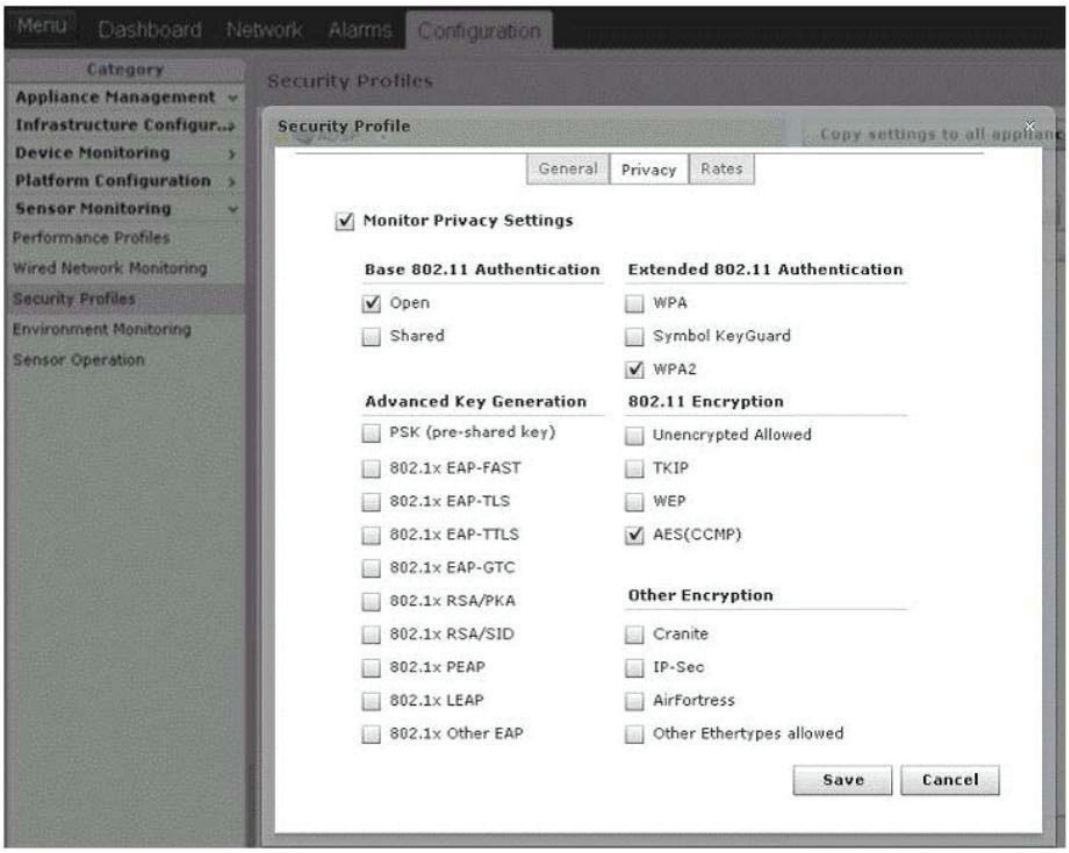
Answer: D

QUESTION: 17
During a wireless security assessment it has been indicated that the wireless WiFi signals can be seen outside the perimeter. The customer does not want this to happen or at least reduce the propagation of the signals outside the perimeter. All of the following are actions that can be used to address this, EXCEPT:

A. Replace the Omni directional antennas with directional antennas.
B. Use metal paint around the building, use wired mesh and tinted windows.
C. Put the APs more inside the office areas and not close to the walls.
D. Use 2.4 Ghz and 5 Ghz RF Jammers around the perimeter.

Answer: D

QUESTION: 18
Please see the image below which represents the configuration of Security Profiles in the AirDefense Services Platform (ADSP). The wireless network infrastructure supports both VVPA- PSK and WPAv2-Enterprise, segmented via a VLAN. When an employee logs into the wireless network using VVPA-PSK, will ADSP generate an alarm?



A. Yes, because the end-user does comply with the security policy as both WPA and WPAv2 are allowed on the wireless network infrastructure.
B. No, because both VVPA and WPAv2 are allowed on the wireless network infrastructure.
C. Yes, because the end-user does not comply to the security policy.
D. No, because the VLAN segmentation will not allow this.

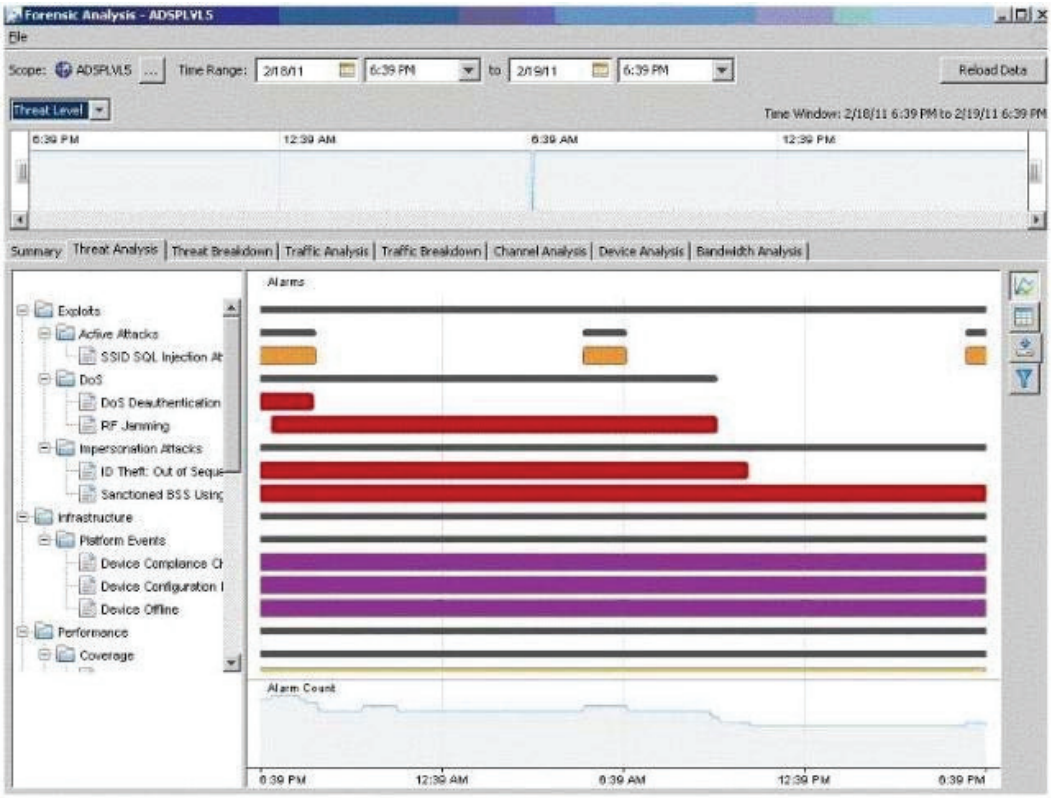
Answer: C

QUESTION: 19
A police department has implemented a WiR network and needs a solution to investigate if someone accessed the WiR network during the last 3 months. They want to see this information in a single view in the AirDefense Services Platform (ADSP). What is the best way to quickly gather this information?

A. Basic Forensics
B. Advanced Forensics
C. Advanced Troubleshooting
D. Advanced Log management

Answer: B

QUESTION: 20
The Advanced Forensics module shows the wireless threats in the threat analysis view. Please see the Advanced Forensics exhibit at the bottom. What is the next step a security operator should do in this particular case?



A. In this particular case, the operator needs to escalate to higher management as there is a serious wireless threat.

B. Go to alarm manager to see in more depth to which particular AP or client the wireless threat alarm relate to. After that he needs to change the scope in the Basic Forensics view and zoom into the appliance view to better understand the wireless threat.
C. The operator needs to inform the end users about the threat
D. Go to the alarm manager to see in more depth to which particular AP or client the wireless threat alarms relate to. After that he needs to change the scope in the Advanced Forensics module to zoom into the particular AP or Client view to better understand the wireless threat.

Answer: D

QUESTION: 21
During the wireless security assessment the consultant noticed that clients authenticate and associate to the customer's network with the 4-way handshake and he also sees AES/CCMP frames over the network. What is his conclusion?

A. The wireless security risk to access the network is medium, because of the AES/CCMP frames
B. The wireless security risk to access the network is medium, because of the 4-way handshake.
C. The wireless security risk to access the network is high, because a Robust Secure Network (RSN) is used.
D. The wireless security risk to access the network is bw, because a Robust Secure Network (RSN) is used.

Answer: D

QUESTION: 22
The following extract of the "AirDefense Sample Policy" has been given to the wireless security assessor. Threat Prevention A Wireless LAN Intrusion Detection System should be deployed to perform dedicated monitoring of the airwaves. The architecture should be able to provide an enterprise view of the WLAN being monitored at a glance with the ability to analyze any specific area/section of the WLAN. The wireless Intrusion Detection System should be able to detect and alert on wireless intrusion activities, including but not limited to:
- Rogue Access Points and any rogue S02.ll devices
- Accidental, Ad-hoc and Malicious Associations
- Probing Stations
- Ad-hoc networks and other device misconfigurations
- Unauthorized Network Access
- MAC spoofing
- Denial of Service (DoS) Attacks, Identity Theft

- Malicious Data Insertion
- 802.11 Protocol misuse

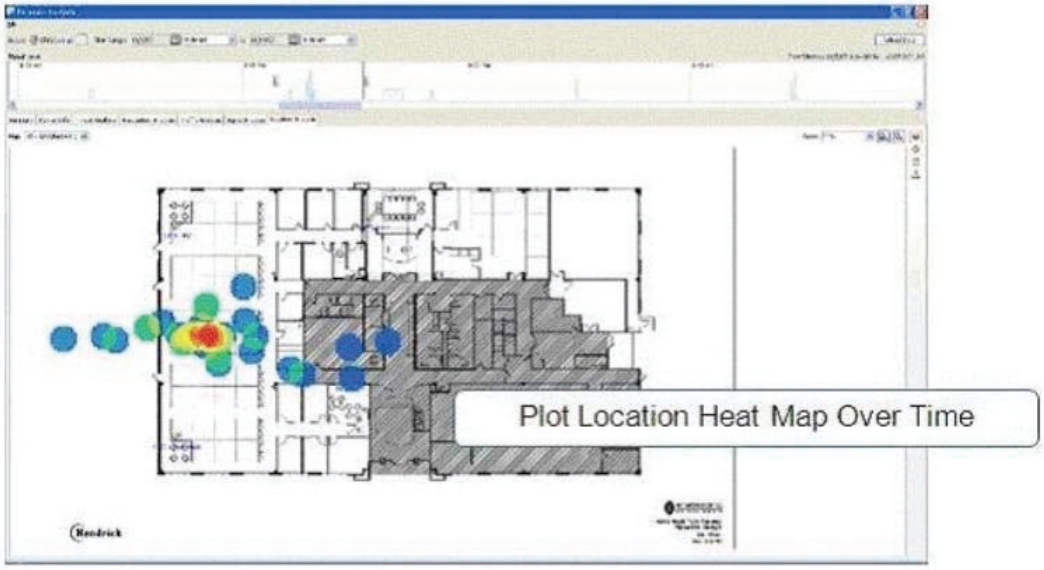
The customer has the ADSP with the VVIPS module installed. During the wireless security assessment the consultant does a MAC-spoofing attack test, but it was not detected by the ADSP. What is the possible root cause?

A. There are two identical MAC addresses and it should not generate an alarm according the policy.
B. MAC Spoofing will not be detected in a wireless network, therefore the ADSP does not generate an alarm.
C. It is a software bug in the ADSP platform and it need to be reported to Motorola's customer support center.
D. The ADSP and sensors might not have had enough time to capture enough wireless frames and to do the correlation and analysis to generate an alarm.

Answer: D

QUESTION: 23

To do forensic locationing in the AirDefense Services Platform (ADSP), what components are required over time?



A. At least 3x Sensors (or APs) and an Advanced Forensics license
B. At least 3x Sensors (or APs) and Basic Forensic functionality
C. At least 3x Sensors (or APs) and the 3rd party location engine (e.g. Ekahau, Aeroscout or other vendor)
D. At least 3x Sensors and Basic Forensic functionality

Answer: A

QUESTION: 24
You have just performed a Wireless Security Assessment and have documented the Wireless Security Risks at the customer site. Following this, what would be the next task?

A. Review your documentation of wireless security risks with the CEO.
B. Review your documentation of wireless security risks with the Security Manager.
C. Start to implement the wireless security solutions immediately in case there is a wireless security exposure (e.g. no encryption is used on the Access Points).
D. Start to implement the wired security solution (so that the wireless infrastructure is separated from the wired infrastructure) until the security department has approved the wireless security improvements stated in the report.

Answer: B

QUESTION: 25
AirDefense Services Platform (ADSP) has built-in Compliance Reports. Please see the Compliance Report exhibit at the bottom. Which of the following statements are TRUE (select TWO)?

A. Compliance Reports can be scheduled automatically
B. Compliance Reports cannot be scheduled automatically
C. Compliance Reports include all related clauses (the complete standard)
D. Compliance Reports only include the wireless related clauses of the standard (not the complete standard)

Answer: A, D

QUESTION: 26
Which of the following user type templates would be used to create user accounts that allow read/write permissions for Connection Troubleshooting only?

A. Guest
B. Admin
C. Operator
D. Helpdesk

Answer: D

QUESTION: 27
You need to determine the compliance status of your organizations Wi-Fi deployment within a given industry standard compliance for the first week of last month, when some testing occurred. How can you do this using the Reports Tool in ADSP without gathering too much information?

A. Set the date range of the report to the desired time frame and run the report.
B. Run the desired report and apply the time range filter prior to viewing.
C. Set the scope of the report to the appliance level and run the desired report.
D. Use Report Builder to create a custom report covering only that time range.

Answer: A

QUESTION: 28
Some of your ADSP services are not functioning properly. What can you do to determine which services are not working properly?

A. Log into the GUI and click the STATUS button in Configuration Manager.
B. Log into the CLI and run the SERVICE command.
C. Log into the CU and run the STATUS command.
D. Log into the GUI and click on the STATUS button in Appliance Manager.

Answer: C

QUESTION: 29
Your business policy requires that if any password becomes compromised it must be changed on all devices using that password. A long term employee that knows your current administrator password for all of your hundreds of AP's and WAN controllers has retired. Now that someone outside your organization knows your password, the Chief Security Officer (CSO) has tasked you with changing the password across the entire deployment as quickly as possible. How can you best use ADSP to accomplish this task?

A. Enable the password modification wizard at the appliance level of the tree and make the required changes.
B. Connect to each device using the direct connect from the drop down and make the required changes.
C. Create and deploy a custom configuration templates for all devices making the required changes.

D. Enable the configuration of Device Access and configure the correct credentials.

Answer: D

QUESTION: 30
There is a compliance report that contains almost all of the information you require built into ADSP. You want to receive all of the information required in a single report. What should you do to achieve this goal?

A. Use Report Builder to construct a new report covering the desired information.
B. Install the latest Service Module for ADSP, which may contain the report you desire.
C. Use Report Builder to create a Custom report by editing the compliance report contained in ADSP.
D. Export all of the relevant alarms into a spread sheet, combining it with the existing reports information.

Answer: C

QUESTION: 31
Which of the following Monitoring thresholds allows a WLAN administrator to be warned about a high incidence of 802.11 traffic collisions?

A. CRC Errors
B. Excessive BSSs
C. Excessive Clients
D. Average Signal Strength

Answer: A

QUESTION: 32
A new service module has been released for ADSP, adding additional features you desire on your appliance. How do you install the service module once you have downloaded it from the support website?

A. Log into the GUI and use SYSTEM UPDATE.
B. Log into the CU and use the UPDATE command.
C. Log into the GUI and use APPLIANCE MANAGER.
D. Log into the CU and use the SERVMOD command.

Answer: D

QUESTION: 33
Which of the following is a drawback to using AirDefense Model 400, 510, or 520 dedicated sensors for an ADSP deployment?

A. No 802.3af support.
B. No 802.11n support
C. No plenum rated models.
D. No external antenna options.

Answer: B

QUESTION: 34
You have created a new Auto Discovery schedule to find manageable devices on your network. You have also created an Auto Placement policy to place devices in the correct location within the tree as they are discovered. Another administrator has deployed new devices on the same network. These devices are not being seen in ADSP, What is the most likely cause of this scenario?

A. The Auto Placement rule has been disabled by the other administrator.
B. The Auto Discovery interval has not been reached,
C. The communication settings need to be refreshed.
D. ADSP has not been rebooted since the last running of Auto Discovery.

Answer: B

QUESTION: 35
You need your ADSP appliance to locate devices by using their fully qualified domain names. Your ADSP appliance must be configured to use the correct DNS servers. How should you make these configurations?

A. Log into the GUI and use the DNS button on the Configuration Tab of APPLIANCE MANAGER.
B. Log into the GUI and use the DNS button on the System Tab of APPLIANCE MANAGER.
C. Log into the CU and use the IP command to configure all L3 connections.

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

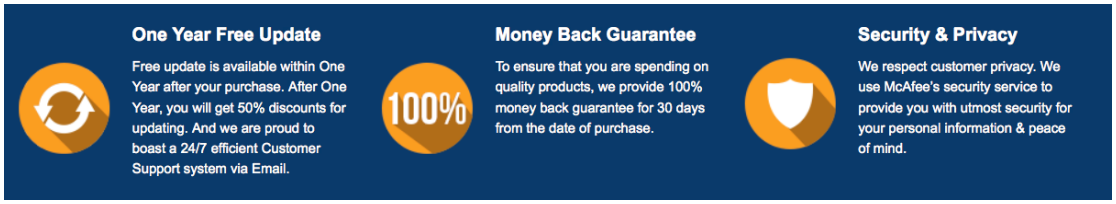
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions