



ACMP_6.3^{Q&As}

Aruba Certified Mobility Professional 6.3

Pass Aruba ACMP_6.3 Exam with 100% Guarantee

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

<https://www.passapply.com/acmp-6-3.html>

100% Passing Guarantee
100% Money Back Assurance

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

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





QUESTION 1

What settings need to be changed on a factory default AP in order for it to use ADP to discover the Aruba Controller?

- A. DNS of the controller
- B. Static route
- C. AP group
- D. enable multicast
- E. no changes needed

Correct Answer: E

QUESTION 2

Which of the following could be used to set a user's post-authentication role or VLAN association? (Choose two)

- A. AAA default role for authentication method
- B. Server Derivation Rule
- C. Vendor Specific Attributes
- D. AP Derivation Rule
- E. The Global AAA profile

Correct Answer: BC

QUESTION 3

With CPSec enabled, which tunnel protocol is used between APs and Controllers in an Aruba environment?

- A. EAP
- B. SSH
- C. IPinIP
- D. Mobile IP
- E. IPSec

Correct Answer: E

QUESTION 4



As illustrated in the above diagram and screen capture, a wireless hacker injects messages into your network to detach a client from your Aruba AP.

I look Like a Real AP

IDS DOS profile > default

Detect Disconnect Station Attack	<input type="checkbox"/>	Disconnect STA Assoc Response Threshold	5
Disconnect STA Deauth and Disassoc Threshold	8	Disconnect STA Detection Quiet Time	900 sec
Spoofed Deauth Blacklist	<input type="checkbox"/>	Detect AP Flood Attack	<input type="checkbox"/>
AP Flood Threshold	50	AP Flood Increase Time	3 sec
AP Flood Detection Quiet Time	900 sec	Detect Client Flood Attack	<input type="checkbox"/>
Client Flood Threshold	150	Client Flood Increase Time	3 sec
Client Flood Detection Quiet Time	900 sec	Detect EAP Rate Anomaly	<input type="checkbox"/>
EAP Rate Threshold	60	EAP Rate Time Interval	3 sec

What action should you take to identify and prevent the Intruder from connecting to your system? (Choose two)

- A. Enable Detect disconnect Station Attack
- B. Enable Spoofed Deauth Blacklist
- C. Take no action as there is no protection against this form of attack
- D. Take no action as the Aruba system ignores this attack because it is against the client
- E. Enable Detect EAP rate Anomaly

Correct Answer: AB

QUESTION 5

Which settings cannot be modified directly from a local controller?

- A. Port VLAN setting
- B. Switch Time Zone
- C. Port trusted



D. Roles

E. SNMP Enable Trap Generation

Correct Answer: D

[Latest ACMP_6.3 Dumps](#)

[ACMP_6.3 Study Guide](#)

[ACMP_6.3 Exam Questions](#)