FCPSecure Wireless LAN 7.4 Administrator

Fortinet FCP_FWF_AD-7.4

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, FortiAP deployment and configuration	10
Topic 2, SSIDs	5
Topic 3, Authentication	3
Topic 4, Wireless security	3
Topic 5, Monitoring and troubleshooting	1
Topic 6, Mix Questions	1
Total	23

QUESTION NO: 1

An administrator has created an SSID that must be advertised on the 5 GHz band by a supported FortiAP model. The FortiAP is authorized and online, but clients cannot find the SSID on 5 GHz.

Which two configuration changes are required? (Choose two.)

A. Enable the 5 GHz radio in the FortiAP profile

B. Assign the SSID to the 5 GHz radio in the FortiAP profile

C. Remove the FortiAP authorization from the controller

D. Configure a static channel on the 2.4 GHz radio

ANSWER: A B

Explanation:

The 5 GHz radio must be enabled in the applicable FortiAP profile, and the SSID must be assigned to that radio. Both conditions are required before the FortiAP can advertise the SSID on the 5 GHz band.

Changing the FortiAP authorization state does not map an SSID to a radio. A static channel can be used when required, but it is not necessary for SSID advertisement when the radio is enabled and configured for automatic channel selection.

QUESTION NO: 2

A guest SSID must permit users to access the internet after captive portal authentication. Guest devices must not be able to communicate directly with other guest devices connected to the same SSID.

Which SSID setting should the administrator enable?

A. Intra-SSID privacy

B. MAC address filtering

C. Captive portal authentication

D. Dynamic VLAN assignment

ANSWER: A

Explanation:

The administrator should enable intra-SSID privacy. This setting prevents direct communication between wireless clients associated with the same SSID while allowing their traffic to be processed through the configured firewall policies for permitted destinations such as the internet.

MAC filtering controls which devices can connect, not communication between connected devices. A captive portal controls authentication, but it does not by itself isolate authenticated clients from each other.