

Exam : [**HP HP0-Y25**](#)

Title : **Building HP ProCurve
Enterprise Mobility
Solutions**

Version : **Demo**

1. A company is using 802.1X authentication with dynamic VLANs on its wired network. The company has three user groups that are assigned to VLANs 10, 20, and 30. You are deploying an Enterprise Mobility Solution with an MSM760 Access Controller and 50 APs. On the MSM Controller, you have configured a VSC that enforces 802.1X authentication.

How do you continue to create a consistent experience for users on wired and wireless connections?

- A. Bind the VSC to the APs' group with VLANs 10, 20, and 30 as egress VLANs.
- B. Enable the dynamic VLANs option in the VSC, and bind the VSC to the APs' group.
- C. Configure VLANs 10, 20, and 30 on the MSM APs' bridge ports, and tag the MSM APs' switch ports for each VLAN.
- D. Bind the VSC to the APs' group, and tag the MSM APs' switch ports for VLANs 10, 20, and 30.

Answer: D

2. You are implementing a public access solution on the MSM Controller because your company wants to grant visitors access to the Internet. The company has only two VLANs: VLAN 1 for users and VLAN 2 for servers. VLAN 2 also includes the Internet connection. You connect the MSM APs and the MSM Controller's LAN port to VLAN 1 and the controller's Internet port to VLAN 2. You must protect the company's workstations on VLAN 1 from unauthorized access by unauthenticated guests.

What must you do on the MSM Controller?

- A. Create an unauthenticated user ACL that prohibits access to all of the VLANs except the controller.
- B. On the VSC for guests, enable the option that terminates WPA at the controller.
- C. On the VSC for guests, enable the wireless security filter that limits wireless traffic to the controller.
- D. Add an entry to the default site ACL that prohibits access to all of the VLANs except the controller.

Answer: C

3. What is a potential risk of enabling the RSSI-based classification feature in an Authorized WLAN policy?

- A. RF Manager might classify your own APs as Rogue APs because their transmit power is too high and take action against them.
- B. RF Manager must rely exclusively on RSSI to detect harmful devices?locations, instead of drawing on network detectors' findings. This might make the prediction less accurate.
- C. RF Manager might classify legitimate APs owned by nearby companies as Rogue APs and take action

against them.

D. Sensors might decide that they should not take action against a potentially harmful device because its RSSI is low and the device might still be a risk.

Answer: C

4. Which devices provide the data integrity and privacy that create a trusted network infrastructure in an Enterprise Mobility Solution?

A. RF Manager and sensors

B. RF Planner and sensors

C. MSM Controllers and APs

D. MSM Controllers and Identity Driven Manager (IDM)

Answer: C

5. You must implement access control for your wireless users on a solution-wide level. You have decided on the access control strategy recommended for guests and have already begun to customize public access settings. Which option must you select in the VSC for these users?

A. Use Service Controller for: Access control (centralized access control)

B. Client data tunnel

C. 802.1X authentication

D. Wireless protection set to WPA

Answer: A