

2023 Updated Verified HPE6-A70 Q&As - Pass Guarantee or Full Refund [Q11-Q35]



2023 Updated Verified HPE6-A70 Q&As - Pass Guarantee or Full Refund [Q11-Q35]

2023 Updated Verified HPE6-A70 Q&As - Pass Guarantee or Full Refund
[Mar-2023] HPE6-A70 Certification with Actual Questions from ValidExam

NEW QUESTION 11

A network administrator configures an Aruba Mobility Master (MM)-based solution to provide wireless access to employees. The solution must meet these criteria:

- * Authenticate users to a network RADIUS server
- * Enforce different Aruba firewall rules based on the user department

How can the administrator meet these criteria in the simplest way?

- * Have the RADIUS server assign users in different departments to different VLANs. Apply firewall policies based on IP ranges.
- * Have the RADIUS server send different roles for users in different departments. Apply role-based firewall policies.
- * Create multiple zones on the MM. Assign different departments and sets of firewall policies to different zones.
- * Create a different WLAN and SSID for each department. Apply different firewall policies to each WLAN.

NEW QUESTION 12

A network administrator configures this policy:

```
ip access-list session Guest
  user any svc-dhcp permit
  user any network 10.0.0.0 255.0.0.0 deny
  user any any permit
```

Users to which this policy apply are unable to receive IP addresses with DHCP. How should the administrator fix the issue?

- * Move the user any svc-dhcp permit rule to the bottom of the list.
- * Remove the deny rule from the policy.
- * Use the correct service alias in the user any svc-dhcp permit rule.
- * Change user to any in the user any svc-dhcp permit rule.

NEW QUESTION 13

A network administrator configures this policy:

```
ip access-list session Guest
  user any svc-dhcp permit
  user any network 10.0.0.0 255.0.0.0 deny
  user any any permit
```

Users to which this policy applies are unable to receive IP addresses with DHCP. How should the administrator fix the issue?

- * Change user to any in the user any svc-dhcp permit rule.
- * Move the user any svc-dhcp permit rule to the bottom of the list.
- * Remove the deny rule from the policy.
- * Use the correct service alias in the user any svc-dhcp permit rule.

NEW QUESTION 14

A WLAN in an Aruba Mobility Master (MM)-based solution uses WPA2-Enterprise security. This WLAN currently authenticates users to Active Directory (AD), and users log in with their Windows domain credentials.

Network administrators now want to authenticate the Windows clients as well, based on the client Computer Names.

What should the administrator do on MM to achieve this goal?

- * Set up MAC Authentication on the WLAN.
- * Set up Machine Authentication on the WLAN.
- * Import the computer names from AD to the MM internal database.
- * Bind individual Mobility Controllers (MCs) to AD at the device level.

Explanation/Reference:

NEW QUESTION 15

A network administrator uses a wireless intrusion detection system (WIDS) to detect 802.11 association floods. At which layer do these attacks occur?

- * Layer 1
- * Layer 2
- * Layer 3
- * Layer 7

NEW QUESTION 16

Refer to the exhibit.

The screenshot shows the configuration page for the 'Exam_Employee' profile, specifically the 'Access' tab. On the left, there is a list of captive portal options: 'Clearpass or other external captive portal' (highlighted in orange), 'Internal captive portal with authentication', 'Internal captive portal with email registration', 'Internal captive portal, no auth or registration', and 'No Captive Portal'. A line connects the 'Clearpass or other external captive portal' option to the 'Captive Portal Options' configuration area on the right. This area includes an 'Auth servers' field with a plus sign, a 'CPPM host' field with the value '10.10.10.10', a 'CPPM page' field with the value '/guest/exam.html', and a 'Redirect URL' field.

A network administrator creates a guest WLAN on an Aruba Mobility Master (MM). The exhibit shows some of the settings for the WLAN.

How should the network administrator handle the Auth server settings?

- * Add an authentication server with the LDAP type and the IP address of the company AD server.
- * Add an authentication server with the LDAP type and IP address 10.10.10.10.
- * Add an authentication server with the RADIUS type and IP address 10.10.10.10.
- * Add an authentication server with the RADIUS type and the IP address of the company AD server.

NEW QUESTION 17

A company wants to provide wireless access for visitors with their Aruba solution. Which configuration feature enables the guest to access the wireless network without authentication?

- * use of internal captive portal with email registration
- * addition of custom rules to control access for unauthenticated guests
- * use of internal captive portal with authentication

- * redirection of guests to an external captive portal that provides encryption services

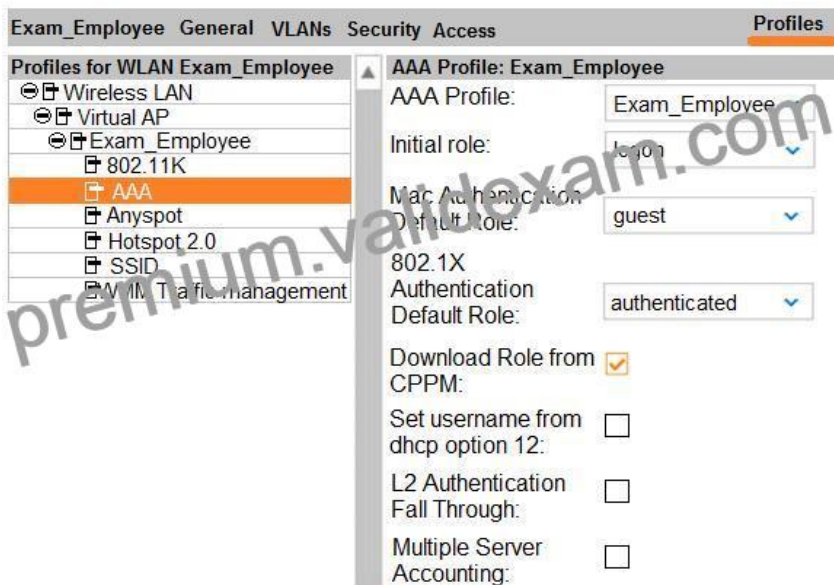
NEW QUESTION 18

What is a role fulfilled by an Aruba Mobility Master (MM)?

- * It forwards and routes traffic for wireless users across multiple sites.
- * It terminates control tunnels for Aruba APs.
- * It provides an advanced Web portal for onboarding Bring Your Own Device (BYOD) devices.
- * It manages VLAN and routing configuration for multiple Mobility Controllers (MCs).

NEW QUESTION 19

Refer to the exhibit.



The exhibit shows the AAA profile for a WLAN on an Aruba solution. This WLAN uses 802.1X to authenticate users to a RADIUS server. A user successfully authenticates with 802.1X, but the RADIUS server does not send a role assignment.

How does the Aruba firewall handle the role assignment for this user?

- * It does not assign a role.
- * It applies the Aruba VSA role employee.
- * It assigns the logon role.
- * It assigns the authenticated role.

NEW QUESTION 20

A network administrator adds several new APs to an Aruba solution that uses AirMatch. The administrator does not want to change the channel for the existing APs, but wants the new APs to receive a provisional plan for their channels and power.

What should the administrator do to meet this goal?

- * Run an on-demand quick AirMatch optimization.
- * Run an on-demand incremental AirMatch optimization.

- * Temporarily enable ARM on the existing and new APs, while AirMatch scheduling remains enabled.
- * Temporarily disable AirMatch scheduling, and then enable ARM on the existing and new APs.

NEW QUESTION 21

Refer to the exhibits.

Exhibit 1

Exam_Guest General **VLANs** Security Access

VLAN:

[Hide](#) [VLAN details](#)

Named VLANs

Name	ID(S)
employee	51
guest	99
--	1,55

+

VLAN IDs

ID	IPV4 ADDRE...	IPV6 ADDRE...	ENABLE NAT	PORT MEM...	ADMIN STATE	OPERATION...	DHCP SETTI..
99	--	--	Enabled	--	Enabled	N/A	None

Exhibit 2

Exam_Guest General **VLANs** Security Access

Clearpass or other external captive portal

Internal captive portal with authentication

Exhibit 3

Exam_Guest General **VLANs** Security Access

Default role:

A network administrator creates a guest WLAN on an Aruba Mobility Manager (MM). The exhibits show some of the settings for the WLAN. The administrator does not change the policies for those roles.

How does the firewall control guest clients when they first connect to the WLAN?

- * It permits them to send any DHCP traffic and DNS and web traffic to the Internet. It redirects web traffic destined to the private network to a login portal.
- * It permits them to send any DHCP and DNS and it redirects all web traffic to a login portal.
- * It permits them to send any DHCP and RADIUS traffic. It redirects all web traffic destined to the Internet to a login portal and drops web traffic destined to the private network.
- * It does not permit them to send any traffic until they are authenticated.

NEW QUESTION 22

Which authentication server option would the network administrator choose to authenticate a wireless user directly against an Active Directory (AD) domain controller without NPS or IAS?

- * LDAP server
- * RFC 3576 server
- * TACACS server
- * RADIUS server

NEW QUESTION 23

Refer to the exhibits.

Exhibit 1

AAA Profile: Exam_Employees

AAA Profile:

Initial role:

MAC Authentication Default Role:

802.1X Authentication Default Role:

Download Role from CPM:

Set user name from dhcp option 12:

L2 Authentication Fail Through:

Multiple Server Accounting:

User Idle timeout: seconds

Max IPv4 for Wireless user:

RADIUS Interim Accounting:

Exhibit 2

Clients(1)							Default C
Client	Health(%)	IP Address	Bond	Radio PHY	Client PHY	Device	Role
employee	48	10.1.51.150	2.4 GHz	HT 2D MHz	HT 2D MHz	Unknown	guest

An Aruba solution supports a WLAN that uses WPA2-Enterprise security. Exhibit 1 shows the AAA policy for the WLAN. Users are supposed to be assigned to different roles after authentication. Network administrators test a connection with the employee user account. Exhibit 2 shows the status for the client after this test.

What is a possible reason for the issue shown in Exhibit 2?

- * The shared key configured for the ClearPass server is incorrect.

- * The RADIUS server is not correctly set up to send a user role for the employee account.
- * MAC authentication is enabled on the WLAN, and the test device does not have an authorized address.
- * The administrators entered the wrong password for the employee account.

NEW QUESTION 24

A network administrator wants to assign an authentication server group to the WPA2-Enterprise WLAN.

Which profile should the administrator modify?

- * Virtual AP
- * SSID
- * AAA
- * L2 Authentication

NEW QUESTION 25

What is one setting that a network administrator can configure for user roles in an Aruba solution?

- * DHCP pool
- * ClientMatch rules
- * source NAT
- * Maximum session

NEW QUESTION 26

Refer to the exhibits.

Exhibit 1

Roles>users1

GLOBAL RULES

RULES FOR THIS ROLE ONLY

- permit all from source any to alias network1
- deny all from source any to network 172.16.0.0/255.255.0.0
- permit all from source user to any destinations

Exhibit 2

Roles Policies Applications

Roles>users2

[Show Advanced View](#)

GLOBAL RULES

RULES FOR THIS ROLE ONLY

- ◇ permit all from source user to network 10.1.1.0/255.255.255.0
- ◇ deny all from source user to network 10.1.2.0/255.255.255.0
- ◇ permit all from source user to network 10.1.0.0/255.255.0.0

A company has an Aruba solution. Client 1 is assigned to the users1 role, and client 2 is assigned to the users2 role. The exhibits show current firewall rules for those roles. The network1 alias used to be 10.1.1.0/24, but the network administrator now changes the network1 alias to 172.16.1.0/24. Client 1 and Client 2 both send a packet destined to 172.16.1.10.

How does the firewall handle these packets?

- * It permits the packet from Client 1 and denies the packet from Client 2.
- * It permits both packets.
- * It denies the packet from Client 1 and permits the packet from Client 2.
- * It denies both packets.

NEW QUESTION 27

A company plans to deploy a Mobility Master (MM). The MM will manage 50 Mobility Controller (MC) appliances that will control a total of 700 APs, and 10 Virtual Mobility Controllers (VMCs) that will control a total of 200 APs.

How many MM licenses does the company require?

- * 60
- * 210
- * 900
- * 960

Explanation

Starting with ArubaOS 8.0.1, the MM license is required to terminate devices (controllers or APs) on Mobility Master. If the Mobility Master does not have sufficient MM licenses and an AP fails to obtain a license, that AP can get an IP address and connect to its controller, but will not broadcast an SSID.

NEW QUESTION 28

Exhibit 1

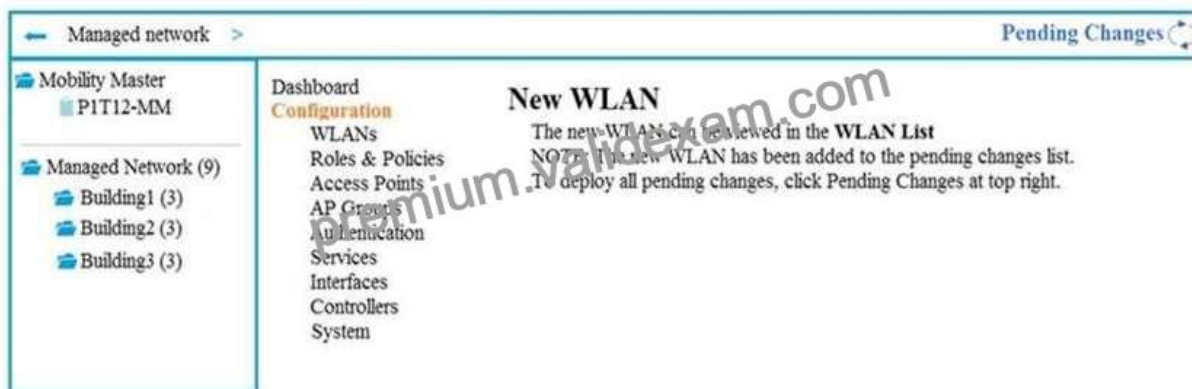
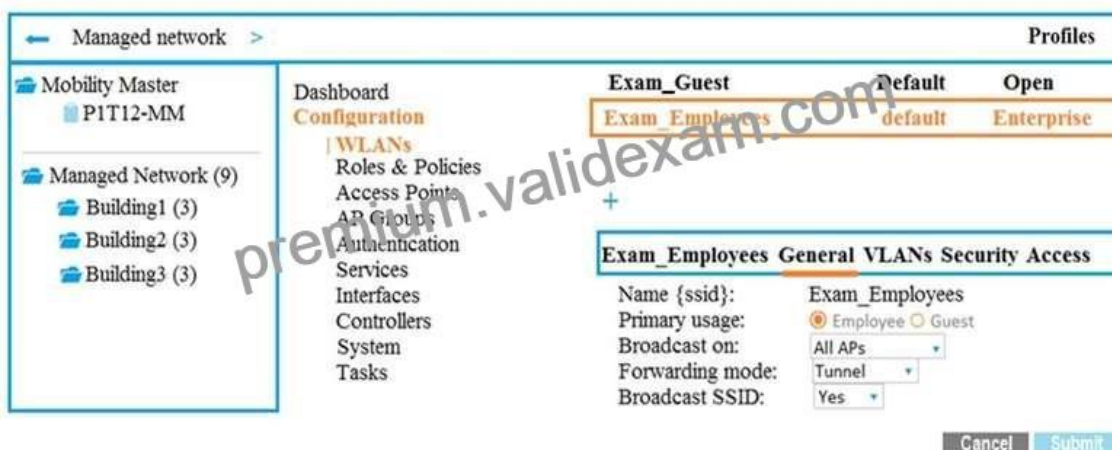


Exhibit 2



A company has an Aruba Mobility Master (MM)-based solution and needs a new WLAN for the corporate campus. A network administrator completes the creation of this WLAN, as shown in Exhibit 1. When administrators try to test a connection to the WLAN, the WLAN does not show up in the list of WLANs on the client. The administrator can see the WLAN in the list, as shown in Exhibit 2.

What is the error?

- * The configuration is not deployed.
- * The WLAN is configured at a lower level in the Managed Network hierarchy.
- * The Mobility Master (MM) does not have an active PEFNG license.
- * The WLAN is configured as a hidden SSID.

NEW QUESTION 29

Refer to the exhibit.

Roles Policies Applications

Roles > admins Policies Bandwidth Captive Portal More [Show Basic View](#)

NAME	RULES COUNT	TYPE	POLICY USAGE
global-sacl	0	session	guest, stateful-dot1x, defa...
aprf-admins-sacl	0	session	admins
admins	0	session	admins
allow-network1	1	session	admins

+

admins Policies > allow-network1

TYPE	SOURCE	DESTINATION	SERVICE/APPLICATI...	ALLOW
ipv4	user	alias	any	permit

The alias in the rule shown in the exhibit is network 10.1.1.0/24.

A wireless client is assigned IP address 10.1.2.10/24 and the 'admins' role. The wireless client at 10.1.2.10 attempts to initiate a Web session with a server at 10.1.1.2. A wired client at 10.1.1.3 attempts to initiate an SSH session with the wireless client at 10.1.2.10.

How does the Aruba firewall handle these attempts?

- * The firewall drops the traffic from the wireless client. The firewall drops the traffic from the wired client.
- * The firewall permits the traffic from the wireless client, but drops the return traffic from the server. The firewall drops the traffic from the wireless client.
- * The firewall permits the traffic from the wireless client and also permits the return traffic from the server. The firewall permits the traffic from the wired client and also permits the return traffic from the wireless client.
- * The firewall permits the traffic from the wireless client and also permits the return traffic from the server. The firewall drops the traffic from the wired client.

NEW QUESTION 30

What is an example of a Layer2 wireless threat that a wireless intrusion detection system (WIDS) should detect?

- * 802.11 association floods
- * RF jamming
- * Bluetooth interference
- * spyware

NEW QUESTION 31

A network administrator creates a user account on an Aruba Mobility Master (MM) with the guest-provisioning role. Which task does this user have the rights to perform?

- * set up portal pages
- * create guest user accounts
- * monitor guest clients
- * create guest WLANs

NEW QUESTION 32

Refer to the exhibits.

Exhibit 1

Exam_Guest General **VLANs** Security Access

VLAN:

[Hide](#) [VLAN details](#)

Named VLANs	
Name	ID(S)
employee	51
guest	99
--	1,55

VLAN IDs							
ID	IPV4 ADDRE...	IPV6 ADDRE...	ENABLE NAT	PORT MEM...	ADMIN STATE	OPERATION...	DHCP SETTI..
99	--	--	Enabled	--	Enabled	N/A	None

Exhibit 2

Exam_Guest General **VLANs** Security Access

Clearpass or other external captive portal

Internal captive portal with authentication

Exhibit 3

Exam_Guest General **VLANs** Security Access

Default role: exam_guest-guest-logon

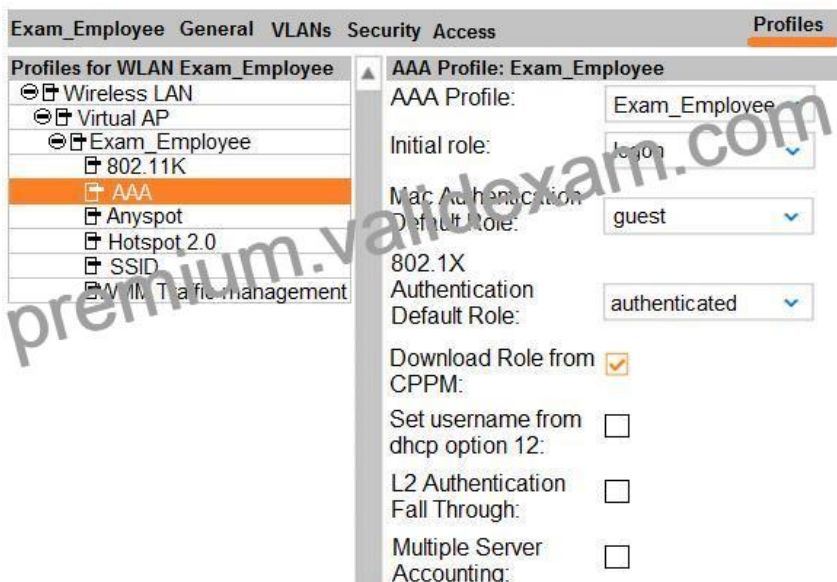
A network administrator creates a guest WLAN on an Aruba Mobility Manager (MM). The exhibits show some of the settings for the WLAN. The administrator does not change the policies for those roles.

How does the firewall control guest clients when they first connect to the WLAN?

- * It permits them to send any DHCP traffic and DNS and web traffic to the Internet. It redirects web traffic destined to the private network to a login portal.
- * It permits them to send any DHCP and DNS and it redirects all web traffic to a login portal.
- * It permits them to send any DHCP and RADIUS traffic. It redirects all web traffic destined to the Internet to a login portal and drops web traffic destined to the private network.
- * It does not permit them to send any traffic until they are authenticated.

NEW QUESTION 33

Refer to the exhibit.



The exhibit shows the AAA profile for a WLAN on an Aruba solution. This WLAN uses 802.1X to authenticate users to a RADIUS server. A user successfully authenticates with 802.1X, but the RADIUS server does not send a role assignment.

How does the Aruba firewall handle the role assignment for this user?

- * It does not assign a role.
- * It applies the Aruba VSA role employee.
- * It assigns the logon role.
- * It assigns the authenticated role.

NEW QUESTION 34

Refer to the exhibits.

Exhibit 1

Exhibit 2

A company has an Aruba Mobility Master (MM)-based solution and needs a new WLAN for the corporate campus. A network administrator completes the creation of this WLAN, as shown in Exhibit 1. When the administrator tries to test a connection to the WLAN in various locations, the WLAN sometimes shows up in the list of WLANs on the client but sometimes does not. The administrator can see the WLAN in the list, as shown in Exhibit 2.

What is the error?

- * The Mobility Master (MM) does not have an active PEFNG license.
- * The WLAN is configured as a hidden SSID.
- * The configuration is not deployed to the Mobility Controller (MC).
- * The WLAN is configured at a lower level in the Managed Network hierarchy.

NEW QUESTION 35

How does WPA2 protect wireless user traffic in the air?

- * It provides data integrity with AES and no data privacy.
- * It provides both data integrity and privacy with AES.
- * It provides data privacy with TKIP and no data integrity.
- * It provides data integrity with TKIP and data privacy with AES.

HPE6-A70 Real Valid Brain Dumps With 133 Questions: <https://www.validexam.com/HPE6-A70-latest-dumps.html>