



# HPE6-A77<sup>Q&As</sup>

Aruba Certified ClearPass Expert Written

## Pass HP HPE6-A77 Exam with 100% Guarantee

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

<https://www.passapply.com/hpe6-a77.html>

100% Passing Guarantee  
100% Money Back Assurance

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

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





### QUESTION 1

What is the Open SSID (otherwise referred to as Dual SSID) Onboard deployment service workflow?

- A. OnBoard Pre-Auth Application service, OnBoard Authorization Application service. OnBoard Provisioning RADIUS service
- B. OnBoard Pre-Auth RADIUS service. OnBoard Authorization Application service. OnBoard Provisioning RADIUS service
- C. OnBoard Authorization Application service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service
- D. OnBoard Authorization RADIUS service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

Correct Answer: C

---

### QUESTION 2

Refer to the exhibit:



**Request Details**

Summary Input Output Alerts

Login Status:	ACCEPT
Session Identifier:	R000001ae-01-5d9cb453
Date and Time:	Oct 08, 2019 12:07:47 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)

**Policies Used -**

Service:	HS_Building 802.1x service
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	[Endpoints Repository], AD1, AD2, Corp SQL
Roles:	VIP User, [Machine Authenticated], [User Authenticated]
Enforcement Profiles:	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-20 records

Change Status Show Configuration Export Show Logs Close

Configuration > Services > Edit - HS\_Building 802.1x service

Services - HS\_Building 802.1x service

Summary Service Authentication Authorization Roles Enforcement Profiles

Role Mapping Policy: HS\_Building Role Mapping Policy Modify Add New Role-Mapping Policy

**Role Mapping Policy Details**

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	first-applicable

Conditions	Role
1. (Connection:Client-Mac-Address <b>BELONGS_TO_GROUP</b> VIP User MAC)	VIP User
2. (Authorization:Corp SQL:MAC <b>EXISTS</b> )	Corp SQL Tablet
3. (Authorization:[Endpoints Repository]:Category <b>EQ</b> VoIP Phone)	IP Phone
4. (Authorization:[Endpoints Repository]:Category <b>EQ</b> SmartDevice)	Personal SmartDevice
5. (Authorization:[Endpoints Repository]:Category <b>EQ</b> Point of Sale devices)	Vending Machine
(Authorization:[Endpoints Repository]:Category <b>EQ</b> Printer)	Printer
6. <b>AND</b> (Authorization:[Endpoints Repository]:MAC Vendor <b>EQ</b> CANON INC.)	Printer
(Authorization:[Endpoints Repository]:Category <b>EQ</b> Network Camera)	IP Camera
7. <b>AND</b> (Authorization:[Endpoints Repository]:MAC Vendor <b>EQ</b> Axis Communications AB)	IP Camera



Conditions	Enforcement Profiles
1. (Authorization:[Endpoints Repository]:OS Family NOT_EXISTS )	Aruba Limited Access for Profiling
2. (Endpoint:MDM Enabled EQUAL true)	Aruba Full Access Profile
3. (Authentication:OuterMethod EQUAL EAP-PEAP) AND (Tips:Role EQUAL Corp-SQL-Tablet)	Redirect to Aruba OnBoard Portal
4. (Authentication:OuterMethod EQUAL EAP-TLS) AND (Tips:Role EQUAL Corp-SQL-Tablet)	Aruba Full Access Profile
5. (Authentication:Source EQUAL AD1) AND (Tips:Posture EQUAL HEALTHY (0)) AND (Authorization:[Endpoints Repository]:OS Family EQUAL Windows) AND (Tips:Role EQUAL [User Authenticated] [Machine Authenticated])	Aruba Full Access Profile
6. (Authentication:Source EQUAL AD1) AND (Tips:Posture EQUAL UNKNOWN (100)) AND (Authorization:[Endpoints Repository]:OS Family EQUAL Windows) AND (Tips:Role EQUAL [User Authenticated] [Machine Authenticated])	Aruba Limited Access Profile, Redirect to Aruba-Dismissible_page_Profile
7. (Authentication:Source EQUAL AD1) AND (Tips:Posture EQUAL HEALTHY (0)) AND (Authorization:[Endpoints Repository]:OS Family EQUAL Windows) AND (Tips:Role EQUAL [User Authenticated] [Machine Authenticated])	Redirect to Aruba Quarantine Profile
8. (Tips:Role EQUAL VIP User)	Aruba VIP Full Access Profile

The customer created a new enforcement policy condition to allow VIP Users access without additional security compliance checks but cannot get it working. The customer has sent you the above screenshots. How would you resolve the issue?

- A. Ask the VIP user to complete the one time web health check to get the VIP profile.
- B. Set the Enforcement Policy rules evaluation algorithm to evaluate all.
- C. Include VIP User role along with the Healthy posture enforcement condition.
- D. Modify the Enforcement Policy and re-order the VIP user condition to the top.

Correct Answer: C

### QUESTION 3

Refer to the exhibit: A customer has configured a Guest Self registration page for their Cisco Wireless network with the settings shown. What should be changed in order to successfully authenticate guests users?



Home > Configuration > Pages > Self-Registrations

## Customize Self-Registration (Admin-GuestCiscoSelfReg)

Use this form to make changes to the self-registration instance Admin-GuestCiscoSelfReg.

### Customize Self-Registration

#### Login

Options controlling logging in for self-registered guests.

Enabled:	<input checked="" type="checkbox"/> Enable guest login to a Network Access Server
* Vendor Settings:	Cisco Systems <small>Select a predefined group of settings suitable for standard network configurations.</small>
Login Method:	Controller-initiated -- Guest browser performs HTTP form submit <small>Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.</small>
* IP Address:	1.1.1.1 <small>Enter the IP address or hostname of the vendor's product here.</small>
Secure Login:	<input type="checkbox"/> Use vendor default <small>Select a security option to apply to the web login process.</small>
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials <small>In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.</small>
Username Suffix:	<input type="text"/> <small>The suffix is automatically appended to the username before logging into the NAC.</small>

#### Default Destination

Options for controlling the destination clients will redirect to after login.

* Default URL:	<input type="text"/> <small>Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.</small>
----------------	--

Override Destination:	<input checked="" type="checkbox"/> Force default destination for all clients <small>If selected, the client's default destination will be overridden regardless of its value.</small>
-----------------------	---

The screenshot shows the Cisco Management Console interface. At the top, there is a navigation bar with the Cisco logo and menu items: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The main content area is titled "HTTP-HTTPS Configuration" and contains a table of settings:

Summary	HTTP Access	Enabled
SNMP	HTTPS Access	Enabled
HTTP-HTTPS	WebAuth SecureWeb	Disabled
Telnet-SSH	HTTPS Redirection	Disabled
Serial Port	Web Session Timeout	30 Minutes
Local Management	Current Certificate	
Users		
User Sessions		

- A. Secure Login should use HTTP
- B. Change the Vendor Settings to Airespace Networks
- C. Change the IP Address to the Cisco Controller DNS name



D. Login Method should be Controller-initiated - using HTTPs form submit

Correct Answer: C

#### QUESTION 4

Refer to the exhibit:

The image shows two screenshots of a 'Request Details' window. The top screenshot shows the 'Summary' tab with the following information:

Login Status:	<b>REJECT</b>
Session Identifier:	R00000218-01-5d9db68b
Date and Time:	Oct 09, 2019 06:29:34 EDT
End-Host Identifier:	78D29437BD68 (Computer / Windows / Windows 10)
Username:	andy07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)

Below this is the 'Policies Used' section:

Service:	HS_Building Aruba 802.1x service
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	AD1
Roles:	[Other], [User Authenticated]
Enforcement Profiles:	[Deny Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Not Available

At the bottom of the first screenshot, there are buttons for 'Show Configuration', 'Export', 'Show Logs', and 'Close', along with a status bar indicating 'Showing 1 of 1-20 records'.

The bottom screenshot shows the 'Alerts' tab for the same request:

Error Code:	206
Error Category:	Authentication failure
Error Message:	Access denied by policy

Below this is the 'Alerts for this Request' section:

RADIUS	Applied 'Reject' profile
--------	--------------------------



Configuration > Services > Edit - HS\_Building Aruba 802.1x service

### Services - HS\_Building Aruba 802.1x service

Summary Service Authentication Roles Enforcement Profiler

**Service:**

Name: HS\_Building Aruba 802.1x service  
 Description: 802.1X wireless access service authenticating users prior to device provisioning with Onboard, and after device provisioning is complete  
 Type: Aruba 802.1X Wireless  
 Status: Enabled  
 Monitor Mode: Disabled  
 More Options: Profile Endpoints

**Service Role**

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3. Radius:Aruba	Aruba-Essid-Name	EQUALS	secure-HS-5007

**Authentication:**

Authentication Methods: 1. [EAP PEAP]  
2. HS\_Branch\_[EAP TLS With OCSP Enabled]  
 Authentication Sources: 1. [Onboard Devices Repository]  
2. AD1  
3. AD2  
 Strip Username Rules: /user  
 Service Certificate: -

**Roles:**

Role Mapping Policy: HS\_Building Role Mapping Policy

**Enforcement:**

Use Cached Results: Enabled  
 Enforcement Policy: HS\_Building 802.1x Enforcement Policy

**Profiler:**

Endpoint Classifications: ANY  
 RADIUS CoA Action: [ArubaOS Wireless - Terminate Session]

[Back to Services](#)
[Disable](#)
[Copy](#)
[Save](#)
[Cancel](#)



Configuration > Services > Edit - HS\_Building Aruba 802.1x service

### Services - HS\_Building Aruba 802.1x service

Summary Service Authentication Roles Enforcement Profiler

Role Mapping Policy: HS\_Building Role Mapping Policy Modify Add New Role Mapping Policy

**Role Mapping Policy Details**

Description:

Default Role: [Other]

Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Connection:Client-Mac-Address <b>BELONGS_TO_GROUP</b> VIP User MAC)	VIP User
2. (Authorization:Corp SQL:MAC <b>EXISTS</b> )	Corp SQL Tablet
3. (Authorization:[Endpoints Repository]:Category <b>EQUALS</b> VoIP Phone)	IP Phone
4. (Authorization:[Endpoints Repository]:Category <b>EQUALS</b> SmartDevice)	Personal SmartDevice
5. (Authorization:[Endpoints Repository]:Category <b>EQUALS</b> Point of Sale devices)	Vending Machine
6. <b>AND</b> (Authorization:[Endpoints Repository]:Category <b>EQUALS</b> Printer)	Printer
<b>AND</b> (Authorization:[Endpoints Repository]:MAC Vendor <b>EQUALS</b> CANON INC.)	
7. <b>AND</b> (Authorization:[Endpoints Repository]:Category <b>EQUALS</b> Network Camera)	IP Camera
<b>AND</b> (Authorization:[Endpoints Repository]:MAC Vendor <b>EQUALS</b> Axis Communications AB)	

Configuration > Services > Edit - HS\_Building Aruba 802.1x service

### Services - HS\_Building Aruba 802.1x service

Summary Service Authentication Roles Enforcement Profiler

Use Cached Results:  Use cached Roles and Posture attributes from previous sessions Add New Enforcement Policy

Enforcement Policy: HS\_Building 802.1x Enforcement Policy Modify

**Enforcement Policy Details**

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Endpoint:MDM Enabled <b>EQUALS</b> true)	Aruba Full Access Profile
2. (Authentication:OuterMethod <b>EQUALS</b> EAP-PEAP) <b>AND</b> (Tips:Role <b>EQUALS</b> Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
3. (Authentication:OuterMethod <b>EQUALS</b> EAP-TLS) <b>AND</b> (Tips:Role <b>EQUALS</b> Corp SQL Tablet)	Aruba Full Access Profile
4. (Tips:Role <b>EQUALS</b> VIP User)	Aruba VIP Full Access Profile
(Tips:Role <b>MATCHES</b> ALL [User Authenticated]) [Machine Authenticated])	Aruba Full Access Profile
5. <b>AND</b> (Authentication:Source <b>EQUALS</b> AD1) <b>AND</b> (Tips:Posture <b>EQUALS</b> HEALTHY (0))	Aruba Full Access Profile
(Tips:Role <b>MATCHES</b> ALL [User Authenticated]) [Machine Authenticated])	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
6. <b>AND</b> (Authentication:Source <b>EQUALS</b> AD1) <b>AND</b> (Tips:Posture <b>EQUALS</b> UNKNOWN (100))	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
(Tips:Role <b>MATCHES</b> ALL [User Authenticated]) [Machine Authenticated])	Redirect to Aruba Quarantine Profile
7. <b>AND</b> (Authentication:Source <b>EQUALS</b> AD1) <b>AND</b> (Tips:Posture <b>NOT_EQUALS</b> HEALTHY (0))	Redirect to Aruba Quarantine Profile





Your company has a postgres SQL database with the MAC addresses of the company-owned tablets. You have configured a role mapping condition to tag the SQL devices. When one of the tablets connects to the network, it does not get the correct role and receives a deny access profile.

How would you resolve the issue?

- A. Remove SQL condition from role mapping policy and add it under the enforcement policy conditions.
- B. Edit the SQL authentication source niter attributes and modify the SQL server filter query.
- C. Add the SQL server as an authentication source and map .t under the authentication tab in the service.
- D. Enable authorization tab in the service and add the SQL server as an authorization source.

Correct Answer: B

---

#### QUESTION 5

A customer has deployed an OnGuard Solution to all the corporate devices using a group policy rule to push the OnGuard Agents. The network administrator is complaining that some of the agents are communicating to the ClearPass server that is located in a DMZ, outside the firewall. The network administrator wants all of the agents' System Health Validation traffic to stay inside the Management subnets. What can the ClearPass administrator do to move the traffic only to the ClearPass Management Ports?

- A. Edit the agent.conf file being deployed to the clients to use the ClearPass Management Port for SHV updates.
- B. Select the correct OnGuard Agent installer, and use the one configured for Management Port for the clients.
- C. Configure a Policy Manager Zone mapping so the OnGuard agent will use the Management Port IP.
- D. Filter TCP port 6658 on the firewall, forcing the OnGuard agent to use the ClearPass Management port.

Correct Answer: C

[HPE6-A77 PDF Dumps](#)

[HPE6-A77 VCE Dumps](#)

[HPE6-A77 Practice Test](#)