



# 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

Which statements are true about Aruba downloadable user roles? (Select three.)

- A. Can be applied only on ports or WLAN users authenticated by ClearPass.
- B. Aruba downloadable user role are universally available across the environment
- C. Aruba downloadable user role is a built in enforcement template in ClearPass
- D. Downloadable role names must be defined in Aruba switch or controller
- E. Can use these roles for other authentication methods not involving ClearPass
- F. Administering downloadable user roles can be difficult for a large enterprise

Correct Answer: ADE

### QUESTION 2

Refer to the exhibit: A customer has configured a service with the Onboard Devices Repository as an Authentication Source and an Active Directory Domain Server as an Authorization Source. What will happen if the client certificate is still valid and the user account associated with the certificate is disabled in Active Directory?

Configuration > Services > Edit - My\_organization\_Onboard Provisioning

#### Services - My\_organization\_Onboard Provisioning

Summary Service Authentication Authorization Roles Enforcement

**Service:**

Name: My\_organization\_Onboard Provisioning  
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: Authorization

**Service Rule**

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	Home_SSID

**Authentication:**

Authentication Methods: [EAP-TLS With OCSP Enabled]



Authentication Methods:	[EAP TLS With OCSP Enabled]
Authentication Sources:	[Onboard Devices Repository]
Strip Username Rules:	/:user:
Service Certificate:	-
<b>Authorization:</b>	
Authorization Details:	AD1
<b>Roles:</b>	
Role Mapping Policy:	-
<b>Enforcement:</b>	
Use Cached Results:	Disabled
Enforcement Policy:	My_organization_ Onboard Provisioning Enforcement Policy

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

- A. ClearPass will not process the request
- B. Enforcement will apply the [Deny Access Profile]
- C. ClearPass will redirect the client to Onboard again
- D. ClearPass will block network access to the device
- E. ClearPass will allow the device to access the network.

Correct Answer: D

### QUESTION 3

Refer to the exhibit:



**Request Details**

Summary | Input | Output | Alerts

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)

**Policies Used -**

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

Showing 1 of 1-20 records

Show Configuration | Export | Show Logs | Close

---

**Request Details**

Summary | Input | Output | Alerts

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

**Alerts for this Request**

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 (10))	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 4

You have recently implemented a self-registration portal in ClearPass Guest to be used on a Guest SSID broadcast from an Aruba controller. Your customer has started complaining that the users are not able to reliably access the internet after clicking the login button on the receipt page. They tell you that the users will click the login button multiple times and after about a minute they gain access. What could be causing this issue?

- A. The self-registration page is configured with a 1 minute login delay.
- B. The guest client is delayed getting an IP address from the DHCP server.
- C. The guest users are assigned a firewall user role that has a rate limit.
- D. The enforcement profile on ClearPass is set up with an IETF:session delay.

Correct Answer: A

---

#### QUESTION 5

Refer to the exhibit:



**Customize Self-Registration**

**Login**  
Options controlling logging in for self-registered guests.

Enabled:

\* Vendor Settings:   
Select a predefined group of settings suitable for standard network configurations.

Login Method:   
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.

\* IP Address:   
Enter the IP address or hostname of the vendor's product here.

Secure Login:   
Select a security option to apply to the web login process.

Dynamic Address:  The controller will send the IP to submit credentials  
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.

Security Hash:   
Select the level of checking to apply to URL parameters passed to the web login page.  
Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

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

\* Default URL:   
Enter the default URL to redirect clients.  
Please ensure you prepend "http://" for any external domain.

Override Destination:  Force default destination for all clients  
If selected, the client's default destination will be overridden regardless of its value.

A customer with multiple Aruba Controllers has just installed a new certificate for "\*.customerdomain.com" on all Aruba Controllers. While testing the existing guest Self-Registration page the customer noticed that the logins are failing. While troubleshooting they are finding no entries in the Event Viewer or Access Tracker for the tests. Suspecting that the Aruba Controllers may not be properly posting the credentials from the guest browser, they open the NAS Vendor Settings for the Guest Self-Registration Page. From the screen shown, how can you fix the errors?

- A. Change the "IP Address: field to" securelogin.customerdomain.com.
- B. Change the "Secure Login:" field to "Use Vendor Default".
- C. Change the "IP Address field to "captiveportal-login.customerdomain.com".
- D. Add PTR records on the DNS server for "securelogin.arubanetworks.com".

Correct Answer: B