



# HPE6-A81<sup>Q&As</sup>

Aruba Certified ClearPass Expert Written Exam

**Pass HP HPE6-A81 Exam with 100% Guarantee**

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

<https://www.passapply.com/hpe6-a81.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

While configuring a guest solution, the customer is requesting that guest user receive access for four hours from their first login. Which Guest Account Expiration would you select?

- A. expire\_after
- B. do\_expire
- C. expire\_time
- D. expire\_postlogin

Correct Answer: A

---

### QUESTION 2

Refer to the exhibit:



Configuration » Services » Edit - ACCX Aruba Device Access Service

## Services - ACCX Aruba Device Access Service

Summary Service Authentication Roles **Enforcement**

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Aruba NAD Tacacs Modify

**Enforcement Policy Details**

Description:

Default Profile: [TACACS Deny Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Tips:Role <b>READONLY</b> [Aruba TACACS read-only Admin])	[TACACS Read-only Admin]
2. (Tips:Role <b>ADMIN</b> [Aruba TACACS root Admin])	[TACACS Network Admin]

#	Server	Source	Username	Service	Login Status
1.	10.1.129.1	TACACS	read-only	ACCX Aruba Device Access Service	REJECT

**TACACS+ Session Details**

Summary Request Policies Alerts

Session ID: T00000006-01-5d55aba6

Username: read-only

Time: Aug 15, 2019 14:59:50 EDT

Status: AUTHEN\_STATUS\_FAIL

Authorizations: 0

Showing 1 of 1-6 records

Export Show Logs Close



#	Server	Source	Username	Service	Login Status
1	10.1.129.1	TACACS	read-only	AGC/ Aruba Device Access Service	REJECT

**TACACS+ Session Details**

SummaryRequestPoliciesAlerts

**Authentication Request Messages**

Error Category:	Tacacs authentication
Error Code:	Authentication privilege level mismatch

**Alerts for this Request:**

Tacacs server	Requested priv_level=0 greater than Max Allowed priv_level=0
---------------	--------------------------------------------------------------

Showing 1 of 1-6 records

ExportShow LogsClose





Configuration » Enforcement » Profiles » Edit Enforcement Profile - [TACACS Read-only Admin]

### Enforcement Profiles - [TACACS Read-only Admin]

Summary Profile **Services**

Privilege Level: 1 (Normal)

Selected Services: cpass:HTTP Remove Export All TACACS+ Services Dictionaries

--Select--

Authorize Attribute Status: ADD

Custom Services: To add new TACACS+ services / attributes, upload the modified dictionary.xml - Update TACACS+ Services Dictionary

Service Attributes			
Type	Name	=	Value
1. cpass:HTTP	AdminPrivilege	=	Read-only Administrator
2. Click to add...			

A customer is trying to configure a TACACS Authentication Service for administrative access to the Aruba Controller, During testing the authentication is not successful.

Given the screen shot what could be the reason for the Login status REJECT?

- A. The password used by the administrative user, user is wrong.
- B. The Enforcement profile is not designed to be used on Aruba Controller.
- C. The Read-only Administrator role does not exist on the Controller.
- D. The Enforcement profile used is not a TACACS profile.

Correct Answer: A

### QUESTION 3

A customer has configured Onboard with Single SSID provision for Aruba IAP Windows devices work as expected but cannot get the Apple iOS devices to work. The Apple iOS devices automatically get redirected to a blank page and do not get the Onboard portal page. What would you check to fix the issue?

- A. Verify if the checkbox "Enable bypassing the Apple Captive Network Assistant" is checked.
- B. Verify if the Onboard URL is updated correctly in the external captive portal profile.
- C. Verify if Onboard Pre-Provisioning enforcement profile sends the correct Aruba user role.
- D. Verify if the external captive portal profile is enabled to use HTTPS with port 443.

Correct Answer: B

**QUESTION 4**

Refer to the exhibit: Your customer configured a ClearPass server to process the Guest and Secure SSIDs broadcasting from both Aruba and Cisco WLAN controllers. When an Employee connects to Aruba or Cisco secure SSID, the authentication hits the guest service causing the client to fail the connection to the network. What change can be implemented to make both the secure and guest services created for Aruba and Cisco devices to work correctly?

The screenshot displays the 'Request Details' window in a ClearPass interface. It features a tabbed menu with 'Summary', 'Input', 'Output', and 'Alerts'. The 'Summary' tab is active, showing a table of request details. The 'Login Status' is 'REJECT'. Below the table, a section titled 'Policies Used -' lists various configuration details. At the bottom, there are navigation buttons: 'Show Configuration', 'Export', 'Show Logs', and 'Close'. A status bar at the very bottom indicates 'Showing 1 of 1-20 records'.

Request Details	
Summary	
Login Status:	REJECT
Session Identifier:	R0000024e-01-5d9de0f7
Date and Time:	Oct 09, 2019 09:30:31 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows 10)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)

  

Policies Used -	
Service:	HS-Guest User Authentication with MAC Caching
Authentication Method:	-
Authentication Source:	None
Authorization Source:	[Endpoints Repository], [Time Source]
Roles:	[Other]
Enforcement Profiles:	[Allow 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

Username: alex07

End-Host Identifier: 78D29437BD69 (Computer / Windows / Windows 10)

Access Device IP/Port: 10.1.70.100:0 (ArubaController / Aruba)

RADIUS Request

Radius:Aruba:Aruba-AP-Group	default
Radius:Aruba:Aruba-Device-Type	Win 10
Radius:Aruba:Aruba-Essid-Name	secure-HS-5007
Radius:Aruba:Aruba-Location-Id	20:4c:03:5b:39:8a
Radius:IETF:Called-Station-Id	000B86B52F87
Radius:IETF:Calling-Station-Id	78D29437BD69
Radius:IETF:Framed-MTU	1100
Radius:IETF:NAS-Identifier	10.1.70.100
Radius:IETF:NAS-IP-Address	10.1.70.100
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	19
Radius:IETF:Service-Type	2

Showing 1 of 1-20 records

Show Configuration Export Show Logs Close

Configuration > Services > Reorder

Reorder Services

To reorder services, first click on the service you want to move. Next, click on another service where you want to move the previously selected service:

OrderName	Service Details:
1 HS-Guest MAC Authentication	Name: HS-Guest User Authentication with MAC Caching
2 HS-Guest User Authentication with MAC Caching	Template: RADIUS Enforcement ( Generic )
3 HS_Building Aruba 802.1x service	Type: RADIUS
4 HS_Building Cisco 802.1x service	Description: Captive Portal authentication with MAC Caching
5 HS_Branch Onboard Authorization	Status: Enabled
6 HS_Branch Onboard Pre-Auth	
7 HS Corp health check service	
8 [AirGroup Authorization Service]	
9 [Policy Manager Admin Network Login Service]	
10 [Aruba Device Access Service]	
11 [Guest Operator Logins]	
12 [Insight Operator Logins]	

Service Rule

```
( (Radius:IETF:Calling-Station-Id EXISTS )  
OR (Connection:Client-Mac-Address NOT_EQUALS %{Radius:IETF:User-Name})  
OR (Radius:Aruba:Aruba-Essid-Name EQUALS guest-HS-5007) )  
AND (Connection:Protocol EQUALS RADIUS)
```

- A. Move the HS-Guest User Authentication with MAC Caching service to the first position.
- B. Modify the service rule matching algorithm to ALL in HS-Guest User Authentication service.
- C. Disable HS-Guest User Authentication service and move HS-Guest MAC Authentication to seventh position.
- D. Move the HS\_Building Aruba 802.1x service to the second position in the service order.



Correct Answer: A

---

#### QUESTION 5

Under Onboard management and control, which option will deny the user from re-provisioning the device a second time?

- A. Revoke and Delete certificate
- B. Delete user
- C. Revoke certificate
- D. Delete certificate

Correct Answer: D

[Latest HPE6-A81 Dumps](#)

[HPE6-A81 VCE Dumps](#)

[HPE6-A81 Braindumps](#)