# HPE6-A77 Q&As

Aruba Certified ClearPass Expert Written

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

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

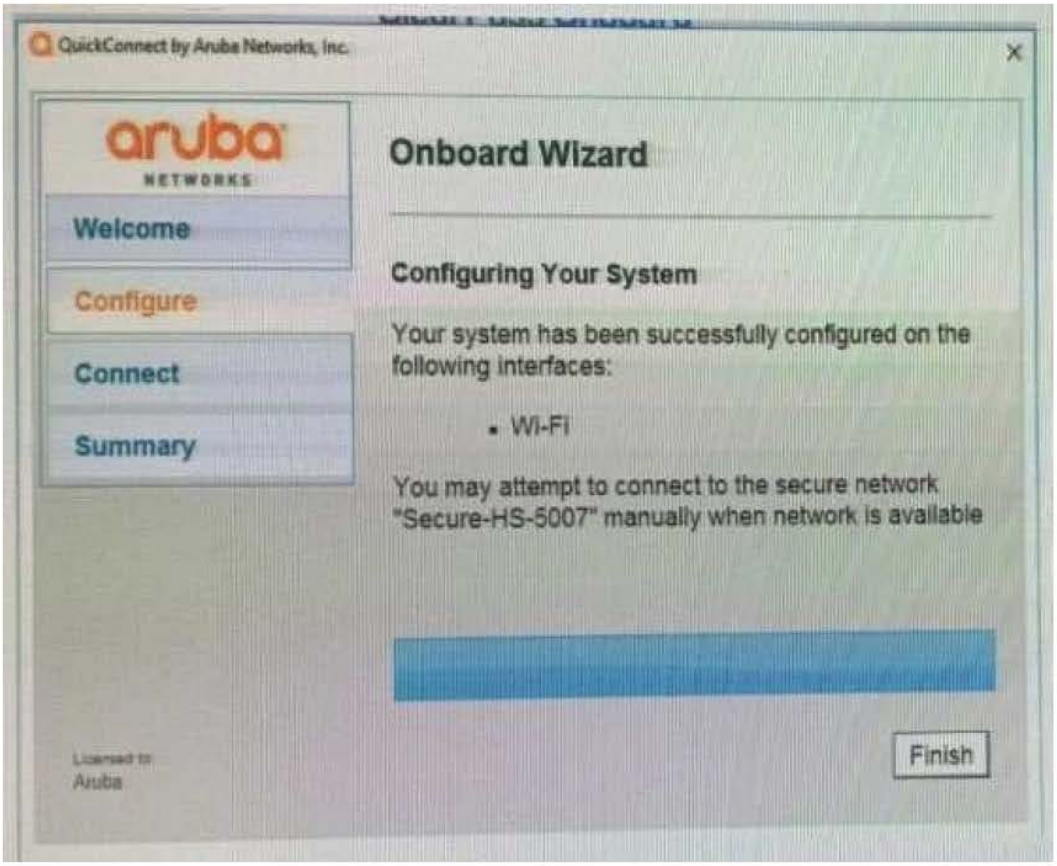
**https://www.leads4pass.com/hpe6-a77.html**

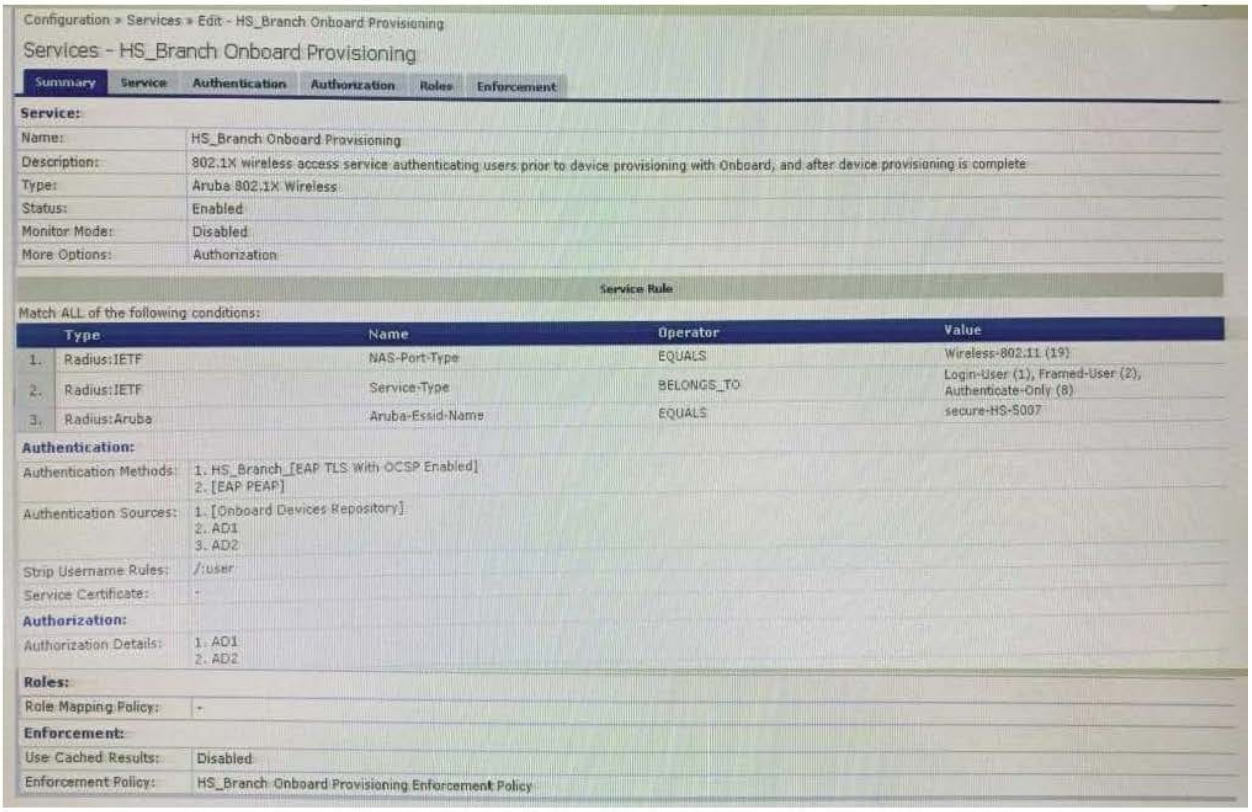
100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

Refer to the exhibit:



Configuration » Services » Edit - HS_Branch Onboard Provisioning

Services - HS_Branch Onboard Provisioning

Summary | Service | Authentication | Authorization | Roles | Enforcement

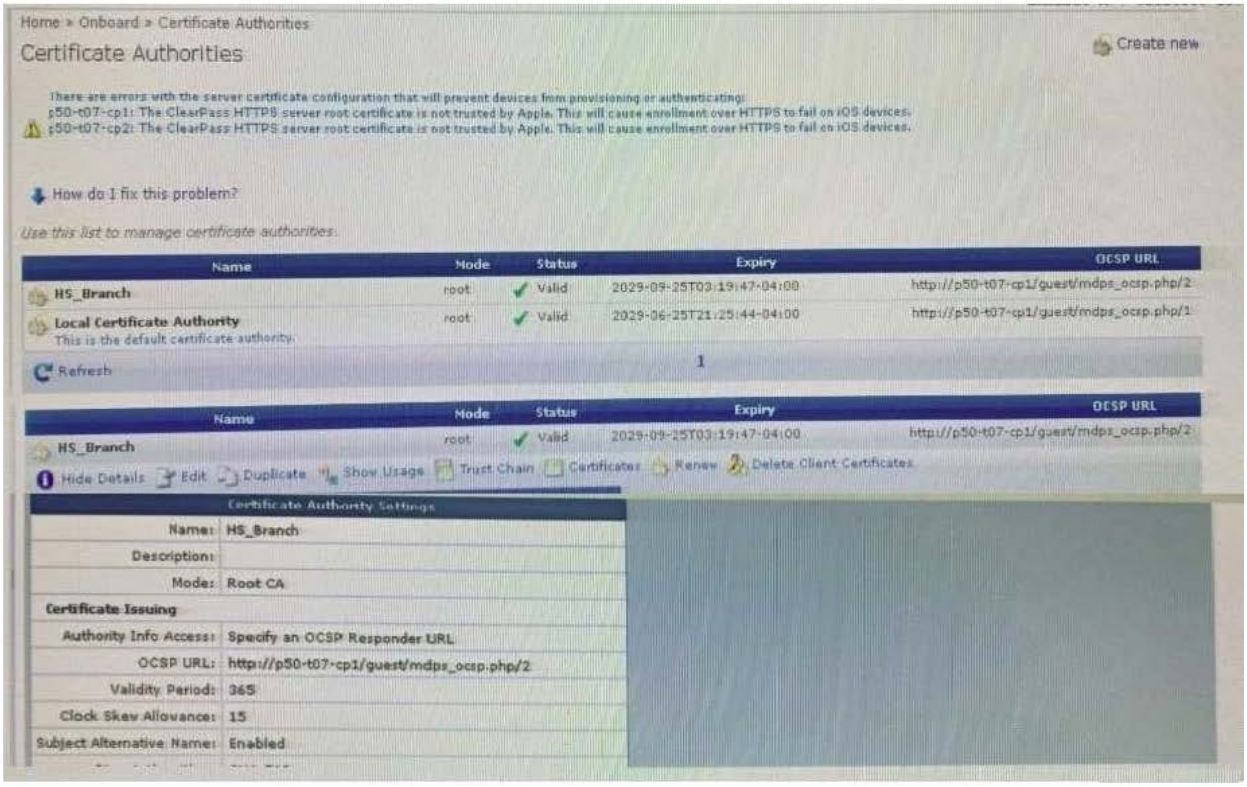
| Service: | |
|---|---|
| Name: | HS_Branch Onboard Provisioning |
| Description: | 802.1X wireless access service authenticating users prior to device provisioning with Onboard, and after device provisioning is complete |
| Type: | Aruba 802.1X Wireless |
| Status: | Enabled |
| Monitor Mode: | Disabled |
| More Options: | Authorization |

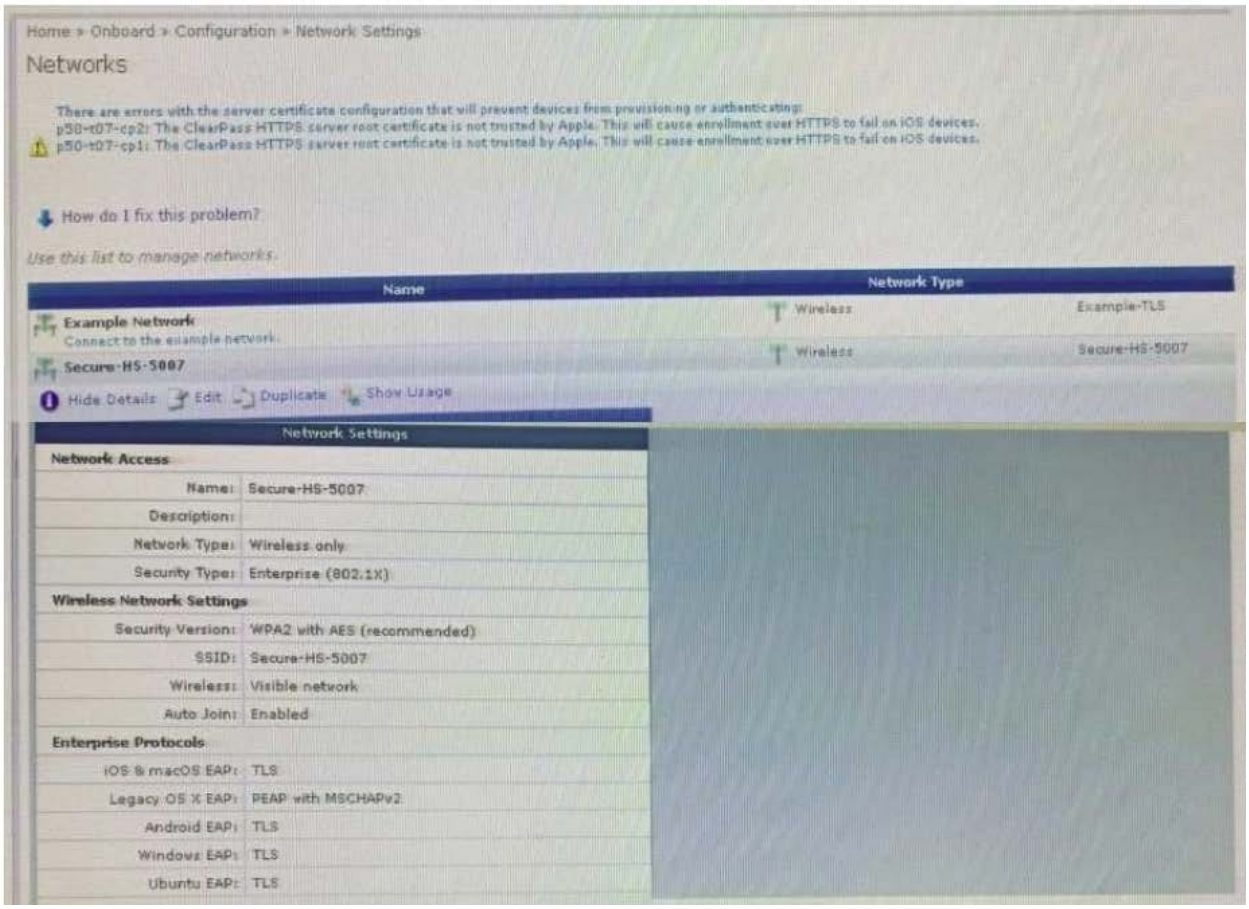
Service Rule

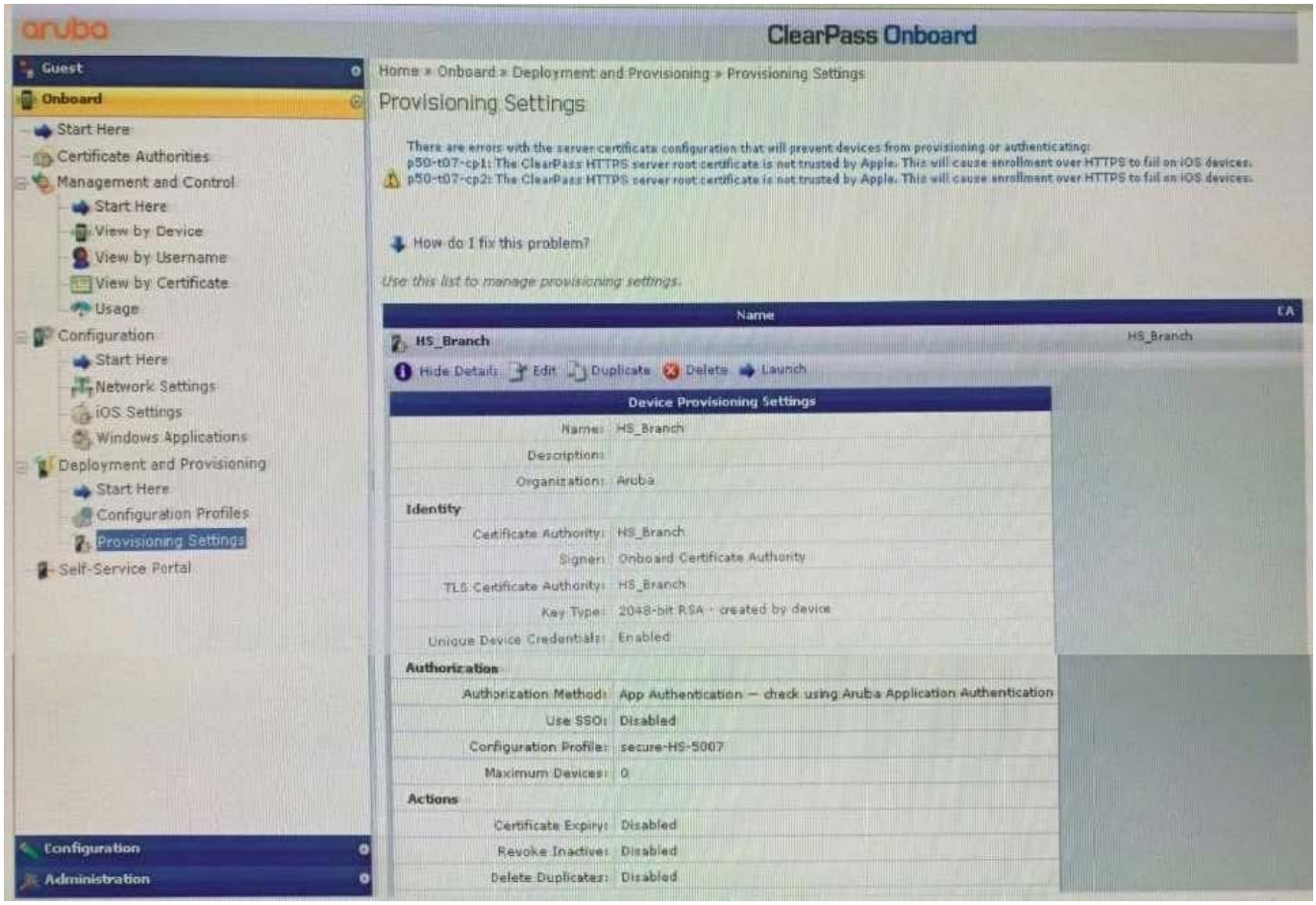
Match ALL of the following conditions:

| | 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 | secure-HS-5007 |

| Authentication: | |
|---|---|
| Authentication Methods: | 1. HS_Branch_[EAP TLS With OCSP Enabled]<br>2. [EAP PEAP] |
| Authentication Sources: | 1. [Onboard Devices Repository]<br>2. AD1<br>3. AD2 |
| Strip Username Rules: | /:user |
| Service Certificate: | - |
| **Authorization:** | |
| Authorization Details: | 1. AD1<br>2. AD2 |
| **Roles:** | |
| Role Mapping Policy: | - |
| **Enforcement:** | |
| Use Cached Results: | Disabled |
| Enforcement Policy: | HS_Branch Onboard Provisioning Enforcement Policy |


Home » Onboard » Certificate Authorities
Certificate Authorities
Create new
There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
p50-t07-cp1: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
p50-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
How do I fix this problem?
Use this list to manage certificate authorities.
Name
Mode
Status
Expiry
OCSP URL
HS_Branch
root
Valid
2029-09-25T03:19:47-04:00
http://p50-t07-cp1/guest/mdps_ocsp.php/2
Local Certificate Authority
This is the default certificate authority.
root
Valid
2029-06-25T21:25:44-04:00
http://p50-t07-cp1/guest/mdps_ocsp.php/1
Refresh
1
Hide Details
Edit
Duplicate
Show Usage
Trust Chain
Certificates
Renew
Delete Client Certificates
Certificate Authority Settings
Name: HS_Branch
Description:
Mode: Root CA
Certificate Issuing
Authority Info Access: Specify an OCSP Responder URL
OCSP URL: http://p50-t07-cp1/guest/mdps_ocsp.php/2
Validity Period: 365
Clock Skew Allowance: 15
Subject Alternative Name: Enabled


Home » Onboard » Configuration » Network Settings
Networks
There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
p50-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
p50-t07-cp1: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
How do I fix this problem?
Use this list to manage networks.
Name
Network Type
Example Network
Connect to the example network.
Wireless
Example-TLS
Secure-HS-5007
Wireless
Secure-HS-5007
Hide Details
Edit
Duplicate
Show Usage
Network Settings
Network Access
Name: Secure-HS-5007
Description:
Network Type: Wireless only
Security Type: Enterprise (802.1X)
Wireless Network Settings
Security Version: WPA2 with AES (recommended)
SSID: Secure-HS-5007
Wireless: Visible network
Auto Join: Enabled
Enterprise Protocols
iOS & macOS EAP: TLS
Legacy OS X EAP: PEAP with MSCHAPv2
Android EAP: TLS
Windows EAP: TLS
Ubuntu EAP: TLS




You have configured an Onboard portal for single SSID provision. During testing you notice that the QuickConnect Application did not display the "Connect" button, only the finish button. To get connected the test user had to manually connect to the secure-HS-5007 SSID but was prompted for a username and password. Using the screenshots as a reference, how would you fix this issue?

A. Check the network settings for the correct SSID name spelling.

B. Change the network settings to use EAP-TLS for the authentication protocol.

C. Install a public signed HTTPs web server certificate on the ClearPass server.

D. Configure the SSID to support both EAP-PEAP and EAP-TLS authentication method.

Correct Answer: A

**QUESTION 2**

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

**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**

You are deploying ClearPass Policy Manager with Guest functionality for a customer with multiple Aruba Networks Mobility Controllers The customer wants to avoid SSL errors during guest access but due to company security policy cannot use a wildcard certificate on ClearPass or the Controllers. What is the most efficient way to configure the customers guest solution? (Select two.)

A. Build multiple Web Login pages with vendor settings configured for each controller

B. Install the same public certificate on all Controllers with the common name "controller {company domain}"

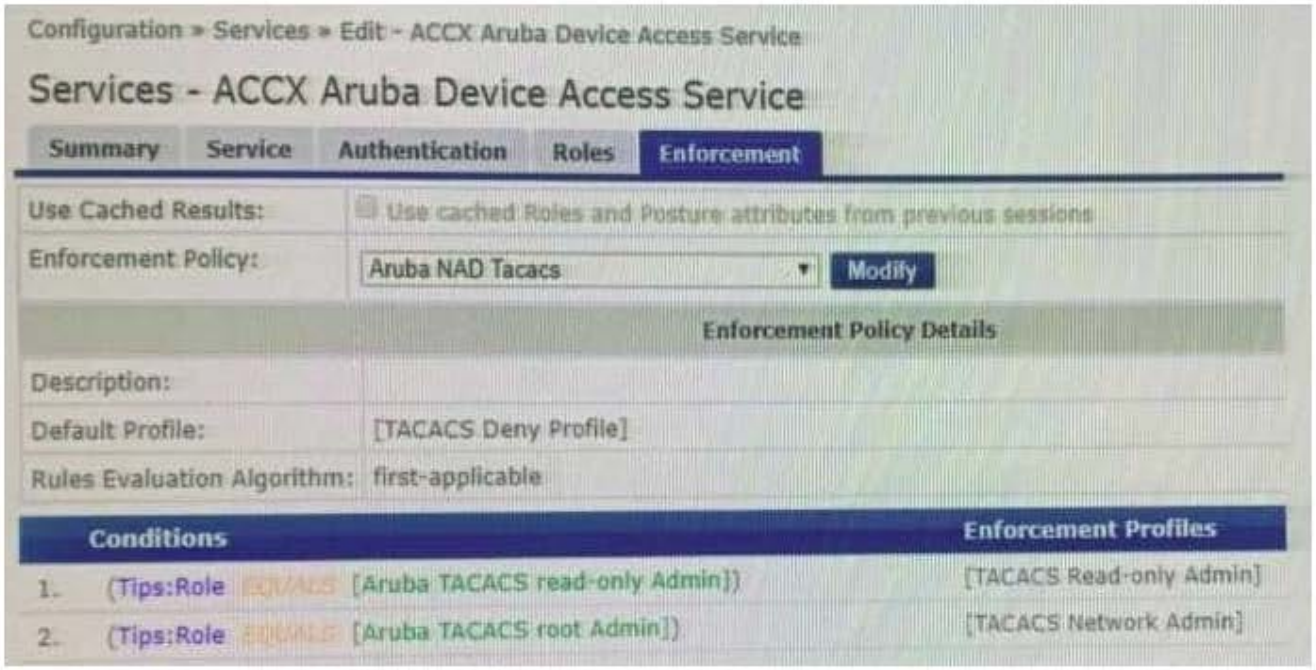
C. Build one Web Login page with vendor settings for controller {company domain)

D. Install multiple public certificates with a different Common Name on each controller

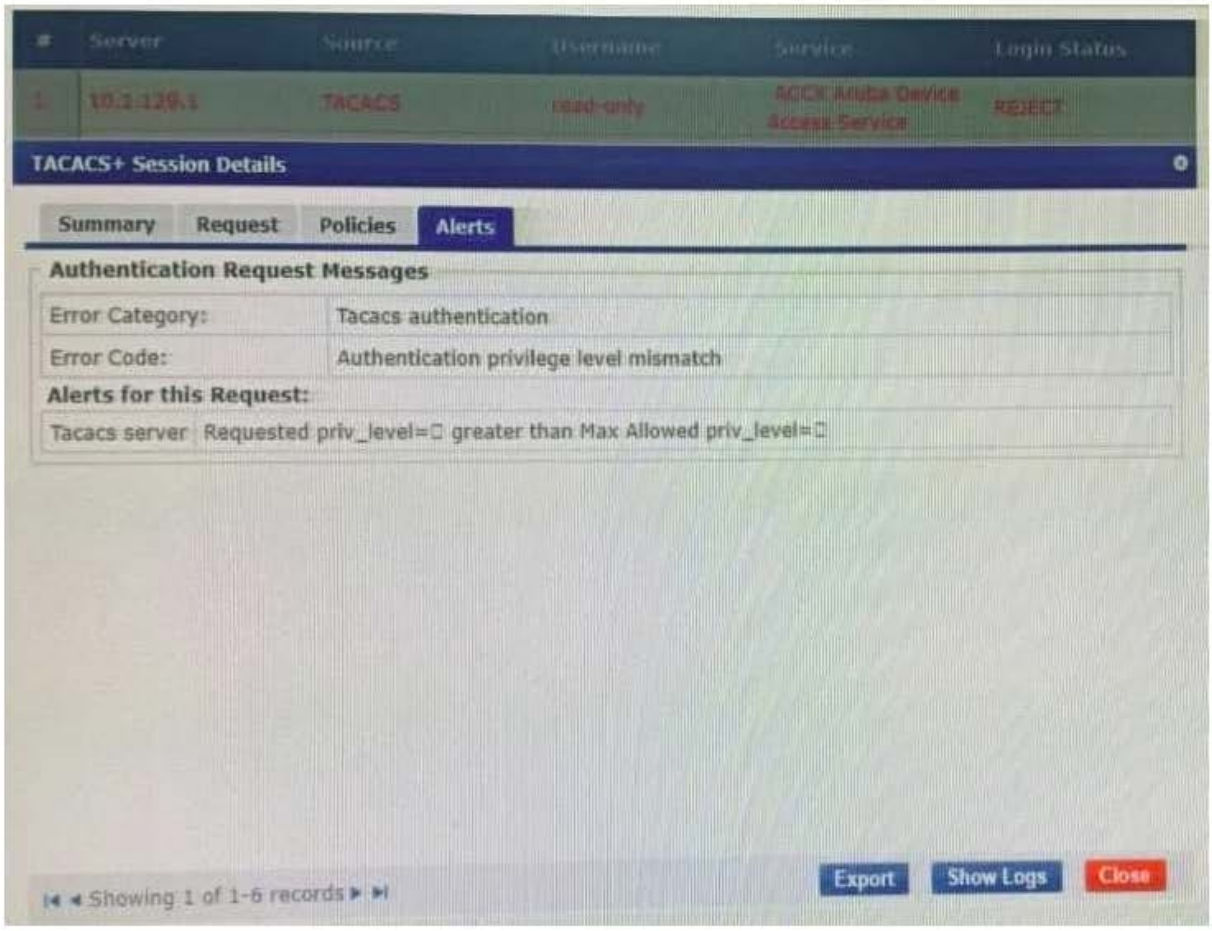
Correct Answer: AB

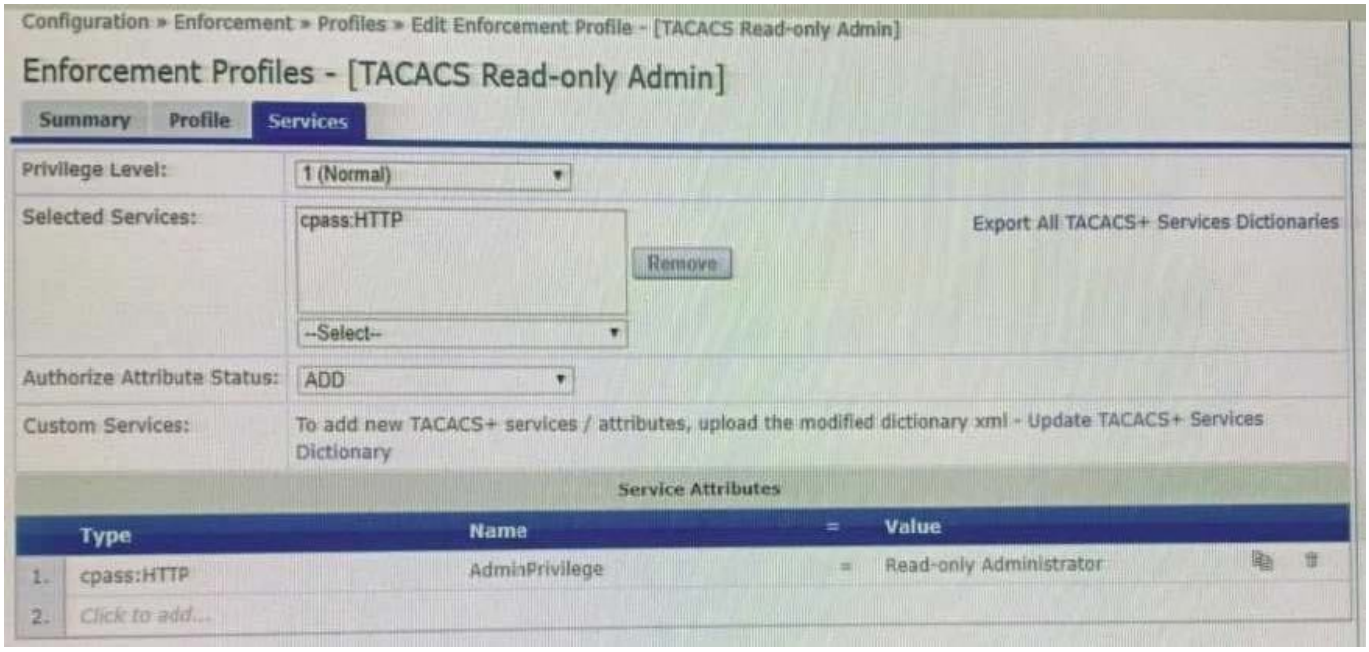
**QUESTION 5**

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 [Aruba TACACS read-only Admin])
[TACACS Read-only Admin]
2. (Tips:Role [Aruba TACACS root Admin])
[TACACS Network Admin]


Server
Source
Username
Service
Login Status
TACACS
read-only
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
TACACS
read-only
REJECT
TACACS+ Session Details
Summary
Request
Policies
Alerts
Authentication Request Messages
Error Category:
Tacacs authentication
Error Code:
Authentication privilege level mismatch
Alerts for this Request:
Tacacs server
Requested priv_level=□ greater than Max Allowed priv_level=□
Showing 1 of 1-6 records
Export
Show Logs
Close




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