HPE6-A81 Q&As

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.pass2lead.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

When is it recommended to use a certificate with multiple entries on the Subject Alternative Name?

A. The ClearPass servers are placed in different OnGuard zones to allow the client agent to send SHV updates.

B. Using the same certificate to Onboard clients and the Guest Captive Portal on a single ClearPass server.

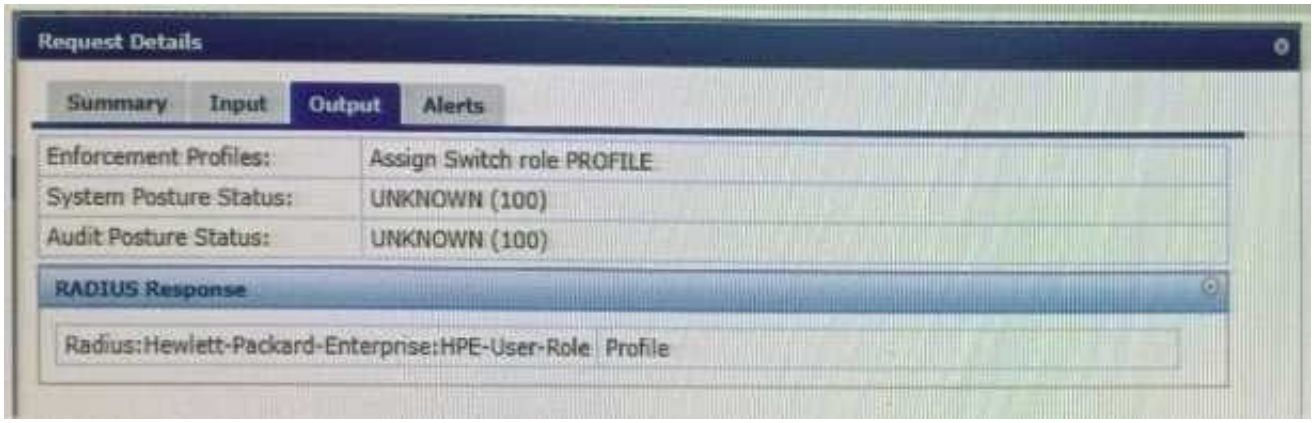
C. The primary authentication server Is not available to authenticate the users.

D. The ClearPass server will be hosting captive portal pages for multiple FQDN entries

Correct Answer: A

QUESTION 2

Refer to the exhibit:


Request Details
Summary
Input
Output
Alerts
Enforcement Profiles:
Assign Switch role PROFILE
System Posture Status:
UNKNOWN (100)
Audit Posture Status:
UNKNOWN (100)
RADIUS Response
Radius:Hewlett-Packard-Enterprise:HPE-User-Role Profile


P50-T7-2930(config)# sho port-access clients
Port Access Client Status
Port Client Name MAC Address IP Address User Role Type
VLAN
3 204c035b4ad2 204c03-5b4ad2 n/a denyall MAC
70
P50-T7-2930(config)# show user-role
User Roles
Enabled : Yes
Initial Role : denyall
Type Name
local PROFILE
predefined denyall
local AP-ACCESS
P50-T7-2930(config)#

You have been asked to help a Customer troubleshoot an issue. They have configured an Aruba OS switch (Aruba 2930 with 16.09) to do MAC authentication with profiling using ClearPass as the authentication source. They cannot get it working.

Using the screenshots as a reference, how will you fix the issue?

A. Delete the initial role in the Aruba OS switch to force the device to get the server derived user roles

B. Use a CoA to bounce the switch port to force the port to change to the correct Aruba user role

C. Change the Vendor settings for the Aruba OS switch to "Aruba" so that the enforcement will use the correct VSAs

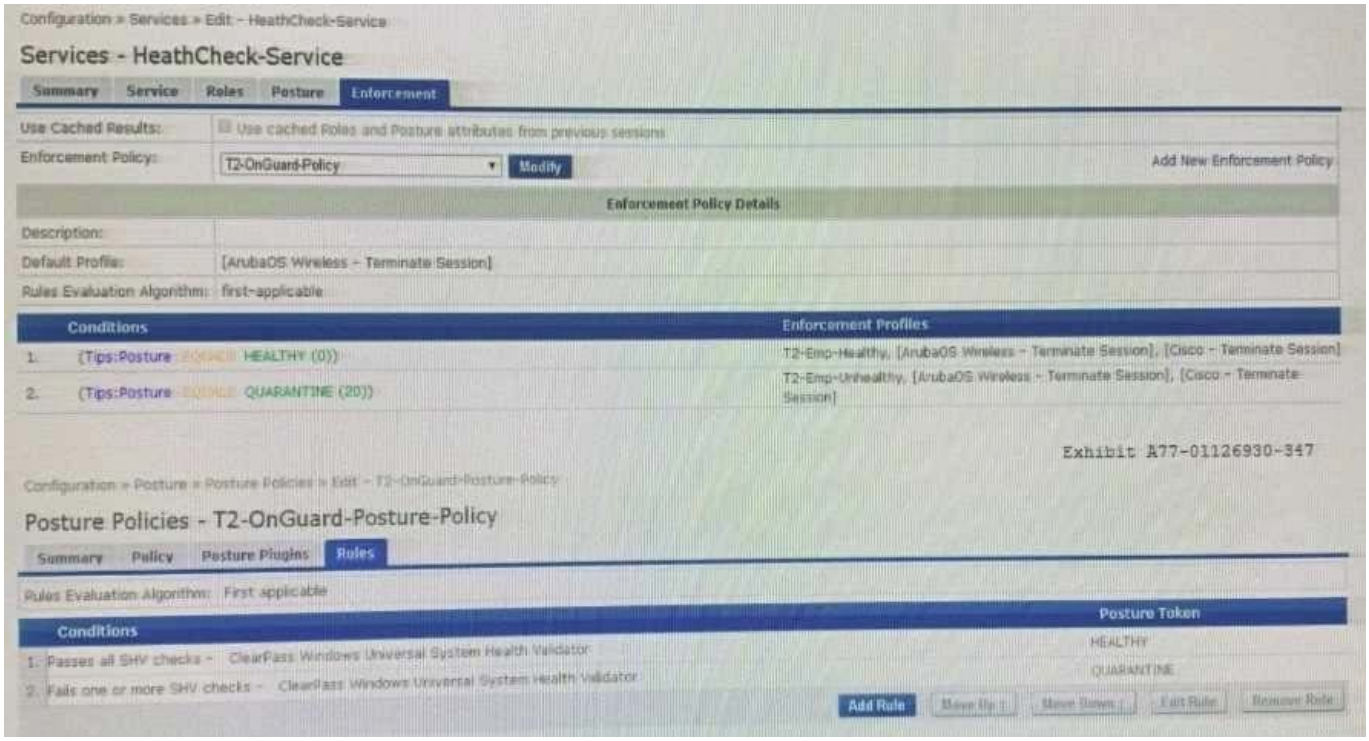
D. Modify the enforcement profile conditions with Aruba Vendor specific attributes and Aruba-user- roles

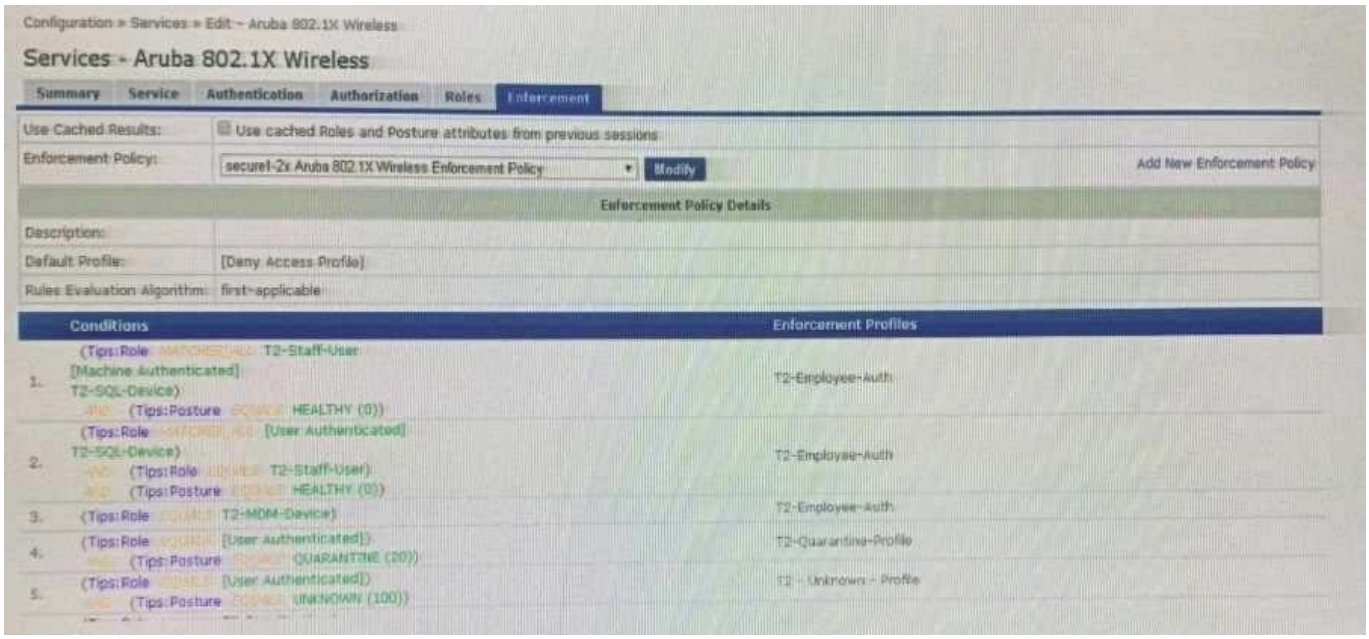
E. User-roles are case sensitive, update the correct role with correct case in the enforcement profile

Correct Answer: D

QUESTION 3

Refer to the Exhibit:





A customer wants to integrate posture validation into an Aruba Wireless 802.1X authentication service

During testing, the client connects to the Aruba Employee Secure SSID and is redirected to the Captive Portal page where the user can download the OnGuard Agent After the Agent is installed, the client receives the Healthy token the client remains connected to the Captive Portal page ClearPass is assigning the endpoint the following roles: T2-Staff-User. (Machine Authenticated! and T2-SOL-Device. What could cause this behavior?

A. The Enforcement Policy conditions for rule 1 are not configured correctly.

B. Used Cached Results: has not been enabled In the Aruba 802.1X Wireless Service

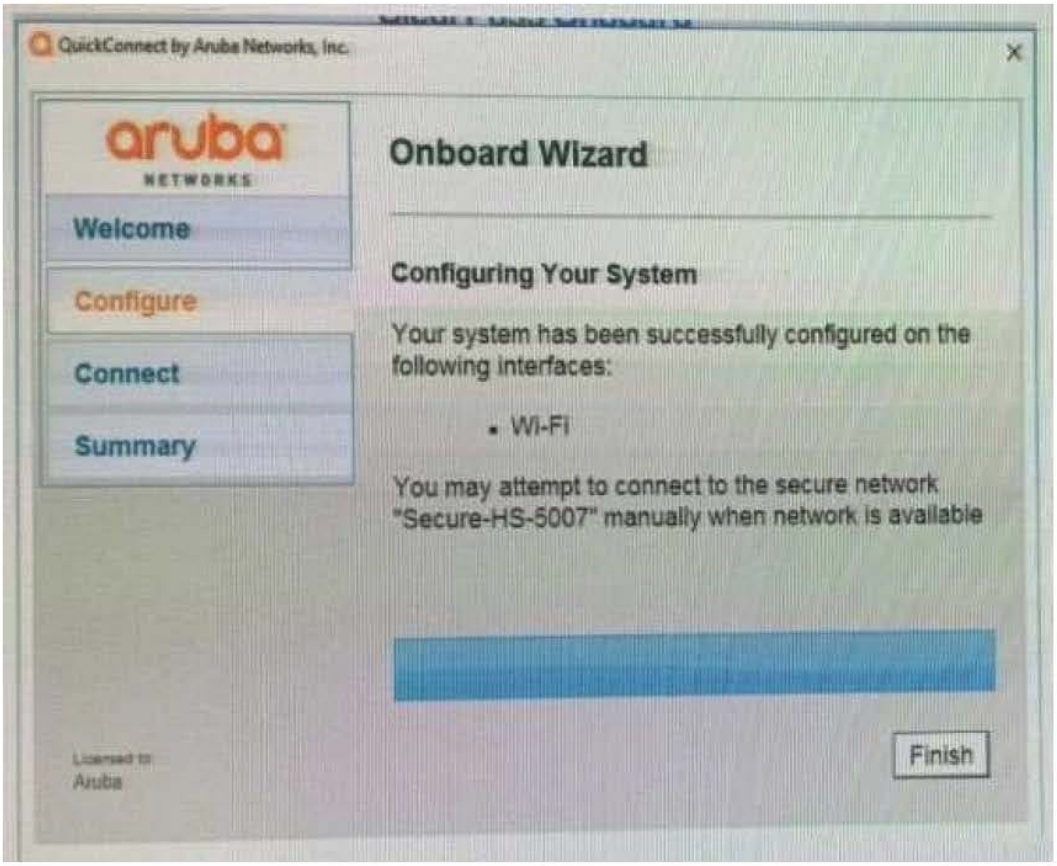
C. RFC-3576 Is not configured correctly on the Aruba Controller and does not update the role.

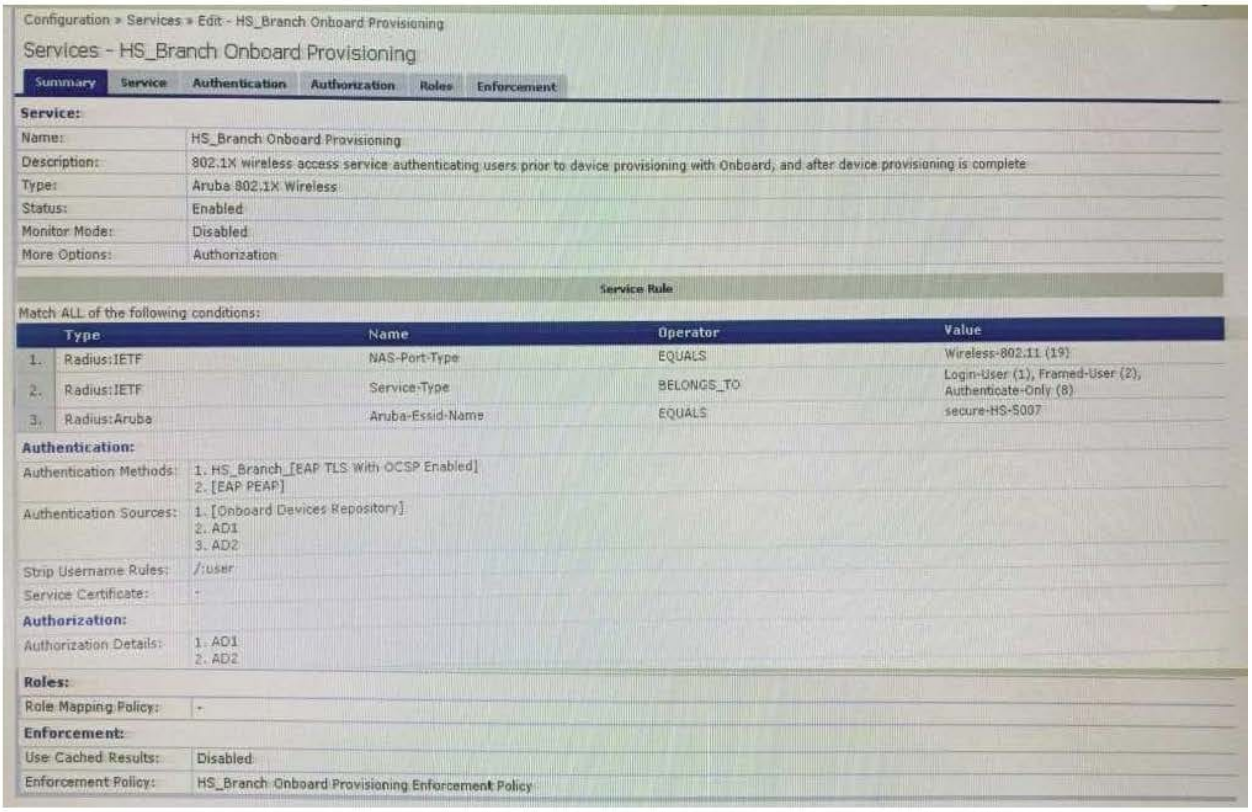
D. The Enforcement Profile should bounce the connection instead of a Terminate session

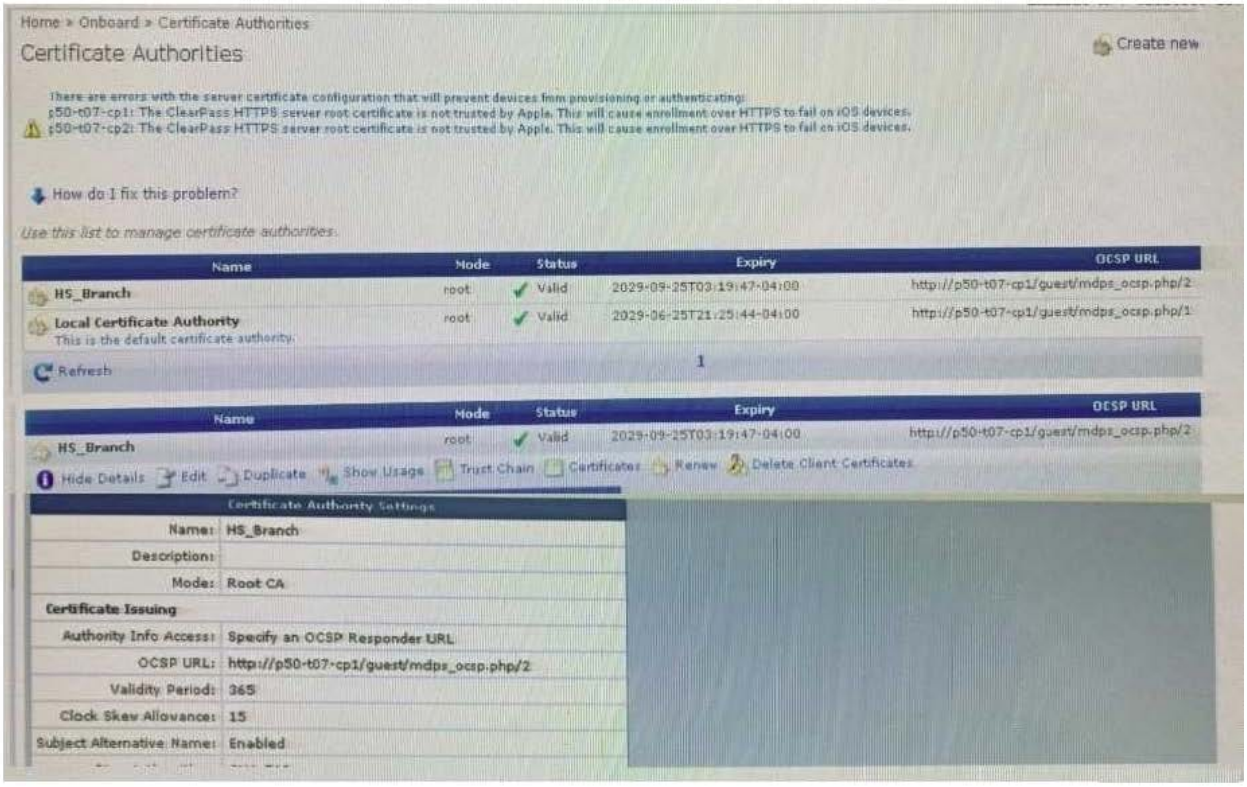
Correct Answer: B

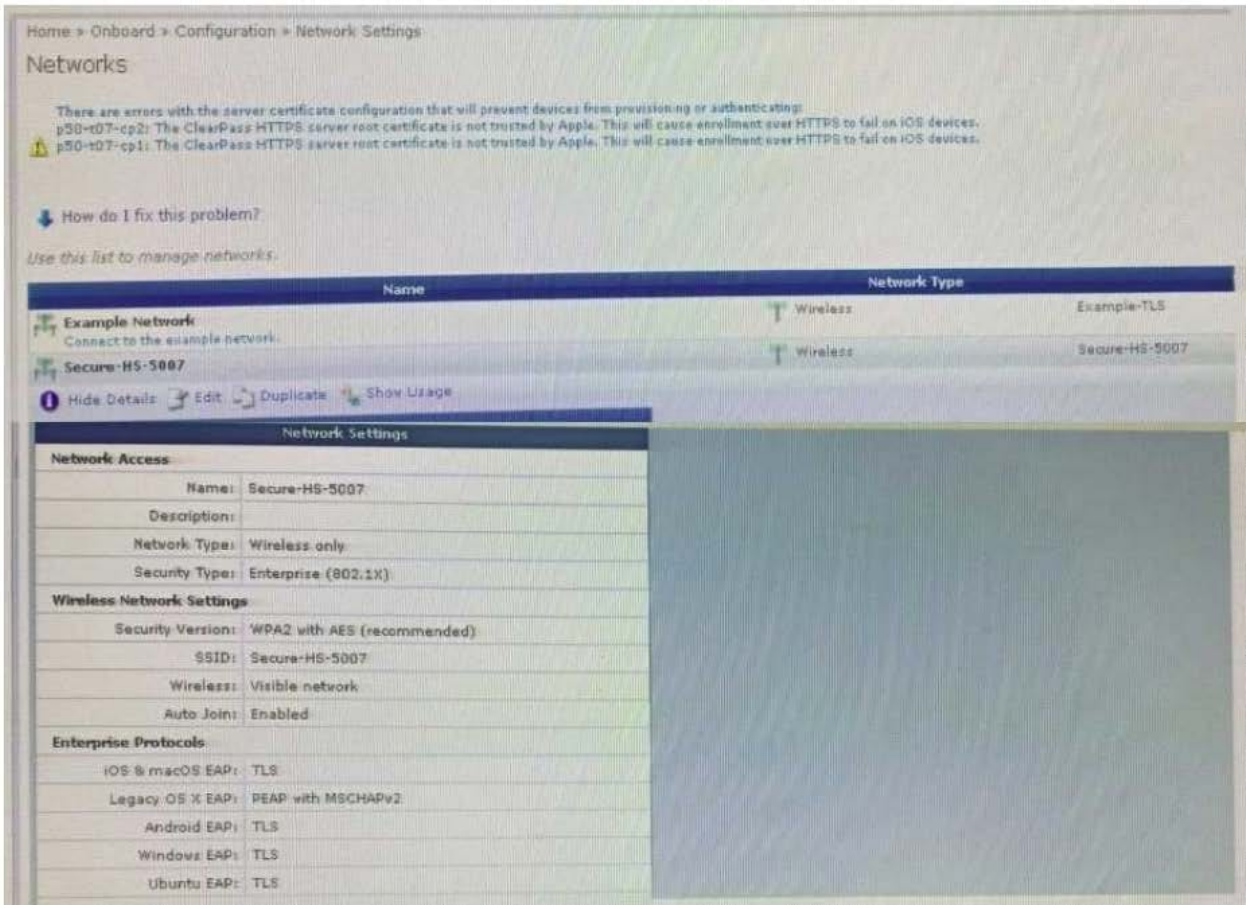
QUESTION 4

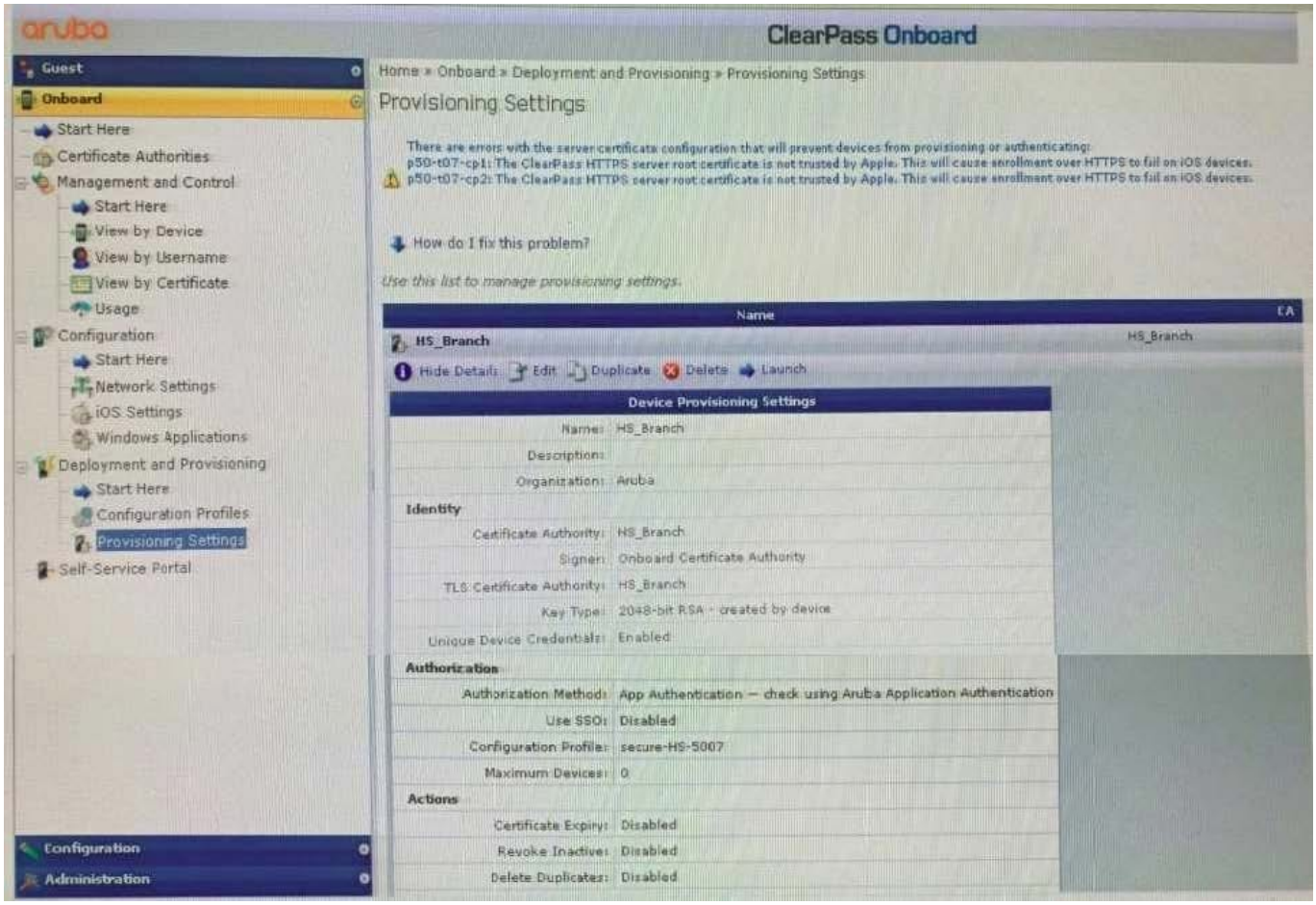
Refer to the exhibit:


QuickConnect by Aruba Networks, Inc.
aruba
NETWORKS
Welcome
Configure
Connect
Summary
Onboard Wizard
Configuring Your System
Your system has been successfully configured on the following interfaces:
• Wi-Fi
You may attempt to connect to the secure network "Secure-HS-5007" manually when network is available
Finish
Aruba


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]
2. [EAP PEAP]
Authentication Sources: 1. [Onboard Devices Repository]
2. AD1
3. AD2
Strip Username Rules: /:user
Service Certificate: -
Authorization:
Authorization Details: 1. AD1
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 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

HPE6-A81 PDF Dumps HPE6-A81 Study Guide HPE6-A81 Braindumps