# 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.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**

What is the Secure SSID {otherwise referred to as Single SSID) OnBoard deployment service workflow?

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

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

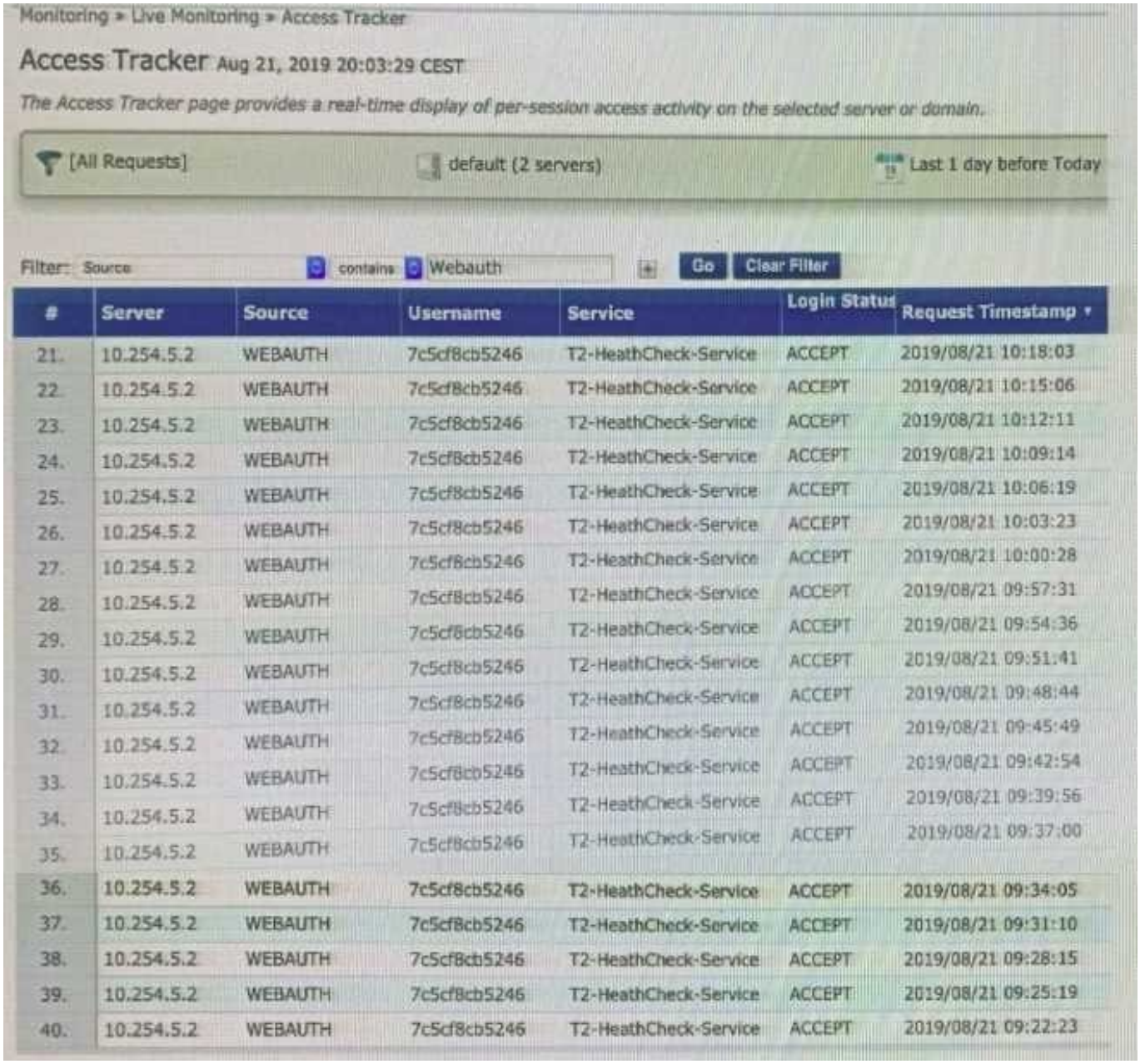
C. OnBoard Provisioning RADIUS service, OnBoard Pre-Auth Application service. OnBoard Authorization Application service, OnBoard Provisioning RADIUS service

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

Correct Answer: A

**QUESTION 2**

Refer to the exhibit:


Monitoring » Live Monitoring » Access Tracker

Access Tracker Aug 21, 2019 20:03:29 CEST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] default (2 servers) Last 1 day before Today

Filter: Source contains Webauth Go Clear Filter

| # | Server | Source | Username | Service | Login Status | Request Timestamp |
|---|---|---|---|---|---|---|
| 21. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 10:18:03 |
| 22. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 10:15:06 |
| 23. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 10:12:11 |
| 24. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 10:09:14 |
| 25. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 10:06:19 |
| 26. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 10:03:23 |
| 27. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 10:00:28 |
| 28. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:57:31 |
| 29. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:54:36 |
| 30. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:51:41 |
| 31. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:48:44 |
| 32. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:45:49 |
| 33. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:42:54 |
| 34. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:39:56 |
| 35. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:37:00 |
| 36. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:34:05 |
| 37. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:31:10 |
| 38. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:28:15 |
| 39. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:25:19 |
| 40. | 10.254.5.2 | WEBAUTH | 7c5cf8cb5246 | T2-HeathCheck-Service | ACCEPT | 2019/08/21 09:22:23 |

A customer has just configured a Posture Policy and the T2-Healthcheck Service. Next they installed the OnGuard Agent on Secure_Employee SSID. When they check Access Tracker they see many WEBAUTH requests are being triggered.

What could be the reason?

A. OnGuard Web-Based Health Check interval has been wrongly configured to three minutes.

B. The OnGuard Agent trigger the events based on changing the Health Status

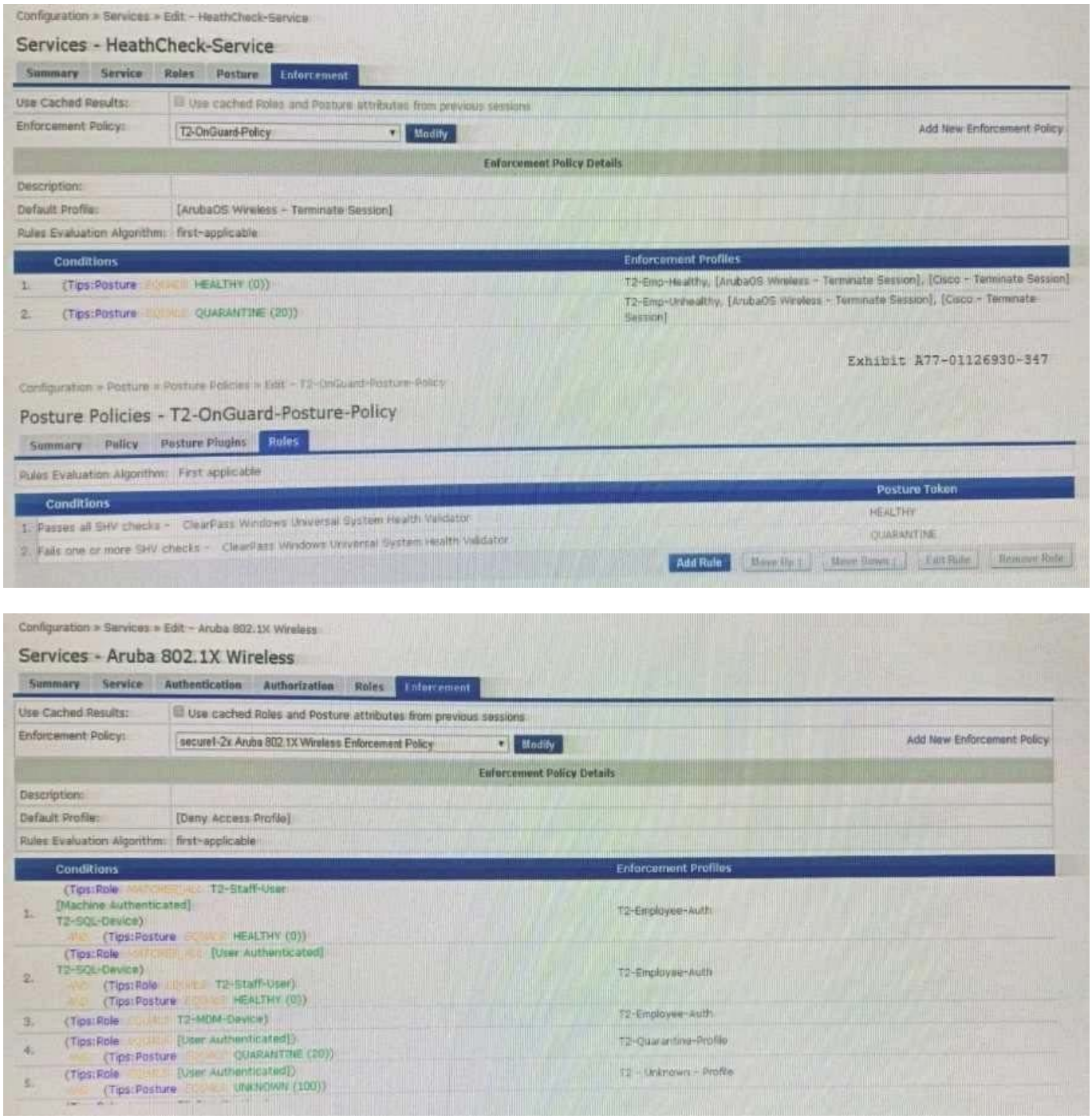
C. TCP port 6658 is not allowed between the client and the ClearPass server

D. The OnGuard Agent is connecting to the Data Port interface on ClearPass

Correct Answer: A

**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

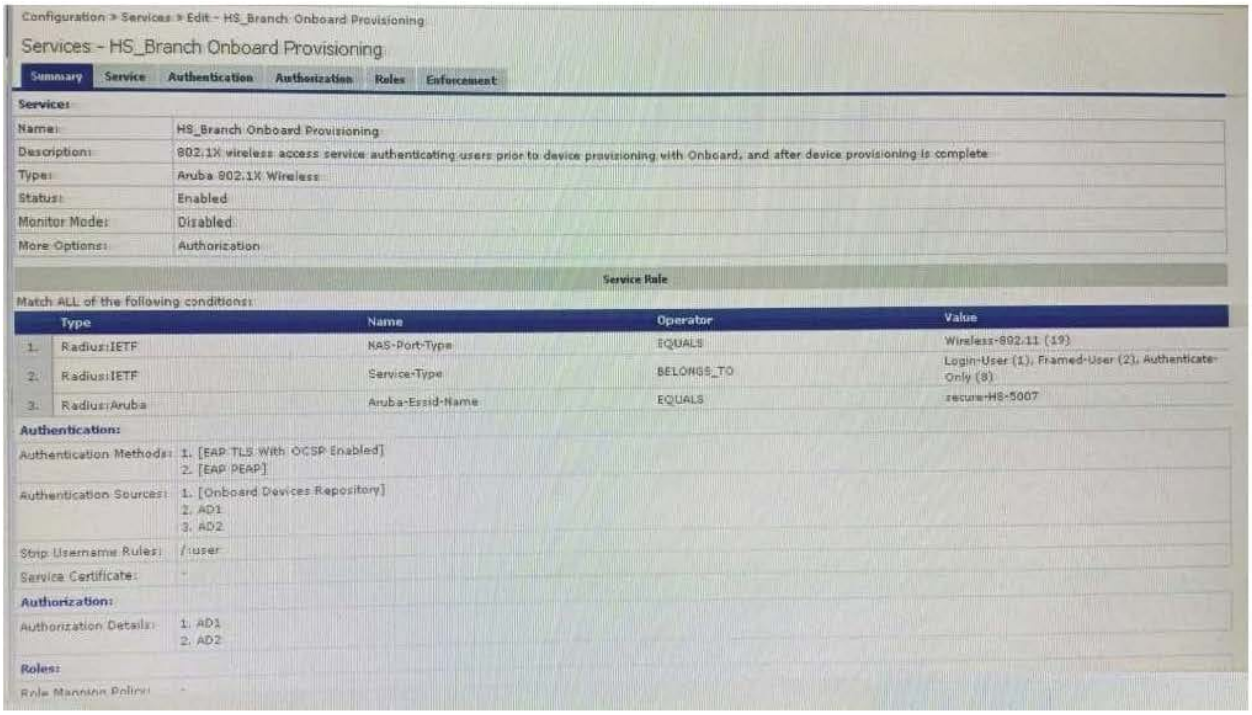
Correct Answer: B

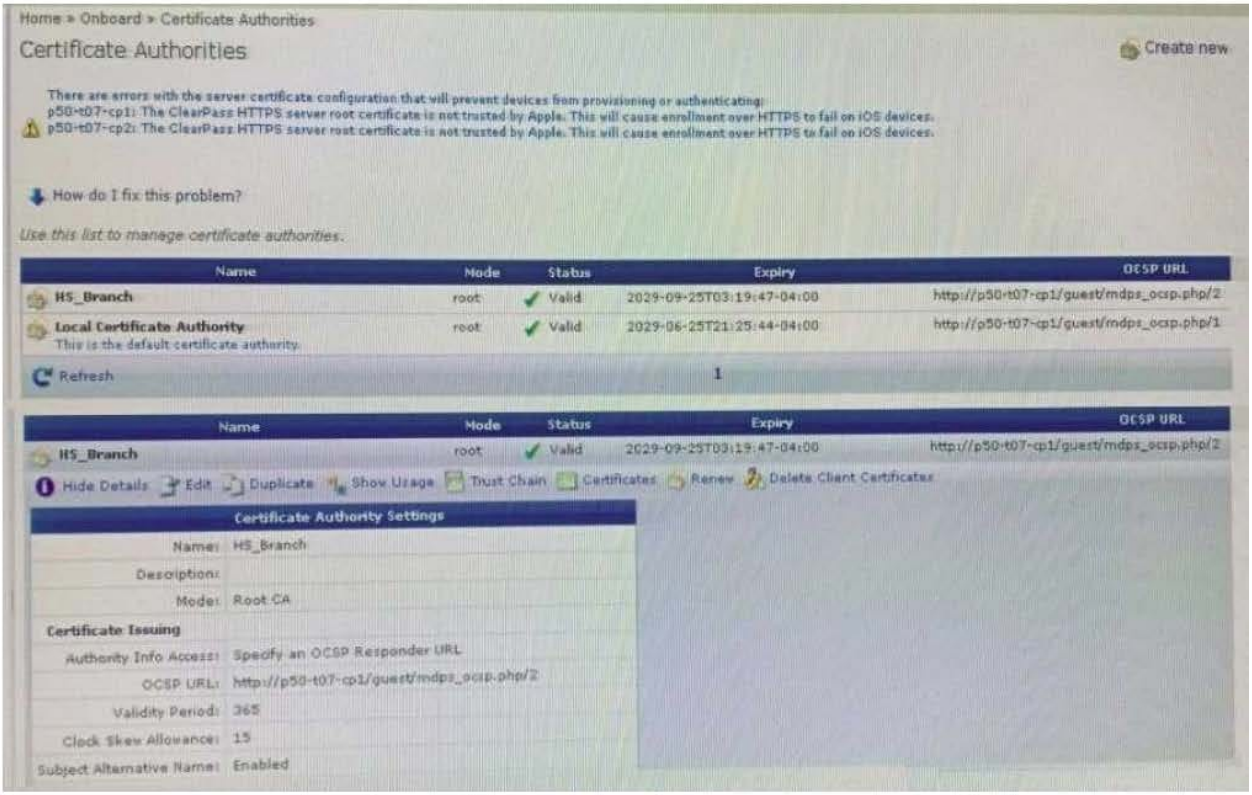
**QUESTION 4**

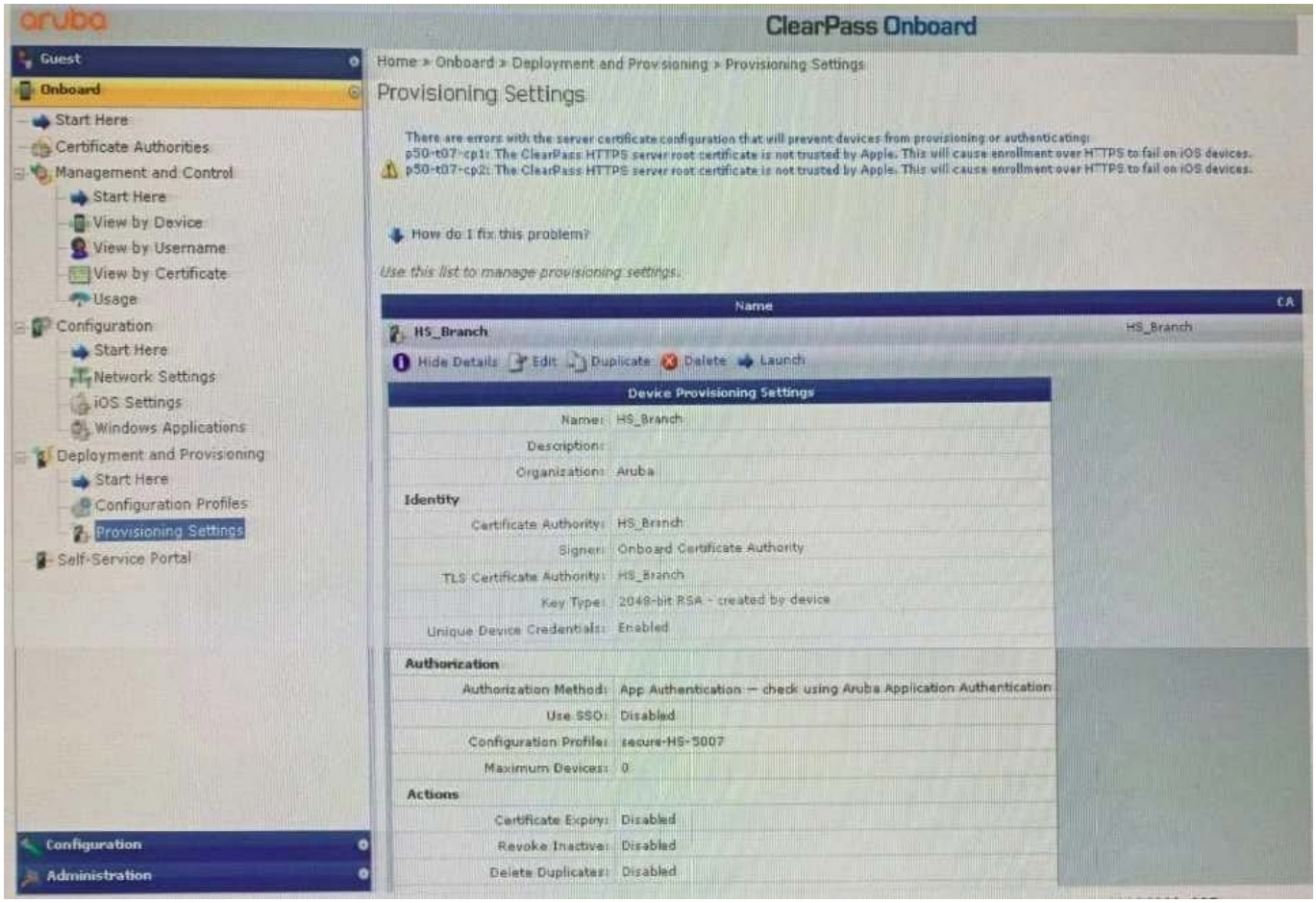
Refer to the exhibit:


QuickConnect by Aruba Networks, Inc.
aruba
NETWORKS
Onboard Wizard
Welcome
Configure
Connect
Summary
Securely Connect to Network
Authentication in progress ...
QuickConnect
Could not authenticate with wireless network
OK
Aruba


Request Details
Summary
Input
Output
Alerts
Login Status: REJECT
Session Identifier: R00000002-01-5d6b2731
Date and Time: Sep 25, 2019 04:37:06 EDT
End-Host Identifier: 78D294992613 (Computer / Windows / Windows 10)
Username: mike07
Access Device IP/Port: 10.1.70.100:0 (ArubaController / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: HS_Branch Onboard Provisioning
Authentication Method: EAP-TLS
Authentication Source: AD:AD1.aruba1.local
Authorization Source: AD1, AD2
Roles: -
Enforcement Profiles: [Allow Access Profile], HS_Branch Onboard Post-Provisioning
Service Monitor Mode: Disabled
Showing 1 of 1-7 records
Show Configuration
Export
Show Logs
Close
Request Details
Summary
Input
Output
Alerts
Error Code: 215
Error Category: Authentication failure
Error Message: TLS session error
Alerts for this Request
RADIUS Certificate Status unknown. Reason (UNKNOWN)
EAP-TLS: fatal alert by server - (internal_error
TLS Handshake failed in SSL_read with error:14089086:SSL
routines:ssl3_get_client_certificate:certificate verify failed
eap-tls: Error in establishing TLS session


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. [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:


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 root Valid 2029-06-25T21:25:44-04:00 http://p50-t07-cp1/guest/mdps_ocsp.php/1
This is the default certificate authority.
Refresh
1
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
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




You have configured Onboard and cannot get it working The customer has sent you the above

screenshots.

How would you resolve the issue?

A. Re-provision the client by running the QuickConnect application as Administrator

B. Install a public signed server authentication certificate on the ClearPass server for EAP

C. Reconnect the client and select the correct certificate when prompted

D. Copy the [EAP-TLS with OSCP Enabled] authentication method and set the correct OCSP URL

Correct Answer: A

**QUESTION 5**

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