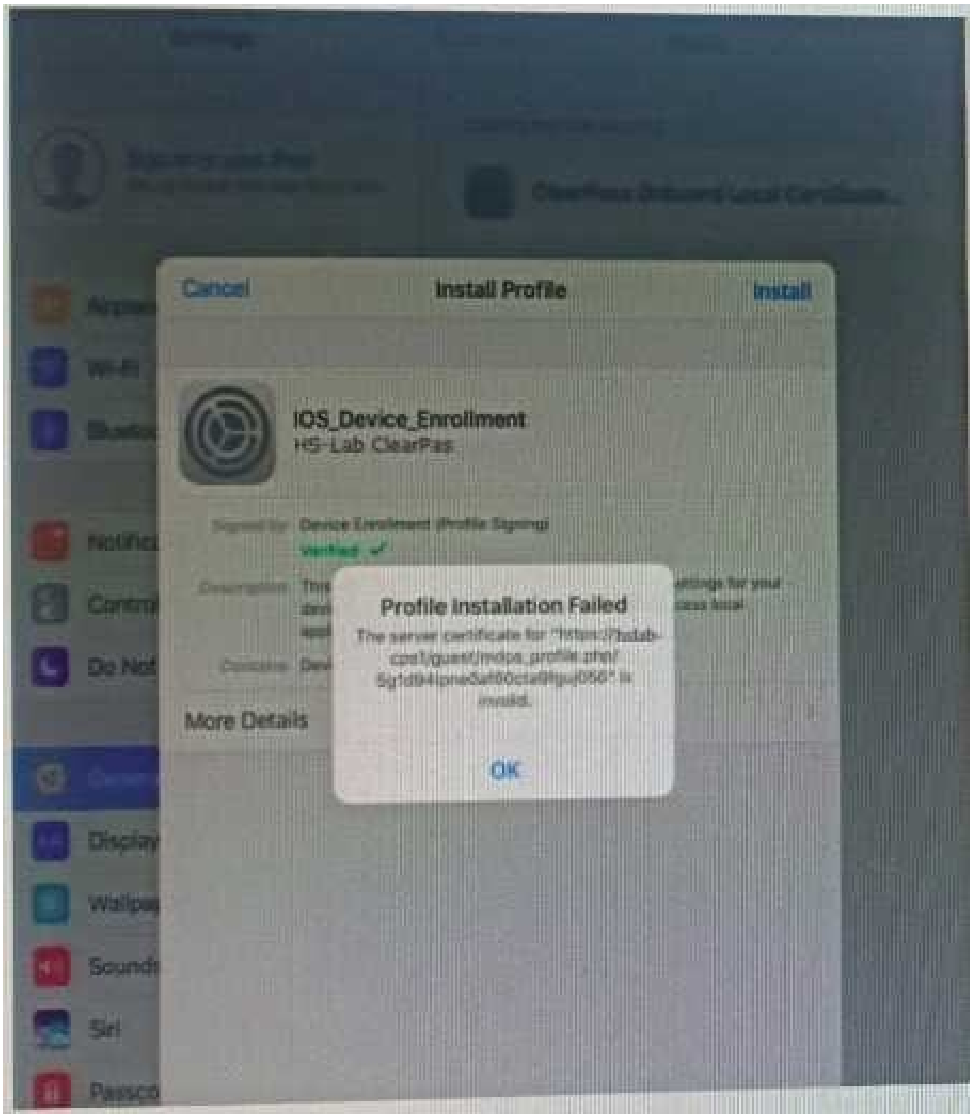
HPE6-A81$^{Q\&As}$

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

QUESTION 1

Refer to the exhibit:



Profile Installation Failed

The server certificate for "https://hslab-cps1/guest/mdps_profile.php/5g1d94lpne0af00cta9fgu056" is invalid.

A customer has configured Onboard and Windows devices work as expected but cannot get the Apple iOS devices to Onboard successfully. Where would you look to troubleshoot the Issued (Select two)

A. Check if the ClearPass HTTPS server certificate installed in the server is issued by a trusted commercial certificate authority.

B. Check if the customer installed the internal PKI Root certificate presented by the ClearPass during the provisioning process.

C. Check if a DNS entry is available for the ClearPass hostname in the certificate, resolvable from the DNS server assigned to the client.

D. Check if the customer has Instated a custom HTTPS certificate for IDS and another internal PKI HTTPS certificate for other devices.

E. Check if the customer has installed the same internal PKI signed RADIUS server certificate as the HTTPS server certificate.

Correct Answer: AC

QUESTION 2

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 3

Where is the following information stored in ClearPass?

1.

Roles and Posture for Connected Clients

2.

System Health for OnGuard

3.

Machine authentication State

4.

CoA session info

5.

Mapping of connected clients to NAS/NAD

A. Multi-Master cache

B. Endpoint database

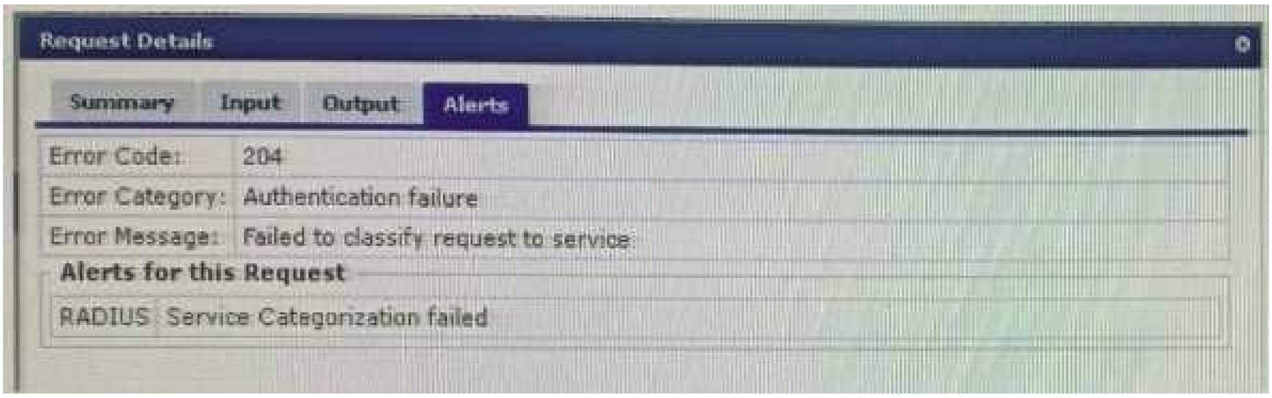
C. insight database

D. ClearPass system cache

Correct Answer: D

QUESTION 4

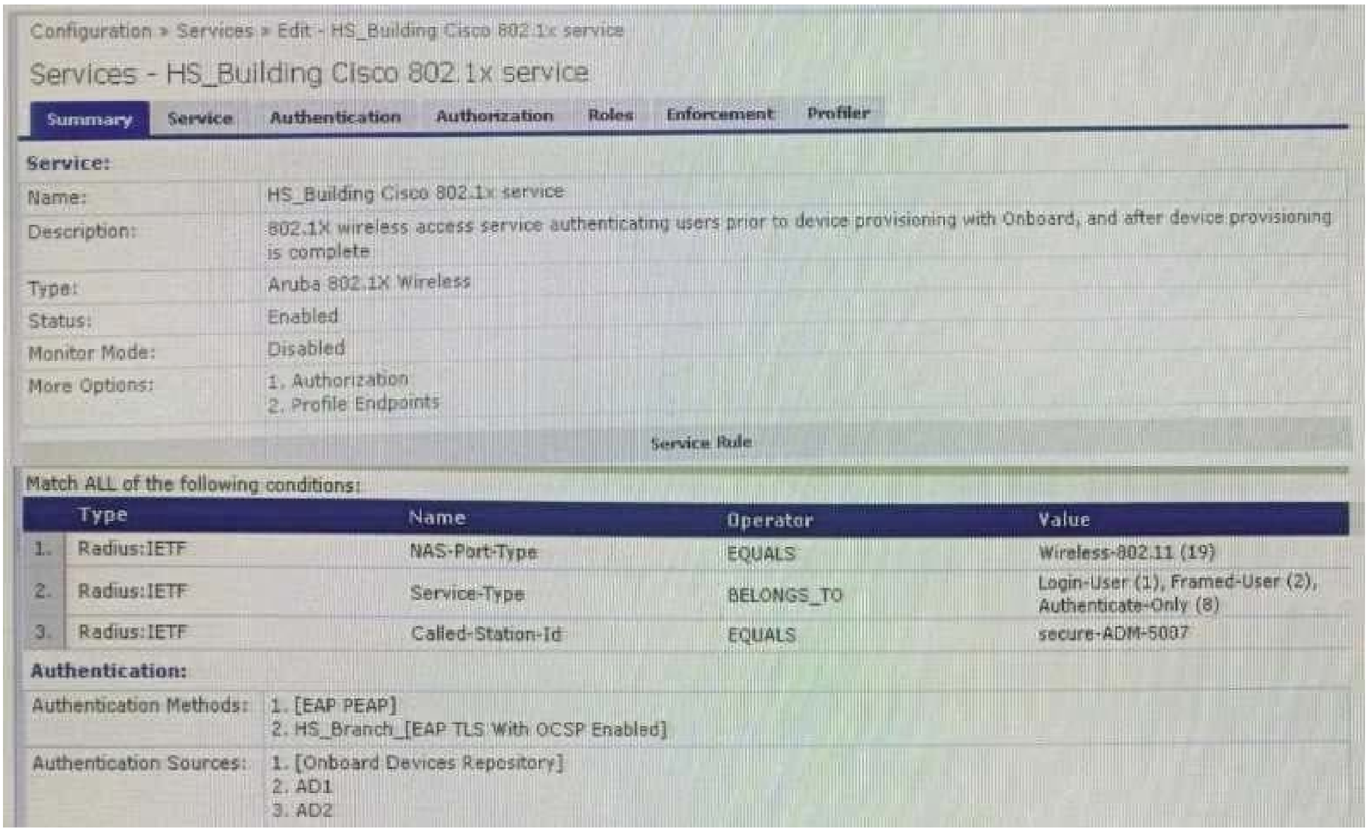
Refer to the exhibit: You configured a new Wireless 802.1X service for a Cisco WLC broadcasting the Secure-ADM-5007 SSID. The client falls to connect to the SSID. Using the screenshots as a reference, how would you fix this issue? (Select two.)



Error Code:	204
Error Category:	Authentication failure
Error Message:	Failed to classify request to service

Alerts for this Request

RADIUS Service Categorization failed


Configuration » Services » Edit - HS_Building Cisco 802.1x service
Summary
Service
Authentication
Authorization
Roles
Enforcement
Profiler

Services - HS_Building Cisco 802.1x service

Service:

Name:	HS_Building Cisco 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:	1. Authorization 2. Profile Endpoints

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:IETF	Called-Station-Id	EQUALS	secure-ADM-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

A. Update the service condition Radius:IETF Called-Station-ld CONTAINS secure-adm-5007

B. Make sure that the Network Devices entry for the Cisco WLC has a vendor setting of "Airspace"

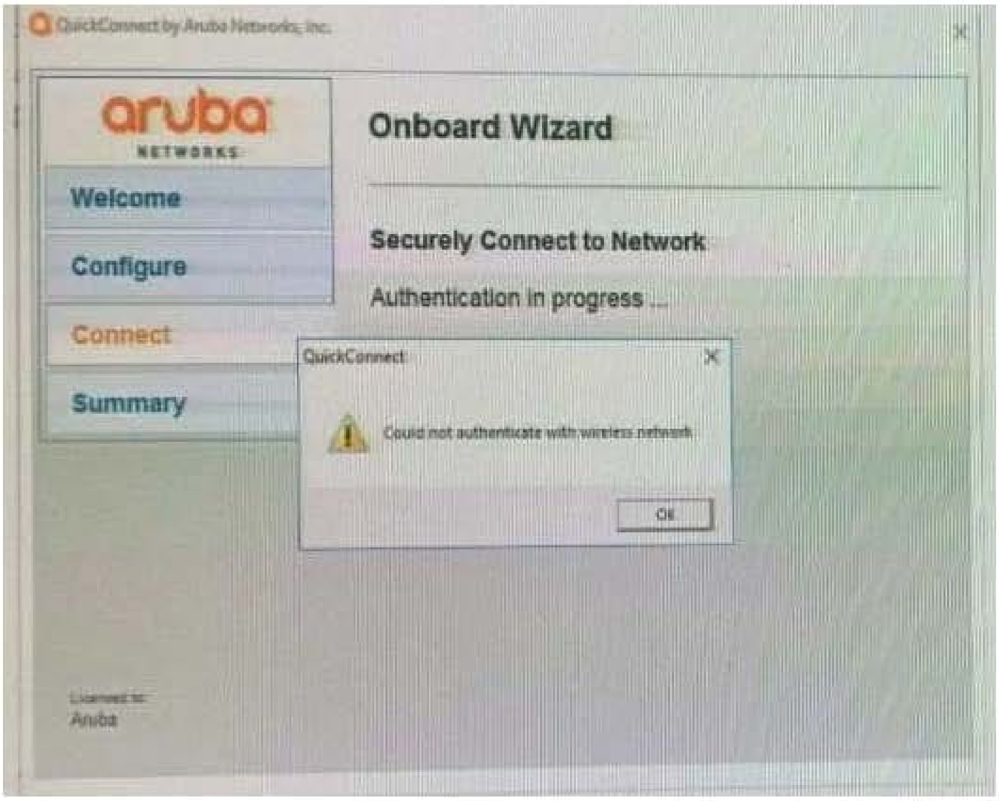
C. Remove the service condition Radius:lETF Service-Type BELONGSJTO Login-User (1). 2. 8

D. Change the service condition to Radius:lETF Calling-Station-ld EQUALS Secure-ADM-5007

Correct Answer: AC

QUESTION 5

Refer to the exhibit:

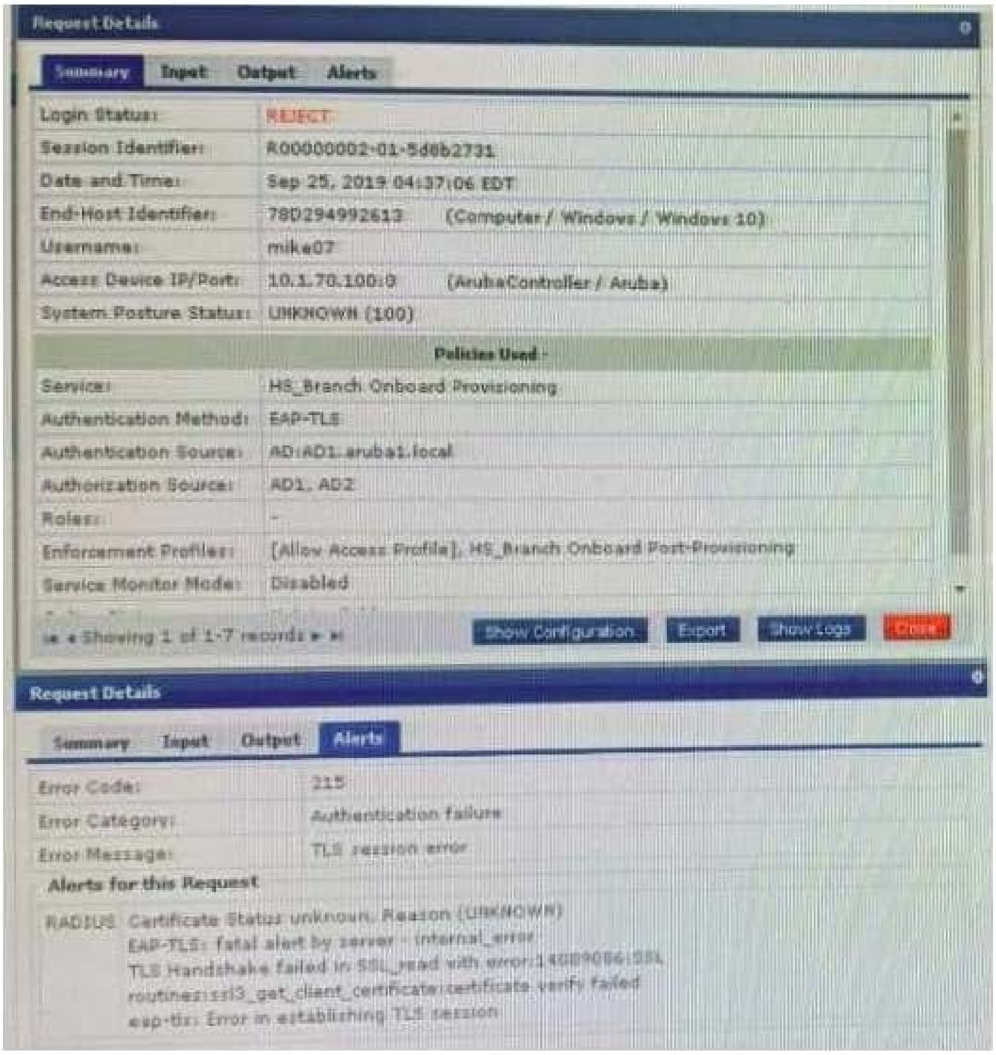


Onboard Wizard

Securely Connect to Network

Authentication in progress ...

Could not authenticate with wireless network

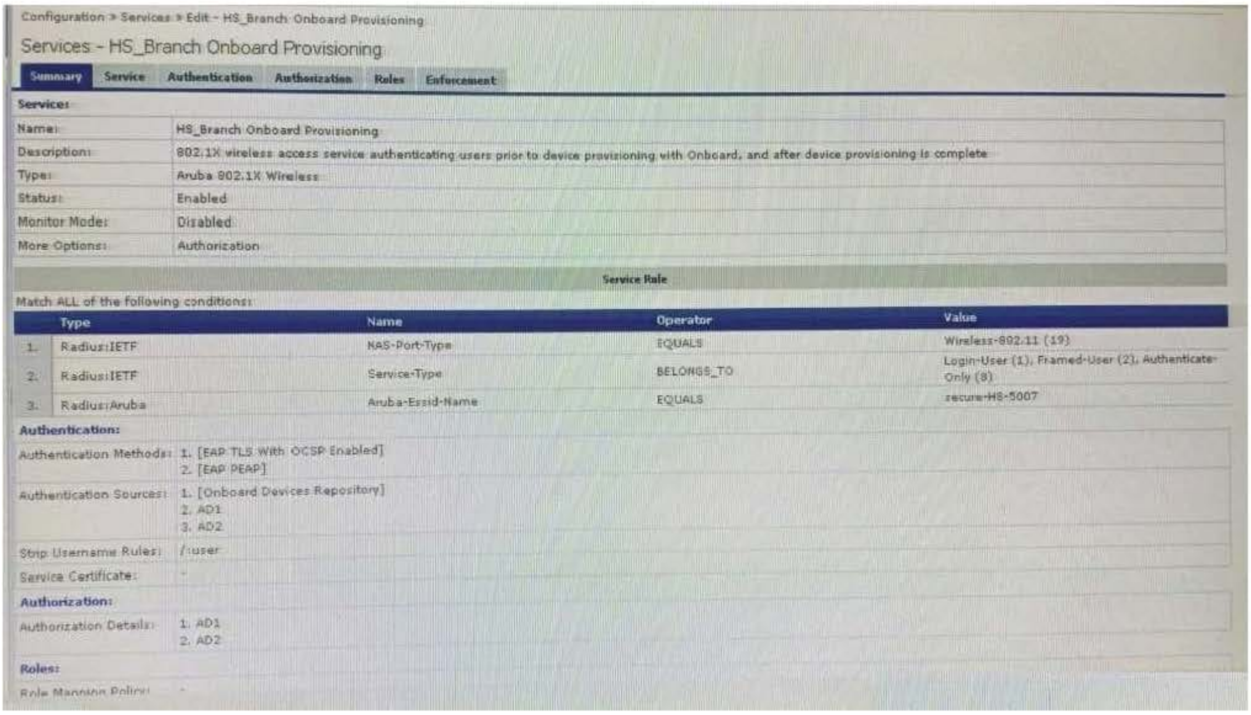


Login Status:	REJECT
Session Identifier:	R00000002-01-5d8b2731
Date and Time:	Sep 25, 2019 04:37:06 EDT
End-Host Identifier:	78D294992613 (Computer / Windows / Windows 10)
Username:	mike07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
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

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

Services:

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:

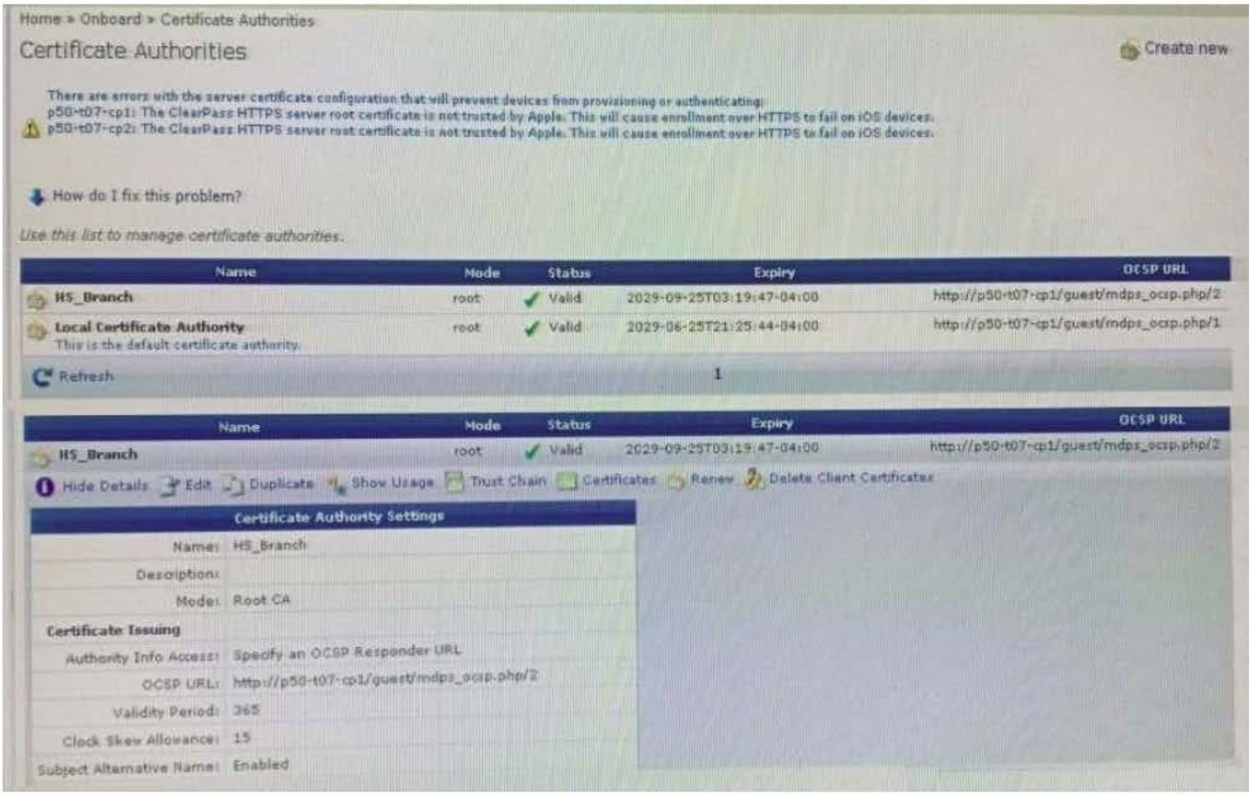
Authentication Methods:	1. [EAP TLS With OCSP Enabled] 2. [EAP PEAP]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2
Strip Username Rules:	/:user
Service Certificate:	-

Authorization:

Authorization Details:	1. AD1 2. AD2

Roles:

Role Mapping Policy: -



Home » Onboard » Certificate Authorities

Certificate Authorities

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.

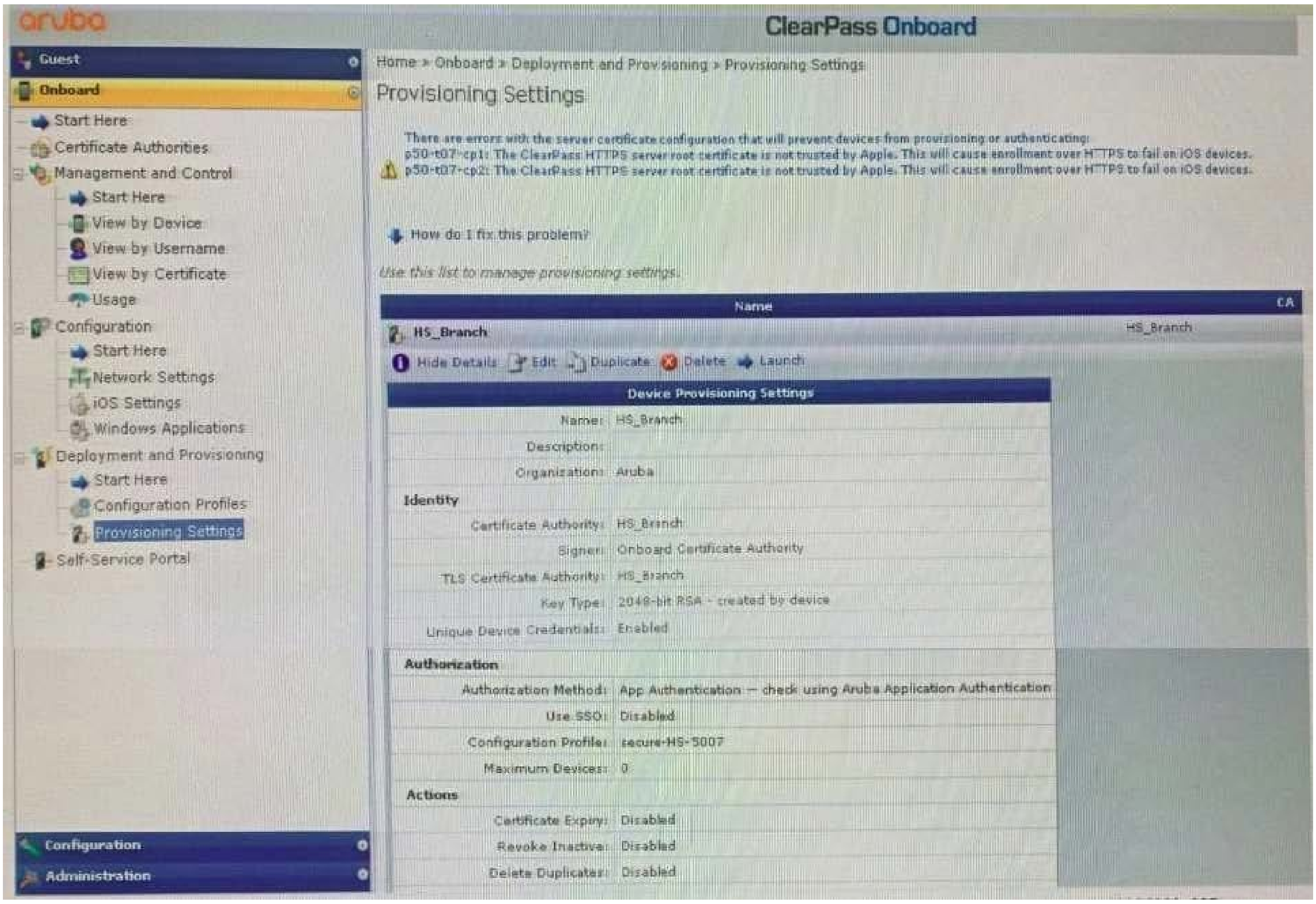
How do I fix this problem?

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

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

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



Provisioning Settings

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 provisioning settings.

Name	CA
HS_Branch	HS_Branch

Device Provisioning Settings

Name:	HS_Branch
Description:	
Organization:	Aruba
Identity	
Certificate Authority:	HS_Branch
Signer:	Onboard Certificate Authority
TLS Certificate Authority:	HS_Branch
Key Type:	2048-bit RSA - created by device
Unique Device Credentials:	Enabled
Authorization	
Authorization Method:	App Authentication — check using Aruba Application Authentication
Use SSO:	Disabled
Configuration Profile:	secure-HS-5007
Maximum Devices:	0
Actions	
Certificate Expiry:	Disabled
Revoke Inactive:	Disabled
Delete Duplicates:	Disabled

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

HPE6-A81 PDF Dumps HPE6-A81 Practice Test HPE6-A81 Study Guide