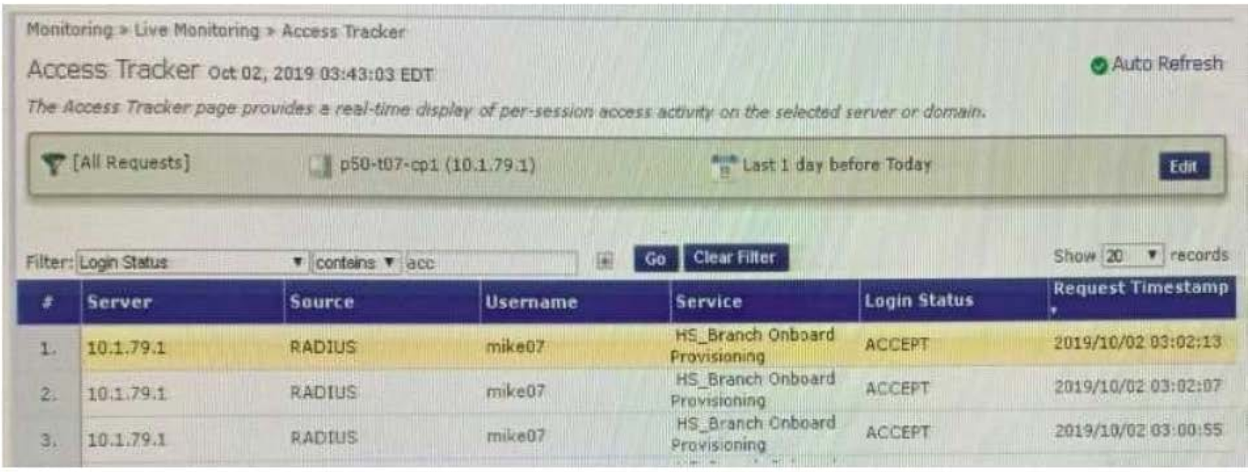
HPE6-A81$^{\text{Q\&As}}$

Aruba Certified ClearPass Expert Written Exam

QUESTION 1

Refer to the exhibit:



Access Tracker Oct 02, 2019 03:43:03 EDT

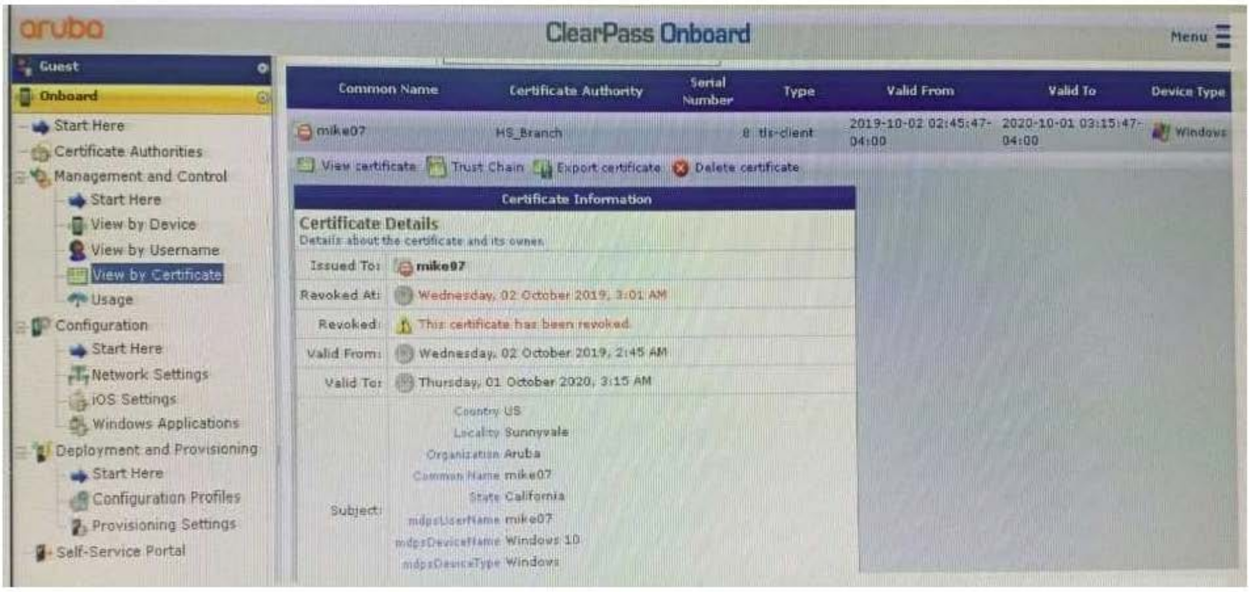
The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] p50-t07-cp1 (10.1.79.1) Last 1 day before Today

Filter: Login Status contains acc

Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:02:13
2.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:02:07
3.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:00:55



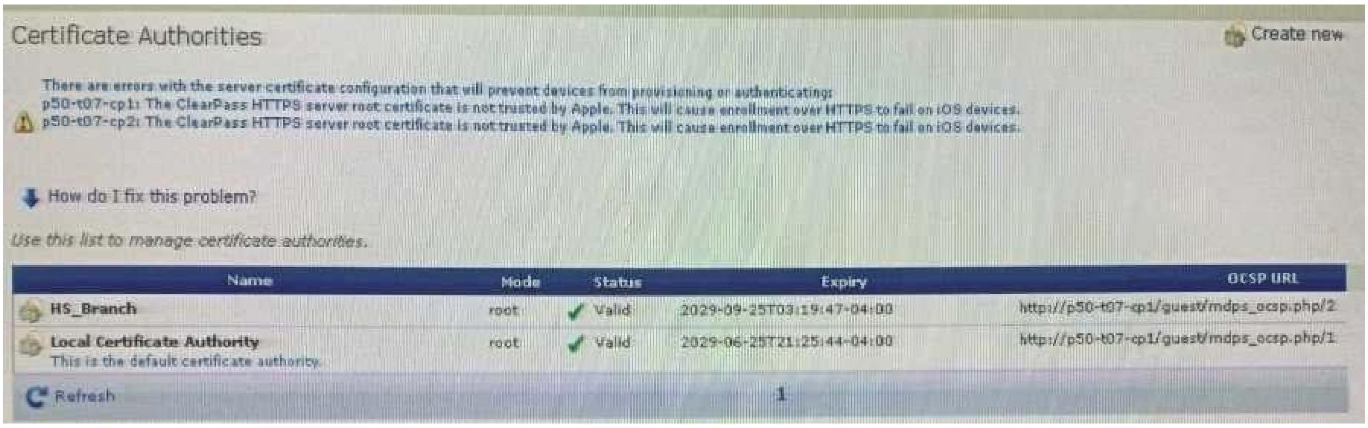
Common Name	Certificate Authority	Serial Number	Type	Valid From	Valid To	Device Type
mike07	HS_Branch	8	tls-client	2019-10-02 02:45:47-04:00	2020-10-01 03:15:47-04:00	Windows

Certificate Information

Certificate Details

Details about the certificate and its owner.

Issued To:	mike07
Revoked At:	Wednesday, 02 October 2019, 3:01 AM
Revoked:	This certificate has been revoked
Valid From:	Wednesday, 02 October 2019, 2:45 AM
Valid To:	Thursday, 01 October 2020, 3:15 AM
Subject:	Country US Locality Sunnyvale Organization Aruba Common Name mike07 State California mdpsUserName mike07 mdpsDeviceName Windows 10 mdpsDeviceType Windows



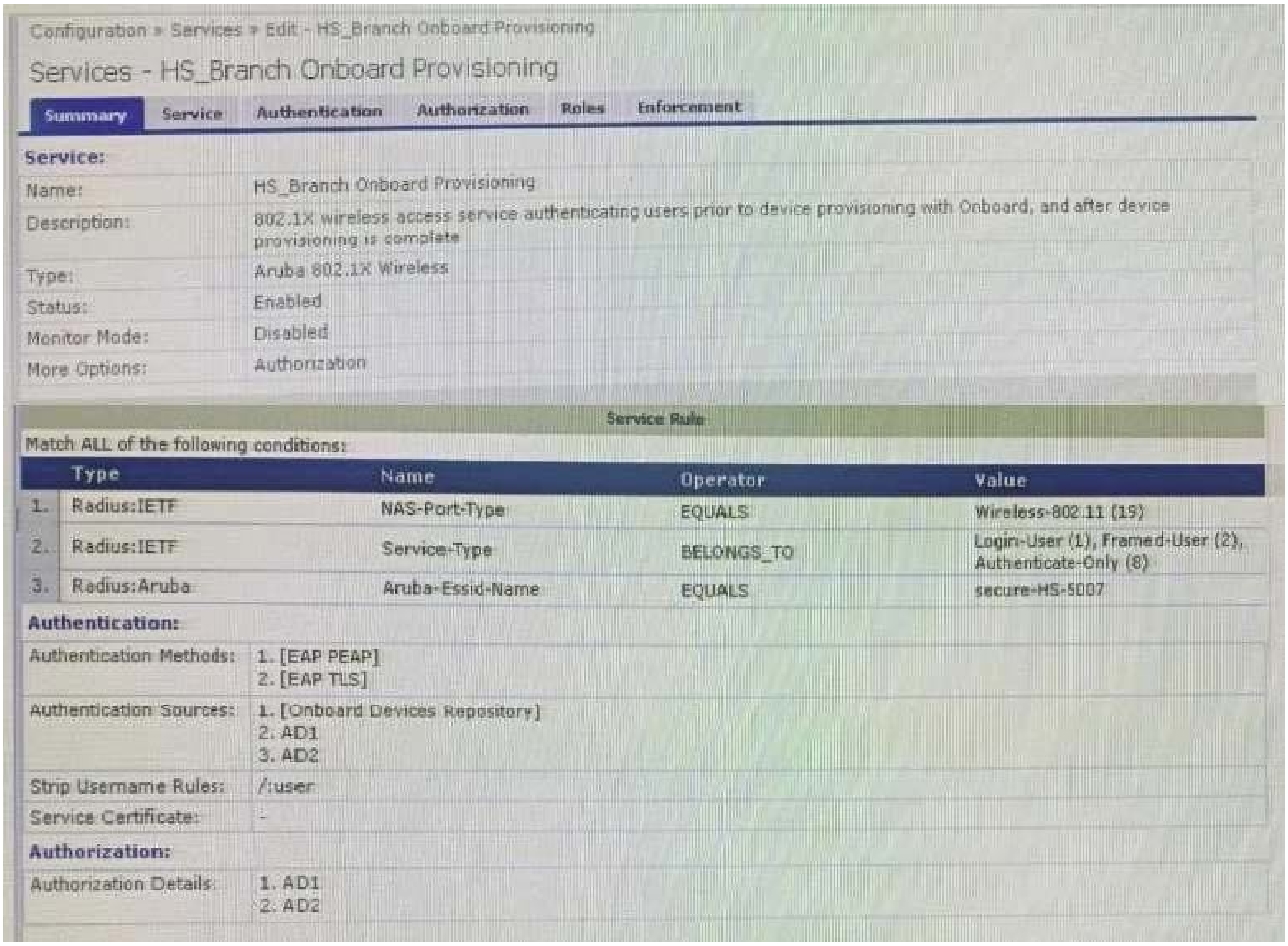
Certificate Authorities

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



Configuration » Services » Edit - HS_Branch Onboard Provisioning

Services - HS_Branch Onboard Provisioning

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

Authorization:

Authorization Details:	1. AD1 2. AD2

After the helpdesk revoked the certificate of a device reported to be lost oy an employee, the lost device

was seen as connected successfully to the secure network. Further testing has shown that device

revocation is not working.

What steps should you follow to make device revocations work?

A. Copy the default [EAP-TLS with OSCP Enabled] authentication method and set The Verify certificate using OSCP option as required then update the correct OSCP URL link of the OnBoard CA. Remove EAP-TLS and map the custom created method to the OnBoard Authorization Service.

B. copy the default [EAP-TLS with OSCP Enabled] authentication method and set the verify certificate using OSCP: option as "required" then configure the correct OSCF URL link for the OnBoard CA. Remove EAP-TLS and map the new [EAP-TLS with OSCP Enabled] method to the 802 1X Radius Service.

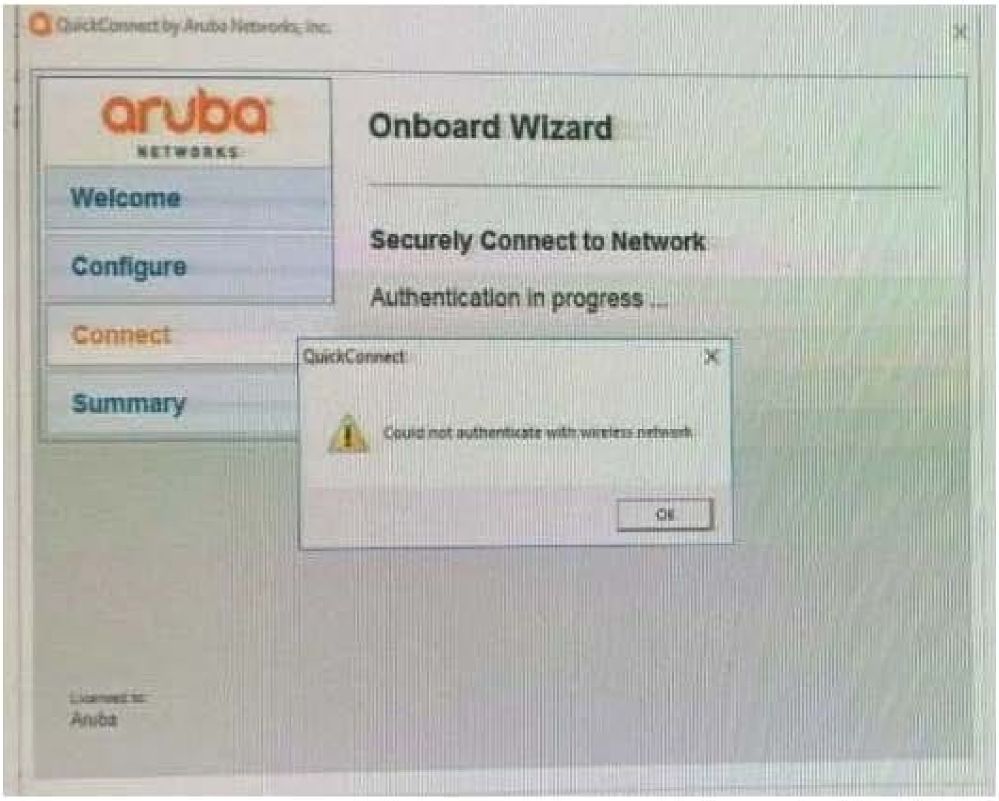
C. Remove the EAP-TLS authentication method configuration changes are required and add "EAP-TLS with OCSP Enabled" authentication method in the OnBoard Provisioning service. No other configuration changes are required.

D. Edit the default [EAP-TLS with OSCP Enabled] authentication method and set the Verify certificate using OSCP option as required then update the correct OSCP URL link of the OnBoard CA Remove EAP-TLS and map the new [EAP-TLS with OSCP Enabled] method to the OnBoard Provisioning Service.

Correct Answer: C

QUESTION 2

Refer to the exhibit:



QuickConnect by Aruba Networks, Inc.

Onboard Wizard

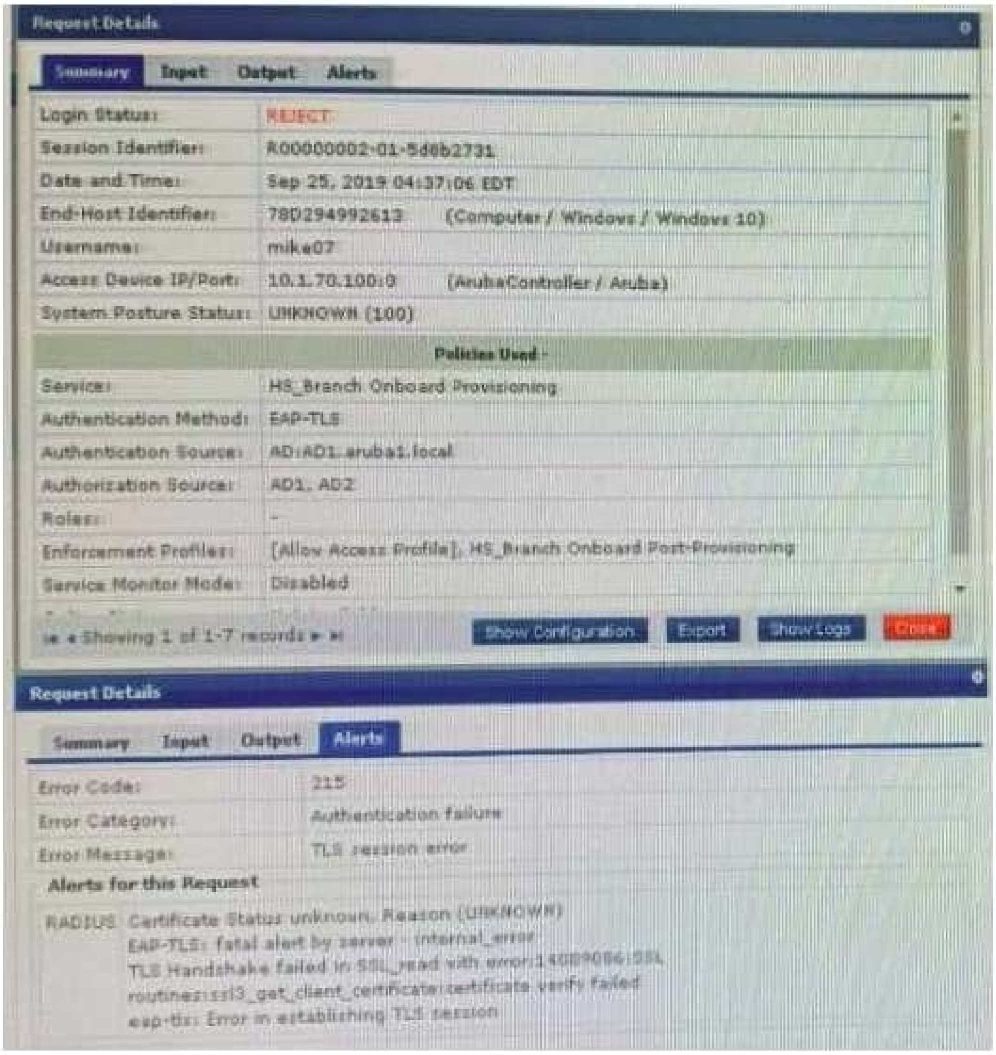
Securely Connect to Network

Authentication in progress ...

QuickConnect

Could not authenticate with wireless network

Licensed to:
Aruba

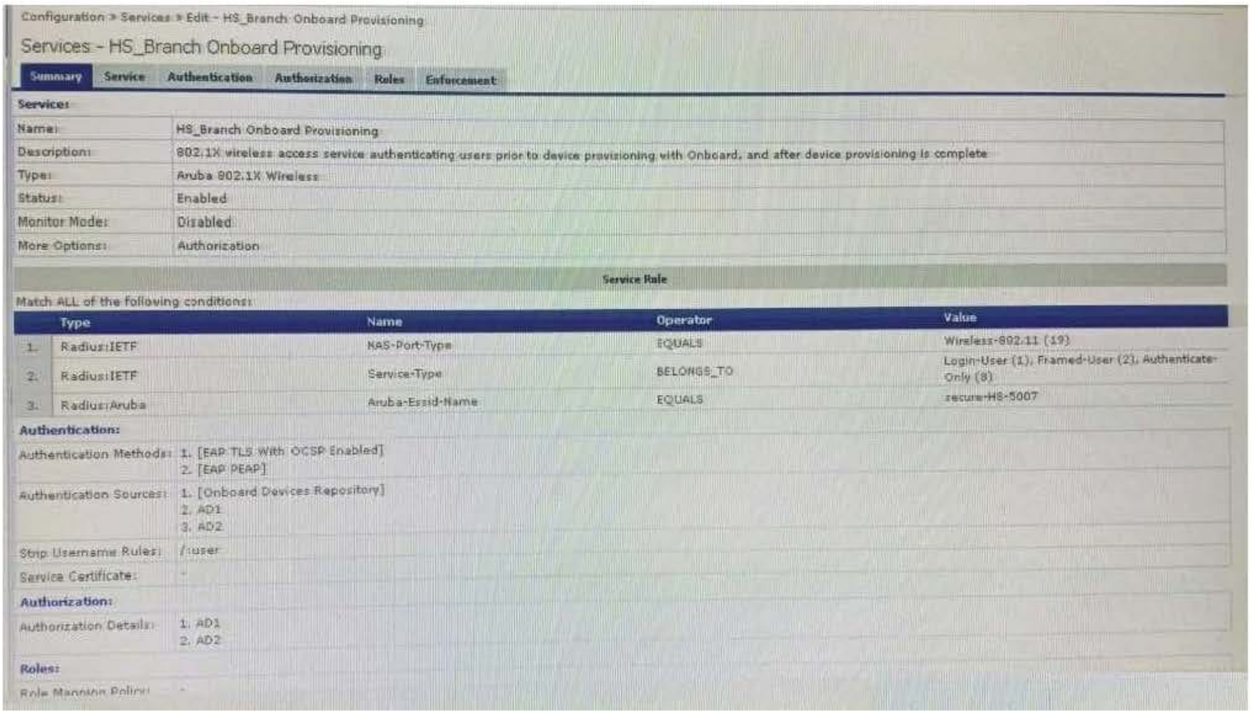


Login Status:	REJECT
Session Identifier:	R00000002-01-5d8b2731
Date and Time:	Sep 25, 2019 04:37:06 EDT
End-Host Identifier:	78D294992613 (Computer / Windows / Windows 10)
Username:	mike07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used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

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:

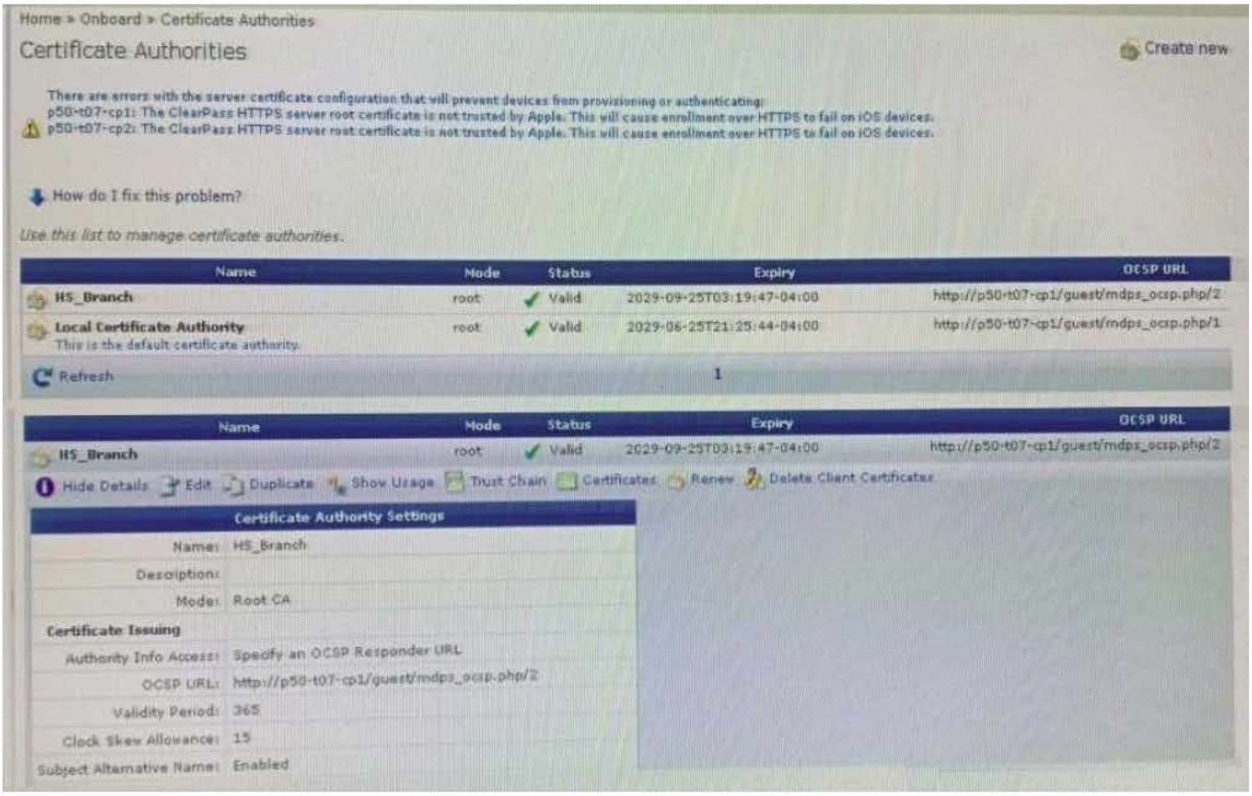
Authentication Methods:	1. [EAP TLS With OCSP Enabled] 2. [EAP PEAP]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2
Strip Username Rules:	/:user
Service Certificate:	-

Authorization:

Authorization Details:	1. AD1 2. AD2

Roles:

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?

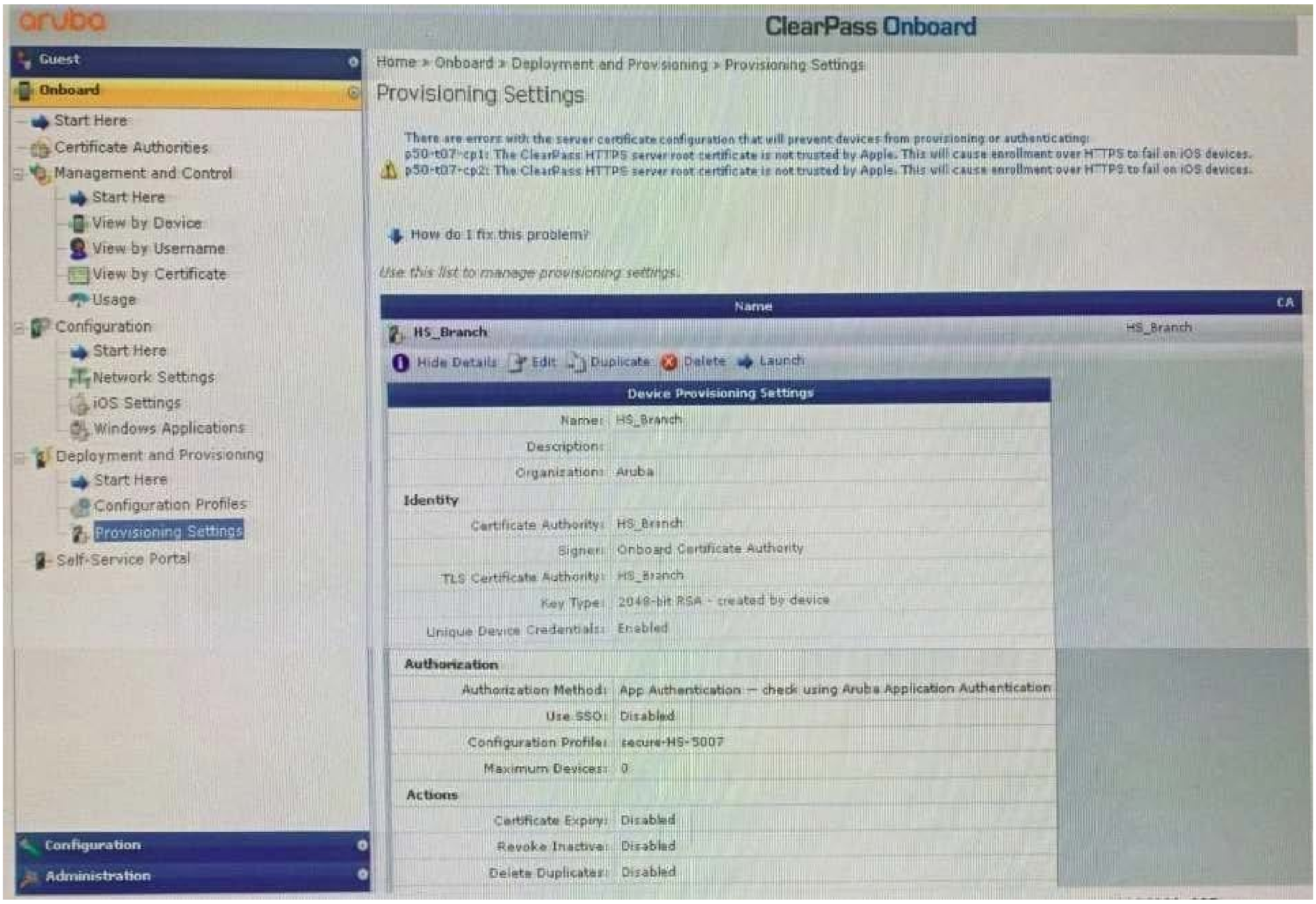
Use this list to manage certificate authorities.

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

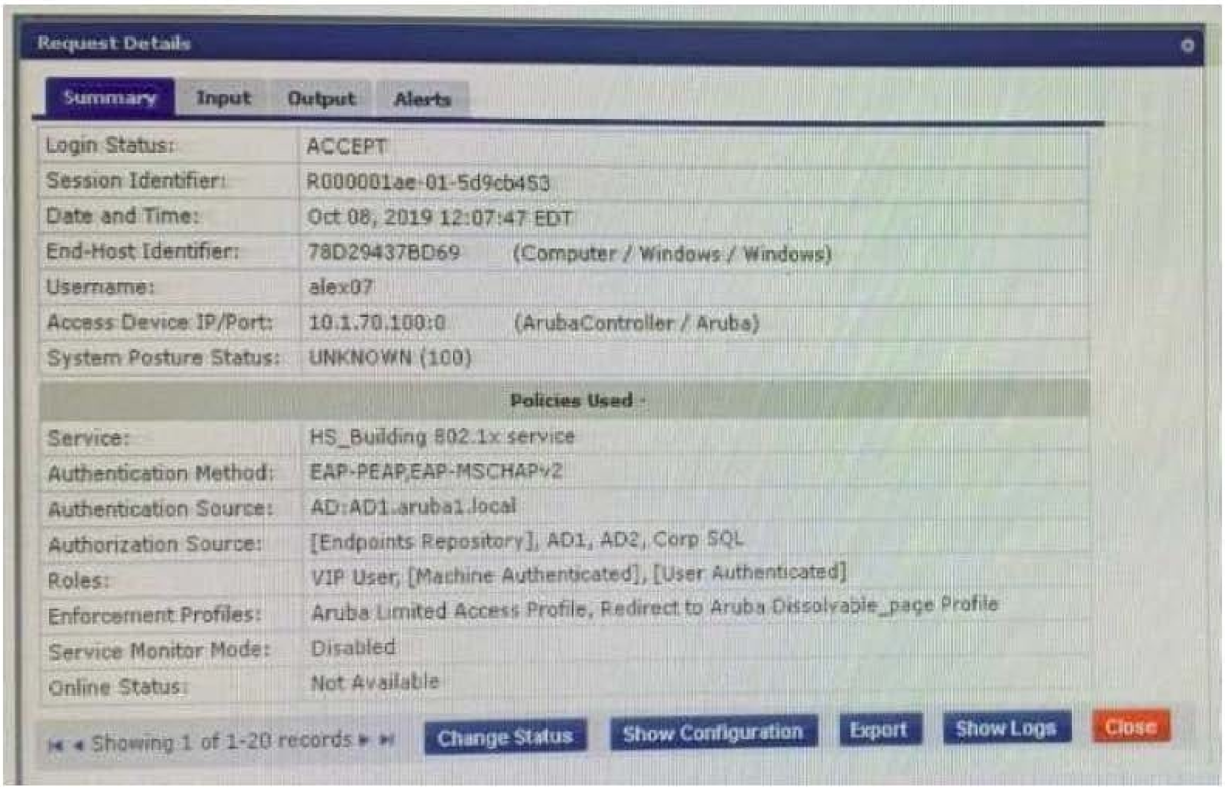
C. Reconnect the client and select the correct certificate when prompted

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

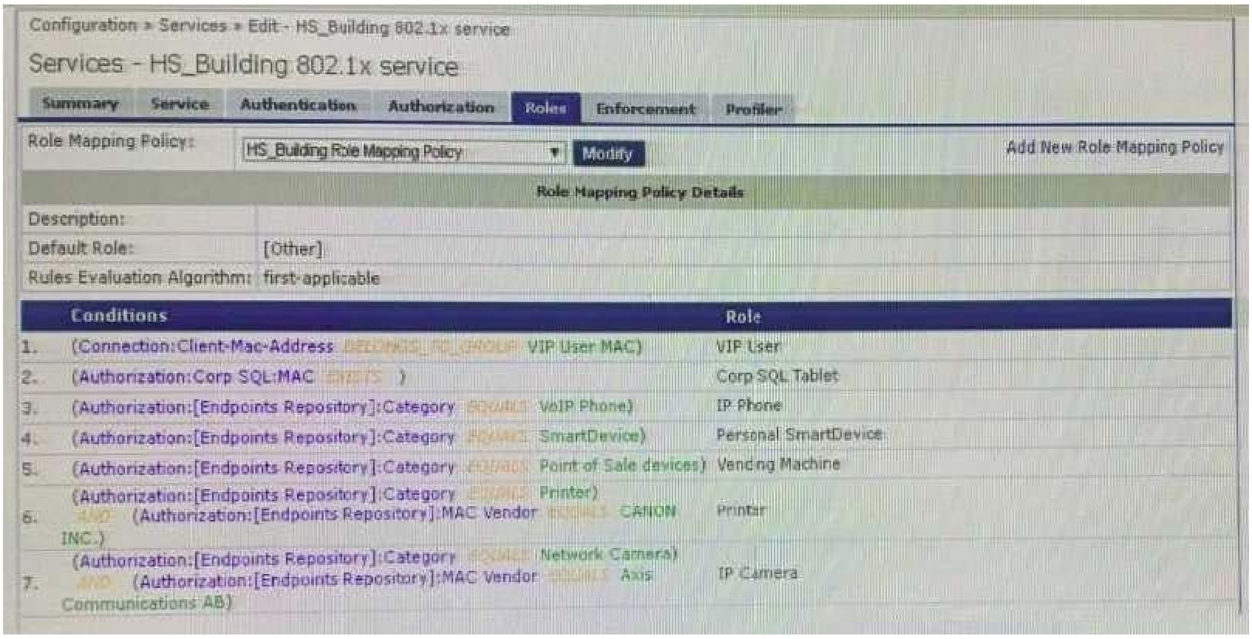
Correct Answer: A

QUESTION 3

Refer to the exhibit:



Login Status:	ACCEPT
Session Identifier:	R000001ae-01-5d9cb453
Date and Time:	Oct 08, 2019 12:07:47 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	HS_Building 802.1x service
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	[Endpoints Repository], AD1, AD2, Corp SQL
Roles:	VIP User, [Machine Authenticated], [User Authenticated]
Enforcement Profiles:	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
Service Monitor Mode:	Disabled
Online Status:	Not Available


Configuration » Services » Edit - HS_Building 802.1x service
Summary
Service
Authentication
Authorization
Roles
Enforcement
Profiler
Modify
Add New Role Mapping Policy

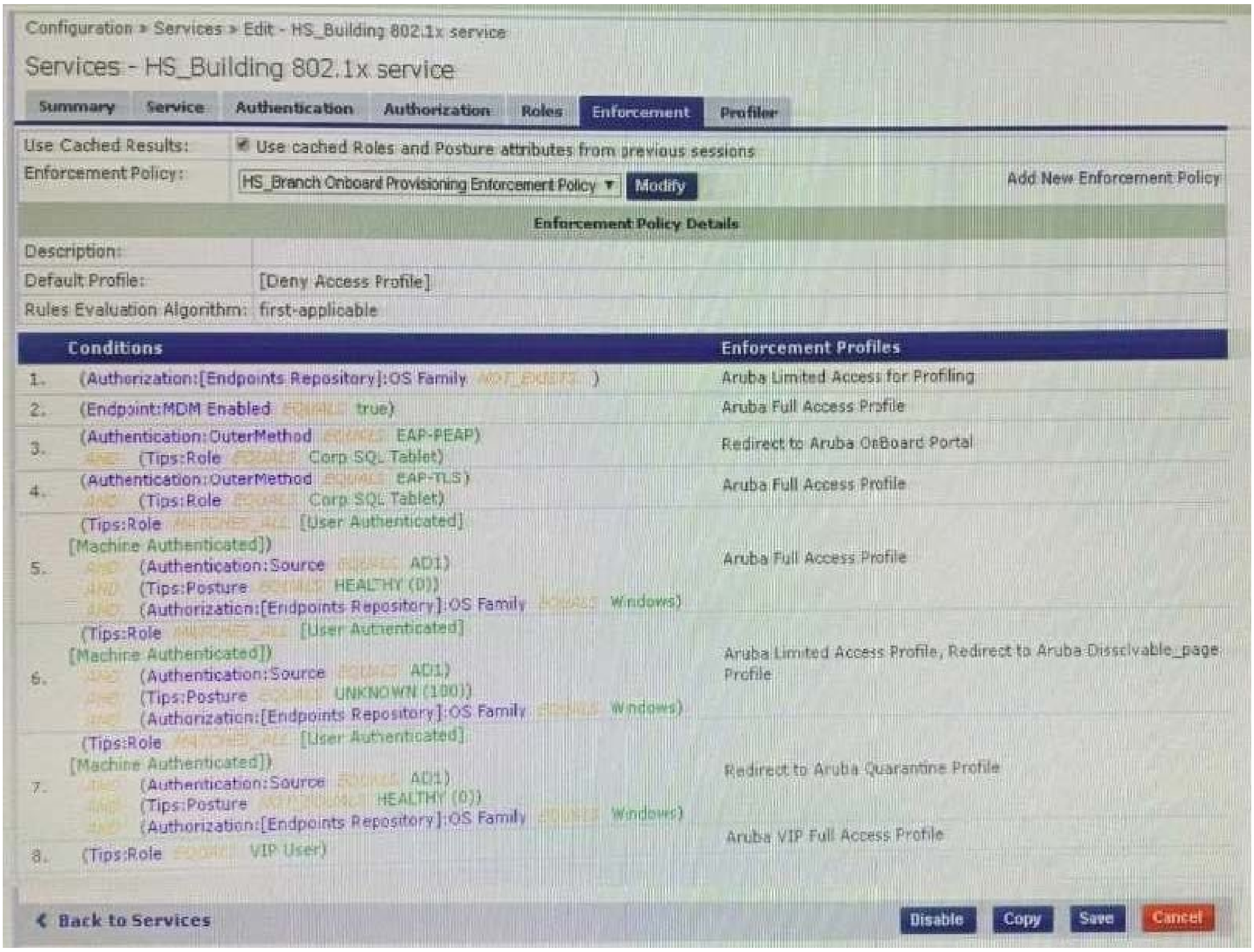
Services - HS_Building 802.1x service

Role Mapping Policy: HS_Building Role Mapping Policy

Role Mapping Policy Details

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
1.	(Connection:Client-Mac-Address BELONGS_TO_GROUP VIP User MAC)	VIP User
2.	(Authorization:Corp SQL:MAC EXISTS)	Corp SQL Tablet
3.	(Authorization:[Endpoints Repository]:Category EQUALS VoIP Phone)	IP Phone
4.	(Authorization:[Endpoints Repository]:Category EQUALS SmartDevice)	Personal SmartDevice
5.	(Authorization:[Endpoints Repository]:Category EQUALS Point of Sale devices)	Vending Machine
6.	(Authorization:[Endpoints Repository]:Category EQUALS Printer) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS CANON INC.)	Printer
7.	(Authorization:[Endpoints Repository]:Category EQUALS Network Camera) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS Axis Communications AB)	IP Camera



Services - HS_Building 802.1x service

Use Cached Results:	☑ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	HS_Branch Onboard Provisioning Enforcement Policy ▾ Modify

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:OS Family NOT_EXISTS)	Aruba Limited Access for Profiling
2.	(Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
3.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
4.	(Authentication:OuterMethod EQUALS EAP-TLS) AND (Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
5.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Aruba Full Access Profile
6.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture NOT_EQUALS HEALTHY (0)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Redirect to Aruba Quarantine Profile
8.	(Tips:Role EQUALS VIP User)	Aruba VIP Full Access Profile

The customer created a new enforcement policy condition to allow VIP Users access without additional security compliance checks hut cannot gel it working. The customer has sent you the above screenshots. How would you resolve the issue?

A. Ask the VIP user to complete the one time web health check to get the VIP profile.

B. Set the Enforcement Policy rules evaluation algorithm to evaluate all.

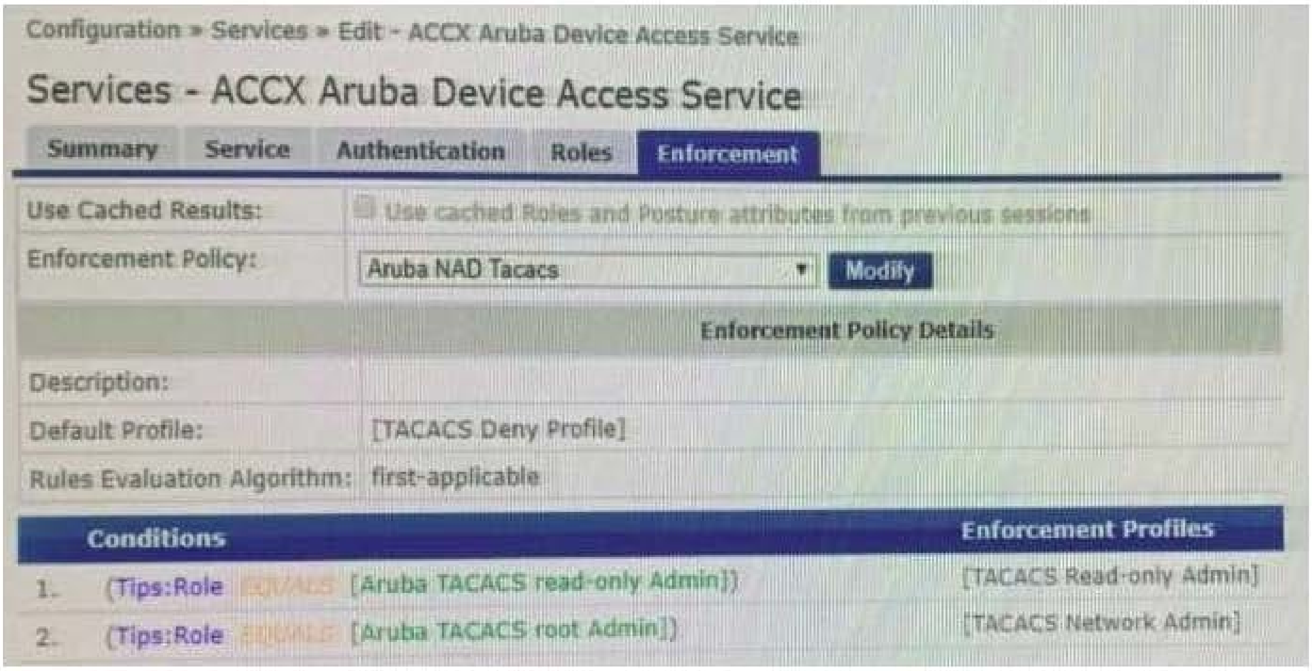
C. Include VIP User role along with the Healthy posture enforcement condition.

D. Modify the Enforcement Policy and re-order the VIP user condition to the lop.

Correct Answer: C

QUESTION 4

Refer to the exhibit:



Configuration » Services » Edit - ACCX Aruba Device Access Service

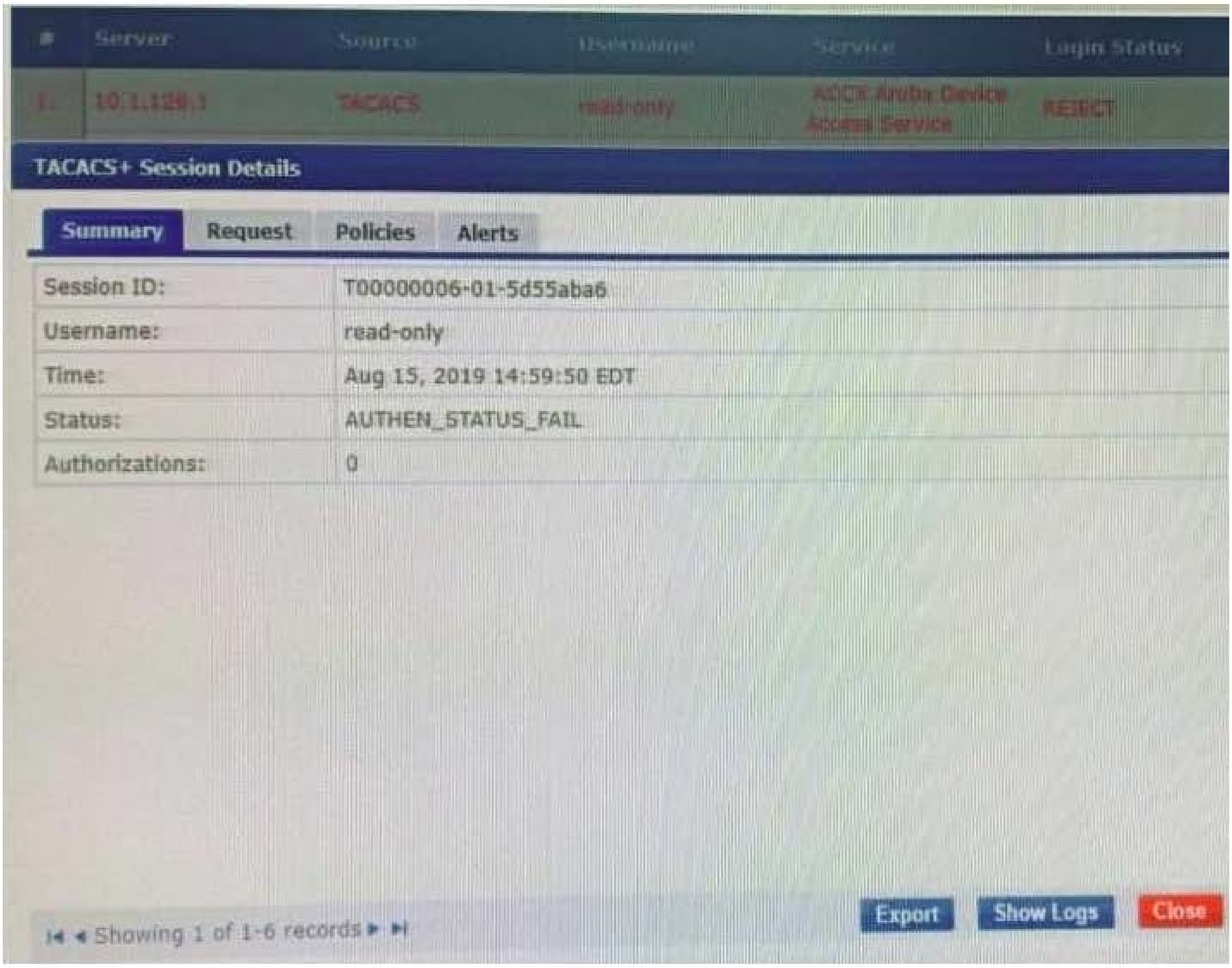
Services - ACCX Aruba Device Access Service

Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	Aruba NAD Tacacs

Enforcement Policy Details

Description:	
Default Profile:	[TACACS Deny Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS [Aruba TACACS read-only Admin])	[TACACS Read-only Admin]
2.	(Tips:Role EQUALS [Aruba TACACS root Admin])	[TACACS Network Admin]

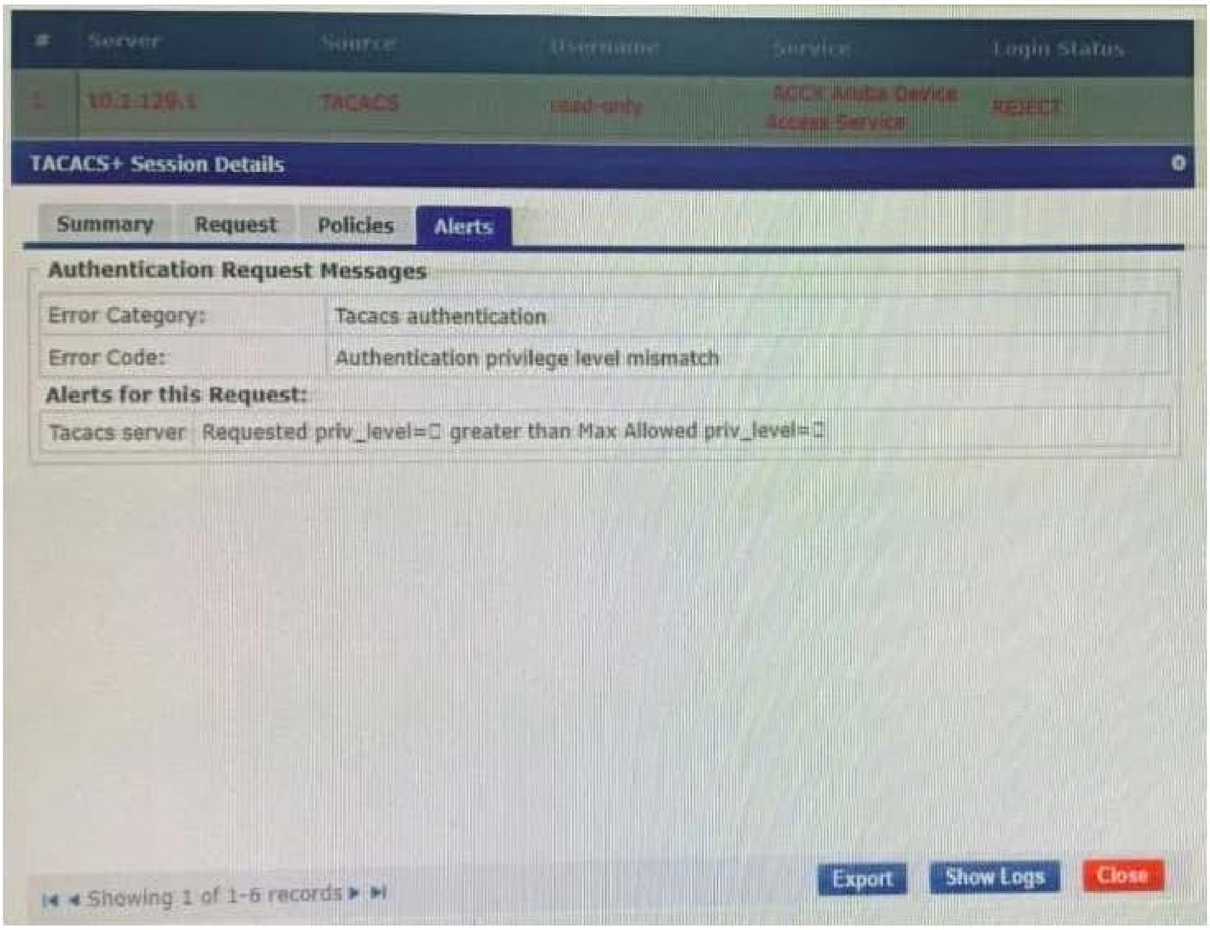


#	Server	Source	Username	Service	Login Status
1.	10.1.128.1	TACACS	read-only	ACCX Aruba Device Access Service	REJECT

TACACS+ Session Details

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



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

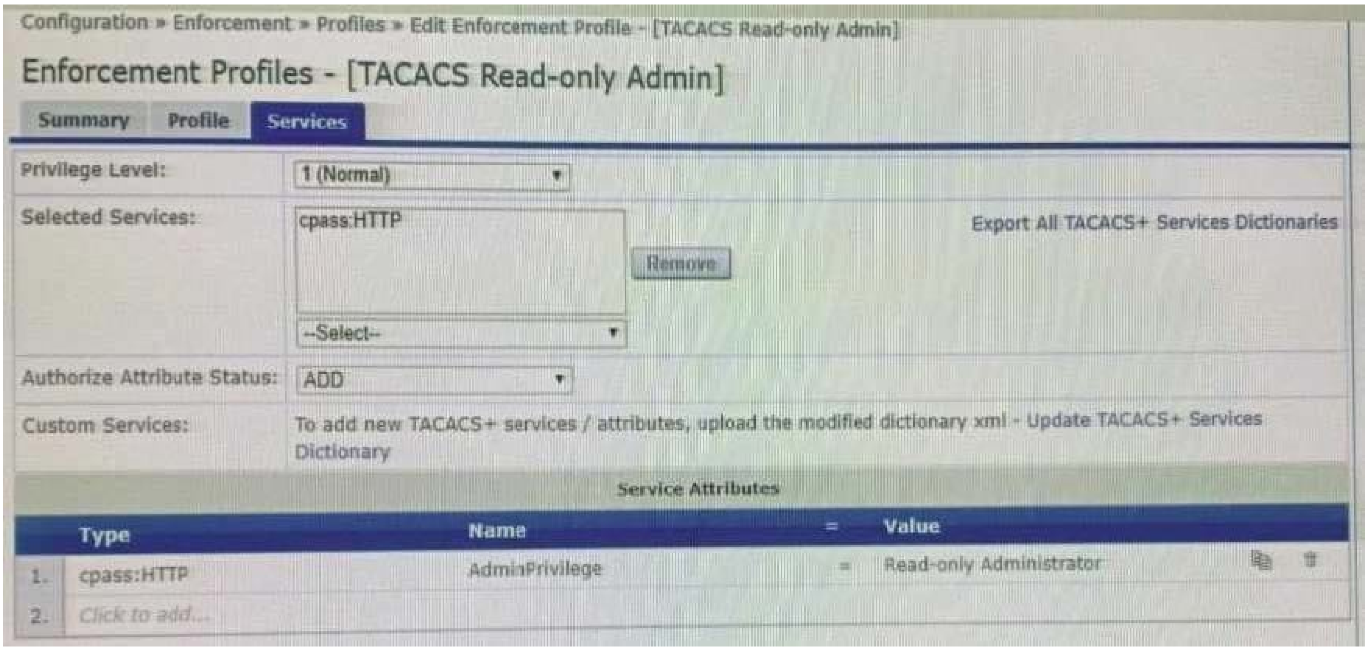
TACACS+ Session Details

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=□



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

Enforcement Profiles - [TACACS Read-only Admin]

Privilege Level: 1 (Normal)

Selected Services: cpass:HTTP

--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.

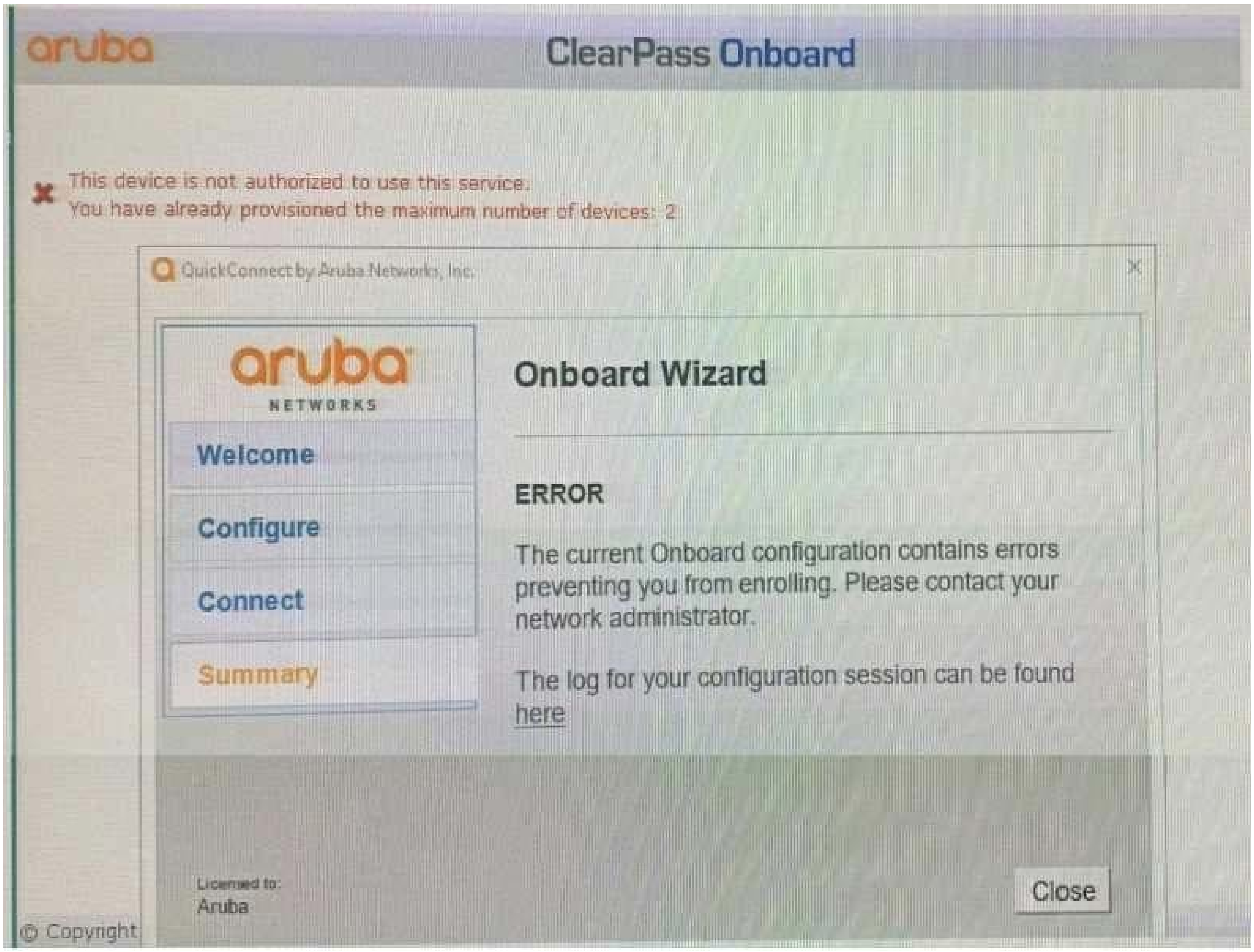
C. The Read-only Administrator role does not exist on the Controller.

D. The Enforcement profile used is not a TACACS profile.

Correct Answer: A

QUESTION 5

Refer to the exhibit: You have configured Onboard but me customer could not onboard one of his devices and has sent you the above screenshots. How could you resolve the issue?



This device is not authorized to use this service.
You have already provisioned the maximum number of devices: 2

Onboard Wizard

ERROR

The current Onboard configuration contains errors preventing you from enrolling. Please contact your network administrator.

The log for your configuration session can be found here

A. Instruct the user to delete the profile on one of their other BYOD devices.

B. Instruct the user to run the Quick connect application in Sponsor Mode.

C. Increase the maximum number of devices allowed by the individual user account.

D. Increase the maximum number of devices that all users can provision to 3.

Correct Answer: D

[Latest HPE6-A81 Dumps](#) [HPE6-A81 VCE Dumps](#) [HPE6-A81 Study Guide](#)