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

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

QUESTION 1

You have Integrated ClearPass Onboard with Active Directory Certificate Services (ADCS) web enrollment to sign the Anal device TLS certificates The Onboard provisioning process completes successfully but when the user finally clicks connect, the user falls to connect to the network with an unknown_ca certificate error. What steps will you follow to complete the requirement?

A. Make sure that the ClearPass servers are using the default self-signed certificates for both SSL and RADIUS server identity

B. Add the ADCS root certificate to both the CPPM Certificate trust list and to the Onboard Certificate Store trust list

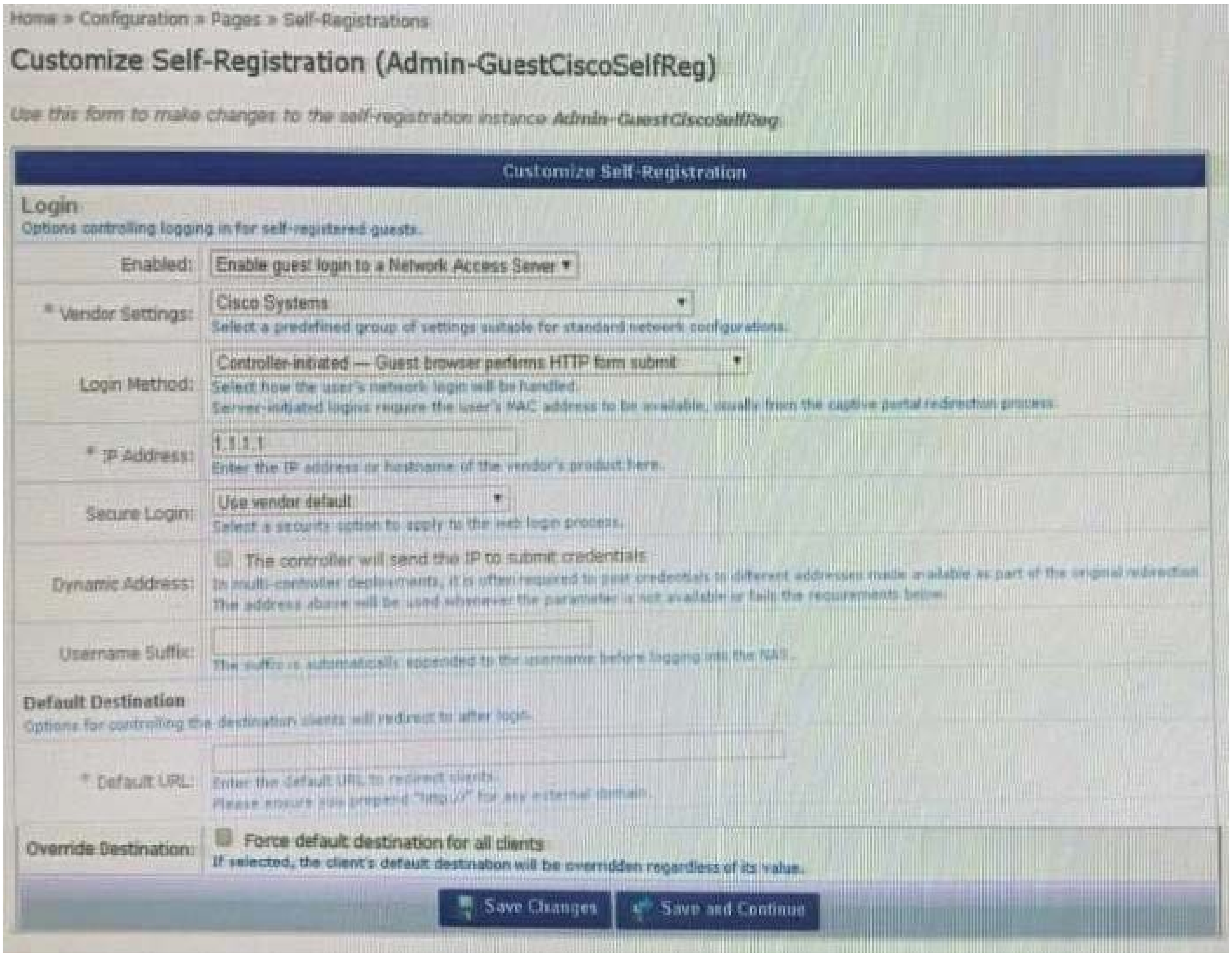
C. Make sure both the ClearPass servers have different certificates used for both SSL and RADIUS server identity.

D. Export the self-signed certificate from the ClearPass servers and manually add them as trusted certificates in clients

Correct Answer: A

QUESTION 2

Refer to the exhibit: A customer has configured a Guest Self registration page for their Cisco Wireless network with the settings shown. What should be changed in order to successfully authenticate guests users?



Home » Configuration » Pages » Self-Registrations

Customize Self-Registration (Admin-GuestCiscoSelfReg)

*Use this form to make changes to the self-registration instance **Admin-GuestCiscoSelfReg***

Customize Self-Registration

Login

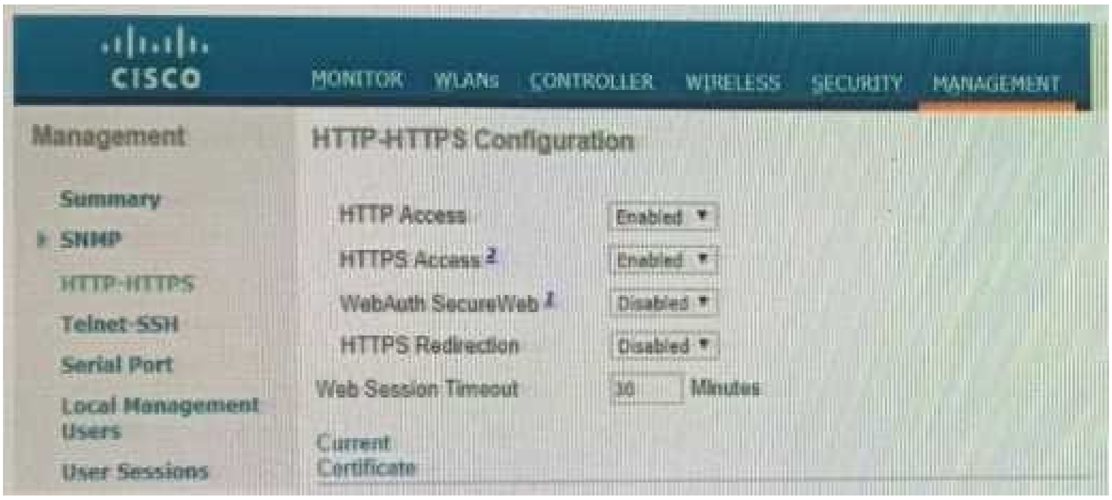
Options controlling logging in for self-registered guests.

Enabled:	Enable guest login to a Network Access Server ▾
* Vendor Settings:	Cisco Systems ▾ Select a predefined group of settings suitable for standard network configurations.
Login Method:	Controller-initiated — Guest browser performs HTTP form submit ▾ Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
* IP Address:	1.1.1.1 Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default ▾ Select a security option to apply to the web login process.
Dynamic Address:	□ The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.
Username Suffix:	 The suffix is automatically appended to the username before logging into the NAS.

Default Destination

Options for controlling the destination clients will redirect to after login.

* Default URL:	 Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	□ Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.



HTTP-HTTPS Configuration

HTTP Access	Enabled ▾
HTTPS Access [2]	Enabled ▾
WebAuth SecureWeb [1]	Disabled ▾
HTTPS Redirection	Disabled ▾
Web Session Timeout	30 Minutes

Current Certificate

A. Secure Login should use HTTP

B. Change the Vendor Settings to Airespace Networks

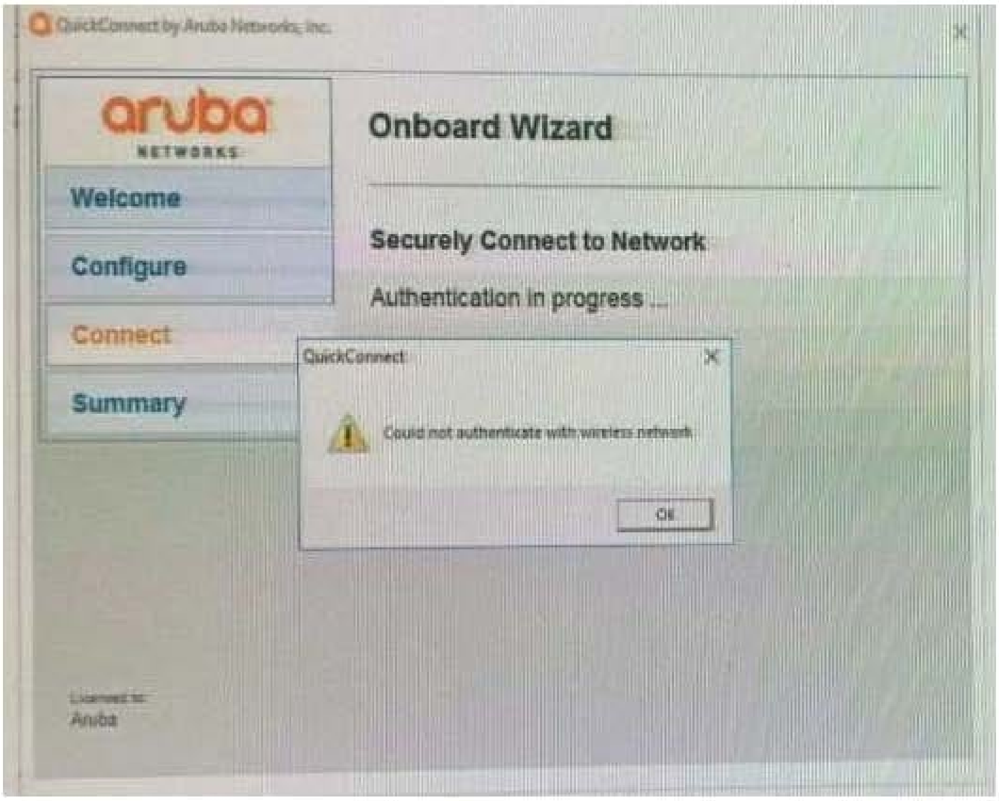
C. Change \he IP Address to the Cisco Controller DNS name

D. Login Method should be Controller-initiated - using HTTPs form submit

Correct Answer: C

QUESTION 3

Refer to the exhibit:



QuickConnect by Aruba Networks, Inc.

Onboard Wizard

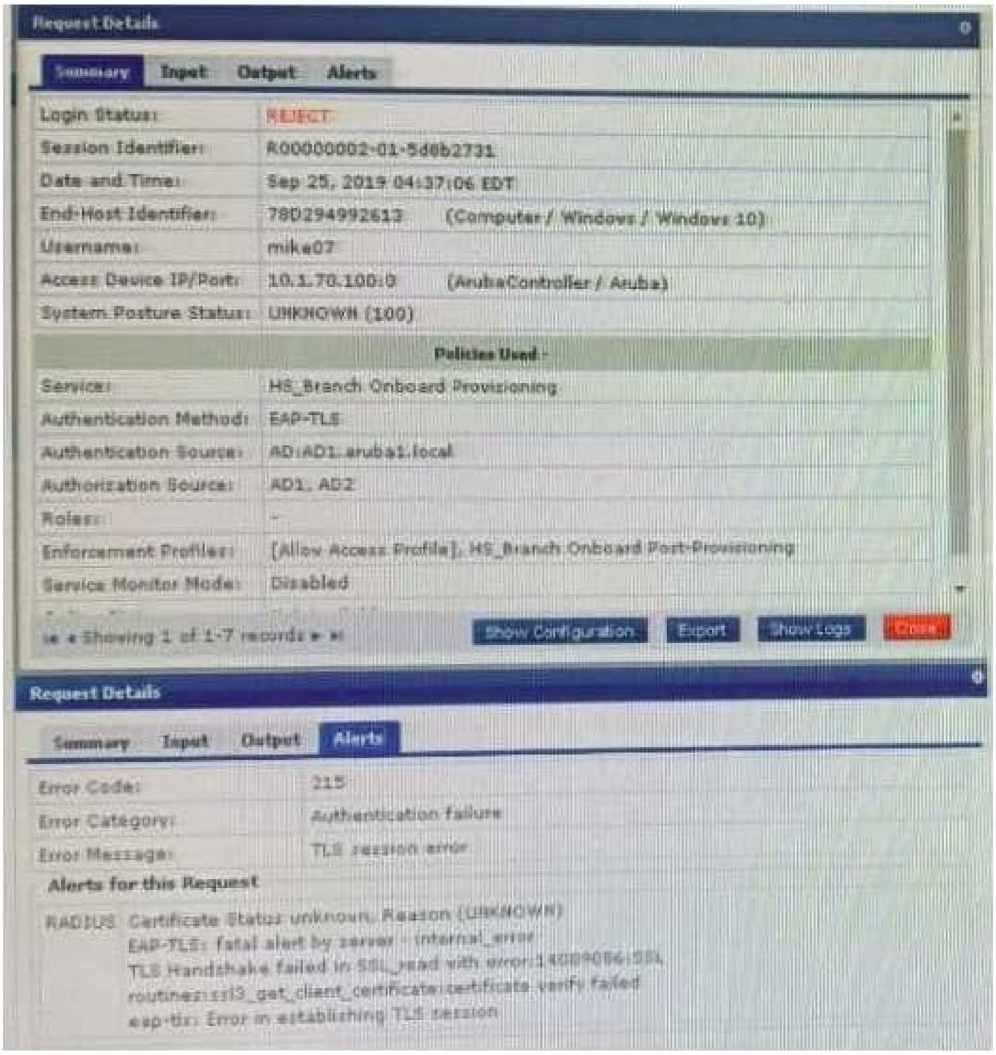
Securely Connect to Network

Authentication in progress ...

QuickConnect

Could not authenticate with wireless network

Licensed to:
Aruba

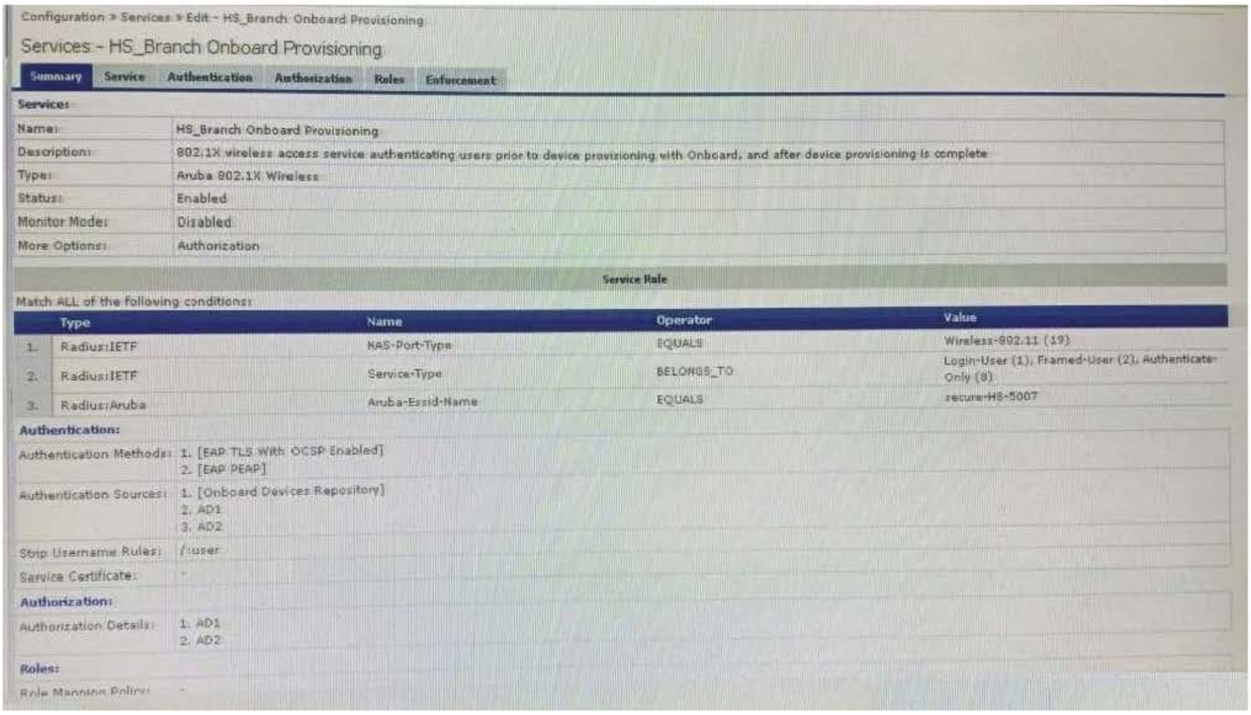


Login Status:	REJECT
Session Identifier:	R00000002-01-5d8b2731
Date and Time:	Sep 25, 2019 04:37:06 EDT
End-Host Identifier:	78D294992613 (Computer / Windows / Windows 10)
Username:	mike07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used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

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:

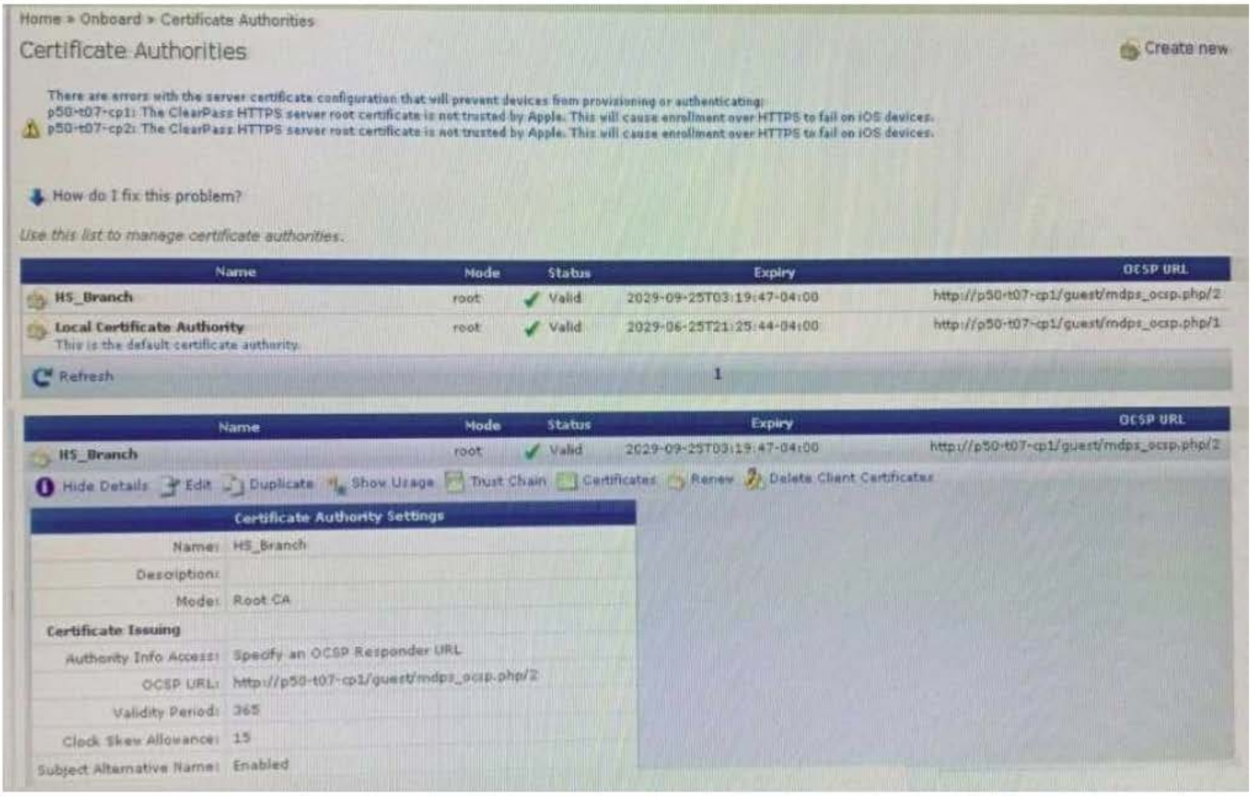
Authentication Methods:	1. [EAP TLS With OCSP Enabled] 2. [EAP PEAP]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2
Strip Username Rules:	/:user
Service Certificate:	-

Authorization:

Authorization Details:	1. AD1 2. AD2

Roles:

Role Mapping Policy: -


Home » Onboard » Certificate Authorities
Create new
How do I fix this problem?
Refresh
1
Hide Details
Edit
Duplicate
Show Usage
Trust Chain
Certificates
Renew
Delete Client Certificates

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.

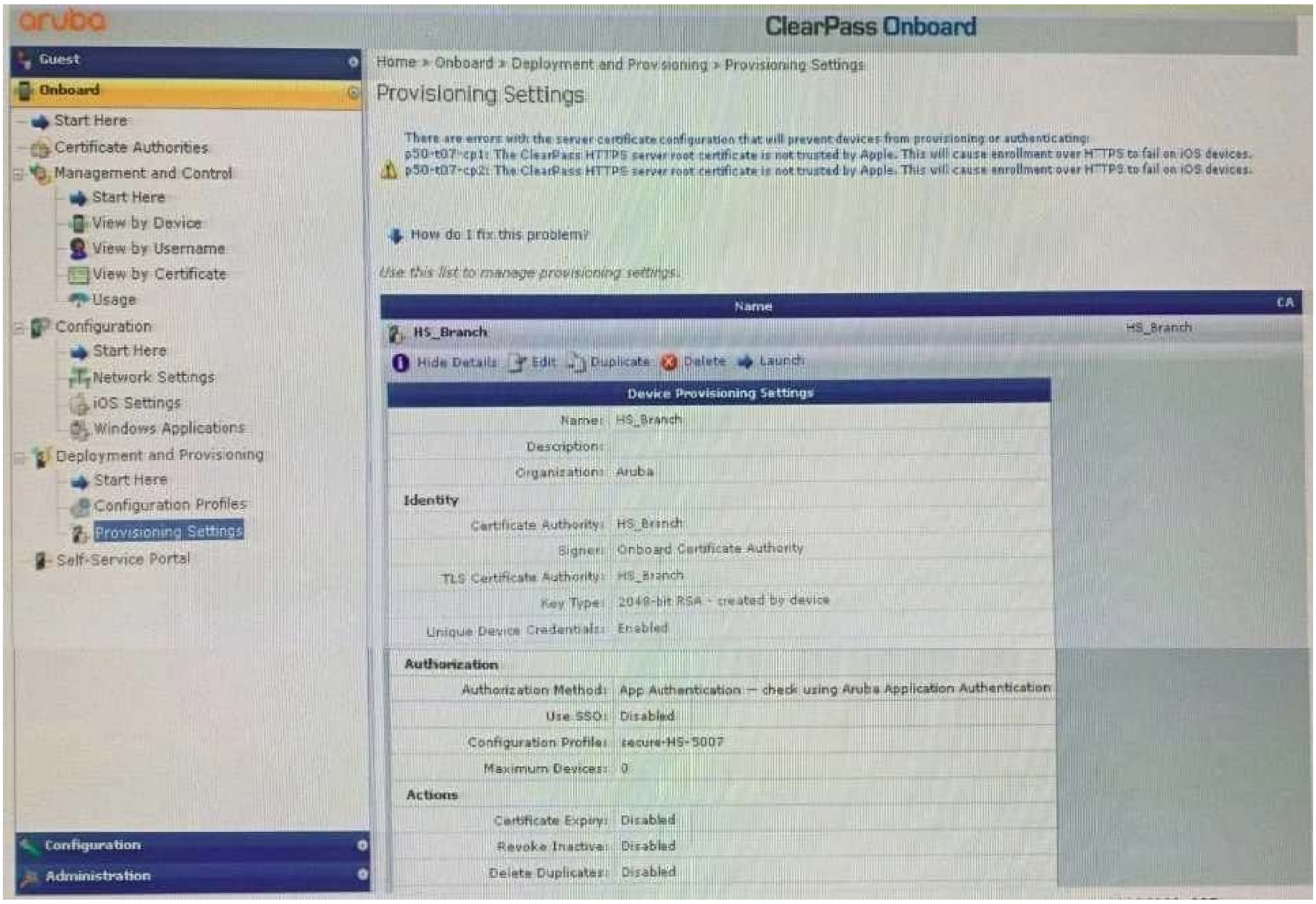
Use this list to manage certificate authorities.

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

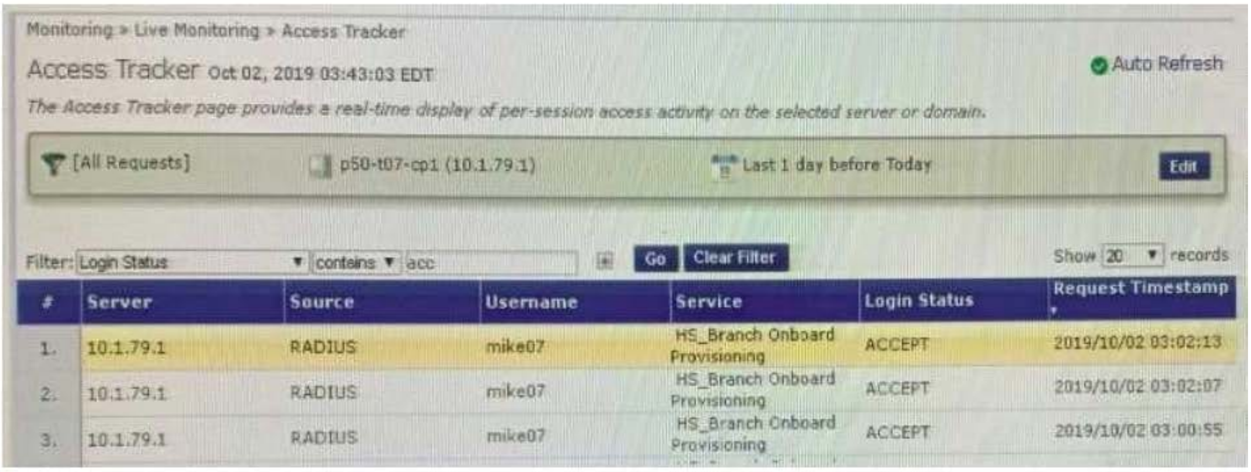
C. Reconnect the client and select the correct certificate when prompted

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

Correct Answer: A

QUESTION 4

Refer to the exhibit:



Monitoring » Live Monitoring » Access Tracker

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

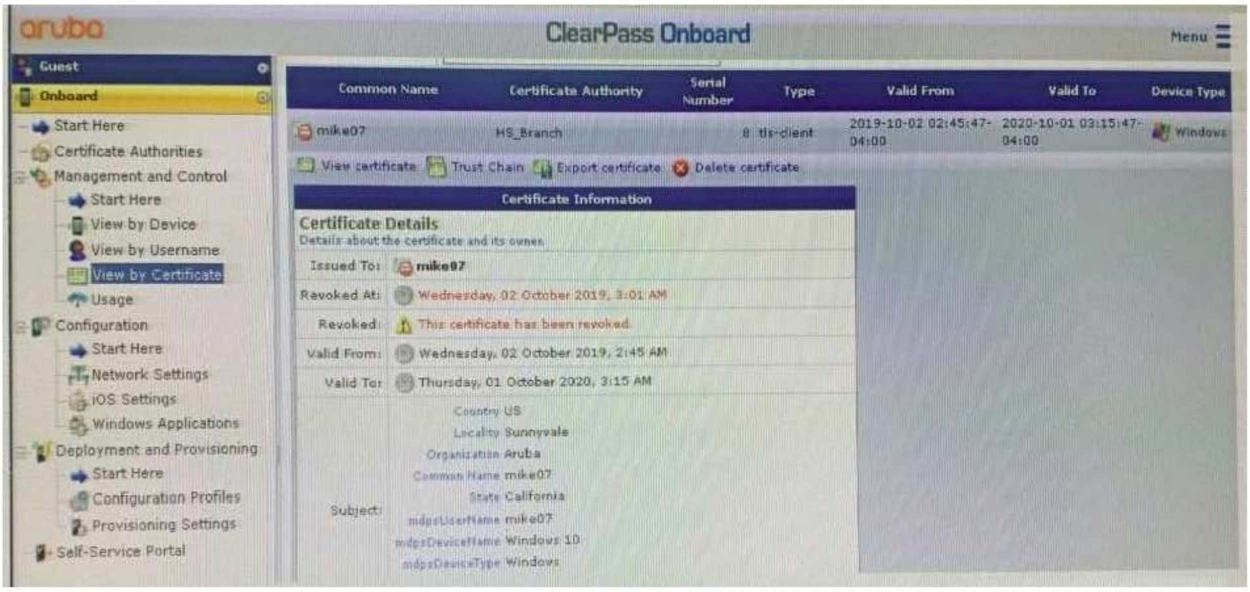
The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[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

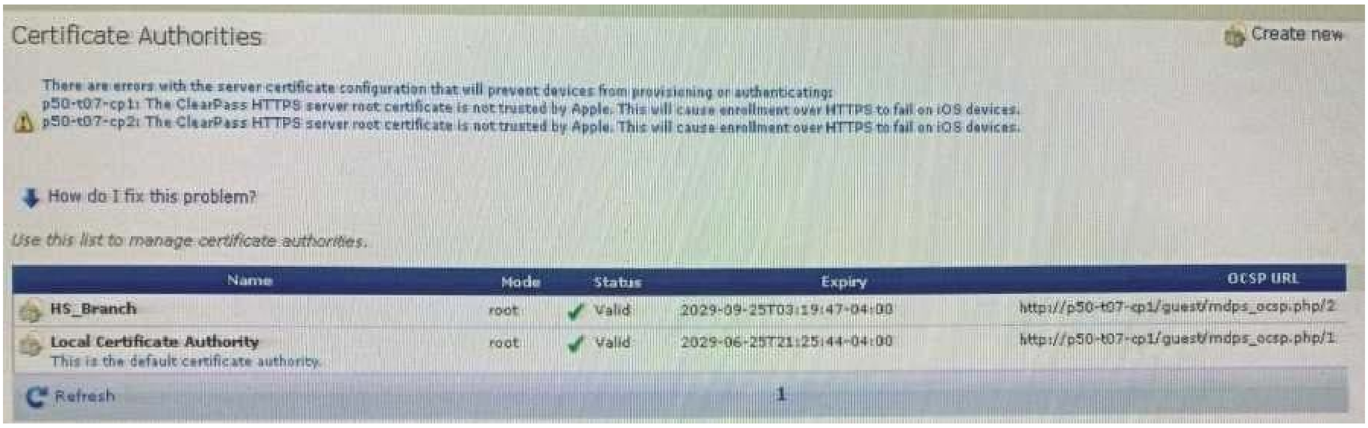


Common Name	Certificate Authority	Serial Number	Type	Valid From	Valid To	Device Type
mike07	HS_Branch	8	tls-client	2019-10-02 02:45:47-04:00	2020-10-01 03:15:47-04:00	Windows

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



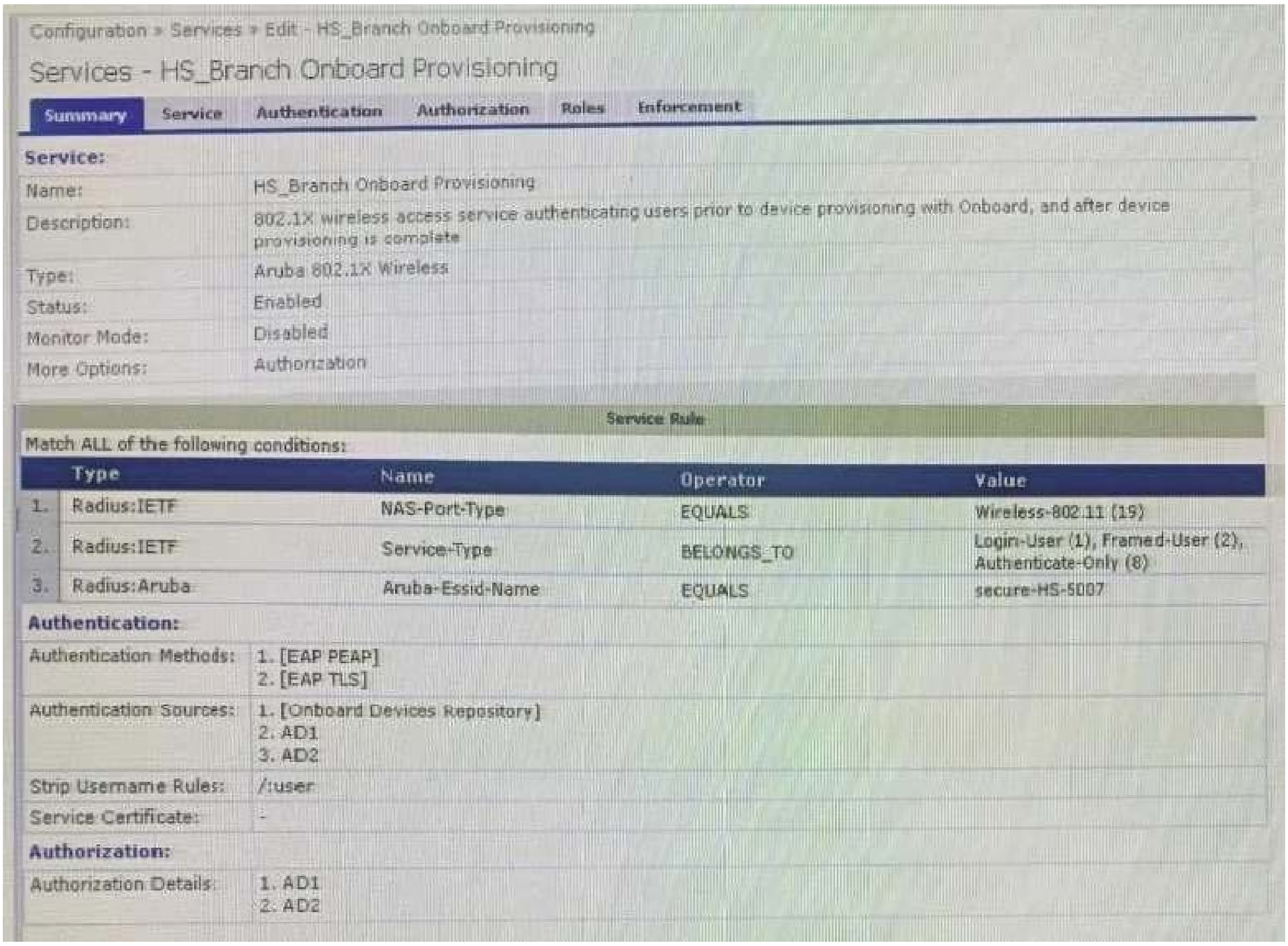
Certificate Authorities

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.

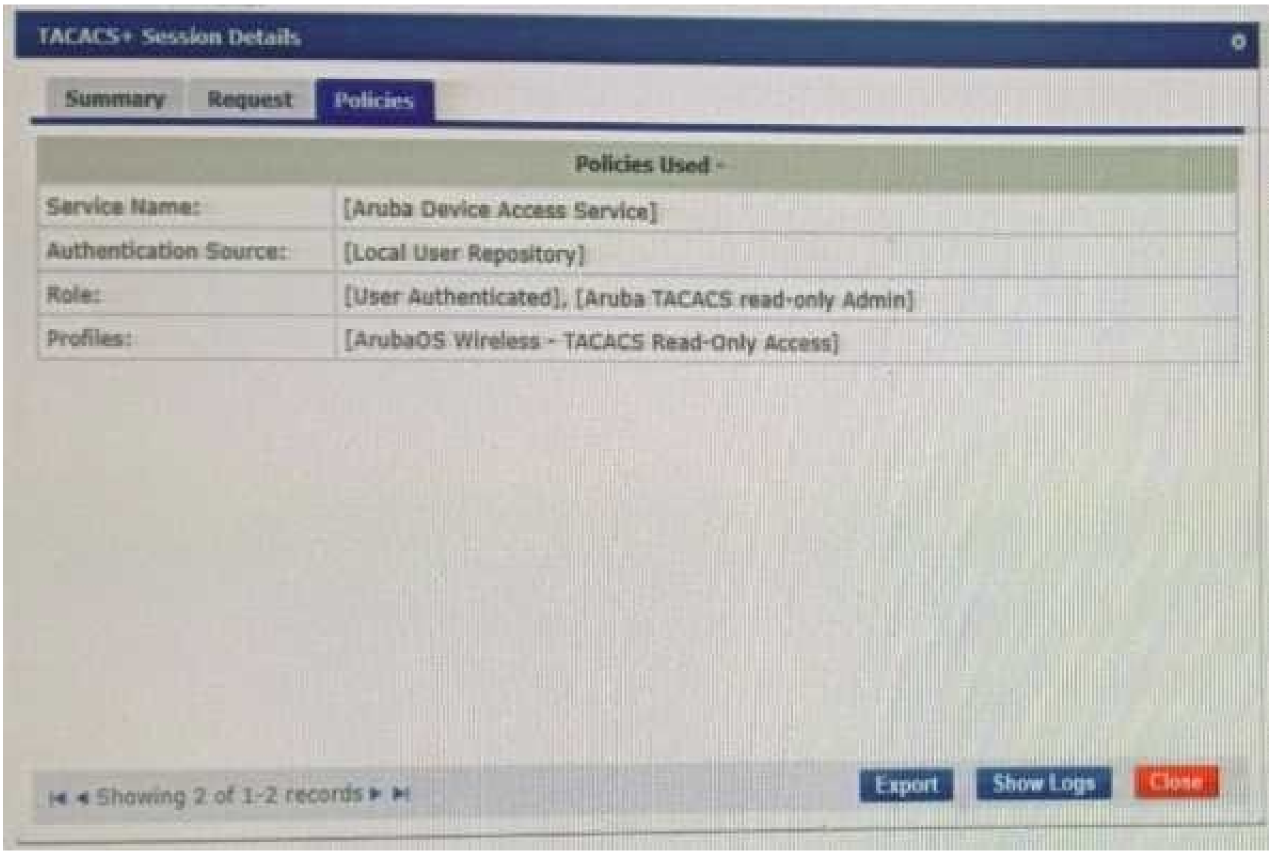
C. Remove the EAP-TLS authentication method configuration changes are required and add "EAP-TLS with OCSP Enabled" authentication method in the OnBoard Provisioning service. No other configuration changes are required.

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 5

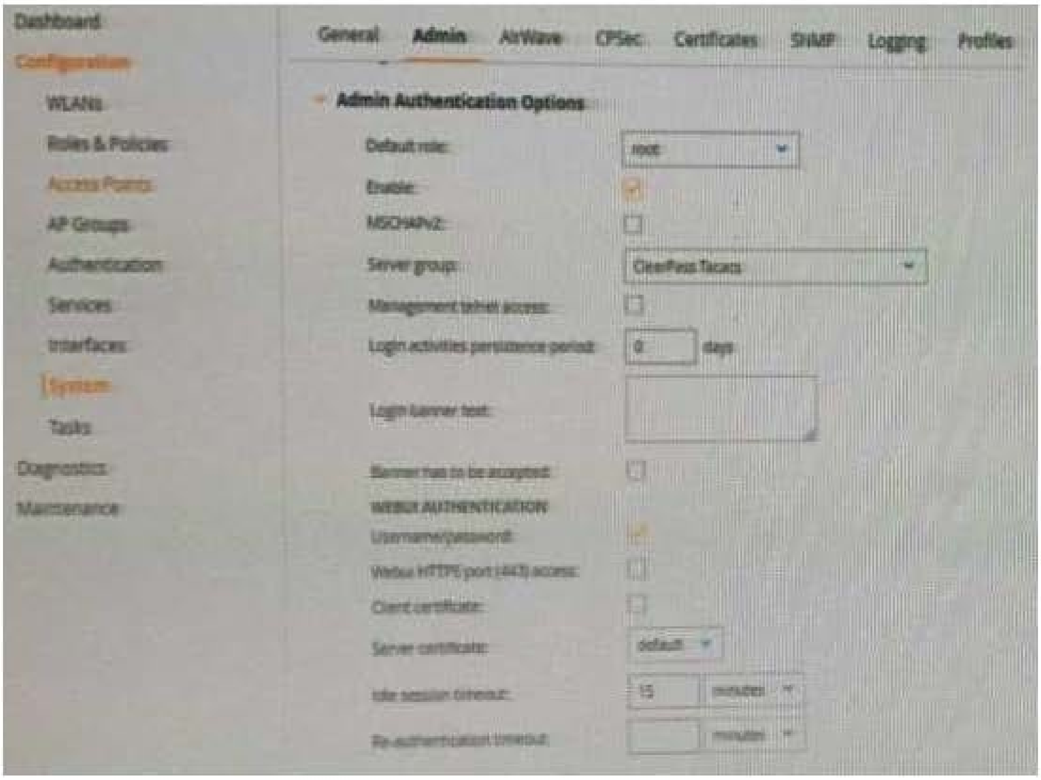
Refer to the exhibit:



Policies Used -

Service Name:	[Aruba Device Access Service]
Authentication Source:	[Local User Repository]
Role:	[User Authenticated], [Aruba TACACS read-only Admin]
Profiles:	[ArubaOS Wireless - TACACS Read-Only Access]

Showing 2 of 1-2 records



Admin Authentication Options

Default role: root

Enable: ☑

MSCHAPv2: □

Server group: ClearPass Tacacs

Management telnet access: □

Login activities persistence period: 0 days

Login banner text:

Banner has to be accepted: □

WEBUI AUTHENTICATION

Username/password: ☑

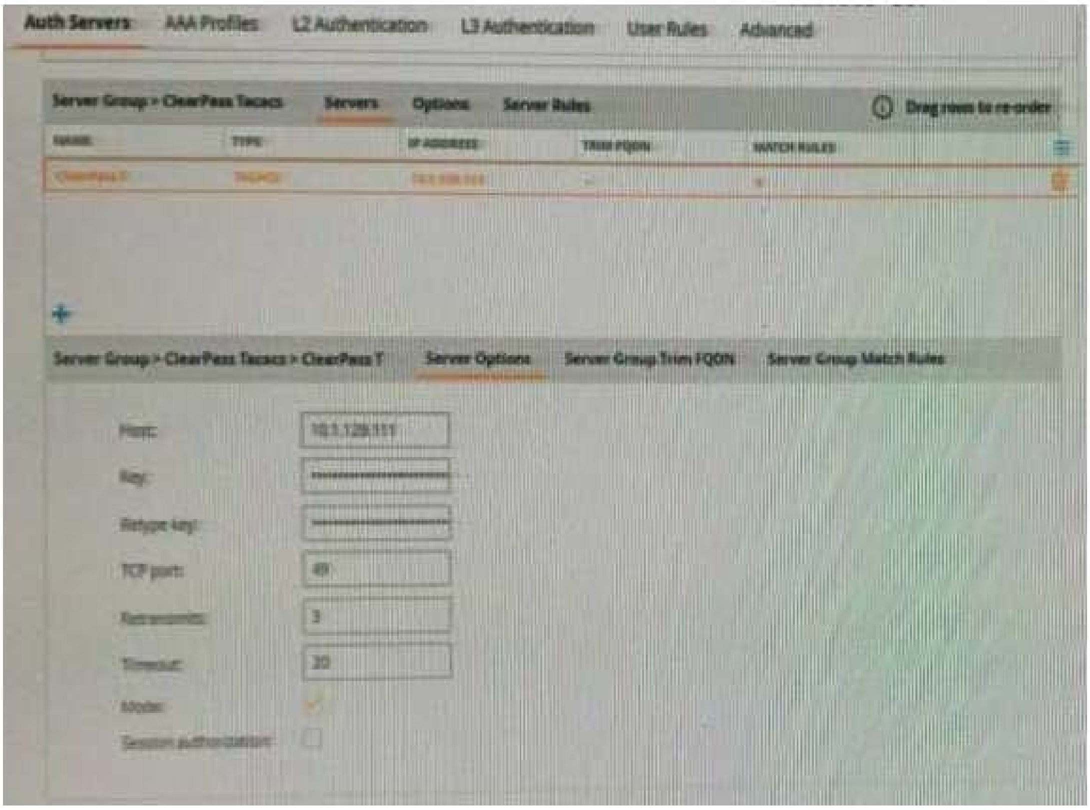
Webui HTTPS port (443) access: □

Client certificate: □

Server certificate: default

Idle session timeout: 15 minutes

Re-authentication timeout: minutes



Server Group > ClearPass Tacacs

NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES
ClearPass T	TACACS	10.1.128.111	-	*

Server Group > ClearPass Tacacs > ClearPass T

Host: 10.1.128.111

Key: ••••••••••••••••••••

Retype key: ••••••••••••••••••••

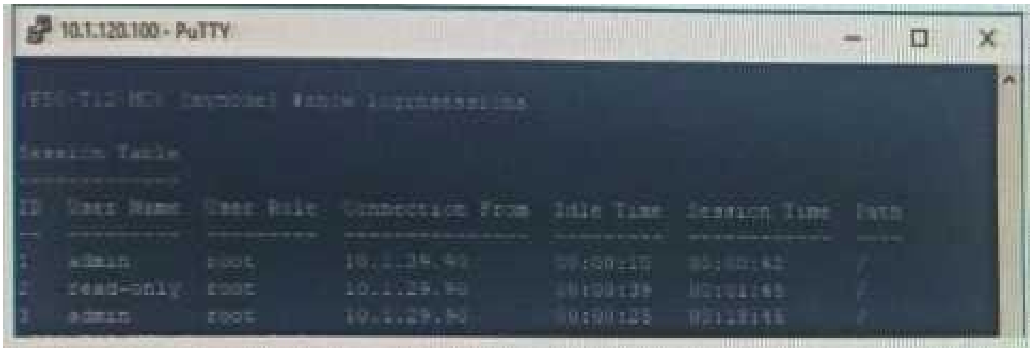
TCP port: 49

Retransmits: 3

Timeout: 20

Mode: ☑

Session authorization: □



```
(ESG-T12-MC) [mynode] #show loginsessions

Session Table
-------------
ID  User Name  User Role  Connection From  Idle Time  Session Time  Path
--  ---------  ---------  ---------------  ---------  ------------  ----
1   admin      root       10.1.29.90       00:00:15   00:00:42      /
2   read-only  root       10.1.29.90       00:00:19   00:01:45      /
3   admin      root       10.1.29.90       00:00:25   [illegible]   /
```

A customer has configured the Aruba Controller for administrative authentication using ClearPass as a TACACS server. During testing, the read-only user is getting the root access role. What could be a possible reason for this behavior? (Select two.)

A. The Controllers Admin Authentication Options Default role is mapped to toot.

B. The ClearPass user role associated to the read-only user is wrong

C. The Controller Server Group Match Rules are changing the user role

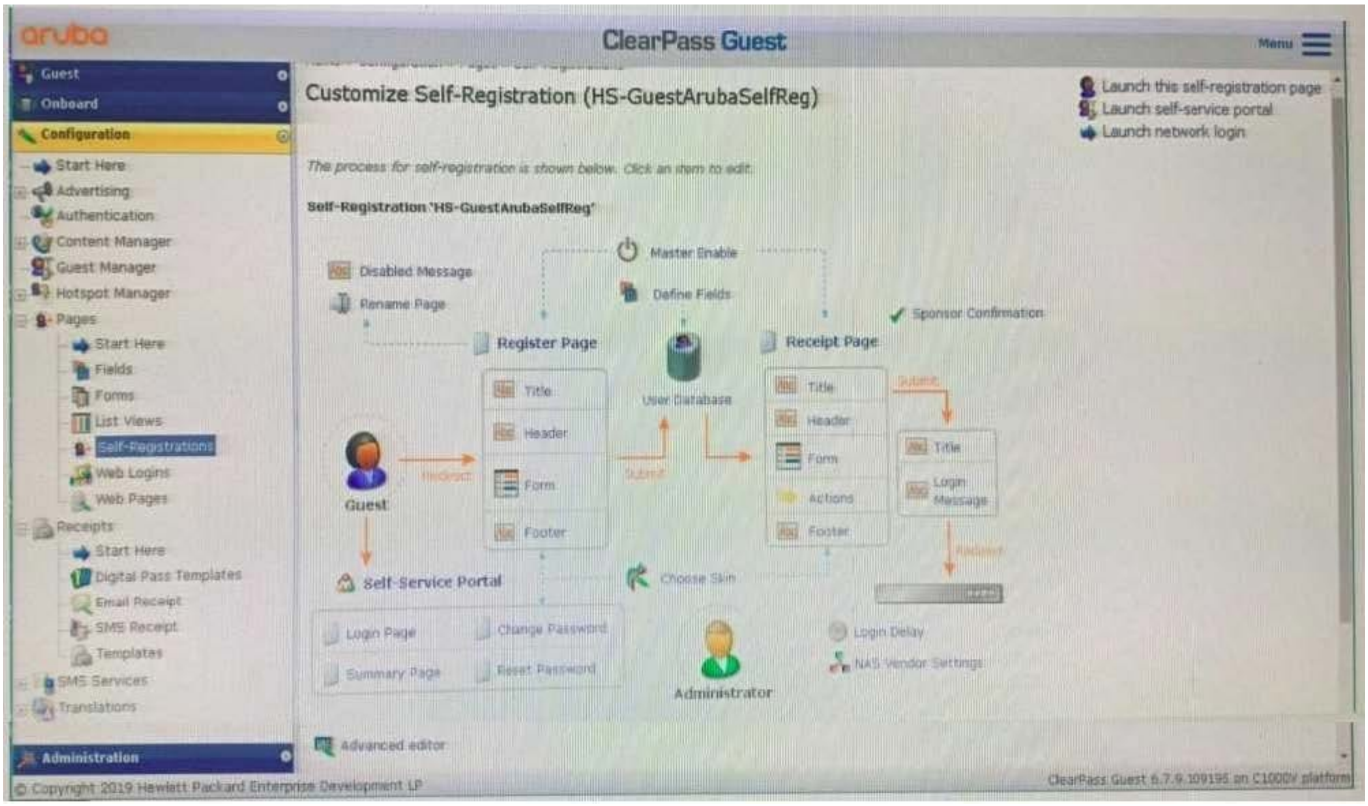
D. The read-only enforcement profile is mapped to the root role

E. On the Controller, the TACAC$ authentication server Is not configured for Session authorization

Correct Answer: CE

QUESTION 6

Refer to the exhibit:



Customize Self-Registration (HS-GuestArubaSelfReg)

The process for self-registration is shown below. Click an item to edit.

Self-Registration 'HS-GuestArubaSelfReg'

© Copyright 2019 Hewlett Packard Enterprise Development LP

ClearPass Guest 6.7.9.109195 on C1000V platform

A customer is deploying Guest Self-Registration with Sponsor Approval but does not like the format of the sponsor email. Where can you change the sponsor email?

A. in the Receipt Page - Actions

B. in the Sponsor Confirmation section

C. in me Configuration - Receipts - Email Receipts

D. in the Configuration - Receipts - Templates

Correct Answer: B

QUESTION 7

What type of EAP certificate are you able to use on ClearPass? (Select two.)

A. Self signed, when all the clients are Onboarded with the same Root CA as the Self signed certificate.

B. Private signed, when the clients are onboarded or are part of the organization domain.

C. Private signed, when some clients are onboarded and some are not part of the organization.

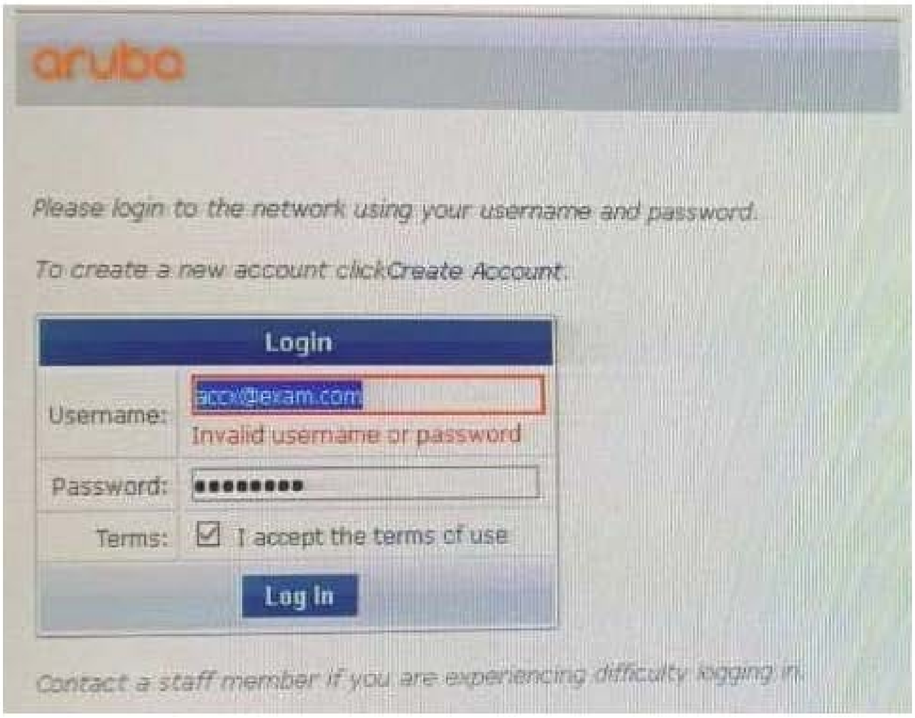
D. Public signed, when not all of the clients are part of the organization domain.

E. Self signed, when all the clients are part of the organization domain.

Correct Answer: CD

QUESTION 8

Refer to the exhibit:



Please login to the network using your username and password.

To create a new account clickCreate Account.

Login

Username:	accx@exam.com Invalid username or password
Password:	●●●●●●●●●
Terms:	☑ I accept the terms of use

Contact a staff member if you are experiencing difficulty logging in.

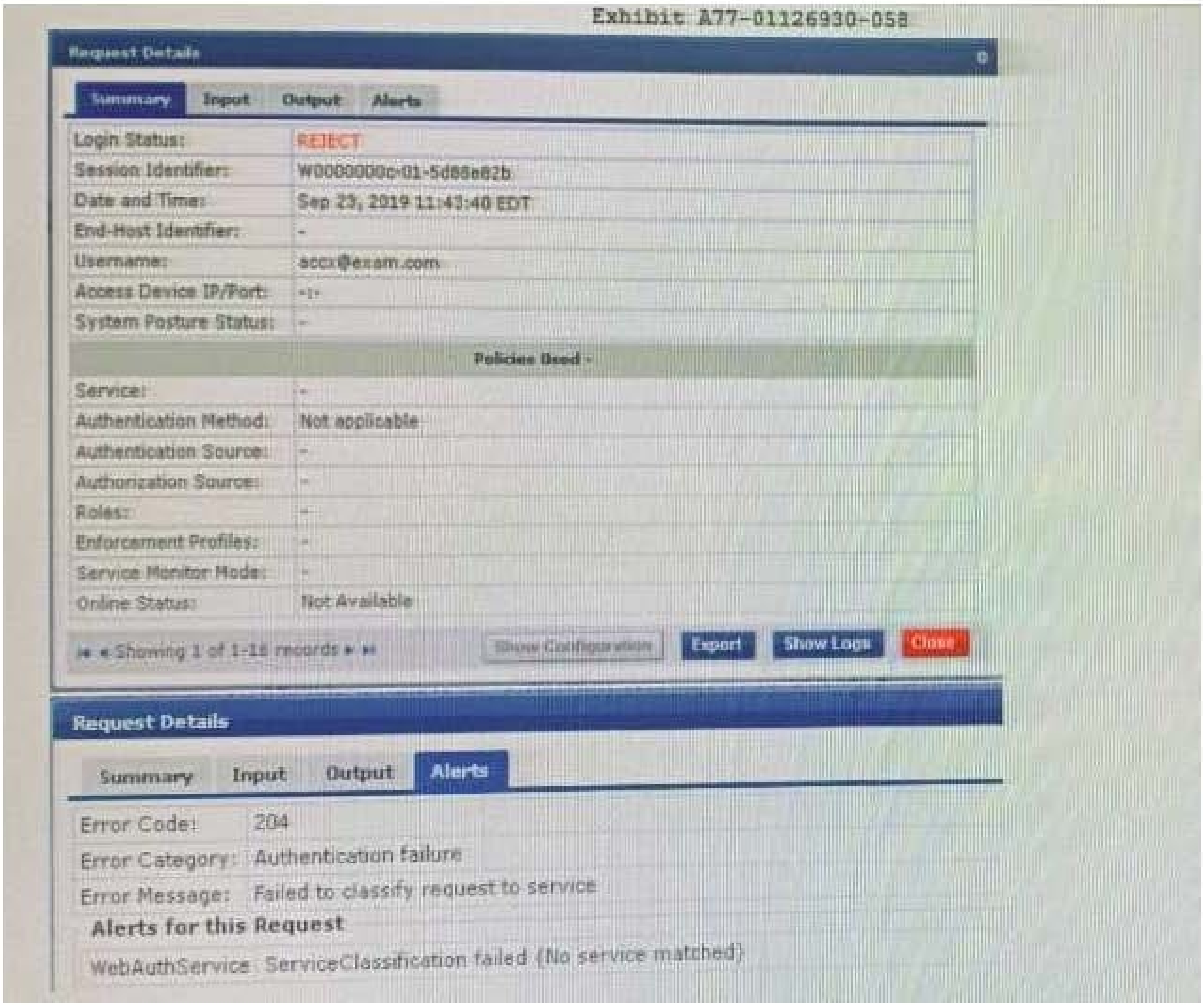


Exhibit A77-01126930-058

Request Details

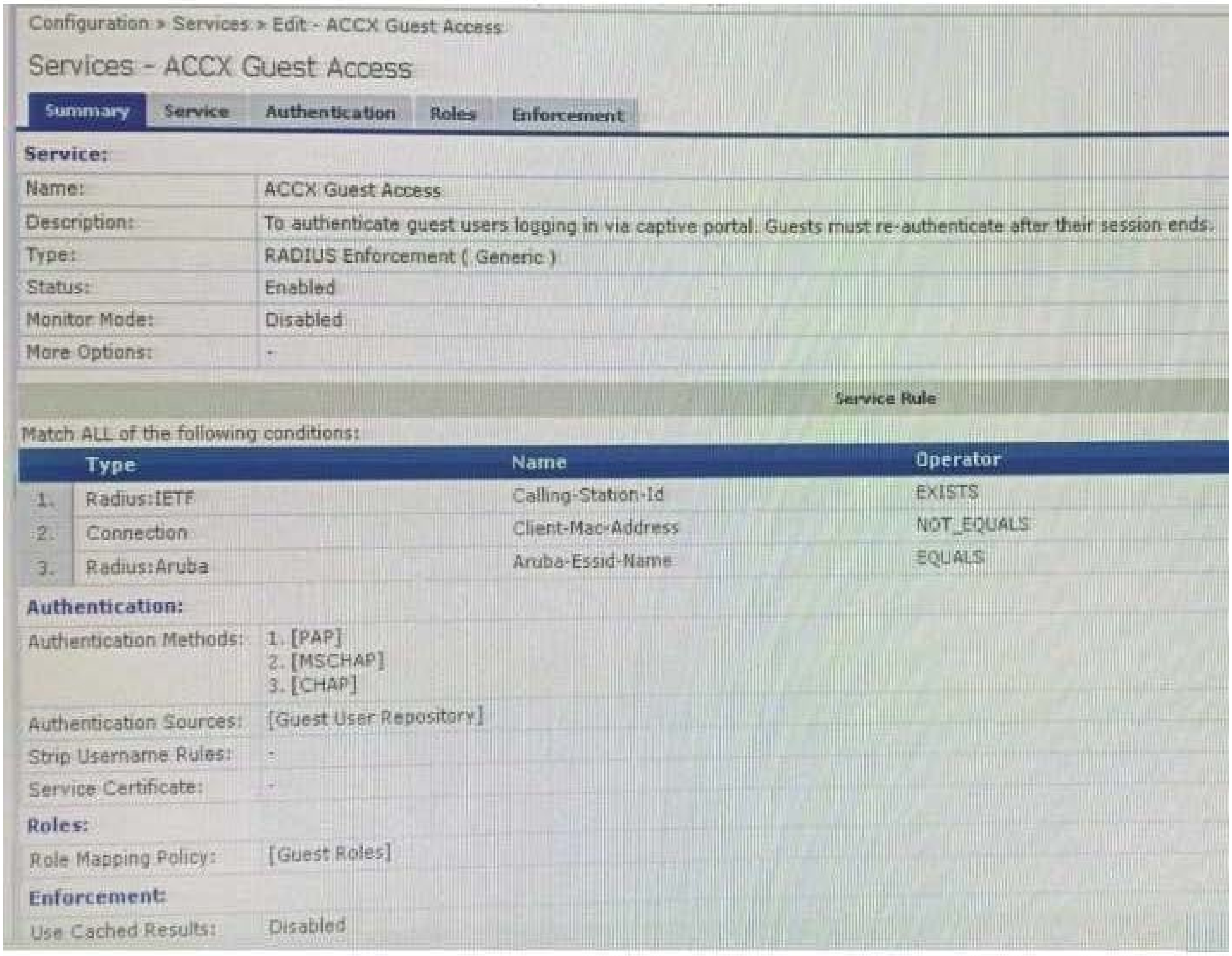
Login Status:	REJECT
Session Identifier:	W0000000c-01-5d88e82b
Date and Time:	Sep 23, 2019 11:43:40 EDT
End-Host Identifier:	-
Username:	accx@exam.com
Access Device IP/Port:	-:-
System Posture Status:	-
Policies Used -	
Service:	-
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	-
Enforcement Profiles:	-
Service Monitor Mode:	-
Online Status:	Not Available

Request Details

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

Alerts for this Request

WebAuthService	ServiceClassification failed (No service matched)



Services - ACCX Guest Access

Service:

Name:	ACCX Guest Access
Description:	To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.
Type:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator
1.	Radius:IETF	Calling-Station-Id	EXISTS
2.	Connection	Client-Mac-Address	NOT_EQUALS
3.	Radius:Aruba	Aruba-Essid-Name	EQUALS

Authentication:

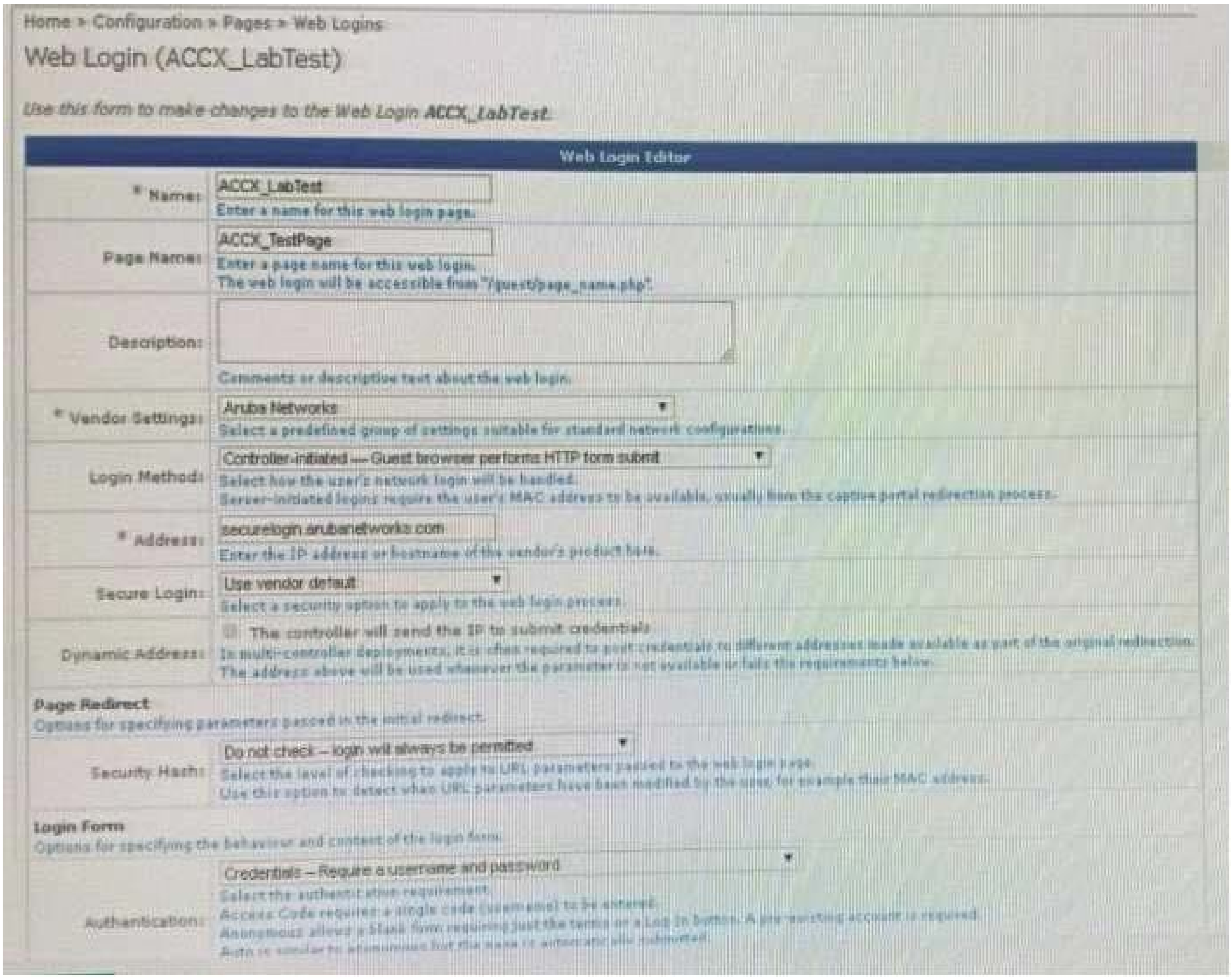
Authentication Methods:	1. [PAP] 2. [MSCHAP] 3. [CHAP]
Authentication Sources:	[Guest User Repository]
Strip Username Rules:	-
Service Certificate:	-

Roles:

Role Mapping Policy:	[Guest Roles]

Enforcement:

Use Cached Results:	Disabled



Home » Configuration » Pages » Web Logins

Web Login (ACCX_LabTest)

*Use this form to make changes to the Web Login **ACCX_LabTest**.*

Web Login Editor

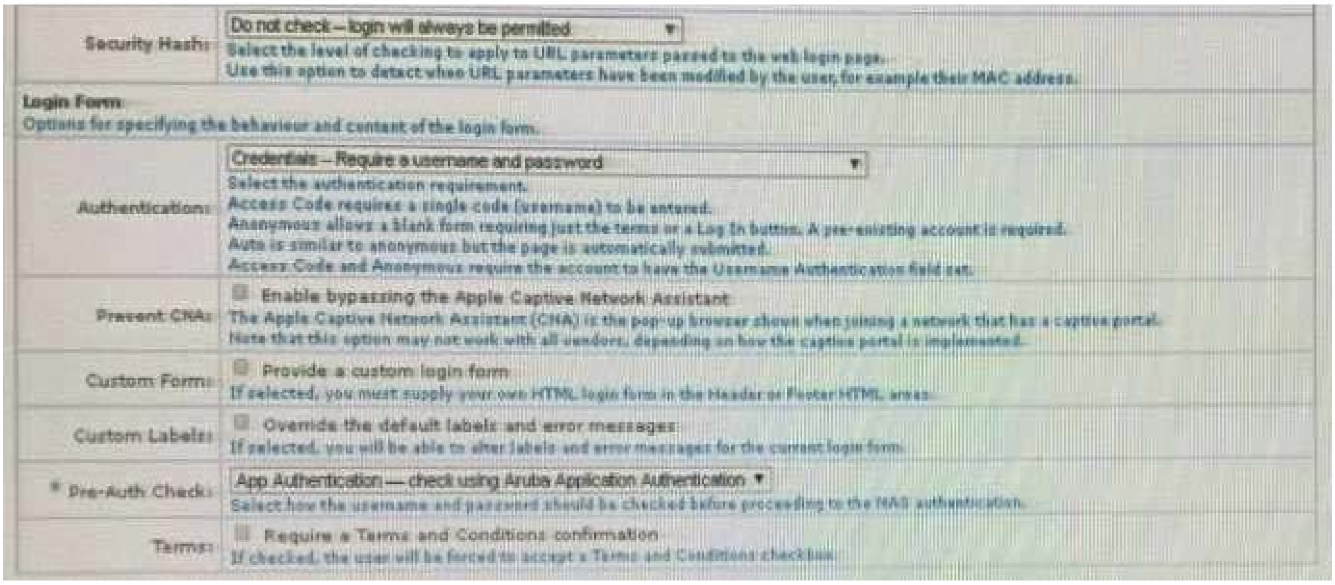
* Name:	ACCX_LabTest Enter a name for this web login page.
Page Name:	ACCX_TestPage Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	Comments or description text about the web login.
* Vendor Settings:	Aruba Networks ▾ Select a predefined group of settings suitable for standard network configurations.
Login Method:	Controller-initiated — Guest browser performs HTTP form submit ▾ Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
* Address:	securelogin.arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default ▾ Select a security option to apply to the web login process.
Dynamic Address:	□ The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

Page Redirect
Options for specifying parameters passed in the initial redirect.

Security Hash:	Do not check – login will always be permitted ▾ Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

Login Form
Options for specifying the behaviour and content of the login form.

Authentication:	Credentials – Require a username and password ▾ Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted.



Security Hash:	Do not check – login will always be permitted ▾ Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

Login Form
Options for specifying the behaviour and content of the login form.

Authentication:	Credentials – Require a username and password ▾ Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set.
Prevent CNA:	□ Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	□ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	□ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	App Authentication — check using Aruba Application Authentication ▾ Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	□ Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

A year ago, your customer deployed an Aruba ClearPass Policy Manager Server for a Guest SSIC hosted in an IAP Cluster. The customer just created a new Web Login Page for the Guest SSID. Even though the previous Web Login page worked test with the new Web Login Page are falling and the customer has

forwarded you the above screenshots.

What recommendation would you give the customer to tix the issue?

A. The service type configured is not correct. The Guest authentication should De an Application authentication type of service.

B. The customer should reset the password tor the username accx@exam com using Guest Manage Accounts

C. The Address filed under the WebLogin Vendor settings is not configured correctly, it should be set to instant arubanetworks.com

D. The WebLogin Pre-Auth Check is set to Aruba Application Authentication which requires a separate application service on the policy manager

Correct Answer: A

QUESTION 9

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 10

You have integrated ClearPass Onboard with Active Directory Certificate Services (ADCS) web enrollment

to sign the final device TLS certificates. The customer would also like to use ADCS for centralized

management of TLS certificates including expiration, revocation, and deletion through ADCS.

What steps will you follow to complete the requirement?

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

B. Copy the [EAP-TLS with OSCP Enabled) authentication method and set the correct ADCS server OCSP URL, remove EAP-TLS and map the custom created method to the Onboard Provisioning Service.

C. Copy the default [EAP-TLS with OSCP Enabled] authentication method and update the correct ADCS server OCSP URL. remove EAP-TLS and map the custom created method to the OnBoard Authorization Service.

D. Edit the [EAP-TLS with OSCP Enabled) authentication method and set the correct ADCS server OCSP URL. remove EAP-TLS and map the [EAP-TLS with OSCP Enabled) method to the Onboard Provisioning Service.

Correct Answer: A