Vendor:HP

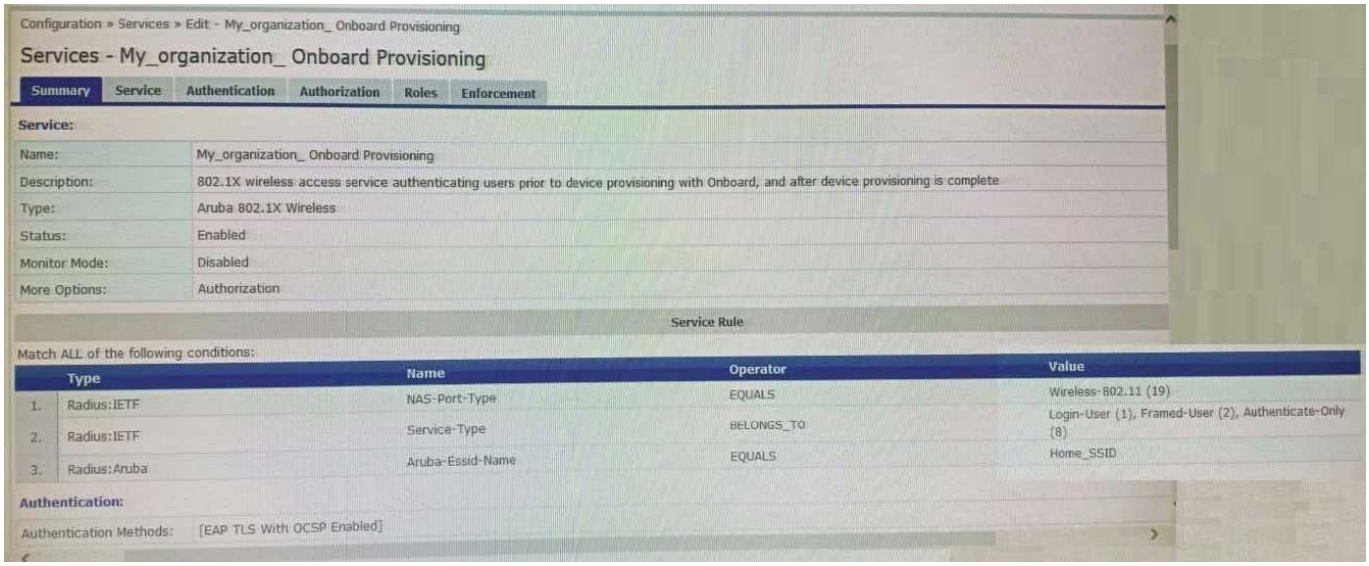
Exam Code:HPE6-A81

Exam Name: Aruba Certified ClearPass Expert Written Exam

Version: Demo

QUESTION 1

Refer to the exhibit: A customer has configured a service with the Onboard Devices Repository as an Authentication Source and an Active Directory Domain Server as an Authorization Source. What will happen if the client certificate is still valid and the user account associated with the certificate is disabled in Active Directory?



A. ClearPass will not process the request

B. Enforcement will apply the [Deny Access Profile]

C. ClearPass will redirect the client to Onboard again

D. ClearPass will block network access to the device

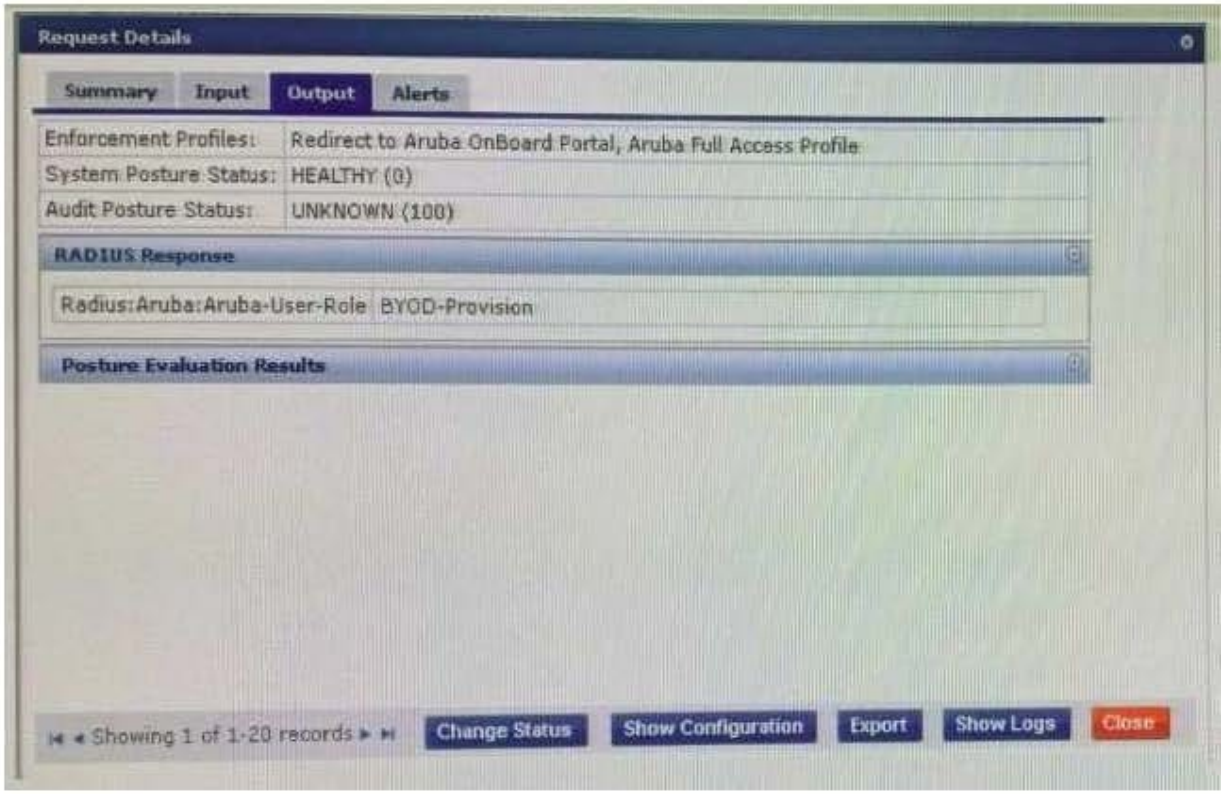
E. ClearPass will allow the device to access the network.

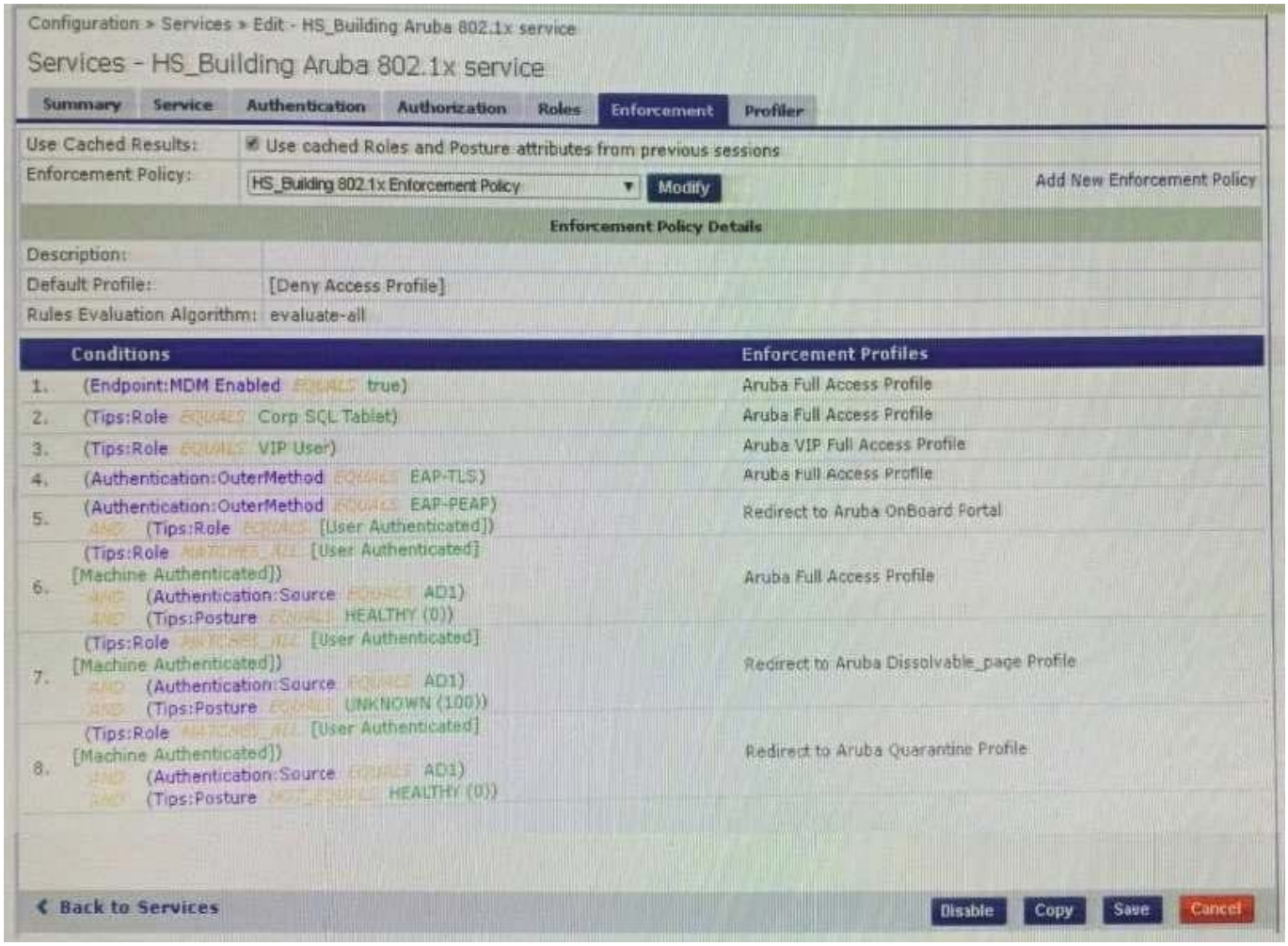
Correct Answer: D

QUESTION 2

Refer to the exhibit:


Request Details
Summary
Input
Output
Alerts
Login Status: ACCEPT
Session Identifier: R00000238-01-5d9dd0b2
Date and Time: Oct 09, 2019 08:21:07 EDT
End-Host Identifier: 78D29437BD69 (Computer / Windows / Windows 10)
Username: alex07
Access Device IP/Port: 10.1.70.100:0 (ArubaController / Aruba)
System Posture Status: HEALTHY (0)
Policies Used -
Service: HS_Building Aruba 802.1x service
Authentication Method: EAP-PEAP,EAP-MSCHAPv2
Authentication Source: AD:AD1.aruba1.local
Authorization Source: [Endpoints Repository], AD1, Corp SQL
Roles: [Machine Authenticated], [Other], [User Authenticated]
Enforcement Profiles: Redirect to Aruba OnBoard Portal, Aruba Full Access Profile
Service Monitor Mode: Disabled
Online Status: Not Available
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Request Details
Summary
Input
Output
Alerts
Enforcement Profiles: Redirect to Aruba OnBoard Portal, Aruba Full Access Profile
System Posture Status: HEALTHY (0)
Audit Posture Status: UNKNOWN (100)
RADIUS Response
Radius:Aruba:Aruba-User-Role BYOD-Provision
Posture Evaluation Results
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close



The customer configured an 802.1x service with different enforcement actions for personal and corporate laptops. The corporate laptops are always being redirected to the BYOD Portal. The customer has sent you the above screenshots.

How would you resolve the issue? (Select two)

A. Modify the enforcement policy and change the rule evaluation algorithm to select first match

B. Modify the enforcement policy and re-order the condition with posture not_equals to healthy as the sixth condition

C. Modify the enforcement policy and re-order the EAP-PEAP with [user authenticated] rule to the last condition.

D. Modify the enforcement policy and re-order the condition with Posture - Unknown as the fifth condition

E. Remove the EAP-PEAP with [user authenticated] condition for Onboard and create another service

Correct Answer: CD

QUESTION 3

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

QUESTION 4

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?

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

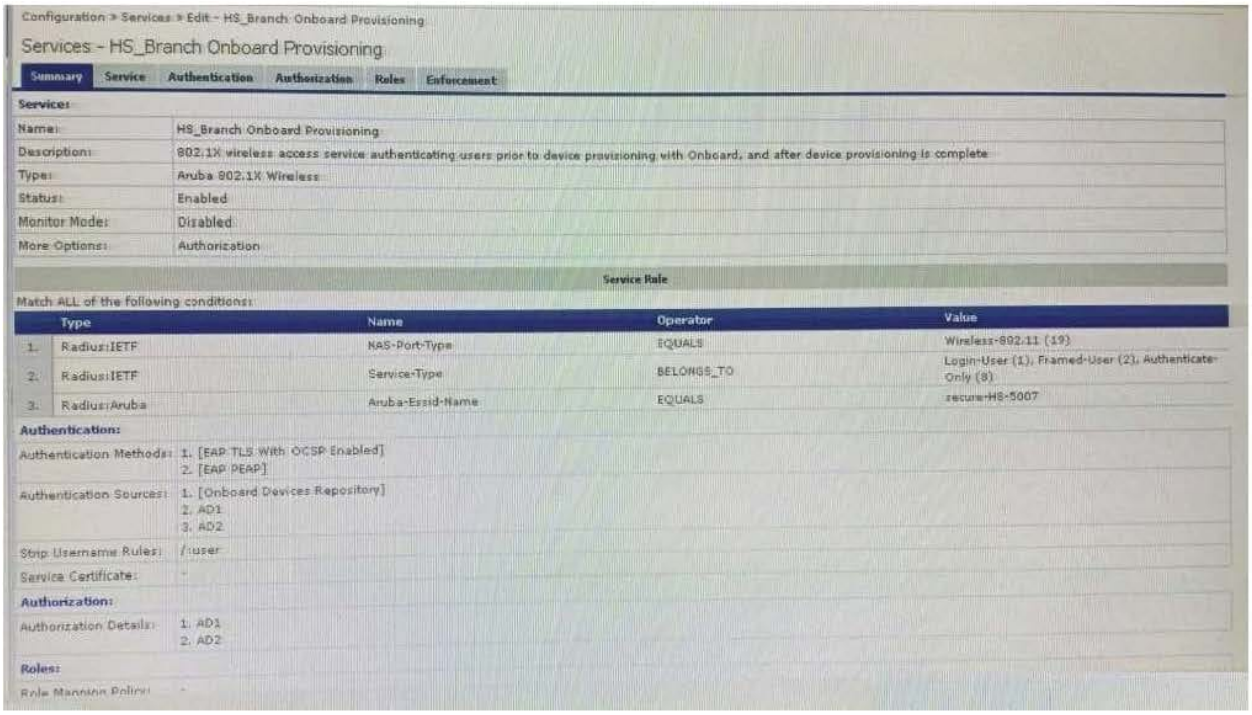
Correct Answer: C

QUESTION 5

Refer to the exhibit:


QuickConnect by Aruba Networks, Inc.
aruba
NETWORKS
Welcome
Configure
Connect
Summary
Onboard Wizard
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:

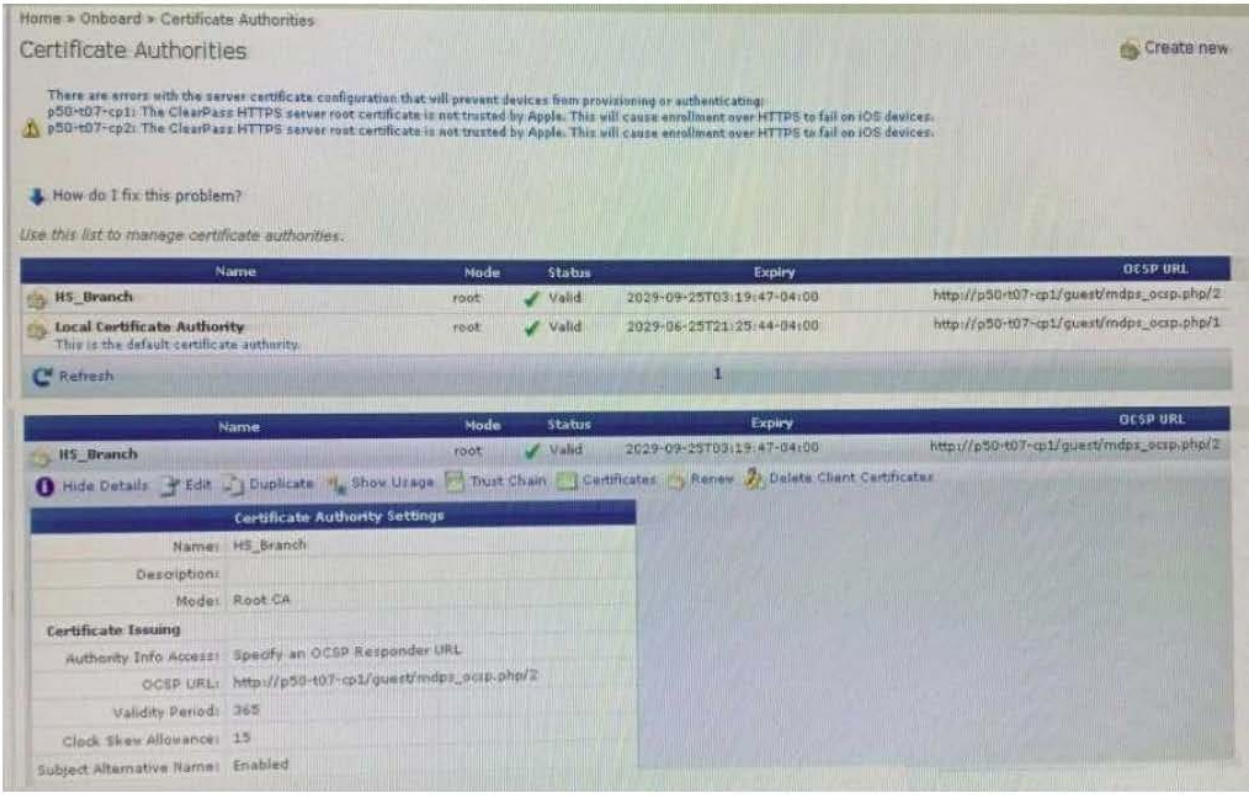
Authentication Methods:	1. [EAP TLS With OCSP Enabled] 2. [EAP PEAP]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2
Strip Username Rules:	/:user
Service Certificate:	-

Authorization:

Authorization Details:	1. AD1 2. AD2

Roles:

Role Mapping 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

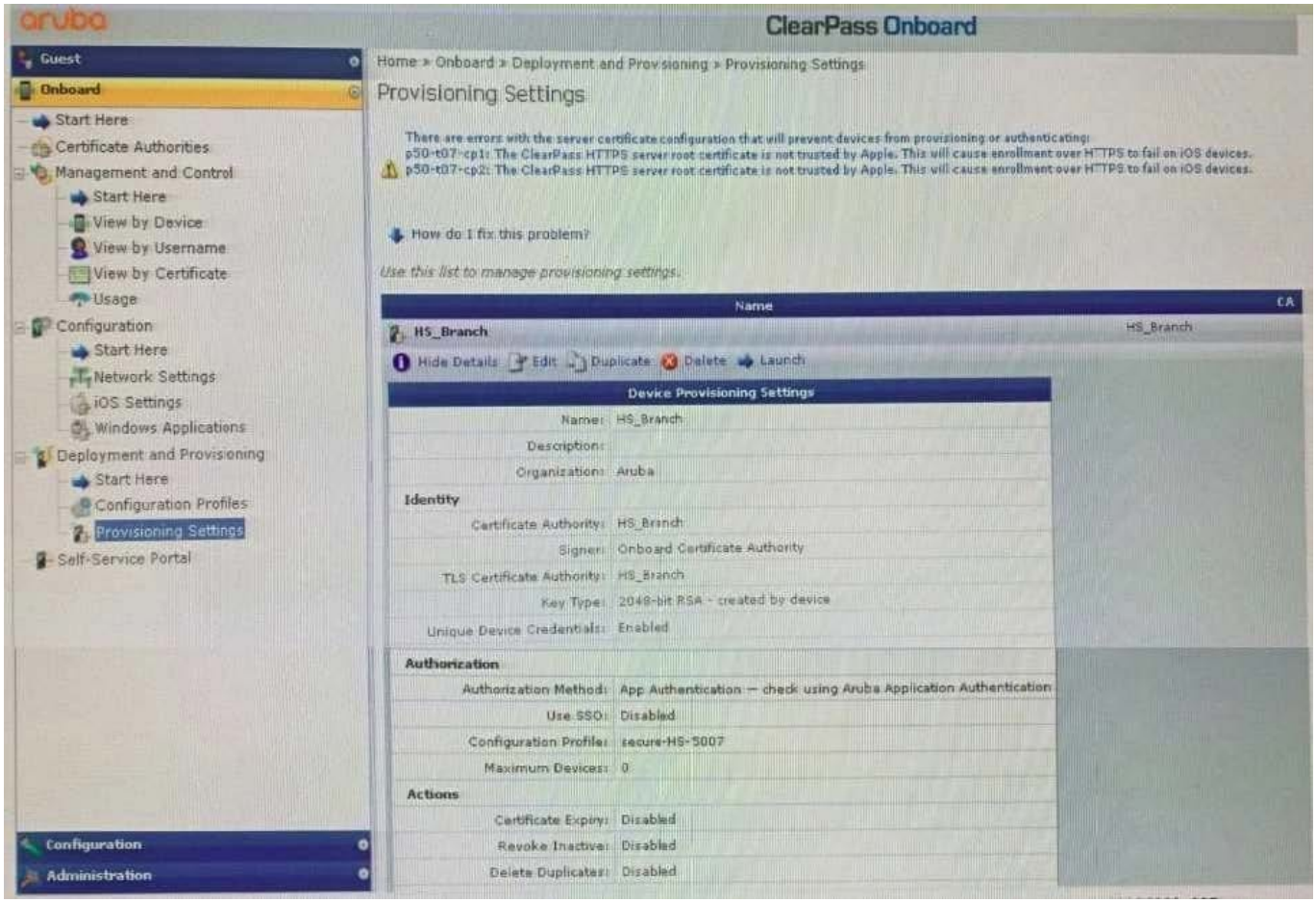
Refresh 1

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

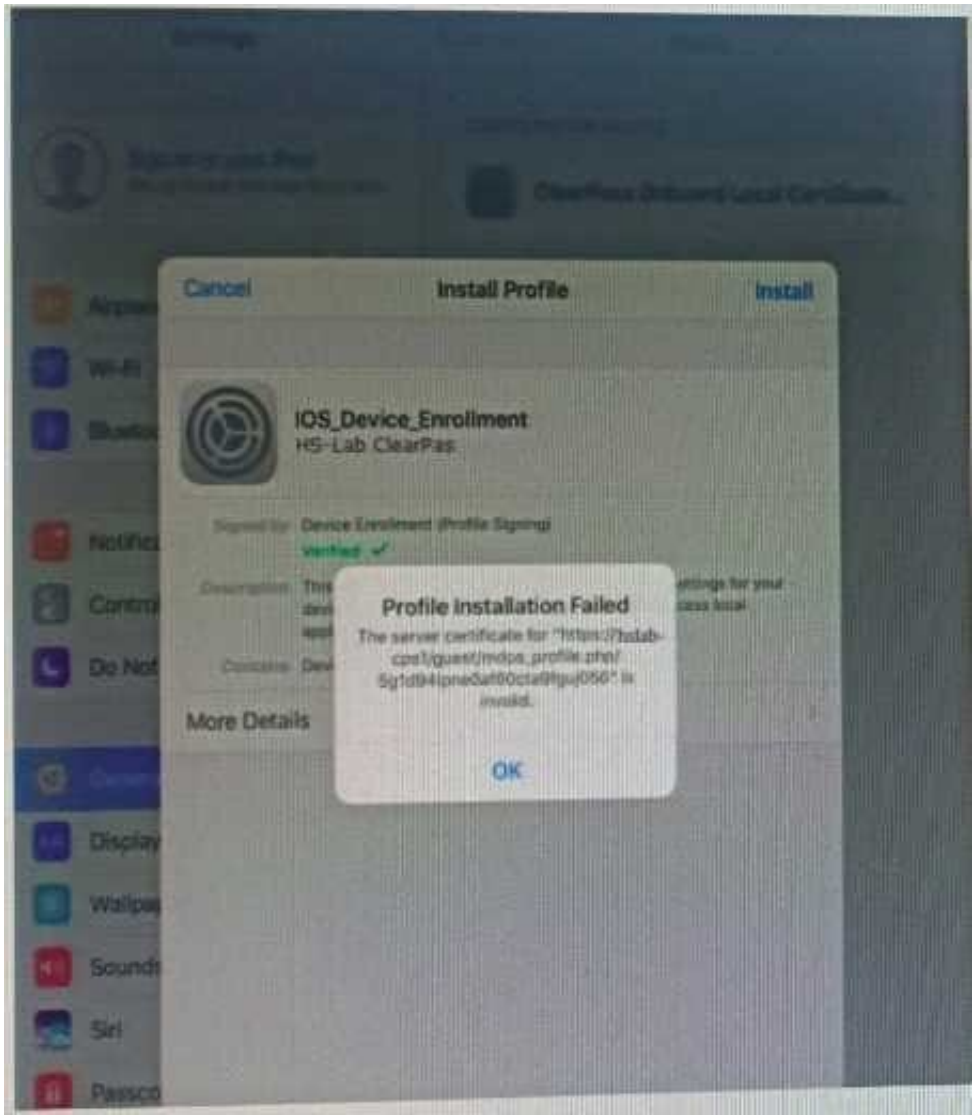
C. Reconnect the client and select the correct certificate when prompted

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

Correct Answer: A

QUESTION 6

Refer to the exhibit:



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.

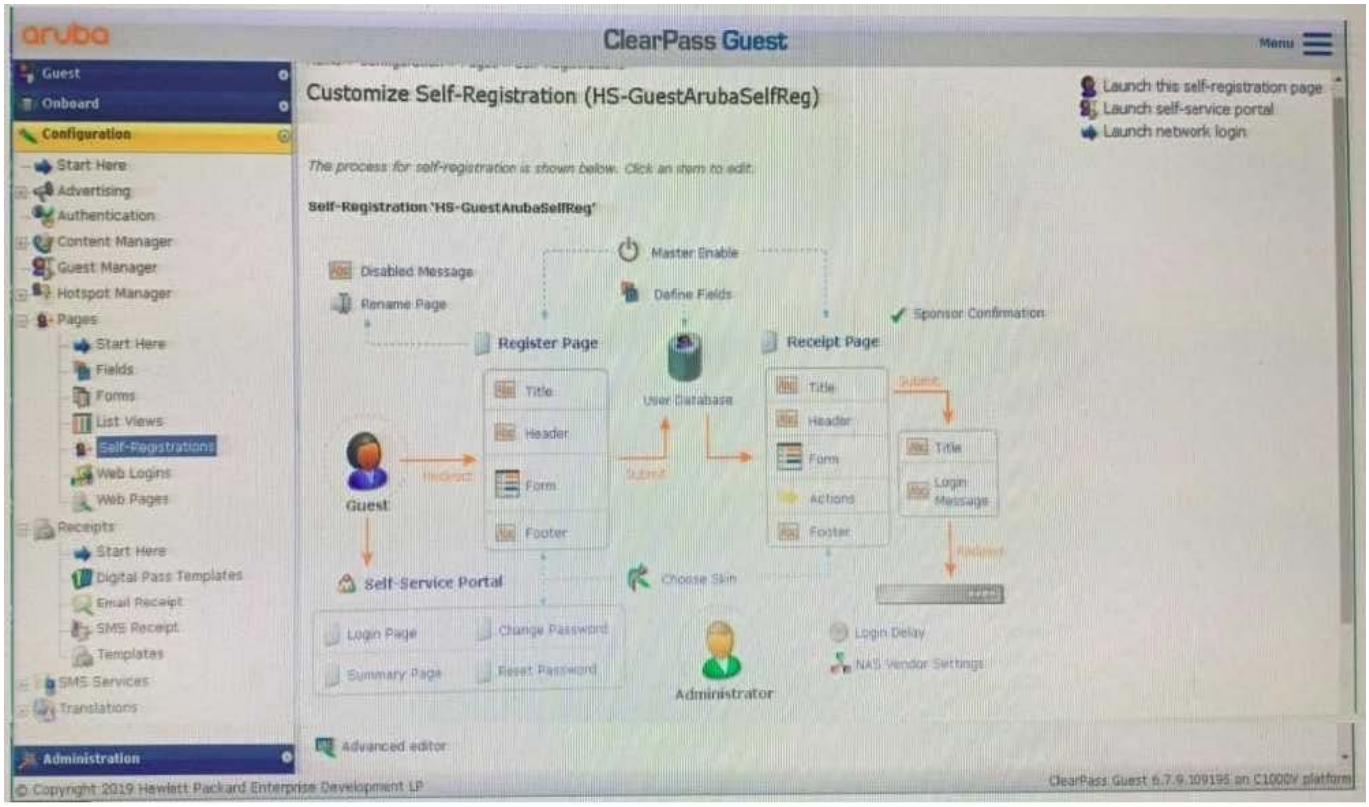
D. Check if the customer has Instated a custom HTTPS certificate for IDS and another internal PKI HTTPS certificate for other devices.

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

Correct Answer: AC

QUESTION 7

Refer to the exhibit:



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

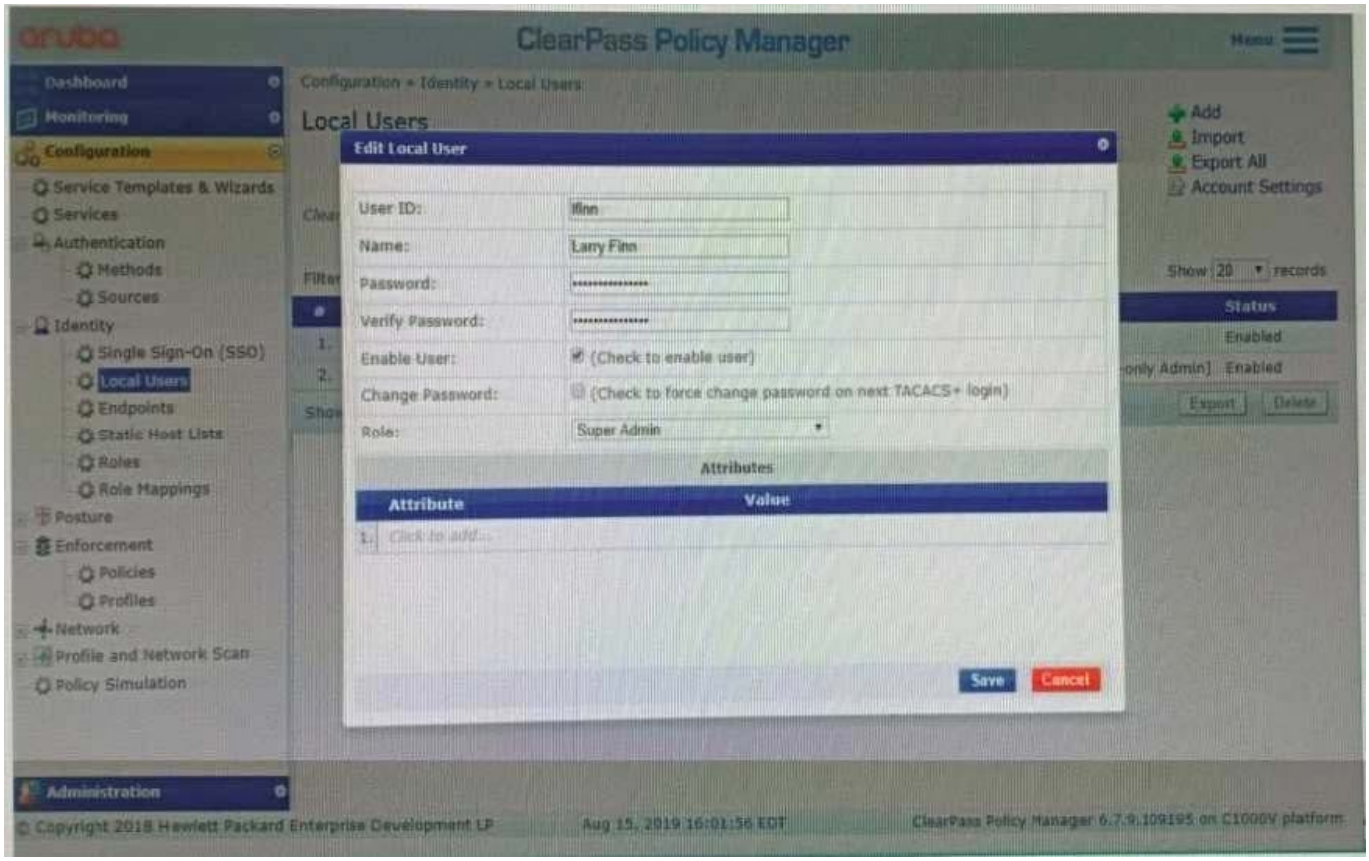
C. in me Configuration - Receipts - Email Receipts

D. in the Configuration - Receipts - Templates

Correct Answer: B

QUESTION 8

Refer to the exhibit:



The customer complains that the user shown cannot log into the ClearPass Server as an administrator using the [Policy Manager Admin Network Login Service]. What could be the reason for this?

A. The user might be used for a TACACS authentication

B. The account created does not fit this purpose.

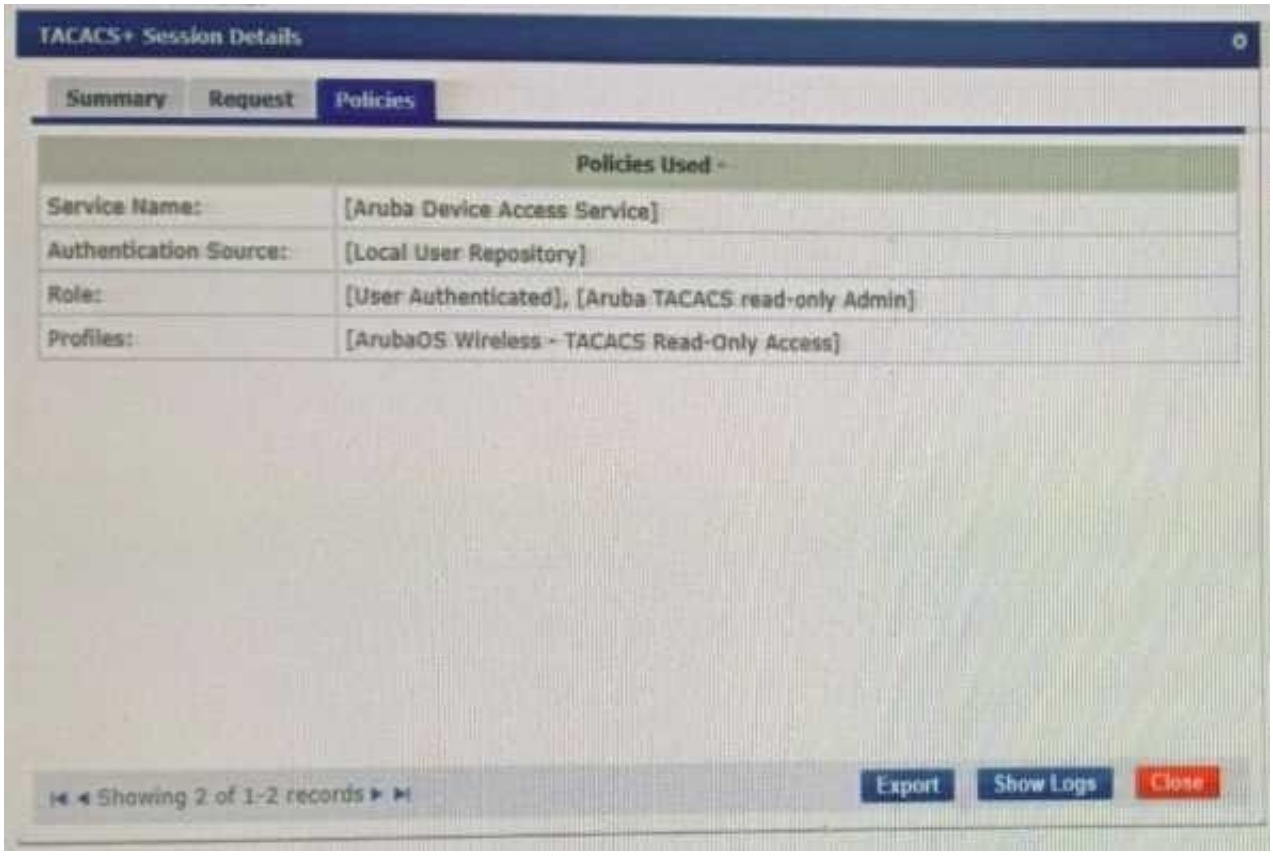
C. The mapping on the role should be changed to [RADIUS Super Admin]

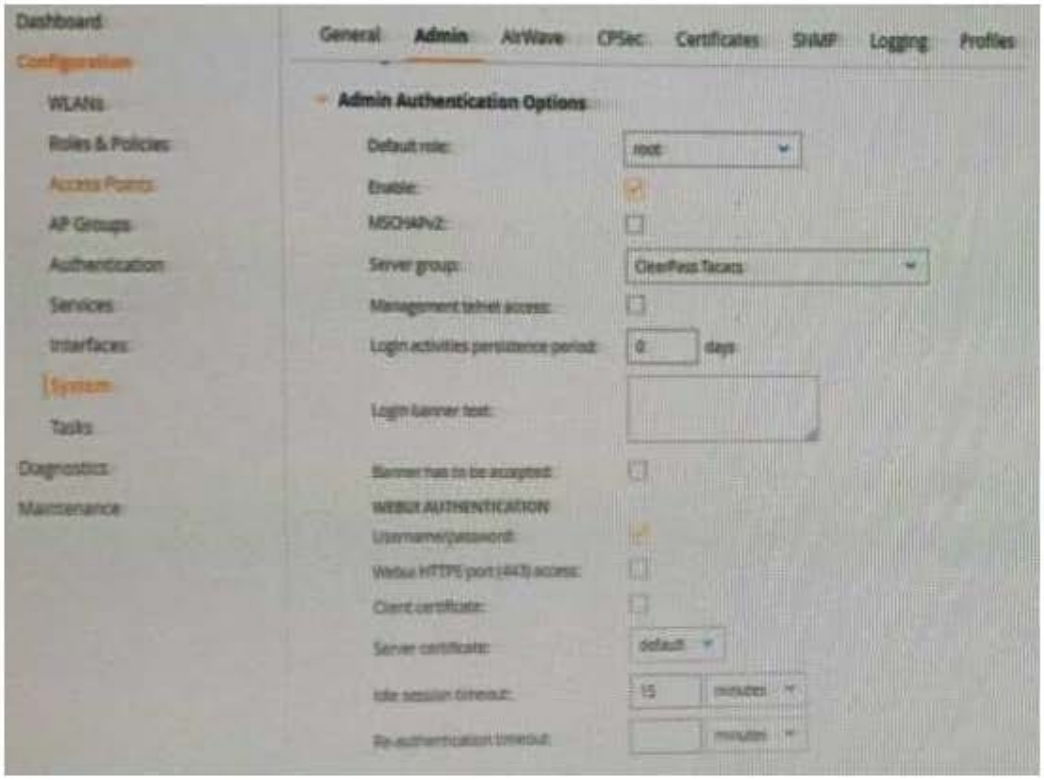
D. The local user authentication might be disabled

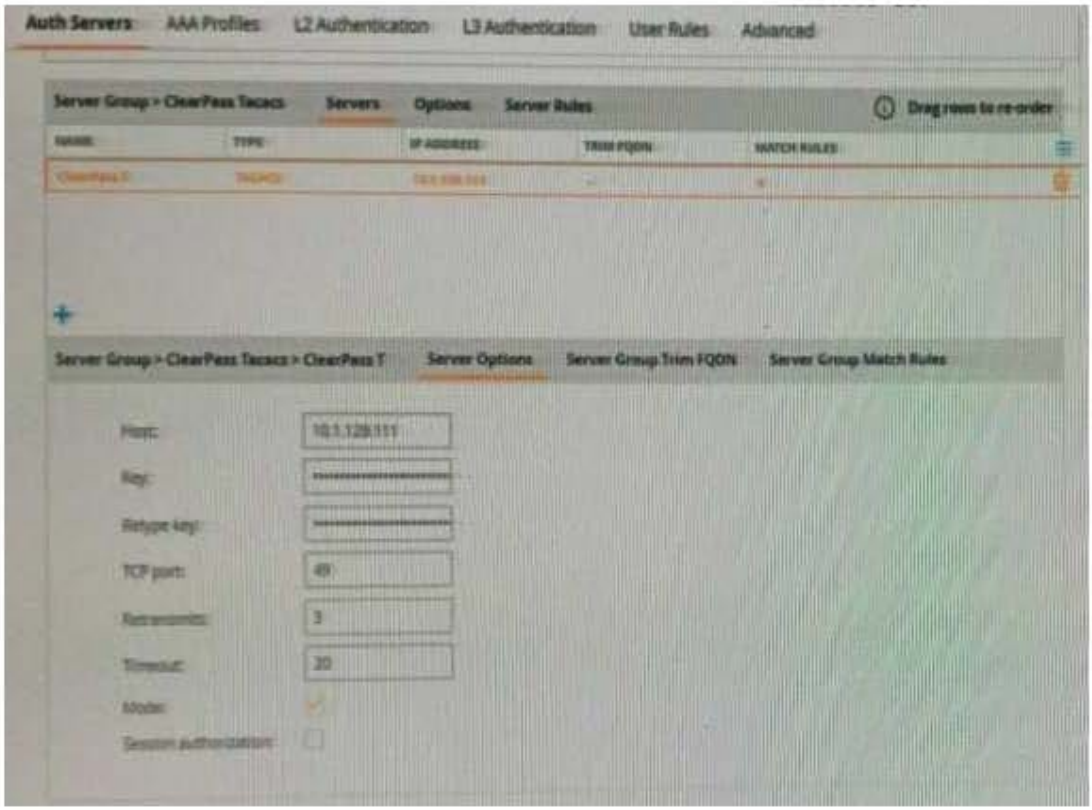
Correct Answer: B

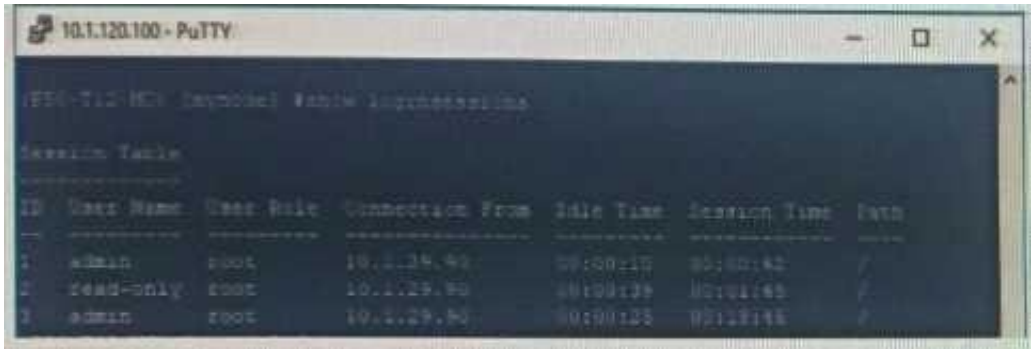
QUESTION 9

Refer to the exhibit:


TACACS+ Session Details
Summary
Request
Policies
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
Export
Show Logs
Close


Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
System
Tasks
Diagnostics
Maintenance
General
Admin
AirWave
CPSec
Certificates
SNMP
Logging
Profiles
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


Auth Servers
AAA Profiles
L2 Authentication
L3 Authentication
User Rules
Advanced
Server Group > ClearPass Tacacs
Servers
Options
Server Rules
Drag rows to re-order
NAME
TYPE
IP ADDRESS
TRIM FQDN
MATCH RULES
Server Group > ClearPass Tacacs > ClearPass T
Server Options
Server Group Trim FQDN
Server Group Match Rules
Host:
10.1.128.111
Key:
Retype key:
TCP port:
49
Retransmits:
3
Timeout:
20
Mode:
Session authentication:



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 10

A customer is planning to implement machine and user authentication on infrastructure with one Aruba

Controller and a single ClearPass Server.

What should the customer consider while designing this solution? (Select three.)

A. The Windows User must log off, restart or disconnect their machine to initiate a machine authentication before the cache expires.

B. The machine authentication status is written in the Multi-master cache on the ClearPass Server for 24 hrs.

C. Onboard must be used to install the Certificates on the personal devices to do the user and machine authentication.

D. The Customer should enable Multi-Master Cache Survivability as the Aruba Controller will not cache the machine state.

E. Machine Authentication only uses EAP TLS, as such a PKI infrastructure should be in place for machine authentication.

F. The customer does not need to worry about Multi-Master Cache Survivability because the Controller will also cache the machine state.

Correct Answer: BCE

QUESTION 11

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 12

A customer would like to allow only the AD users with the "Manager" title from the "HQ" location to Onboard their personal devices. Any other AD users should not be authorized to pass beyond the initial device provisioning page.

Which Onboard service will you use to implement this requirement?

A. Onboard CP login service

B. Onboard Authorization service

C. Onboard Provisioning service

D. Onboard Pre-Auth service

Correct Answer: A