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.pass4itsure.com/hpe6-a81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

A customer has completed all the required configurations in the Windows server in order for Active Directory Certificate Services (ADCS) to sign Onboard device TLS certificates. The Onboard portal and the Onboard services are also configured. Testing shows that the Client certificates ate still signed by the Onboard Certificate Authority and not ADCS. How can you help the customer with the situation?

A. Educate the customer that, when integrating with Active Directory Certificate Services (ADCS) the Onboard CA will the same authority used for signing me final TLS certificate of the device.

B. Configure the identity certificate signer as Active Directory Certificate Services and enter the ADCS URL http://ADCSVVeoEnrollmentServemostname/certsrv in the OnBoard Provisioning settings.

C. Enable access to EST servers from the Certificate Authority to make ClearPass Onboard to use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

D. Enable access to SCEP servers from the Certificate Authority to make ClearPass Onboard to use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

Correct Answer: C

QUESTION 2

Which statements are true about Aruba downloadable user roles? (Select three.)

A. Can be applied only on ports or WLAN users authenticated by ClearPass.

B. Aruba downloadable user role are universally available across the environment

C. Aruba downloadable user role is a built in enforcement template in ClearPass

D. Downloadable role names must be defined in Aruba switch or controller

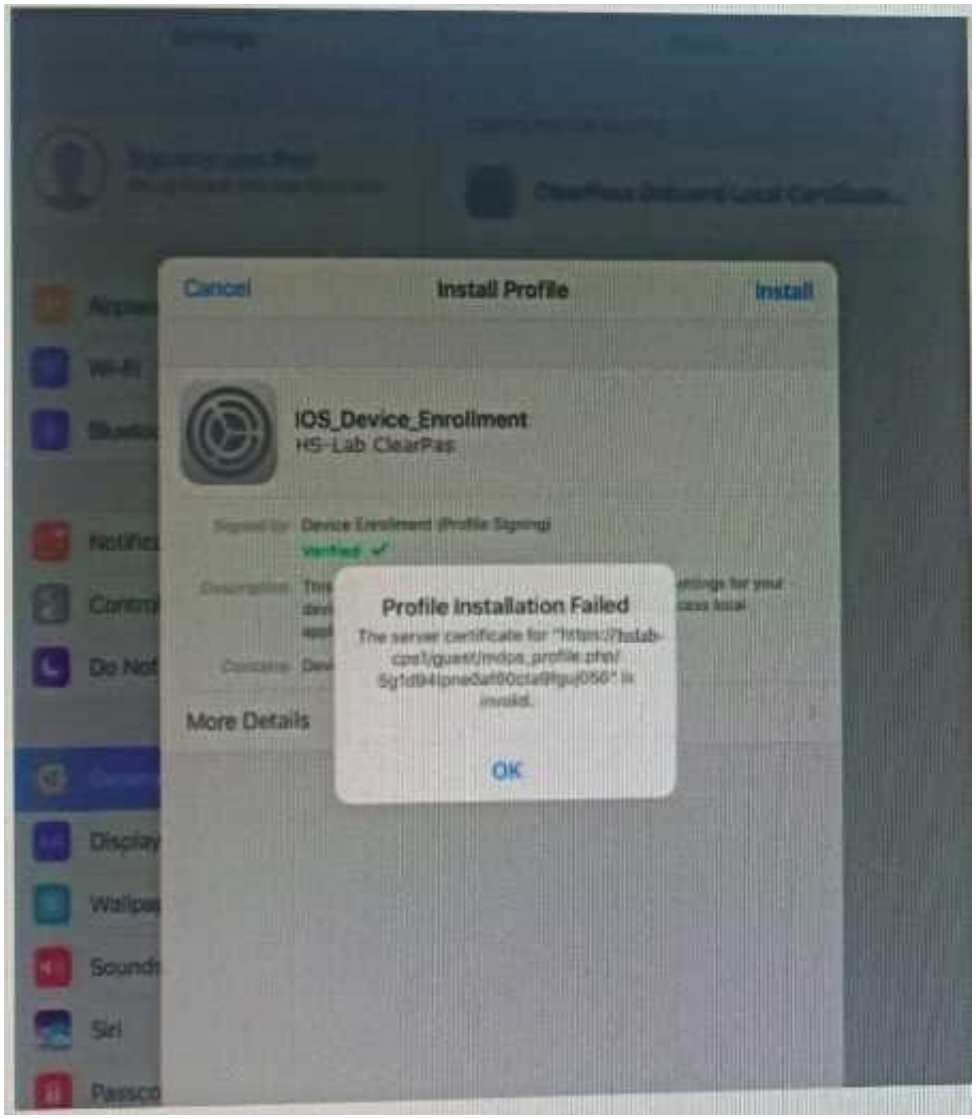
E. Can use these roles for other authentication methods not involving ClearPass

F. Administering downloadable user roles can be difficult for a large enterprise

Correct Answer: ADE

QUESTION 3

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.

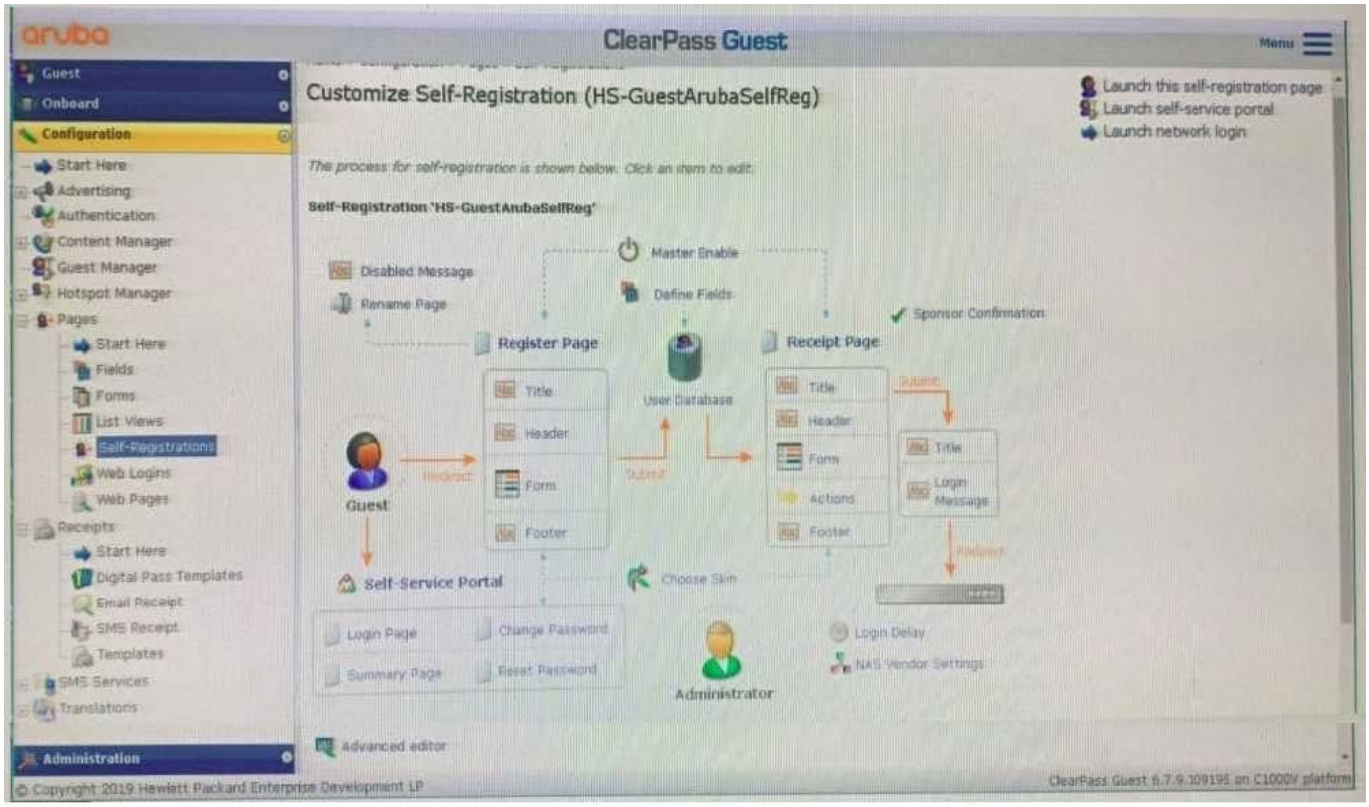
D. Check if the customer has Instated a custom HTTPS certificate for IDS and another internal PKI HTTPS certificate for other devices.

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

Correct Answer: AC

QUESTION 4

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

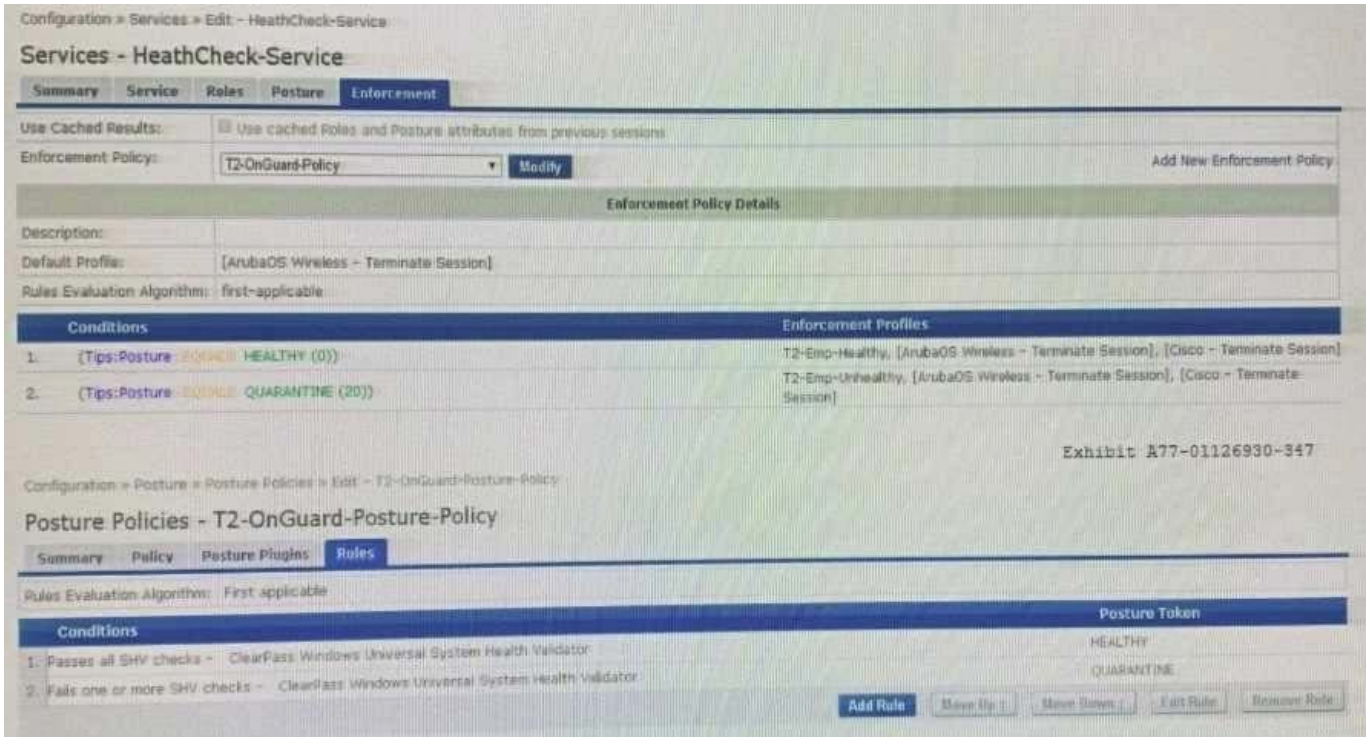
C. in me Configuration - Receipts - Email Receipts

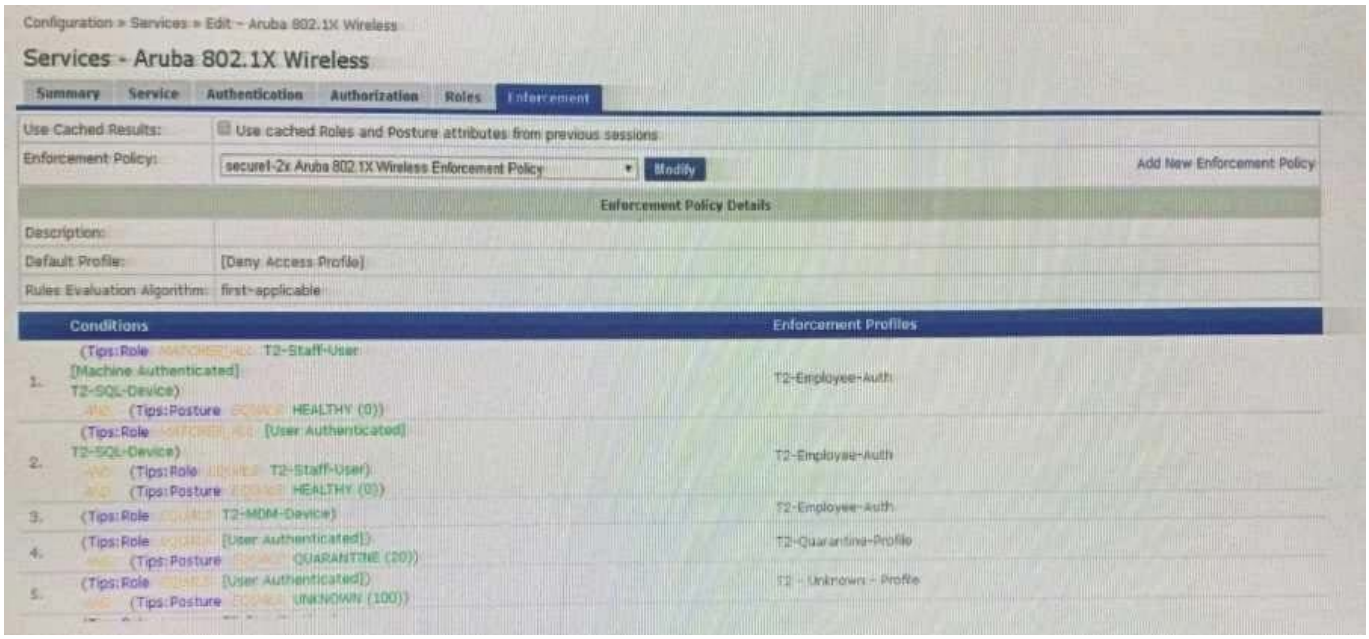
D. in the Configuration - Receipts - Templates

Correct Answer: B

QUESTION 5

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

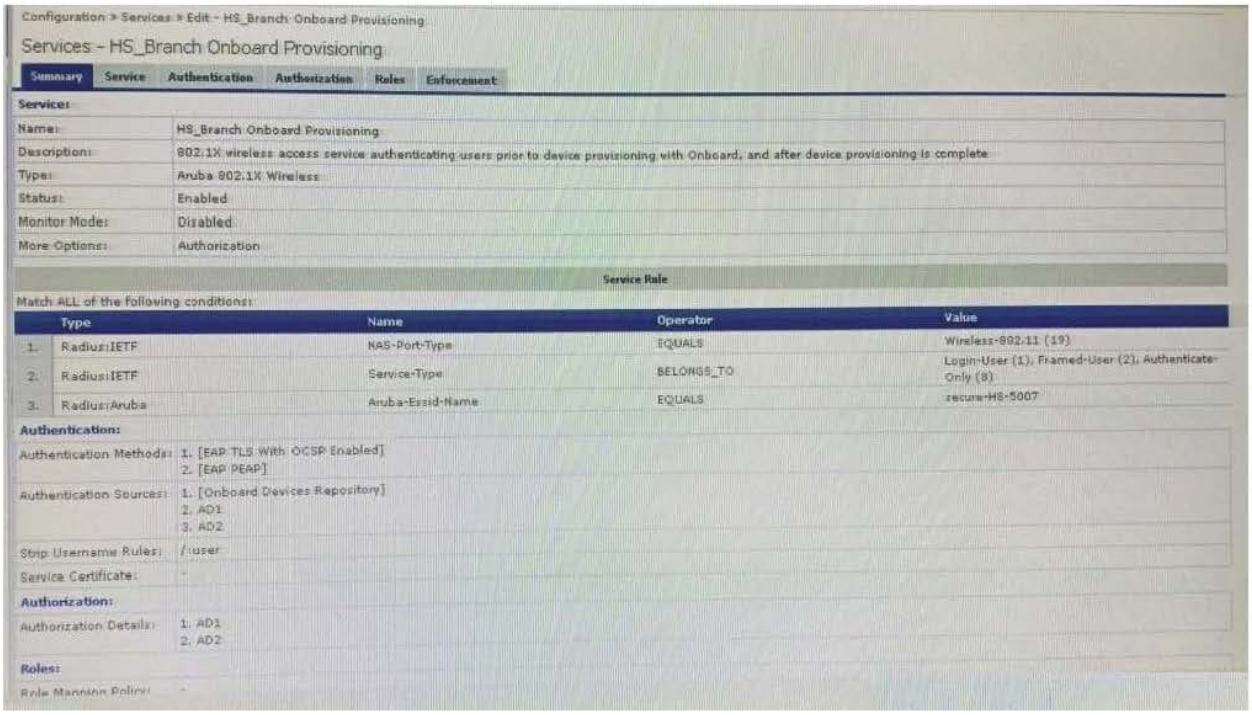
Correct Answer: B

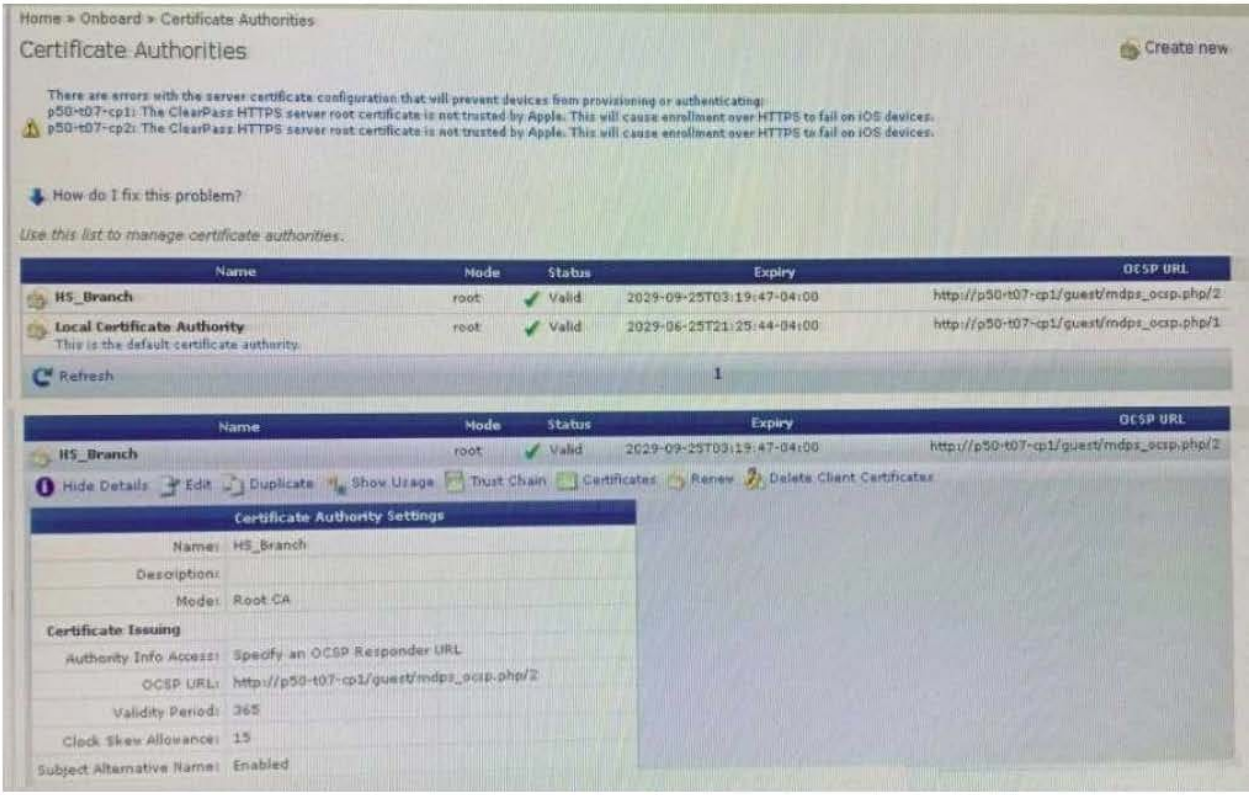
QUESTION 6

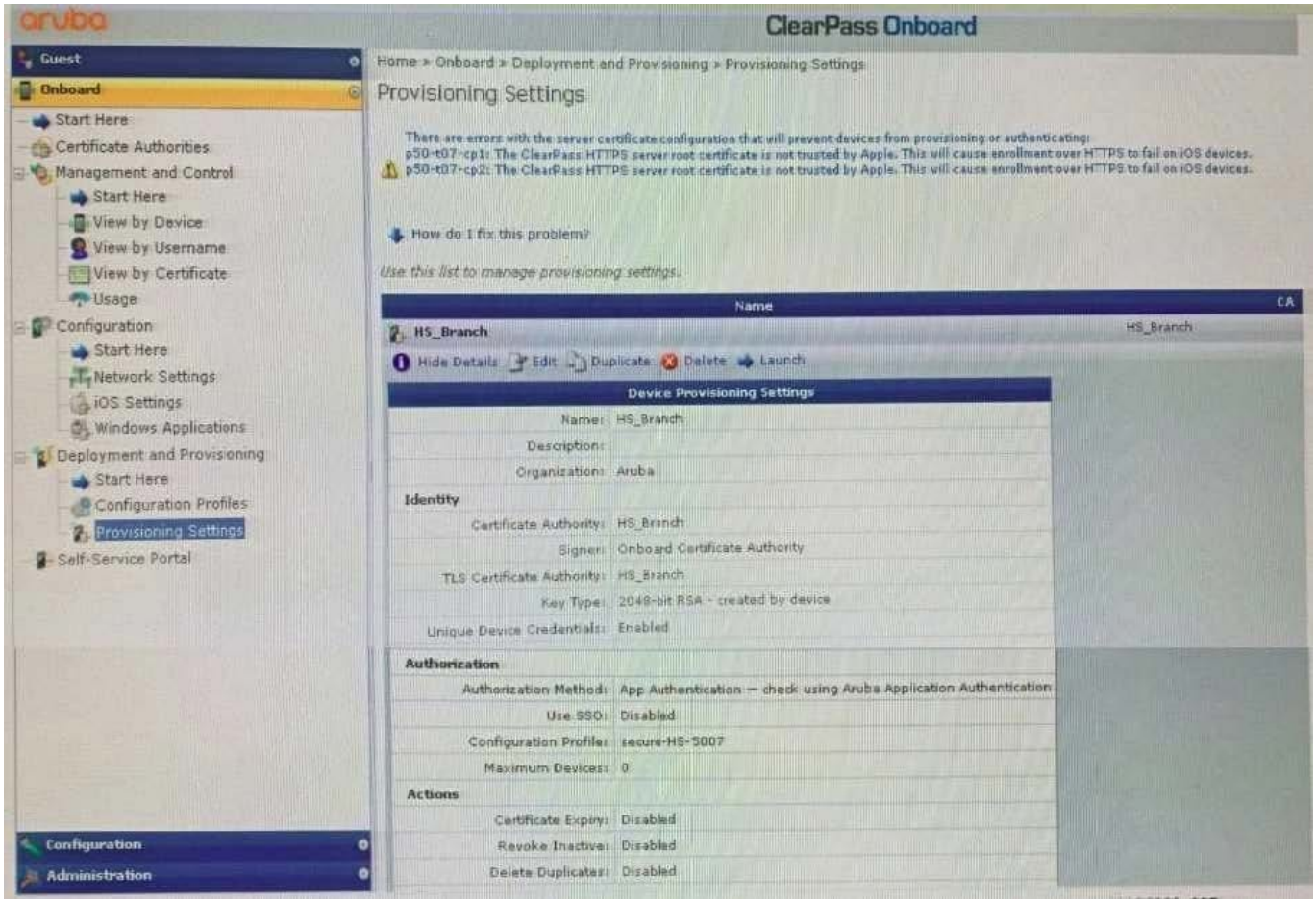
Refer to the exhibit:


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 7

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.

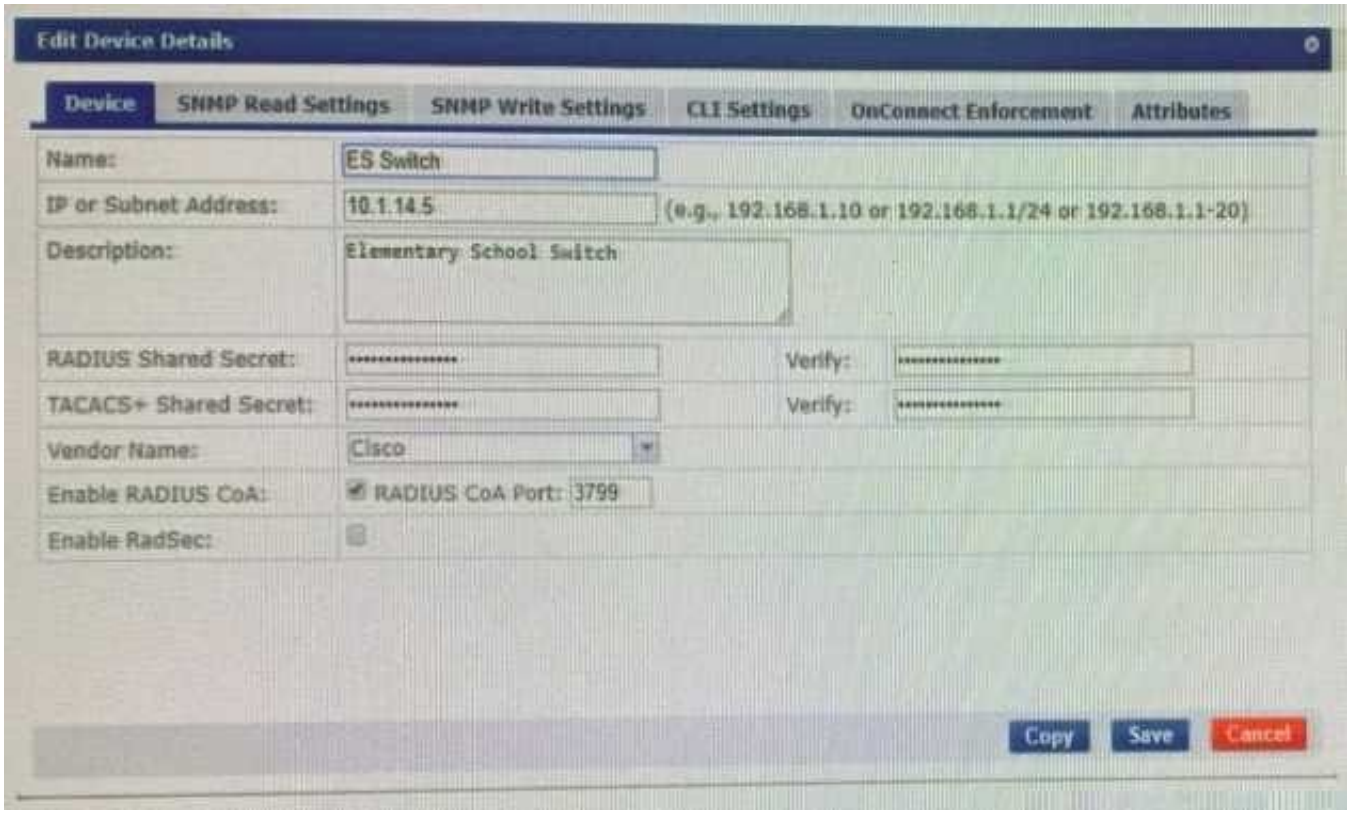
E. Machine Authentication only uses EAP TLS, as such a PKI infrastructure should be in place for machine authentication.

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 8

Refer to the exhibit: What are valid options for Network Access Device Settings? (Select two.)



A. You can configure SNMP Read Settings to monitor the load of a NAD in order not to overload it with the requests.

B. In CLI settings, you can define the access credentials and the command templates that will be used.

C. You can configure SNMP Write Settings to send commands to the devices that do not support other methods.

D. On the Attributes tab. you can enable the service to write attributes like Location and Device type based on policy.

E. The OnConnect Enforcement allows you to enable specific ports that trigger Enforcement when any device connects.

Correct Answer: DE

QUESTION 9

A customer is complaining that some of the devices, in their manufacturing network, are not getting profiled while other IoT devices from the same subnet have been correctly profiled. The network switches have been configured for DHCP IP helpers and IF-MAP has been configured on the Aruba Controllers. What can the customer do to discover those devices as well? (Select two.)

A. Update the Fingerprints Dictionary to the latest in case new devices have been added.

B. Open a TAC case to help you troubleshoot the DHCP device profile functionality.

C. Add the ClearPass Server IP as an IP helper address on the default gateway as well.

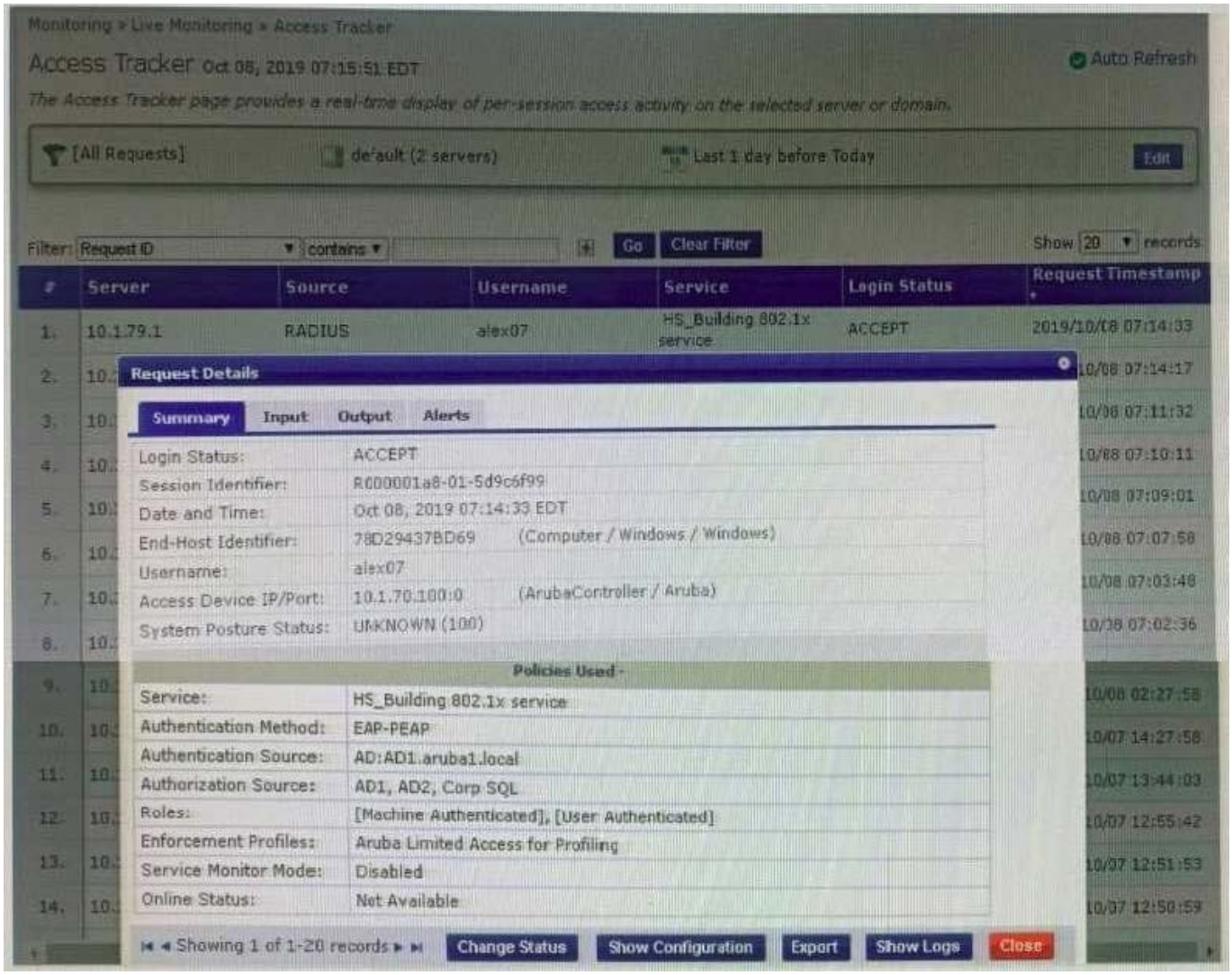
D. Allow time for IF-MAP service on the controller to discover the new devices as well.

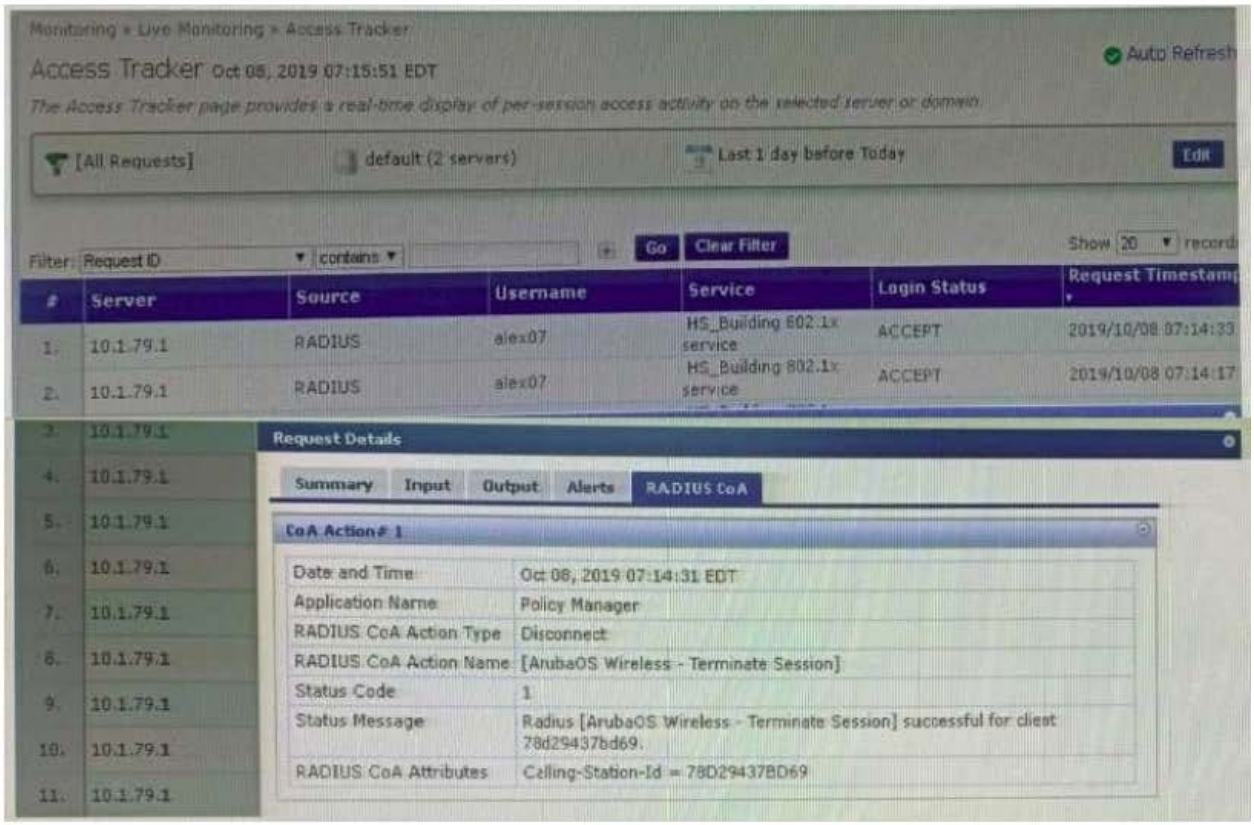
E. Manually create a new device fingerprint for the devices that are not being profiled.

Correct Answer: DE

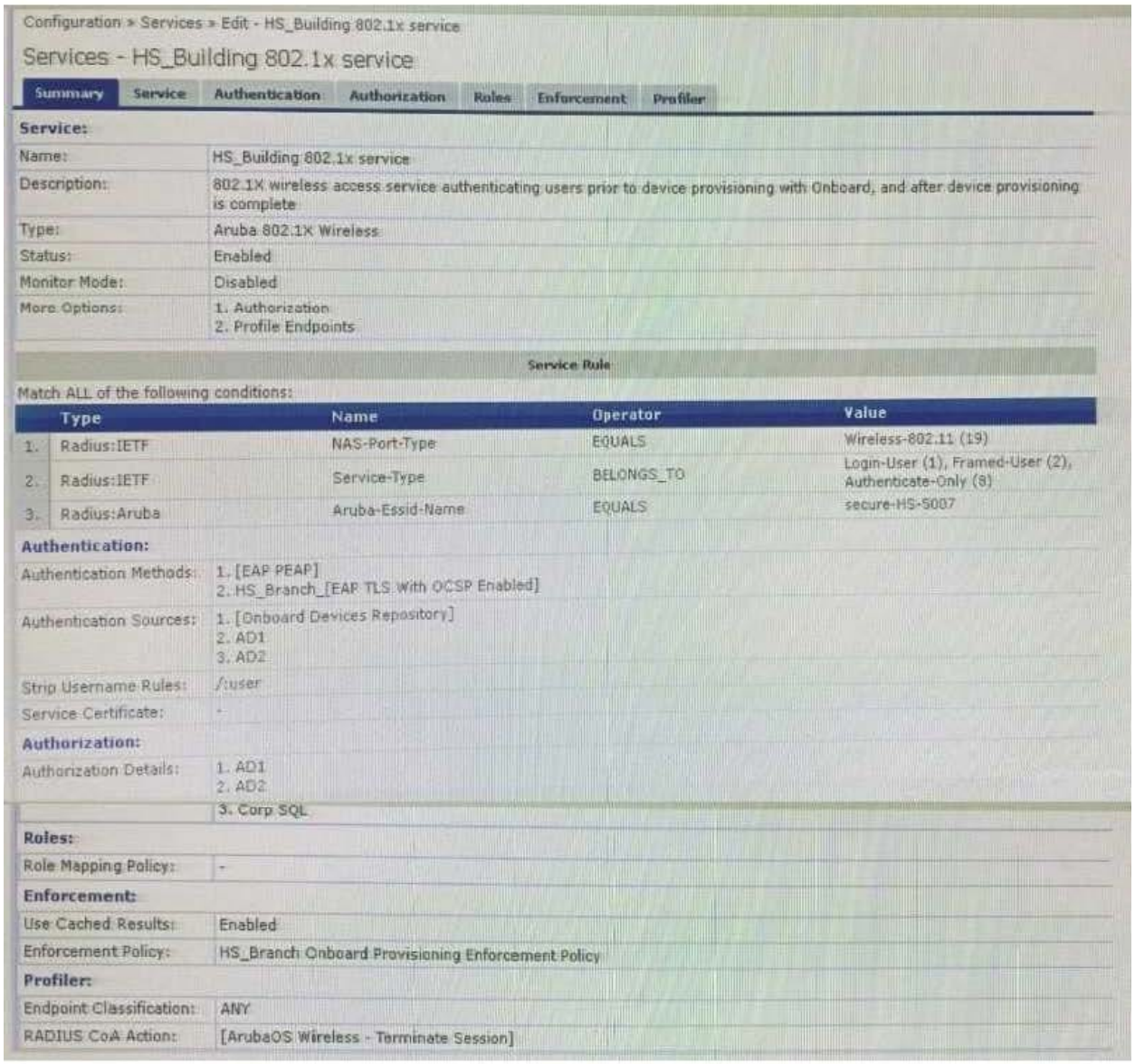
QUESTION 10

Refer to the exhibit:


Monitoring » Live Monitoring » Access Tracker
Access Tracker Oct 08, 2019 07:15:51 EDT
Auto Refresh
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
Edit
Filter: Request ID contains Go Clear Filter
Show 20 records
Server Source Username Service Login Status Request Timestamp
1. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:14:33
Request Details
Summary Input Output Alerts
Login Status: ACCEPT
Session Identifier: R000001a8-01-5d9c6f99
Date and Time: Oct 08, 2019 07:14:33 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
Authentication Source: AD:AD1.aruba1.local
Authorization Source: AD1, AD2, Corp SQL
Roles: [Machine Authenticated], [User Authenticated]
Enforcement Profiles: Aruba Limited Access for Profiling
Service Monitor Mode: Disabled
Online Status: Not Available
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Monitoring » Live Monitoring » Access Tracker
Access Tracker Oct 08, 2019 07:15:51 EDT
Auto Refresh
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
Edit
Filter: Request ID contains Go Clear Filter
Show 20 records
Server Source Username Service Login Status Request Timestamp
1. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:14:33
2. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:14:17
Request Details
Summary Input Output Alerts RADIUS CoA
CoA Action# 1
Date and Time Oct 08, 2019 07:14:31 EDT
Application Name Policy Manager
RADIUS CoA Action Type Disconnect
RADIUS CoA Action Name [ArubaOS Wireless - Terminate Session]
Status Code 1
Status Message Radius [ArubaOS Wireless - Terminate Session] successful for client 78d29437bd69.
RADIUS CoA Attributes Calling-Station-Id = 78D29437BD69


Configuration » Identity » Endpoints
Endpoints
Add
Import
Export All
This page automatically lists all authenticated endpoints. An endpoint device is an Internet-capable hardware device on a TCP/IP network (e.g. laptops, smart phones, tablets, etc.).
Filter: MAC Address contains 78D29437BD69 Go Clear Filter
Show 20 records
MAC Address Hostname Device Category Device OS Family Status Profiled
1. 78d29437bd69 p50-t07-vlt4 Computer Windows Unknown Yes
Showing 1-1 of 1
Authentication Records Bulk Update Bulk Delete Trigger Server Action Update Fingerprint Export Delete



Configuration » Services » Edit - HS_Building 802.1x service

Services - HS_Building 802.1x service

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Service:

Name:	HS_Building 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:Aruba	Aruba-Essid-Name	EQUALS	secure-HS-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
Strip Username Rules:	/:user
Service Certificate:	-

Authorization:

Authorization Details:	1. AD1 2. AD2 3. Corp SQL

Roles:

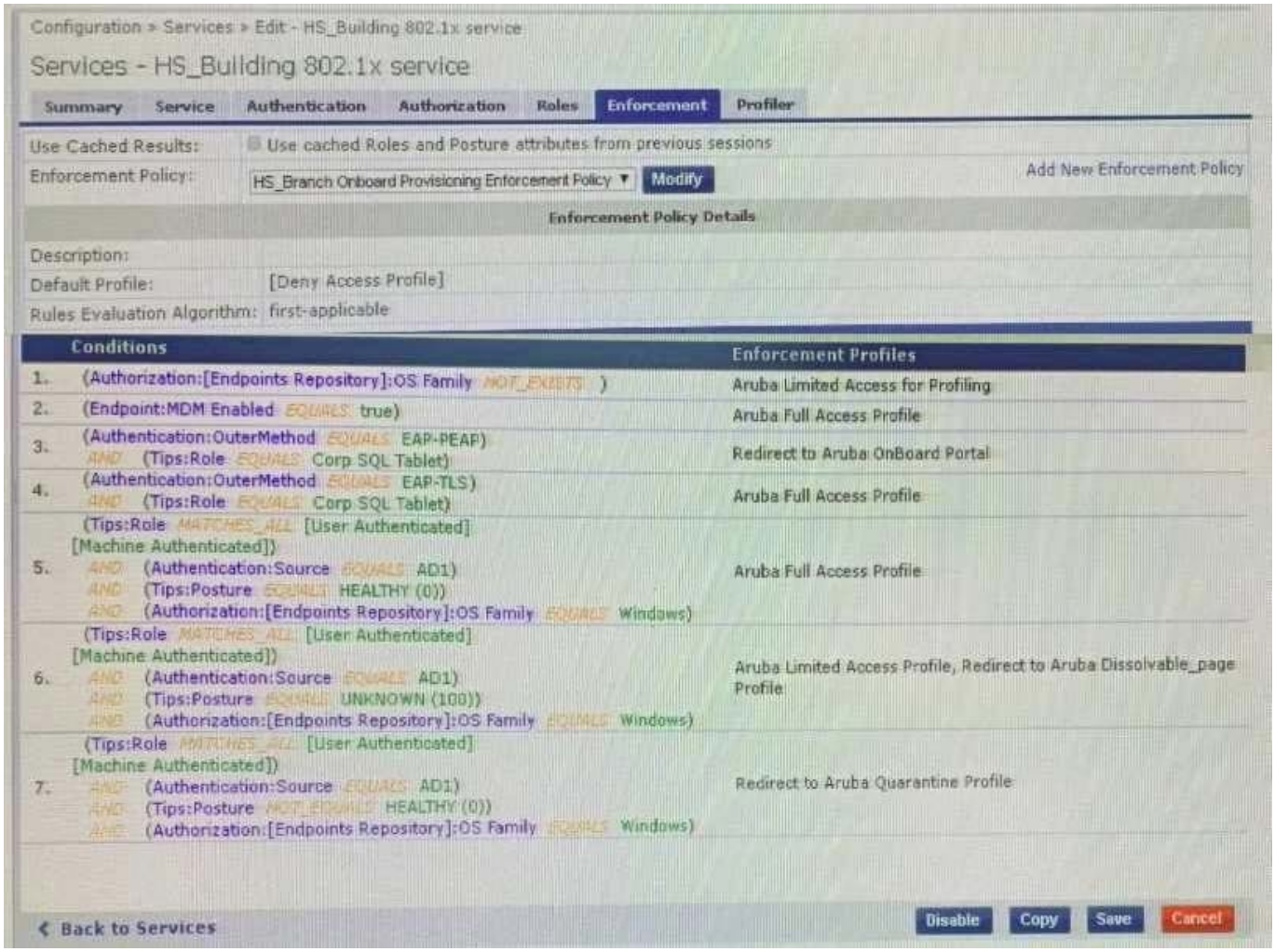
Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Enabled
Enforcement Policy:	HS_Branch Onboard Provisioning Enforcement Policy

Profiler:

Endpoint Classification:	ANY
RADIUS CoA Action:	[ArubaOS Wireless - Terminate Session]



You configured the 802 1 x service enforcement conditions with the Endpoint profiling data. When the client connects to the network. ClearPass successfully profiles the client but the client always receives an incorrect enforcement profile The configurations in the Aruba controller are completed correctly. What is the cause of the issue?

A. An additional authorization source should be configured for profiling to work.

B. The enforcement policy conditions configured with profiling data are not correct.

C. The enforcement policy rules evaluation algorithm Is not configured correctly.

D. The option, use cached roles and posture from previous sessions should be enabled.

Correct Answer: B