HPE6-A77 Q&As

Aruba Certified ClearPass Expert Written

Pass HP HPE6-A77 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/hpe6-a77.html

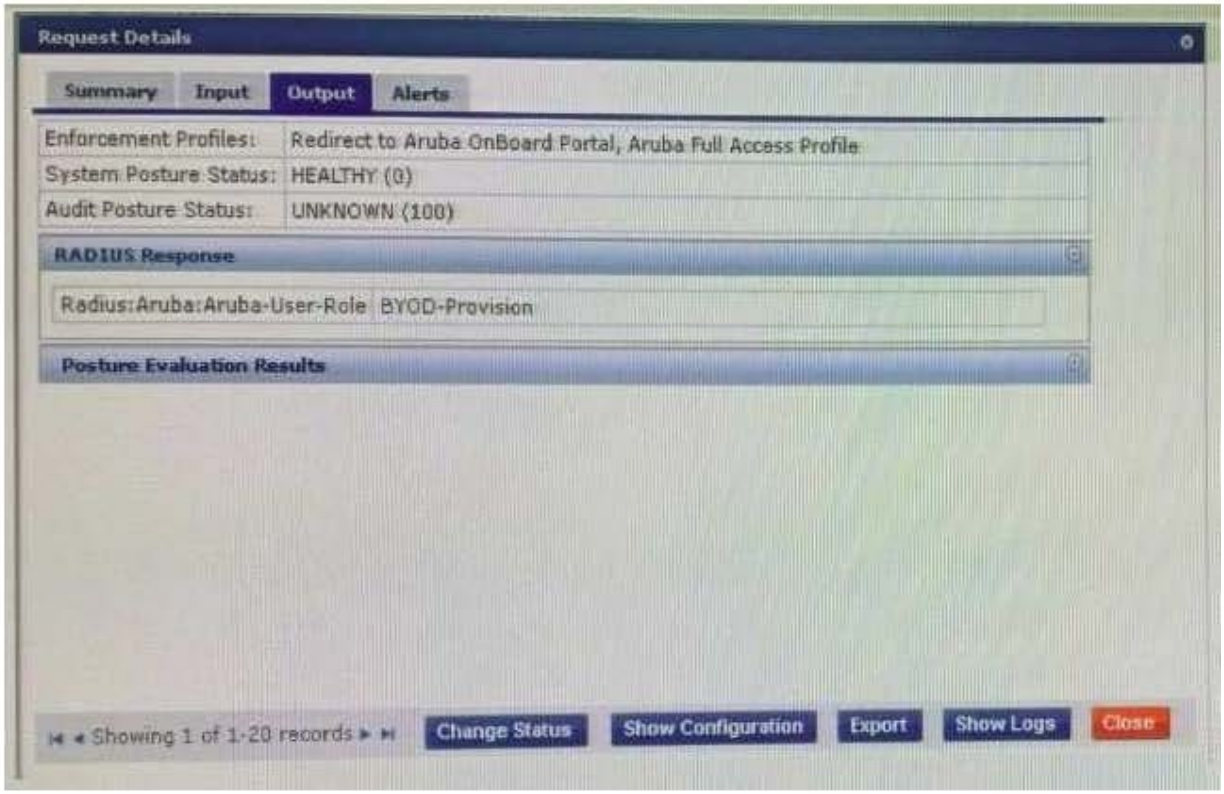
100% Passing Guarantee
100% Money Back Assurance

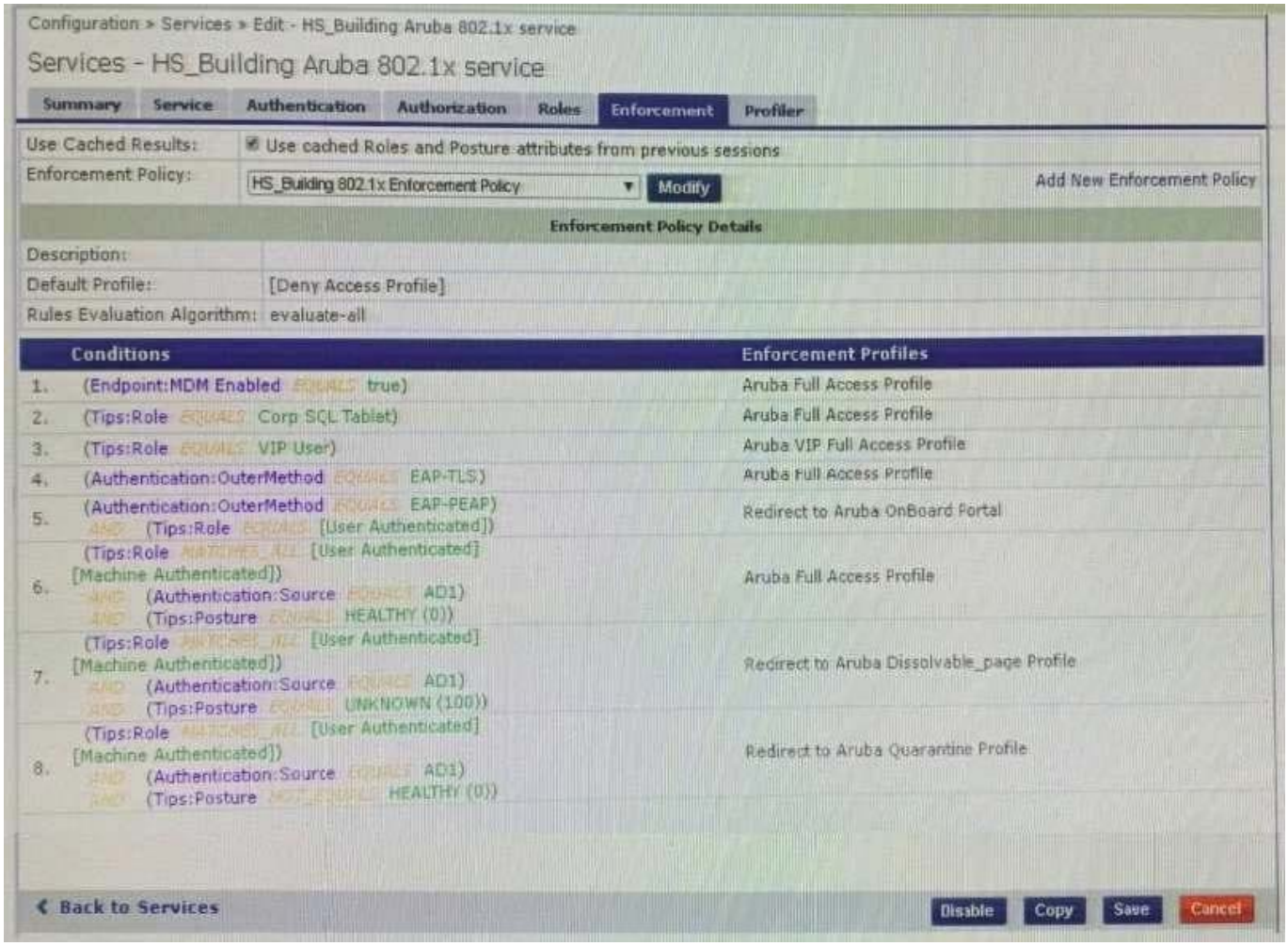
Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

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.

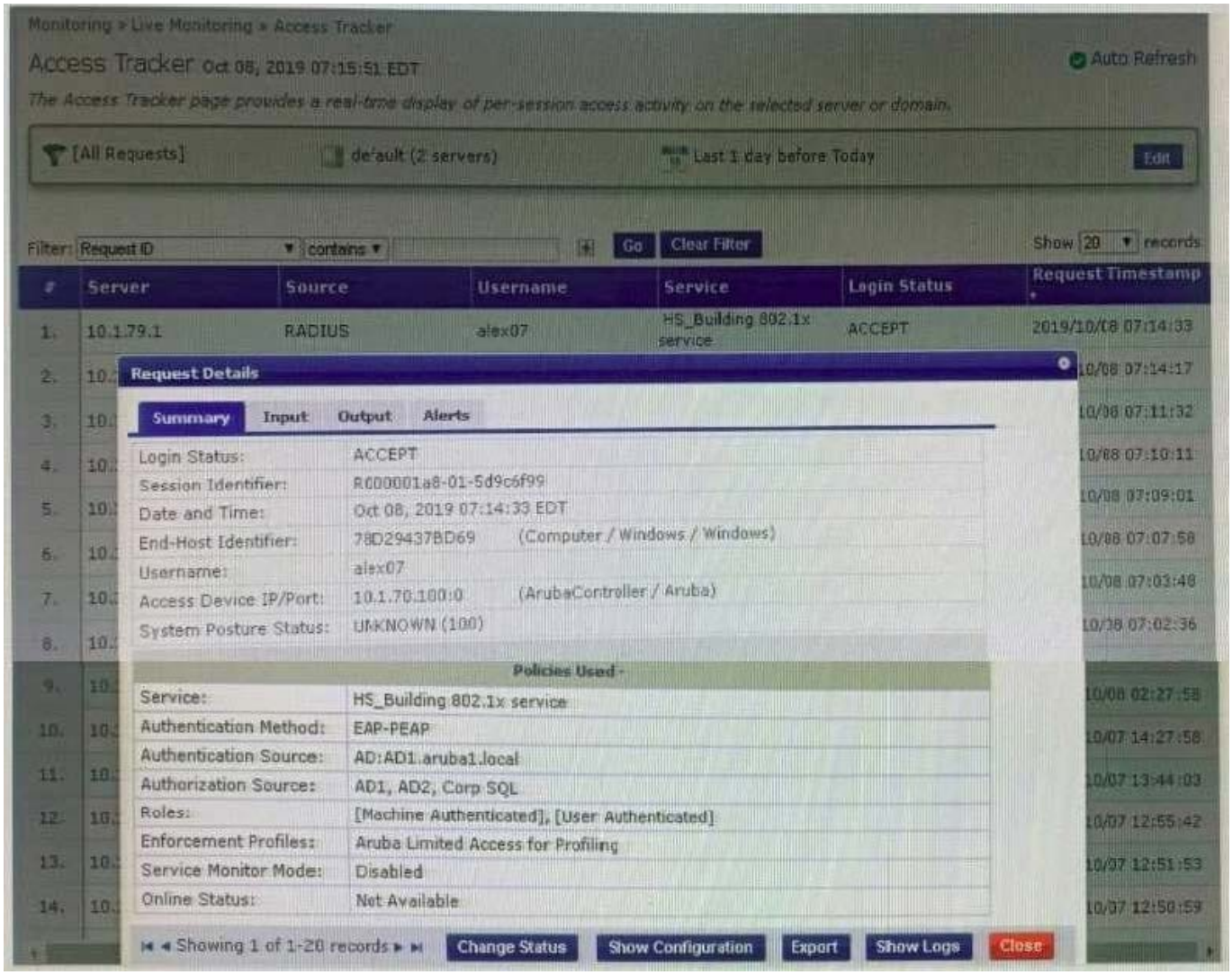
D. Modify the enforcement policy and re-order the condition with Posture - Unknown as the fifth condition

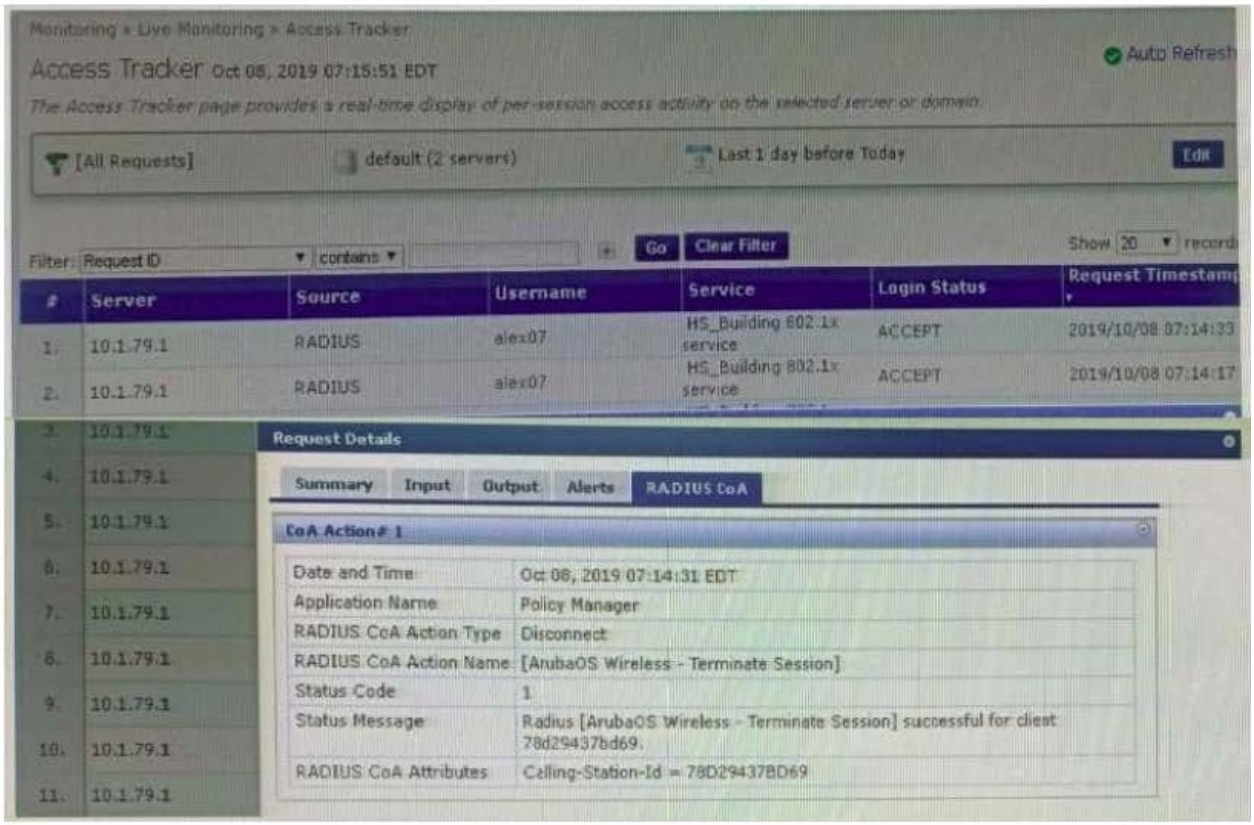
E. Remove the EAP-PEAP with [user authenticated] condition for Onboard and create another service

Correct Answer: CD

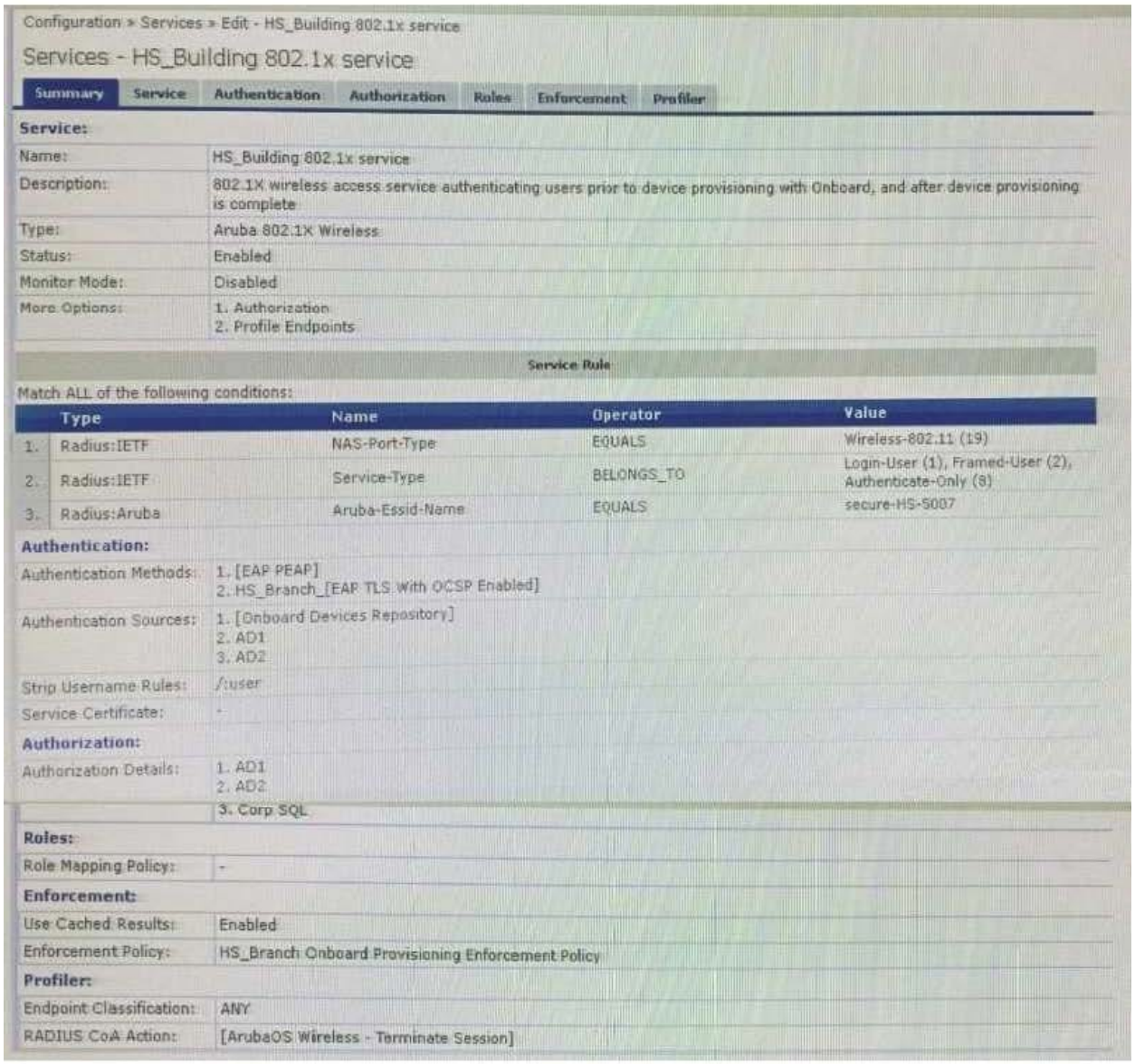
QUESTION 2

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
2. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/08 07:14:17
3. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/08 07:11:32
4. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/08 07:10:11
5. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/08 07:09:01
6. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/08 07:07:58
7. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/08 07:03:48
8. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/08 07:02:36
9. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/08 02:27:58
10. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/07 14:27:58
11. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/07 13:44:03
12. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/07 12:55:42
13. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/07 12:51:53
14. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 10/07 12:50:59
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:

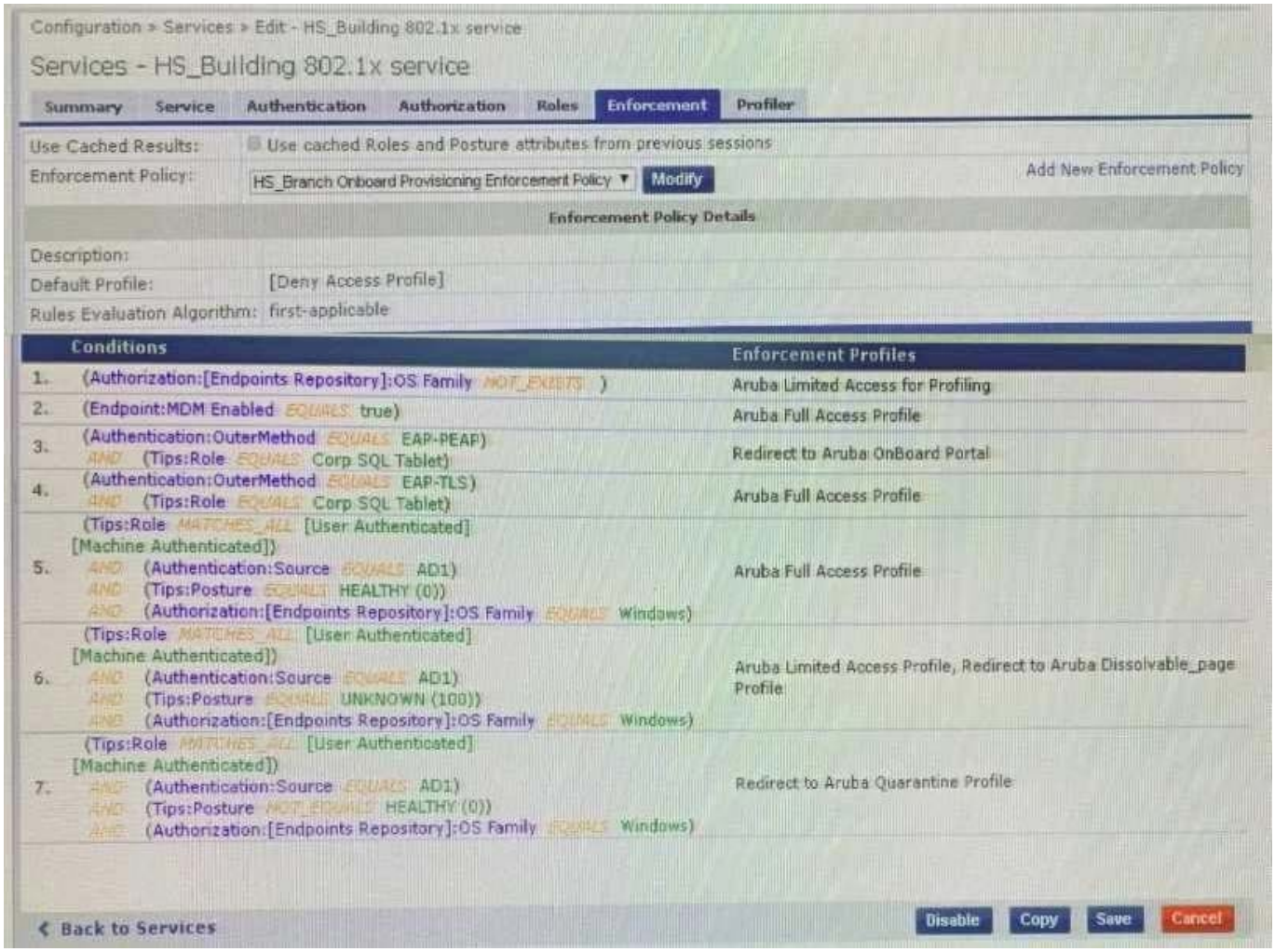
Role Mapping Policy:	-

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

QUESTION 3

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.

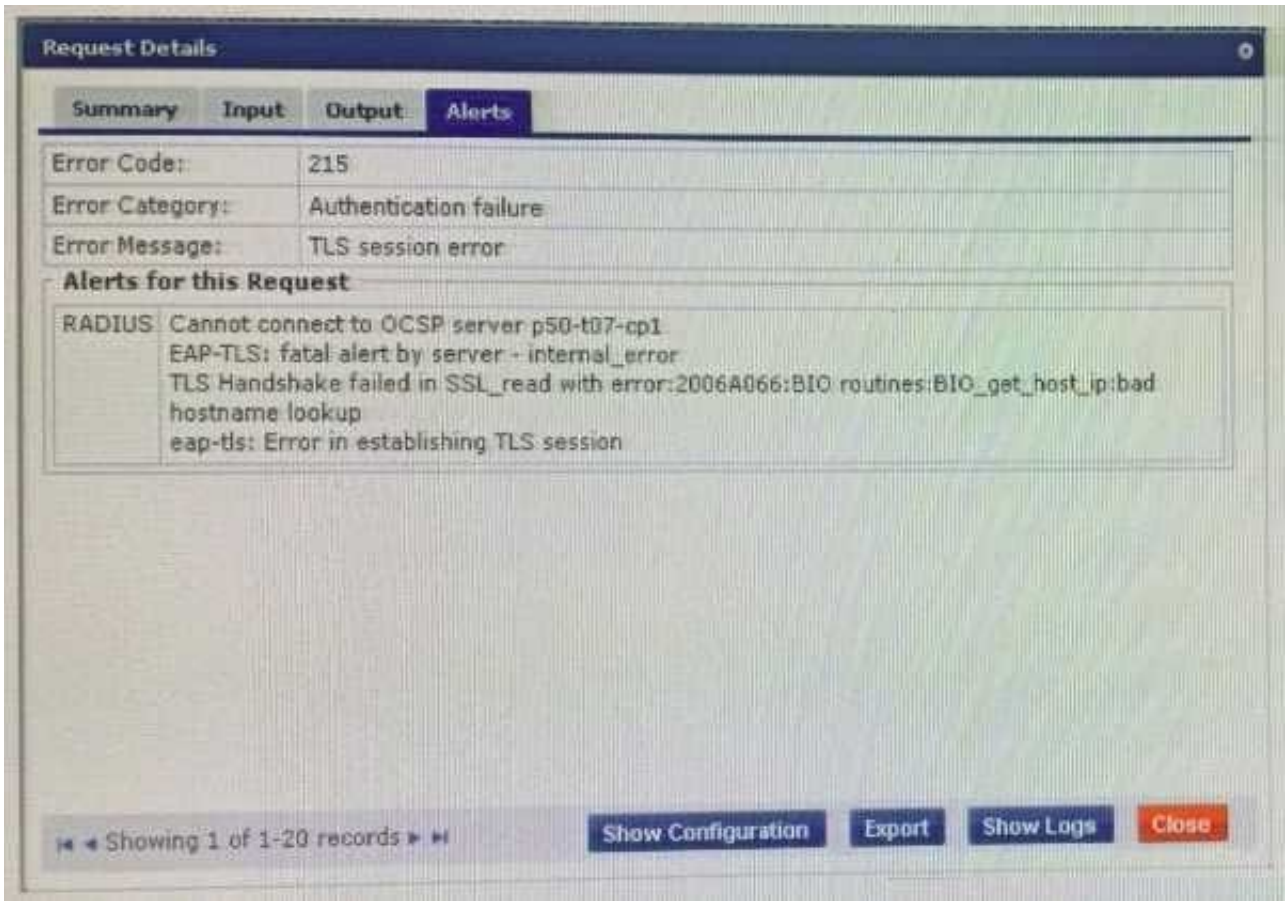
C. Verify if Onboard Pre-Provisioning enforcement profile sends the correct Aruba user role.

D. Verify if the external captive portal profile is enabled to use HTTPS with port 443.

Correct Answer: B

QUESTION 4

Refer to the exhibit: A customer has configured Onboard in a cluster. After the Primary server\\'s failure, the BYOD devices fail to connect to the network. What would you do to troubleshoot?



A. Verify the OSCP URL under TLS authentication method is mapped to http://localhost/ guestmdps_ocsp.php/2

B. Reboot the active ClearPass server and reconnect the client to the SSID by selecting the correct certificate when prompted

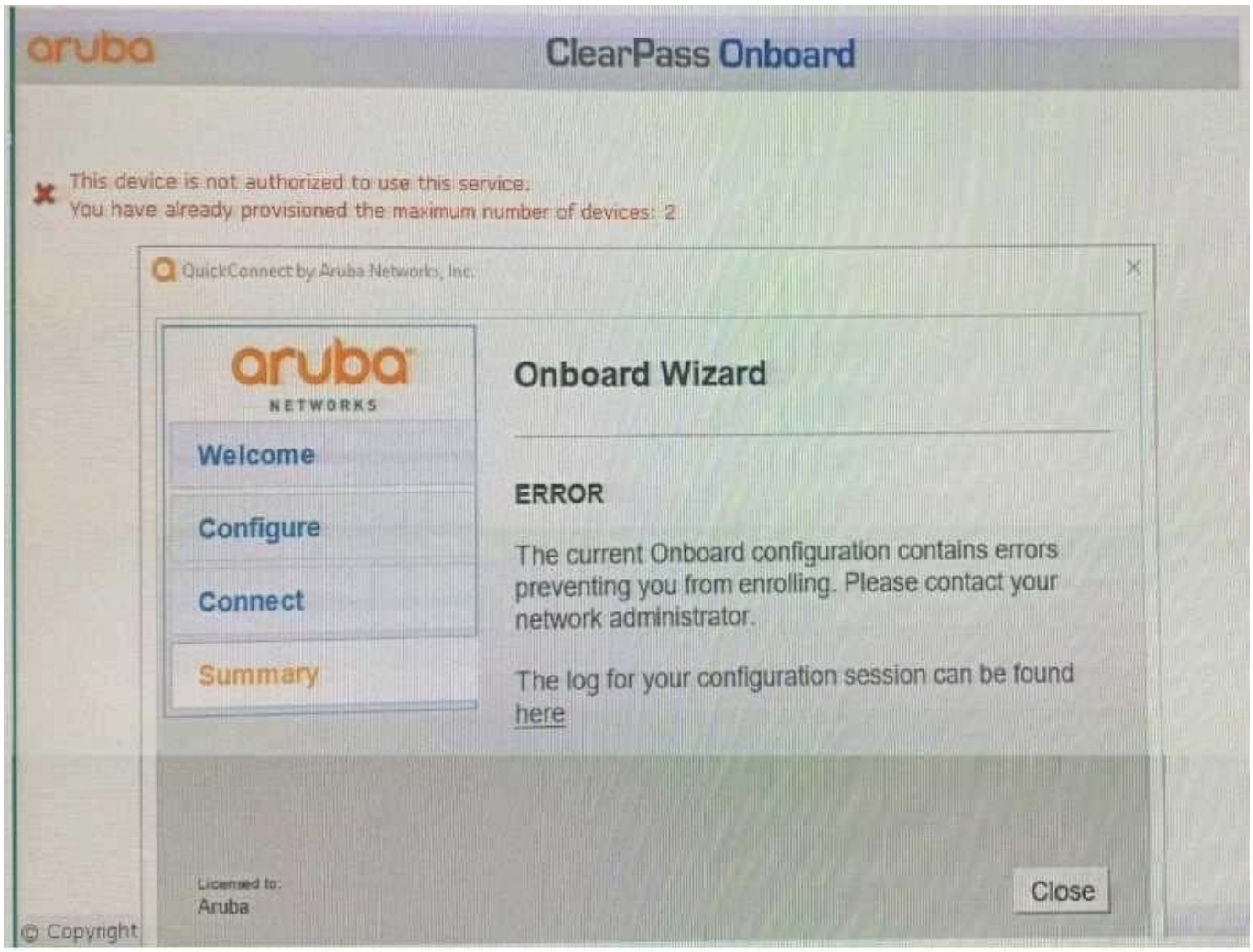
C. Check EAP certificate on the secondary node is issued by the same common root Certificate Authority (CA)

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

Correct Answer: B

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?



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