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.pass2lead.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

A customer is looking to implement a Web-Based Health Check solution with the following requirements:

for the HR user\\'s client devices, check if a USB stick is mounted.

for the RandD user\\'s client devices, check if the hard disk is fully encrypted.

The Web-Based Health Check service has been configured but the customer it is not sure how to design

the Profile Policy.

How can be accomplished this customer request?

A. create two Posture Policies and customize the OnGuard Agent (Persistent or Dissolvable) to select the correct SHV checks

B. create one Posture Policy and define Rules Conditions that will apply different Tokens for each SHV check condition

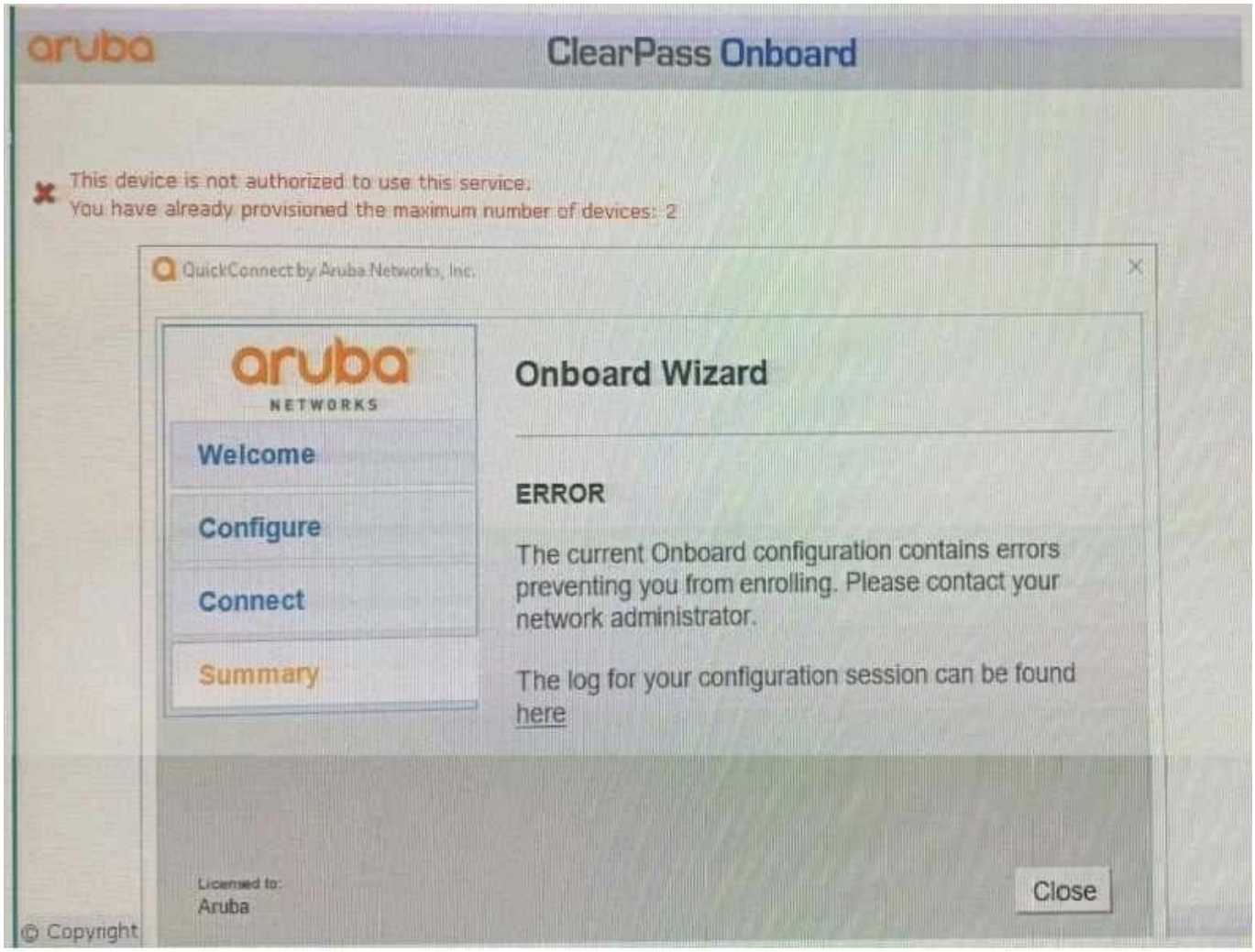
C. create two Posture Policies and use the Restrict by Roles option to filter for HR and RandD user roles and apply the correct SHV checks

D. create one Posture Policy to check the HR users client devices and use the NAP Agent to check RandD users client devices

Correct Answer: A

QUESTION 2

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

QUESTION 3

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

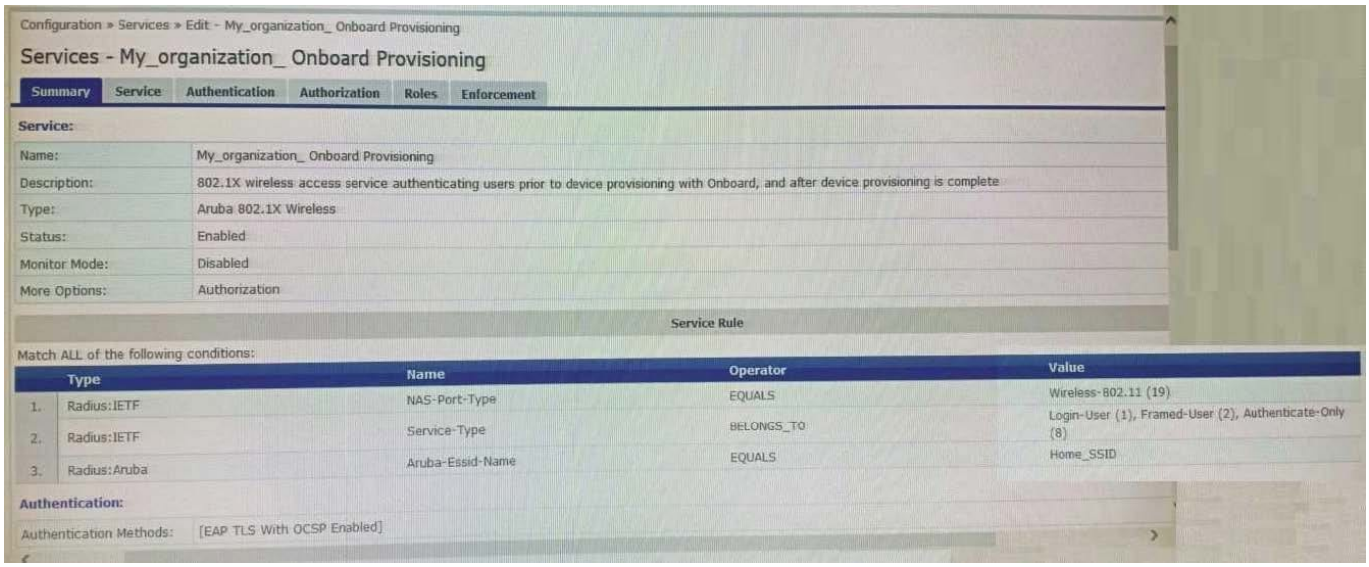
C. Onboard Provisioning service

D. Onboard Pre-Auth service

Correct Answer: A

QUESTION 4

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

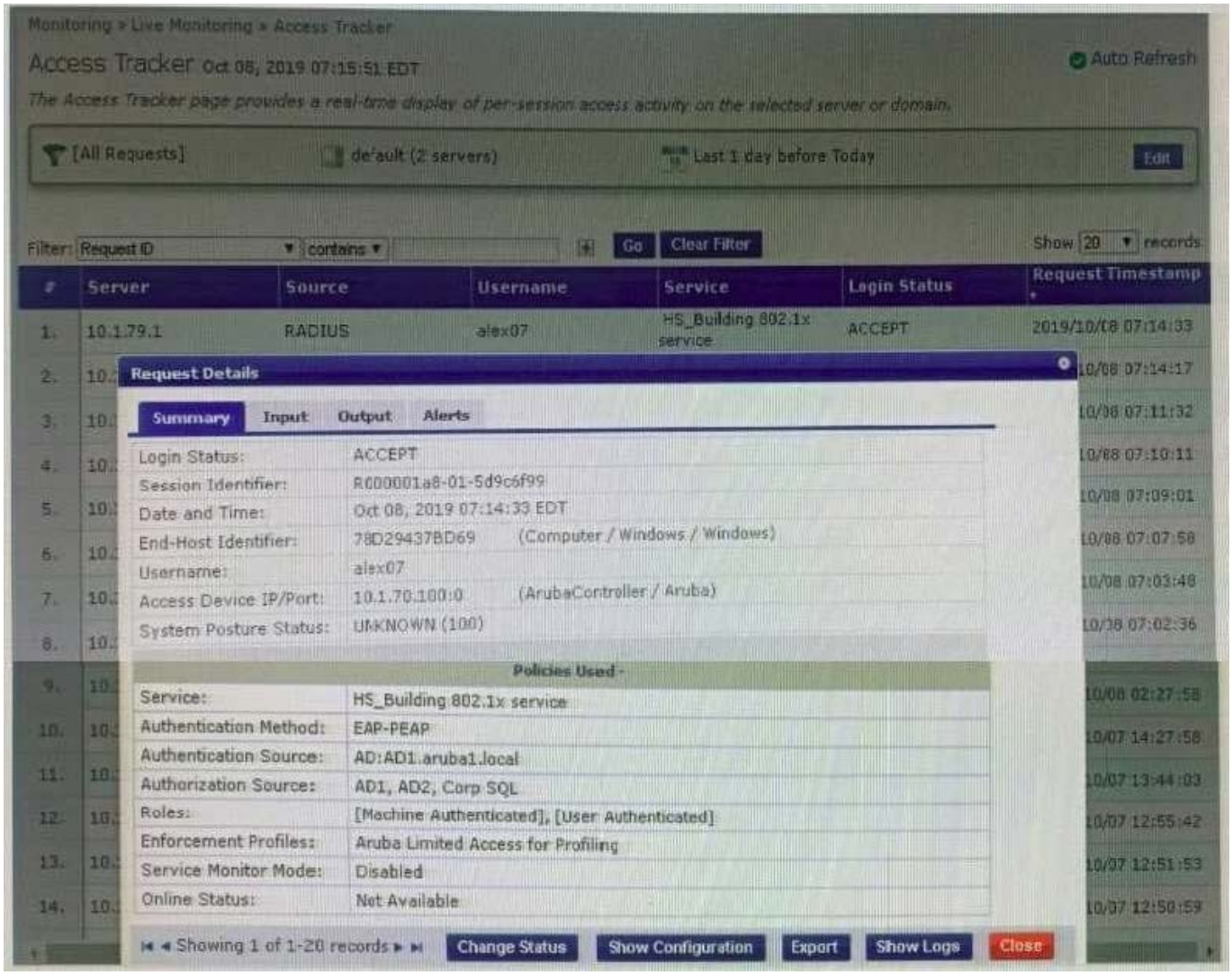
D. ClearPass will block network access to the device

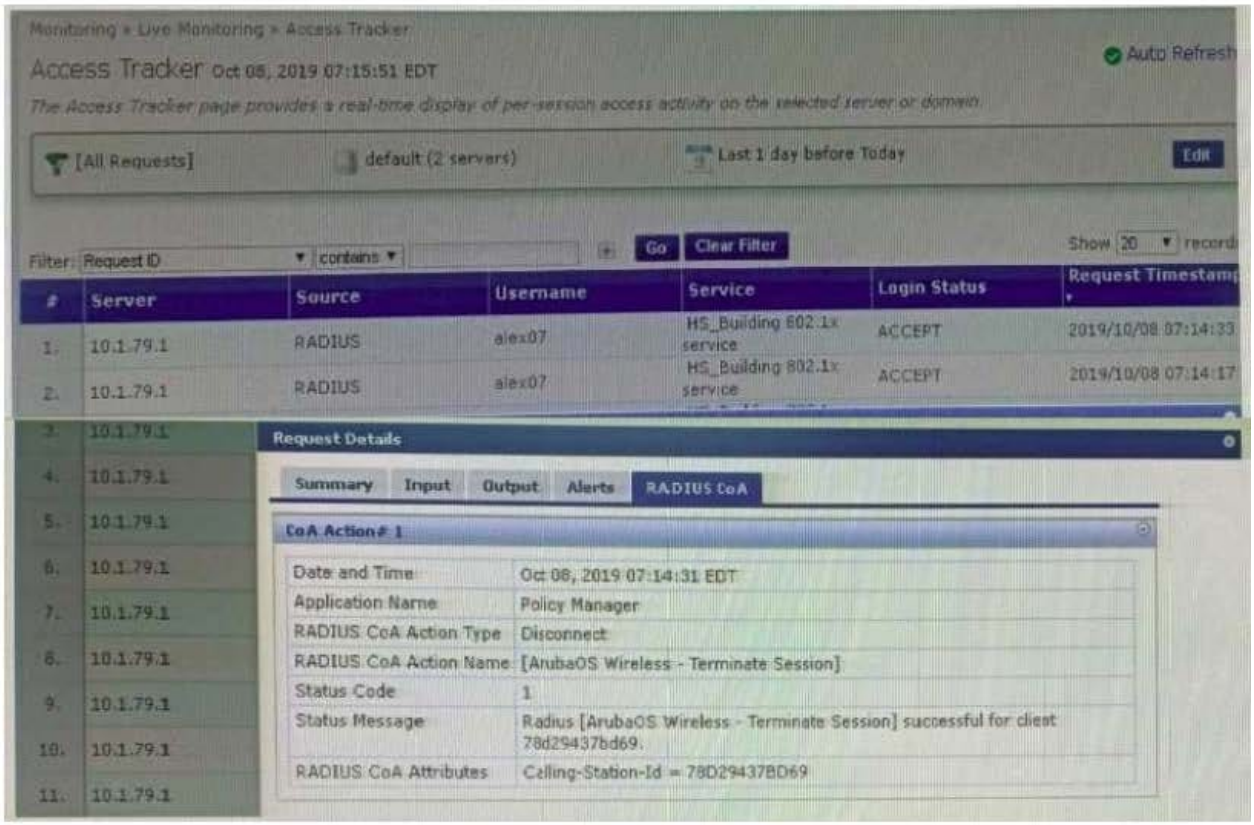
E. ClearPass will allow the device to access the network.

Correct Answer: D

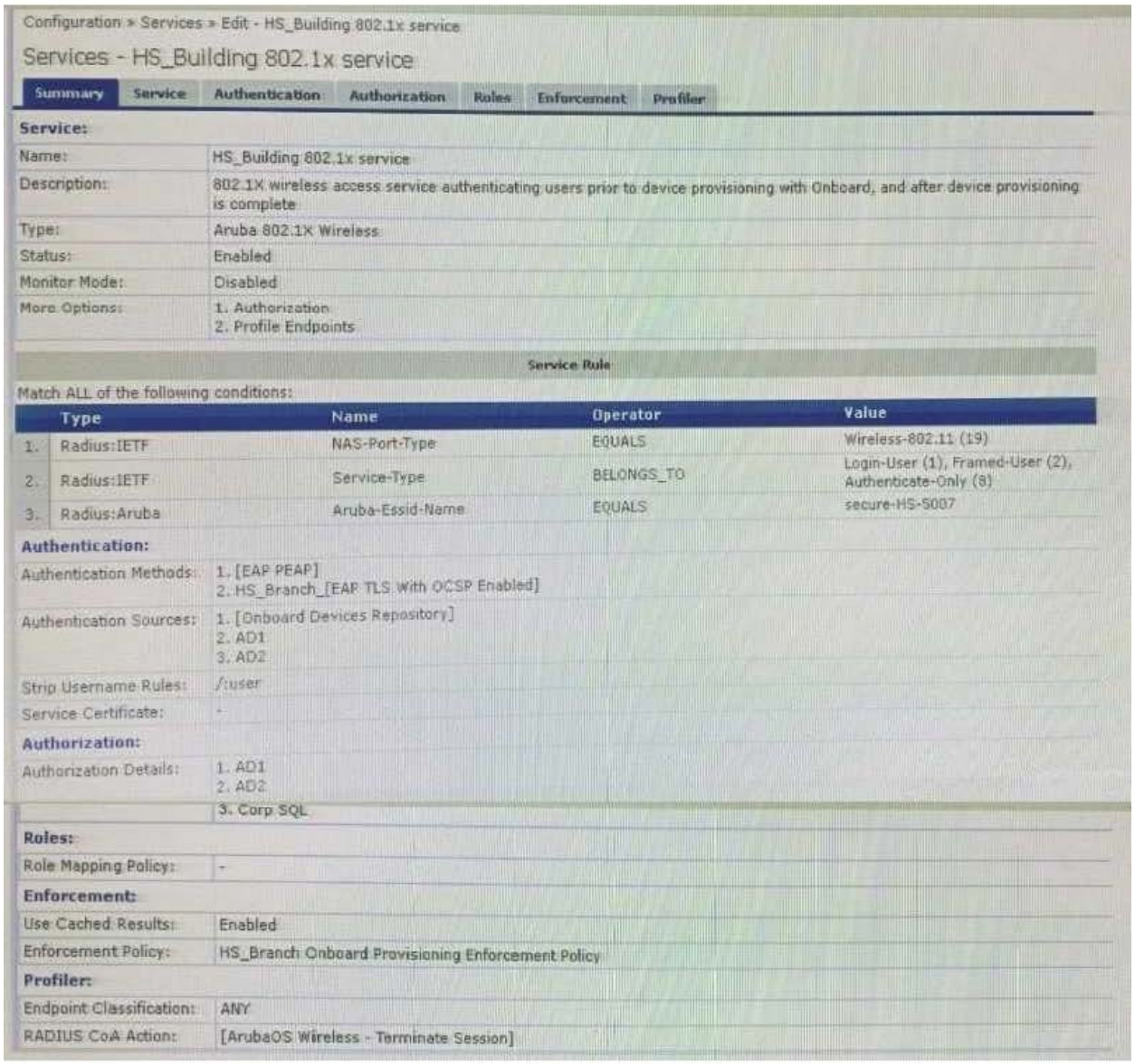
QUESTION 5

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 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-t67-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:

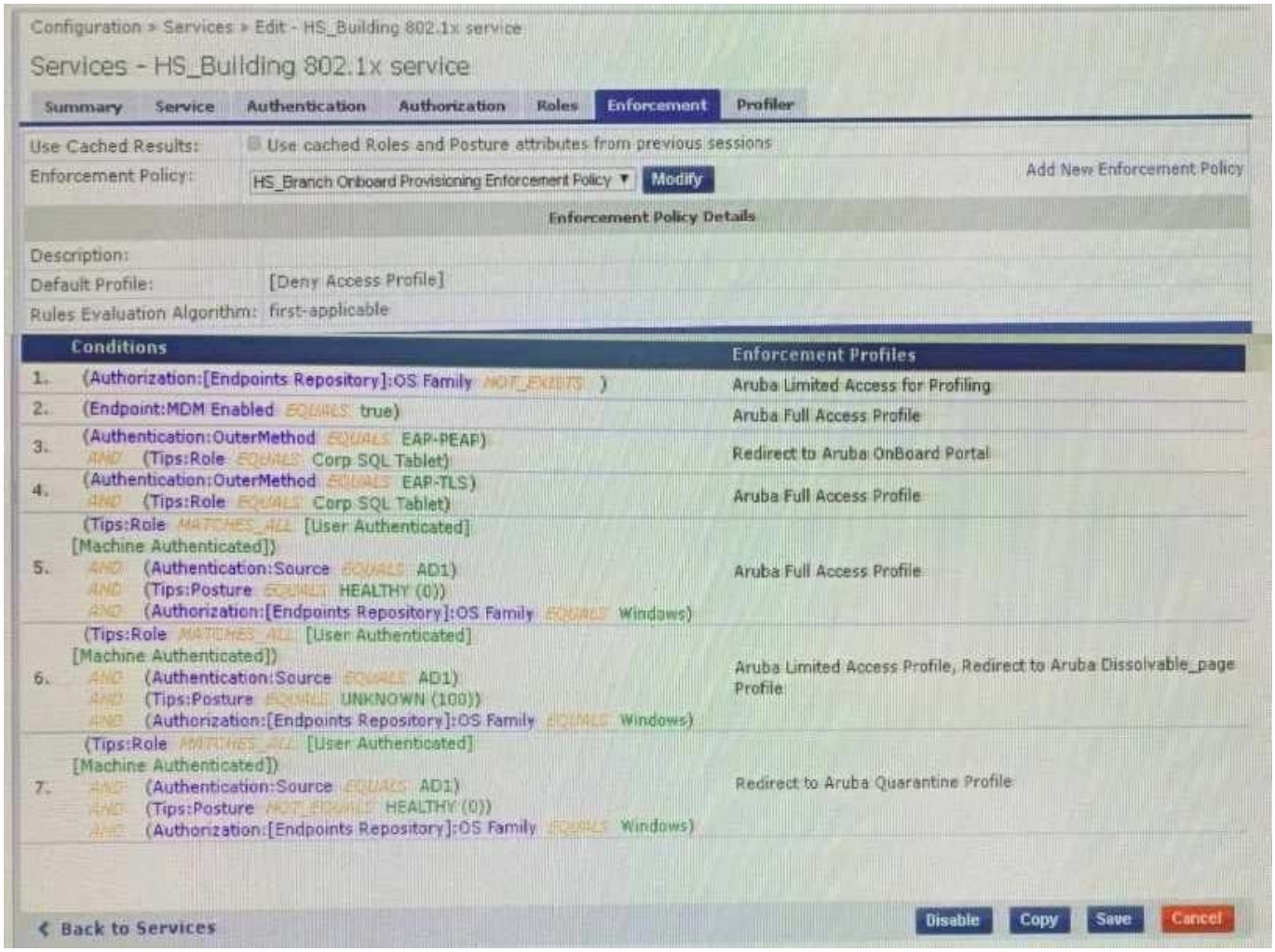
Role Mapping Policy:	-

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