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

What is the Open SSID (otherwise referred to as Dual SSID) Onboard deployment service workflow?

A. OnBoard Pre-Auth Application service, OnBoard Authorization Application service. OnBoard Provisioning RADIUS service

B. OnBoard Pre-Auth RADIUS service. OnBoard Authorization Application service. OnBoard Provisioning RADIUS service

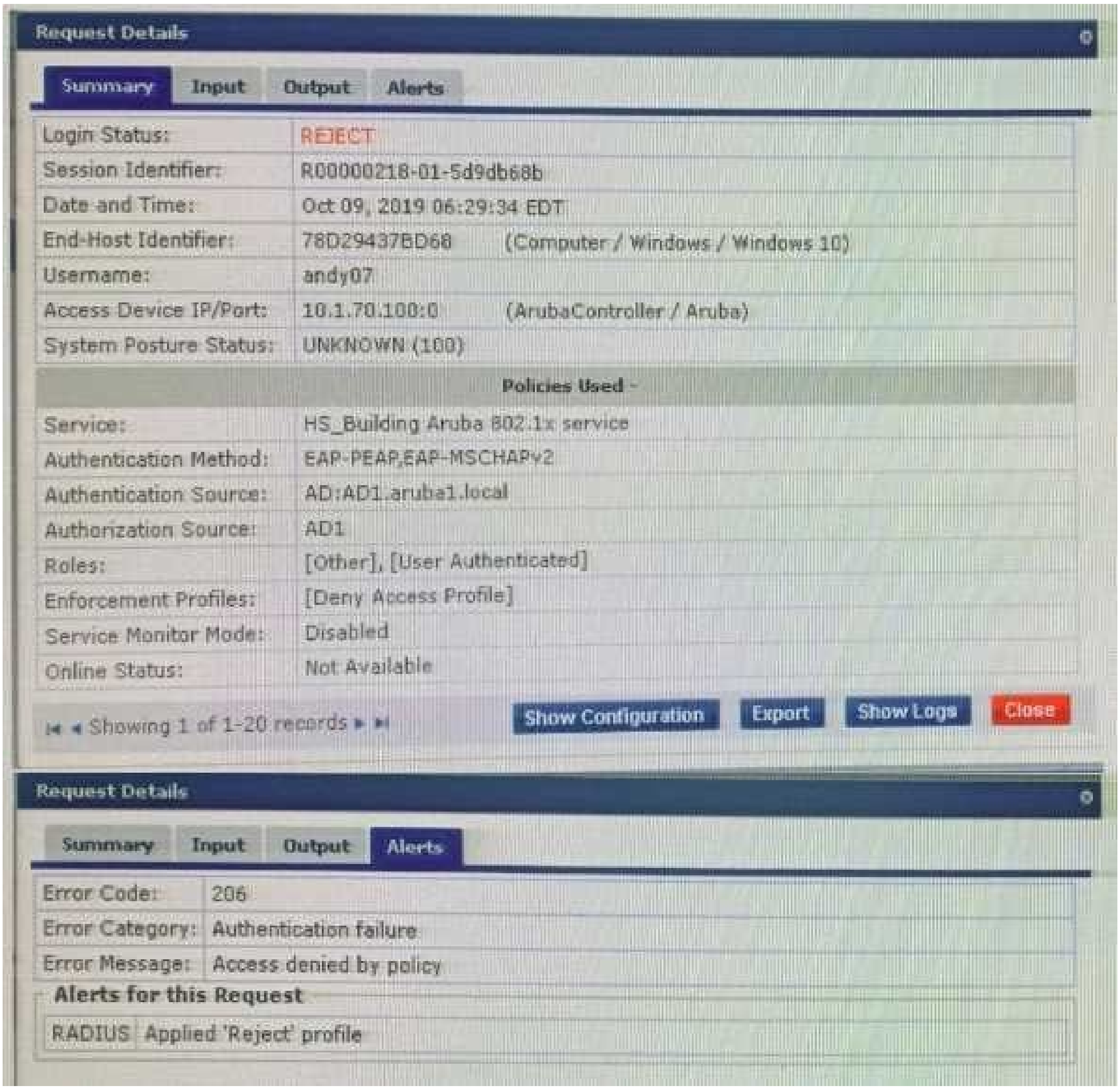
C. OnBoard Authorization Application service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

D. OnBoard Authorization RADIUS service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

Correct Answer: C

QUESTION 2

Refer to the exhibit:



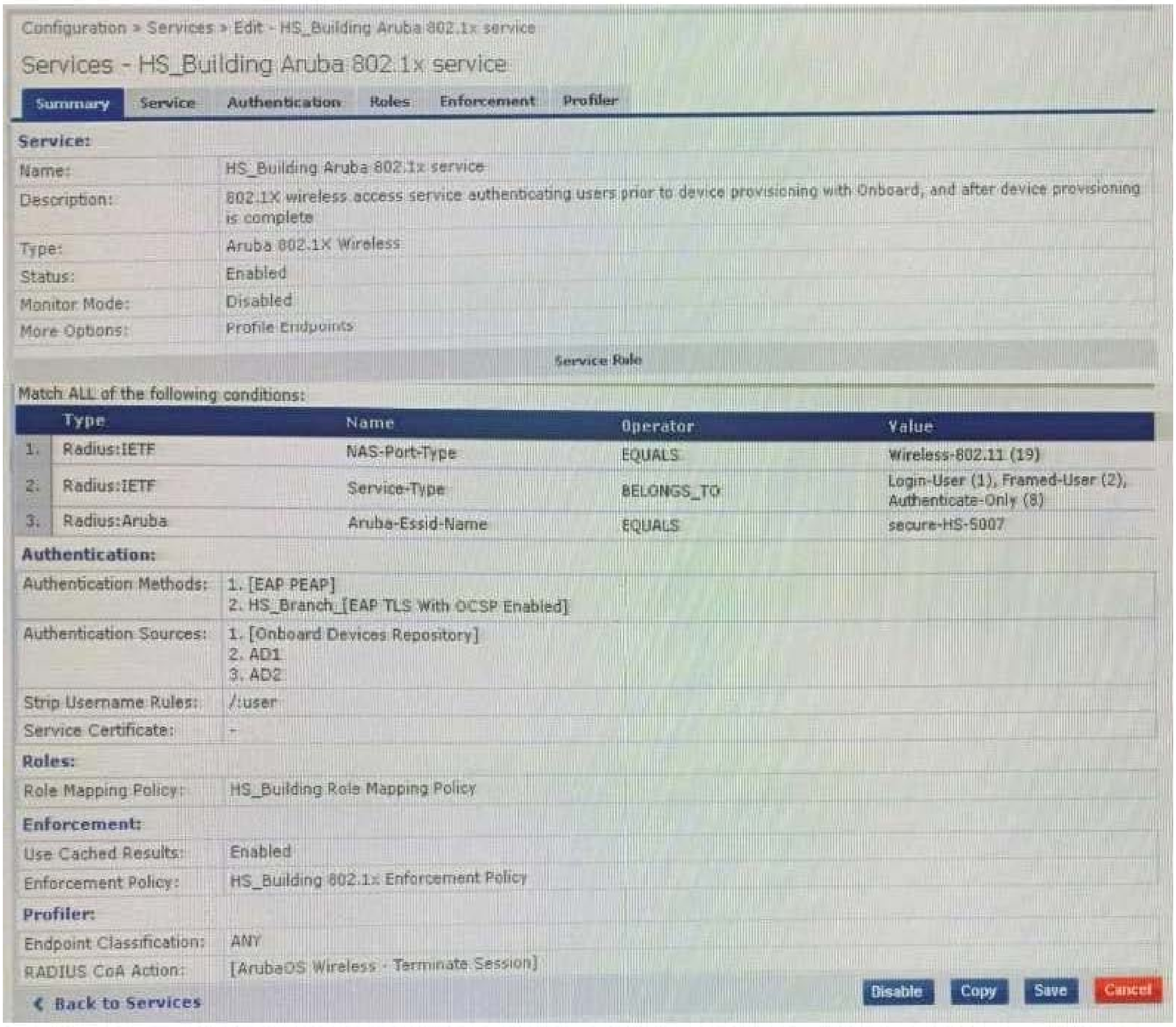
Login Status:	REJECT
Session Identifier:	R00000218-01-5d9db68b
Date and Time:	Oct 09, 2019 06:29:34 EDT
End-Host Identifier:	78D29437BD68 (Computer / Windows / Windows 10)
Username:	andy07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	HS_Building Aruba 802.1x service
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	AD1
Roles:	[Other], [User Authenticated]
Enforcement Profiles:	[Deny Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-20 records

Error Code:	206
Error Category:	Authentication failure
Error Message:	Access denied by policy

Alerts for this Request

RADIUS	Applied 'Reject' profile


Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary
Service
Authentication
Roles
Enforcement
Profiler

Service:

Name:	HS_Building Aruba 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:	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:	-

Roles:

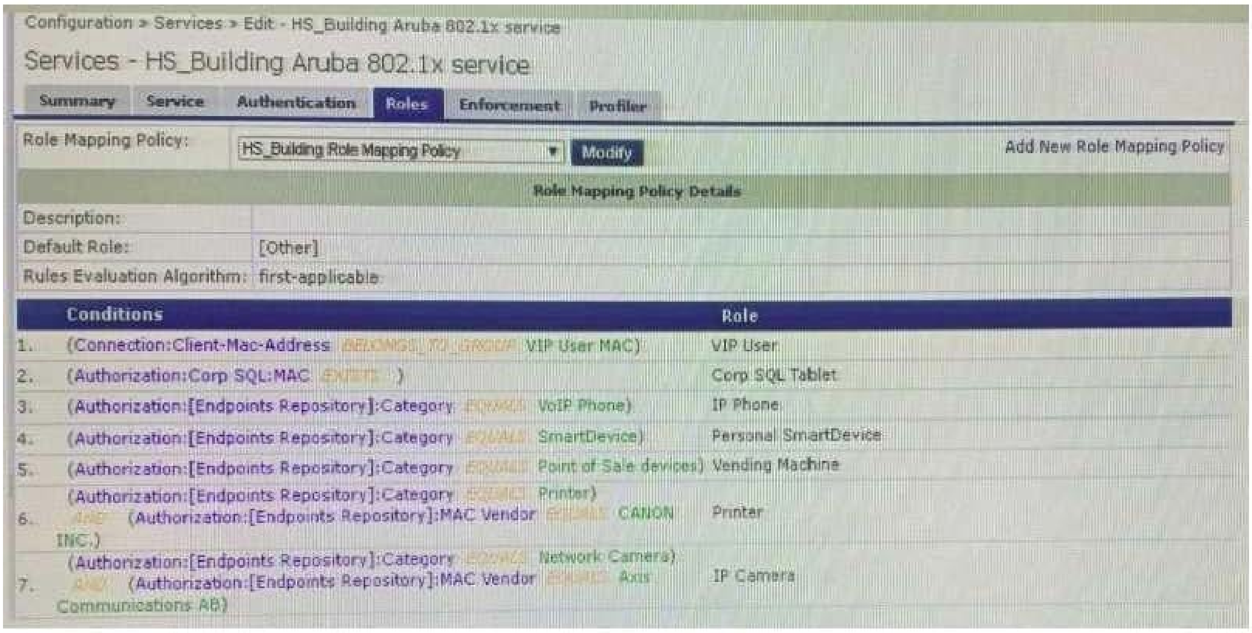
Role Mapping Policy:	HS_Building Role Mapping Policy

Enforcement:

Use Cached Results:	Enabled
Enforcement Policy:	HS_Building 802.1x Enforcement Policy

Profiler:

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



Configuration » Services » Edit - HS_Building Aruba 802.1x service

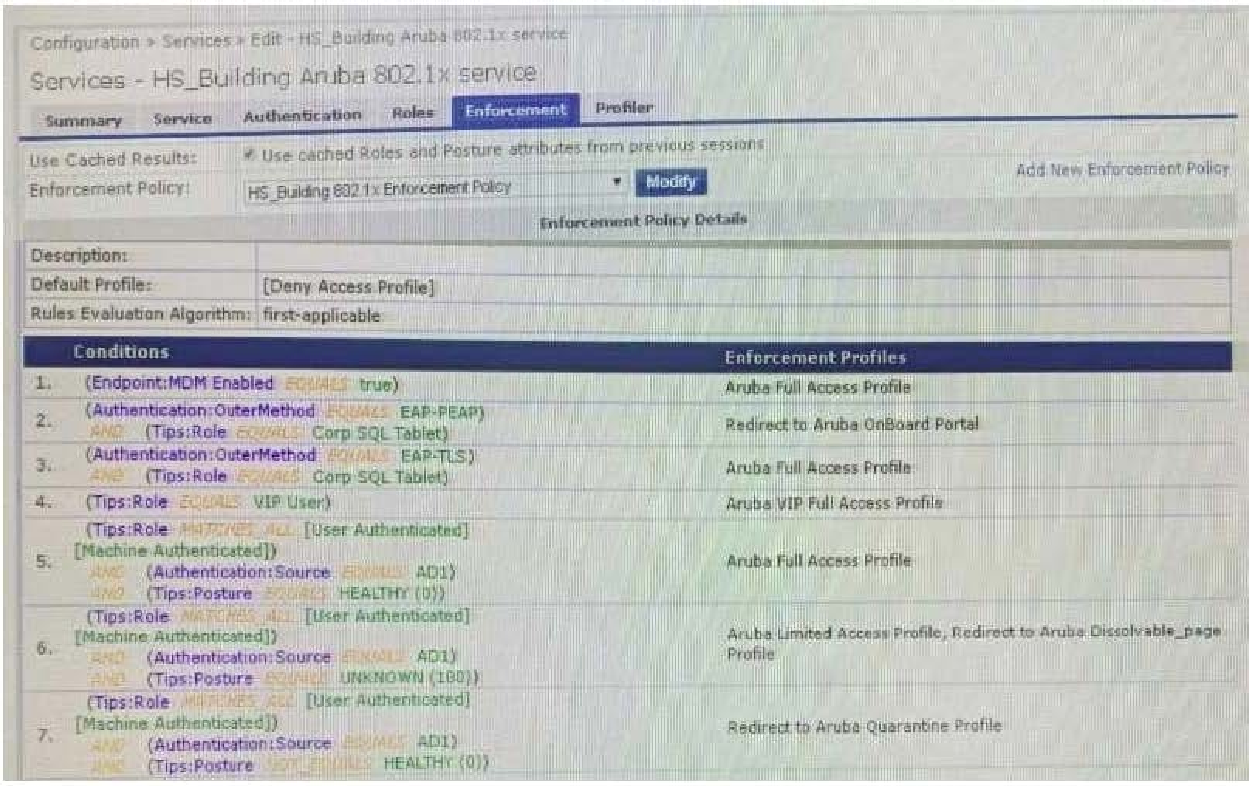
Services - HS_Building Aruba 802.1x service

Role Mapping Policy: HS_Building Role Mapping Policy

Role Mapping Policy Details

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
1.	(Connection:Client-Mac-Address BELONGS_TO_GROUP VIP User MAC)	VIP User
2.	(Authorization:Corp SQL:MAC EXISTS)	Corp SQL Tablet
3.	(Authorization:[Endpoints Repository]:Category EQUALS VoIP Phone)	IP Phone
4.	(Authorization:[Endpoints Repository]:Category EQUALS SmartDevice)	Personal SmartDevice
5.	(Authorization:[Endpoints Repository]:Category EQUALS Point of Sale devices)	Vending Machine
6.	(Authorization:[Endpoints Repository]:Category EQUALS Printer) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS CANON INC.)	Printer
7.	(Authorization:[Endpoints Repository]:Category EQUALS Network Camera) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS Axis Communications AB)	IP Camera



Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Use Cached Results: ☑ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: HS_Building 802.1x Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
2.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
3.	(Authentication:OuterMethod EQUALS EAP-TLS) AND (Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
4.	(Tips:Role EQUALS VIP User)	Aruba VIP Full Access Profile
5.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0))	Aruba Full Access Profile
6.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100))	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	Redirect to Aruba Quarantine Profile

Your company has a postgres SQL database with the MAC addresses of the company-owned tablets You

have configured a role mapping condition to tag the SQL devices. When one of the tablets connects to the

network, it does not get the correct role and receives a deny access profile.

How would you resolve the issue?

A. Remove SQL condition from role mapping policy and add it under the enforcement policy conditions.

B. Edit the SQL authentication source niter attributes and modify the SQL server filter query.

C. Add the SQL server as an authentication source and map .t under the authentication tab in the service.

D. Enable authorization tab in the service and add the SQL server as an authorization source.

Correct Answer: B

QUESTION 3

What is used to validate the EAP Certificate? (Select three.)

A. Common Name

B. Date

C. Key usage

D. Server Identity

E. SAN entries

F. Trust chain

Correct Answer: ACF

QUESTION 4

A customer is complaining that some of the devices, in their manufacturing network, are not getting profiled while other loT 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.

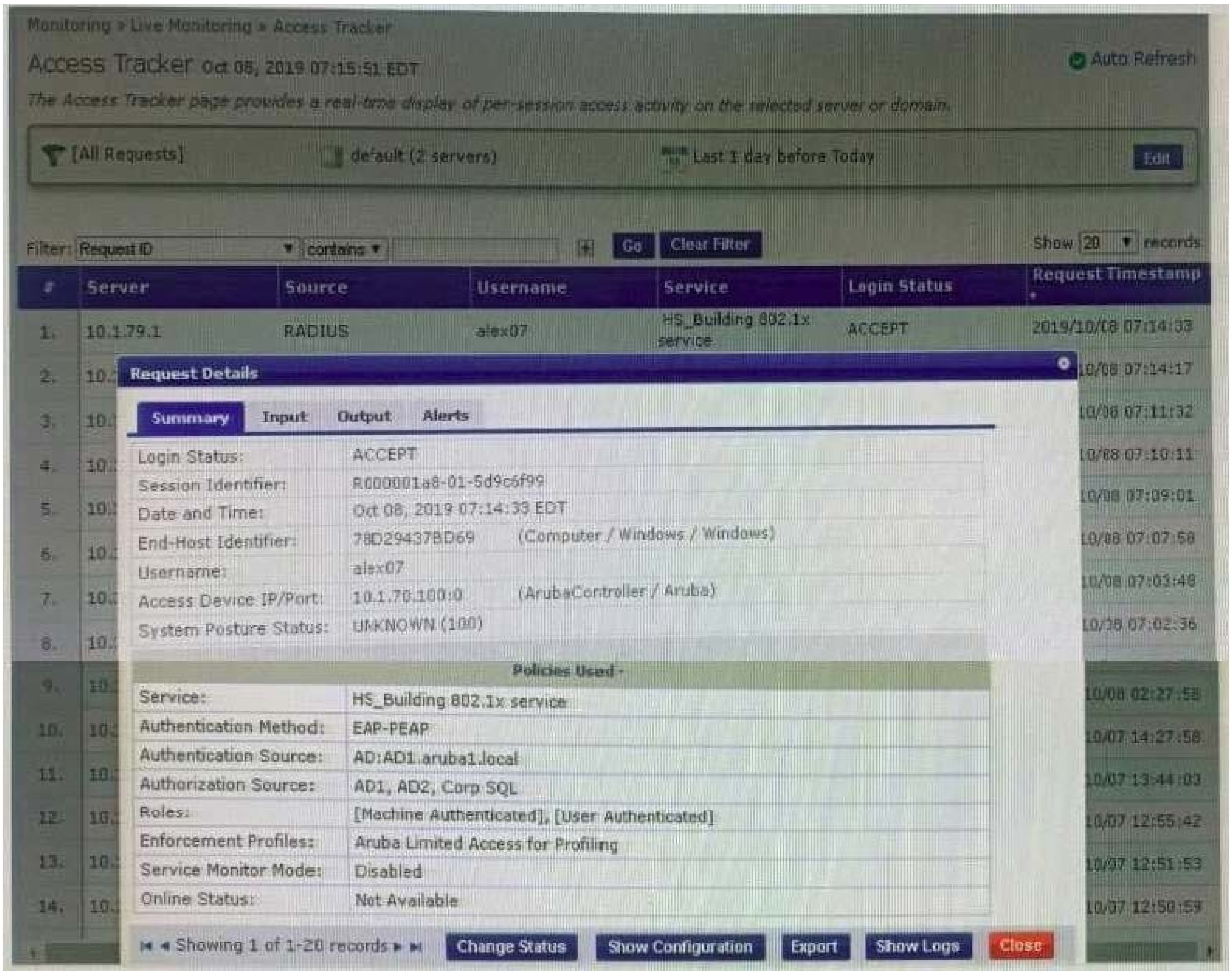
D. Allow time for IF-MAP service on the controller to discover the new devices as well.

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

Correct Answer: DE

QUESTION 5

Refer to the exhibit:



Monitoring » Live Monitoring » Access Tracker

Access Tracker Oct 08, 2019 07:15:51 EDT

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

Filter: Request ID ▼ contains ▼ 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.					10/08 07:14:17
3.	10.					10/08 07:11:32
4.	10.					10/08 07:10:11
5.	10.					10/08 07:09:01
6.	10.					10/08 07:07:58
7.	10.					10/08 07:03:48
8.	10.					10/08 07:02:36
9.	10.					10/08 02:27:58
10.	10.					10/07 14:27:58
11.	10.					10/07 13:44:03
12.	10.					10/07 12:55:42
13.	10.					10/07 12:51:53
14.	10.					10/07 12:50:59

Request Details

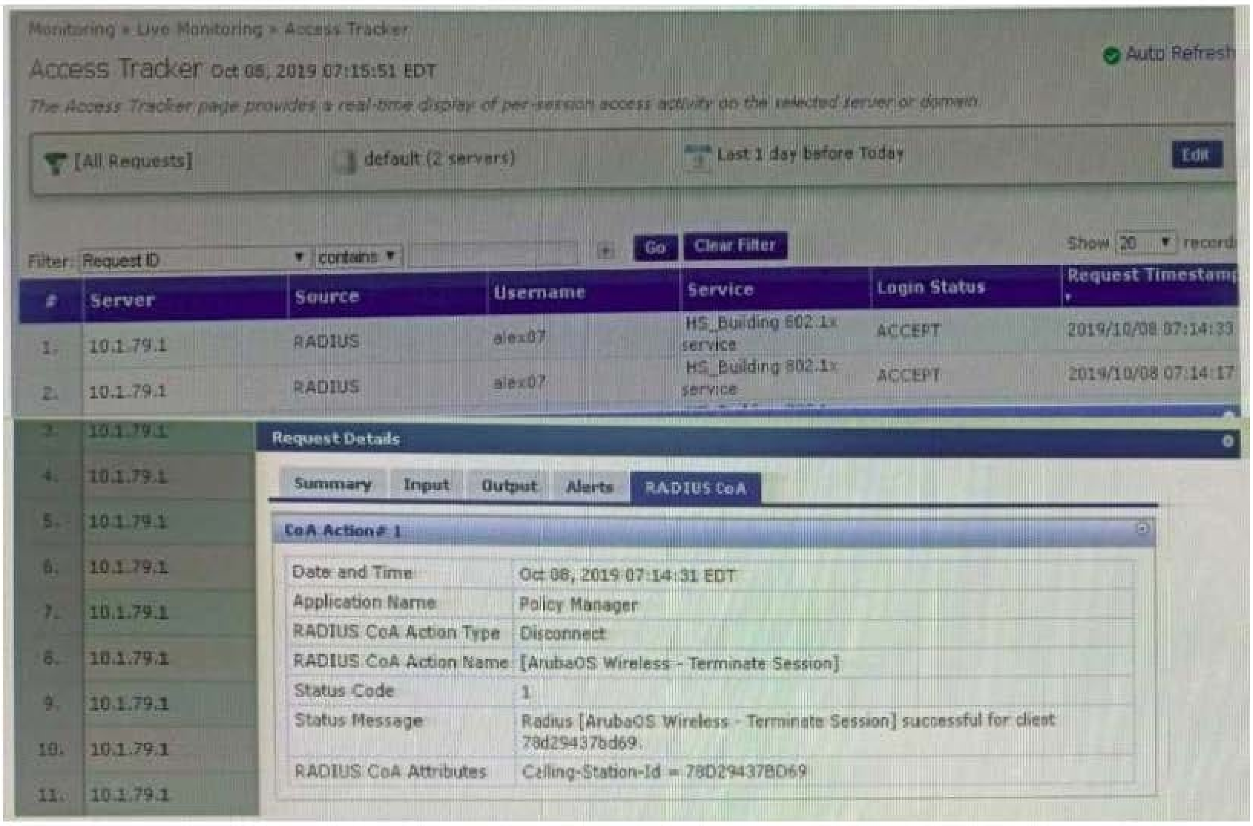
Summary | Input | Output | Alerts

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



Monitoring » Live Monitoring » Access Tracker

Access Tracker Oct 08, 2019 07:15:51 EDT

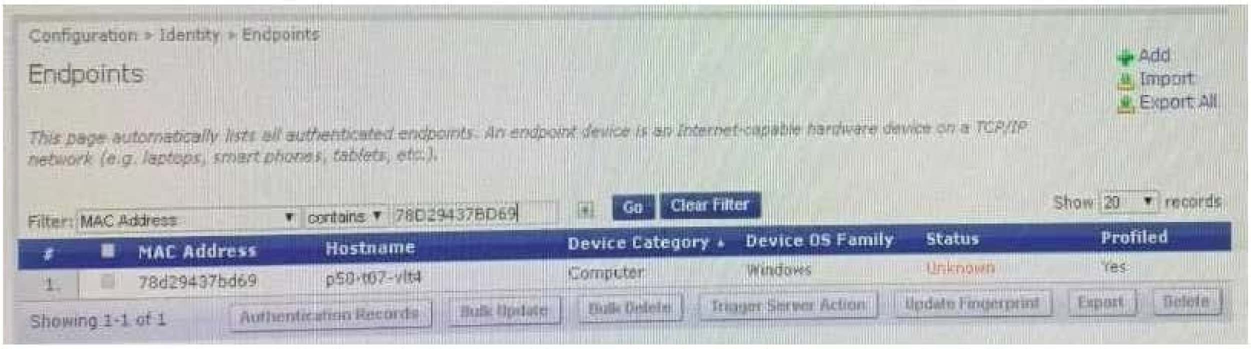
The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

#	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
3.	10.1.79.1					
4.	10.1.79.1					
5.	10.1.79.1					
6.	10.1.79.1					
7.	10.1.79.1					
8.	10.1.79.1					
9.	10.1.79.1					
10.	10.1.79.1					
11.	10.1.79.1					

Request Details

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



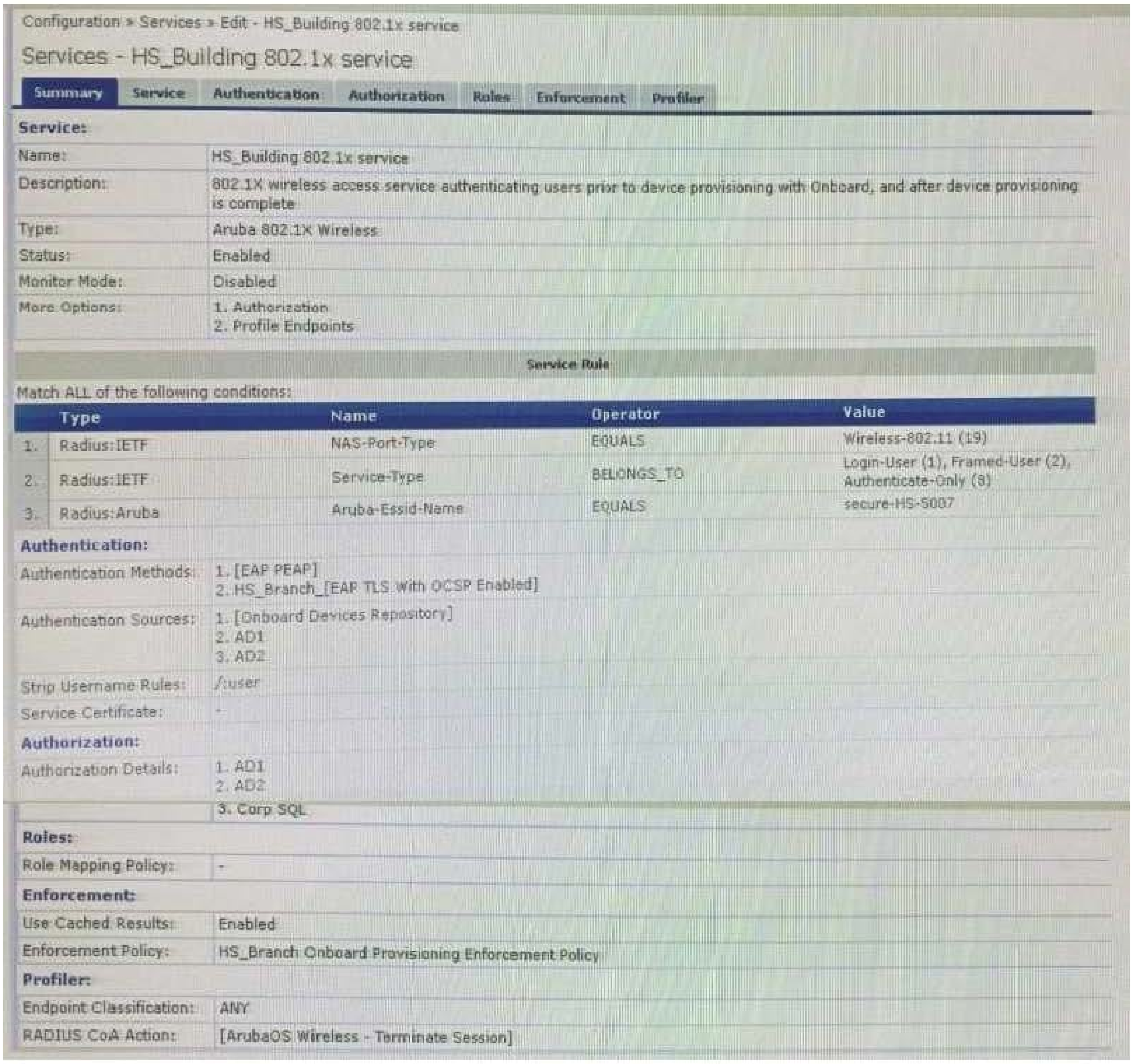
Configuration » Identity » Endpoints

Endpoints

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.).

#	■	MAC Address	Hostname	Device Category ↓	Device OS Family	Status	Profiled
1.	□	78d29437bd69	p50-t07-vlt4	Computer	Windows	Unknown	Yes

Showing 1-1 of 1



Configuration » Services » Edit - HS_Building 802.1x service

Services - HS_Building 802.1x service

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:

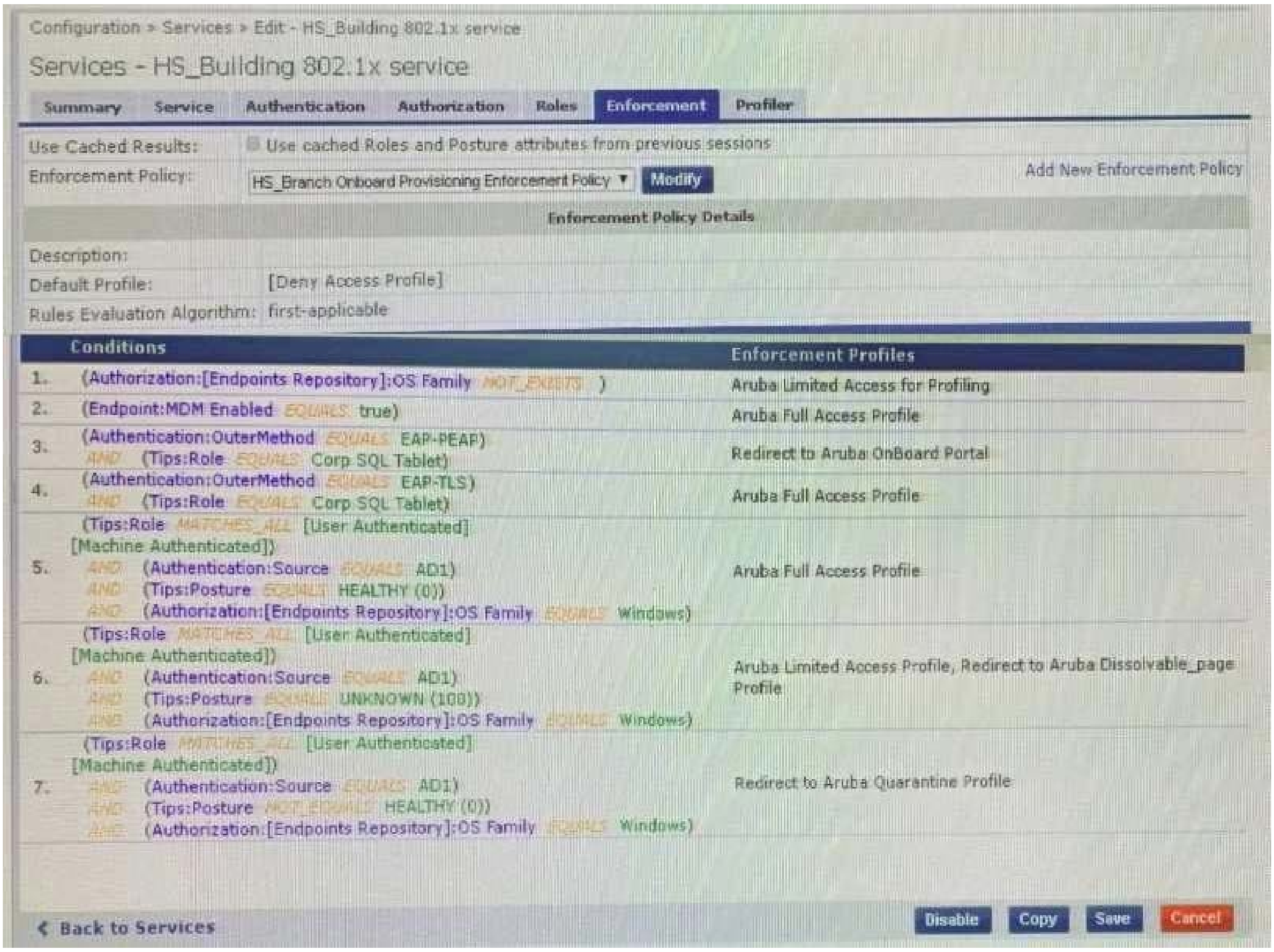
Role Mapping Policy:	-

Enforcement:

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

Profiler:

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



Configuration > Services > Edit - HS_Building 802.1x service

Services - HS_Building 802.1x service

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: HS_Branch Onboard Provisioning Enforcement Policy ▼ Modify

Enforcement Policy Details

Description:
Default Profile: [Deny Access Profile]
Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:OS Family NOT_EXISTS)	Aruba Limited Access for Profiling
2.	(Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
3.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
4.	(Authentication:OuterMethod EQUALS EAP-TLS) AND (Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
5.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Aruba Full Access Profile
6.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture NOT_EQUALS HEALTHY (0)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Redirect to Aruba Quarantine Profile

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

Latest HPE6-A77 Dumps HPE6-A77 PDF Dumps HPE6-A77 Practice Test