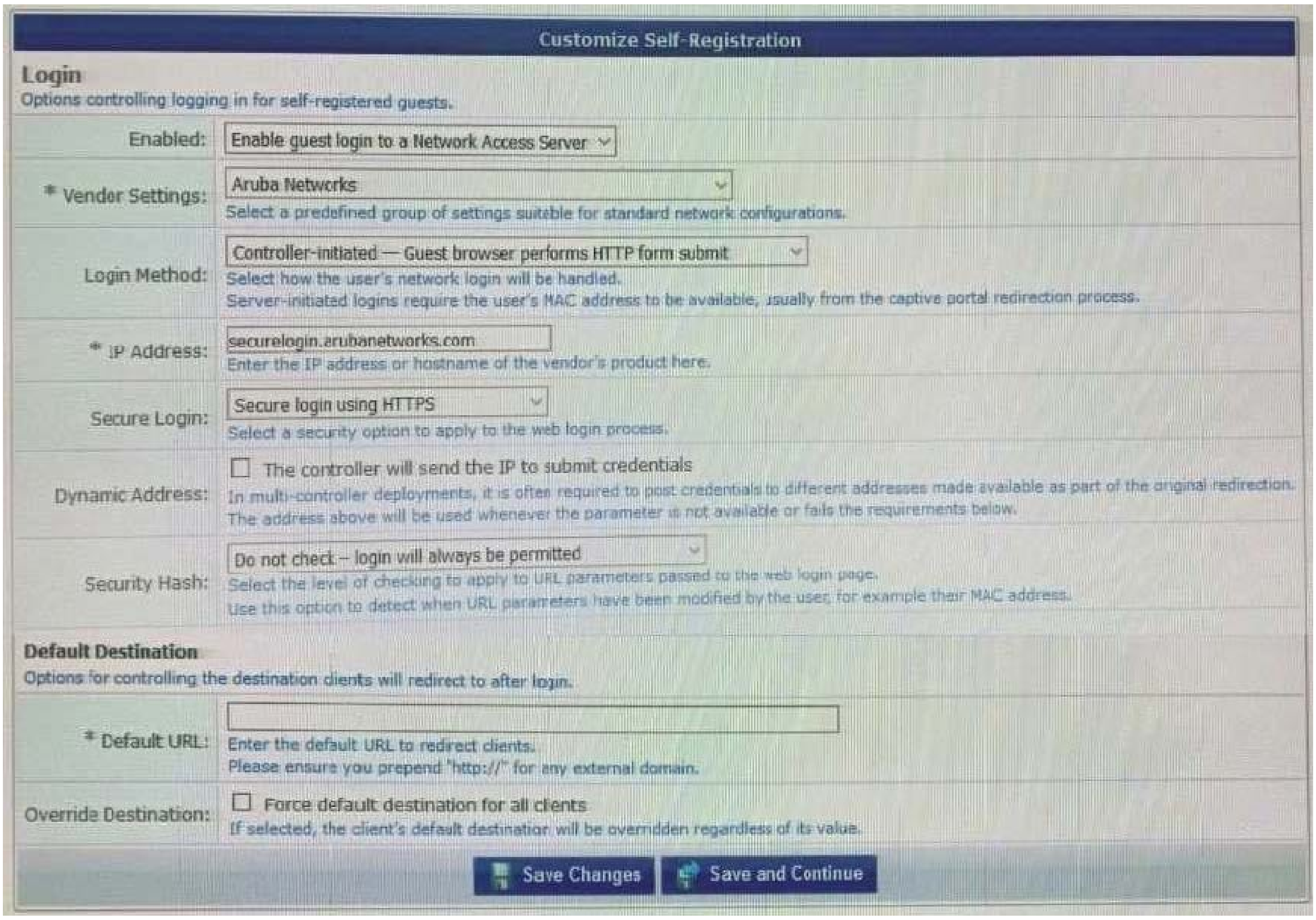
HPE6-A81$^{\text{Q\&As}}$

Aruba Certified ClearPass Expert Written Exam

QUESTION 1

Refer to the exhibit:



Customize Self-Registration

Login
Options controlling logging in for self-registered guests.

Enabled:	Enable guest login to a Network Access Server
* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable for standard network configurations.
Login Method:	Controller-initiated — Guest browser performs HTTP form submit Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
* IP Address:	securelogin.arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Secure login using HTTPS Select a security option to apply to the web login process.
Dynamic Address:	□ The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.
Security Hash:	Do not check – login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

Default Destination
Options for controlling the destination clients will redirect to after login.

* Default URL:	Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	□ Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.

A customer with multiple Aruba Controllers has just installed a new certificate for "*.customerdomain com" on all Aruba Controllers. While testing the existing guest Self-Registration page the customer noticed that the logins are failing. While troubleshooting they are finding no entries in the Event Viewer or Access Tracker for the tests. Suspecting that the Aruba Controllers may not be properly posting the credentials from the guest browser, they open the NAS Vendor Settings for the Guest Self-Registration Page. From the screen shown, how can you fix the errors?

A. Change the "IP Address: field to" securelogin.customerdomain.com.

B. Change the "Secure Login:" field to "Use Vendor Default".

C. Change the "IP Address field to "captiveportal-login.customerdomain.com".

D. Add PTR records on the DNS server for "securelogin.arubanetworks.com".

Correct Answer: B

QUESTION 2

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 3

Where is the following information stored in ClearPass?

1.

Roles and Posture for Connected Clients

2.

System Health for OnGuard

3.

Machine authentication State

4.

CoA session info

5.

Mapping of connected clients to NAS/NAD

A. Multi-Master cache

B. Endpoint database

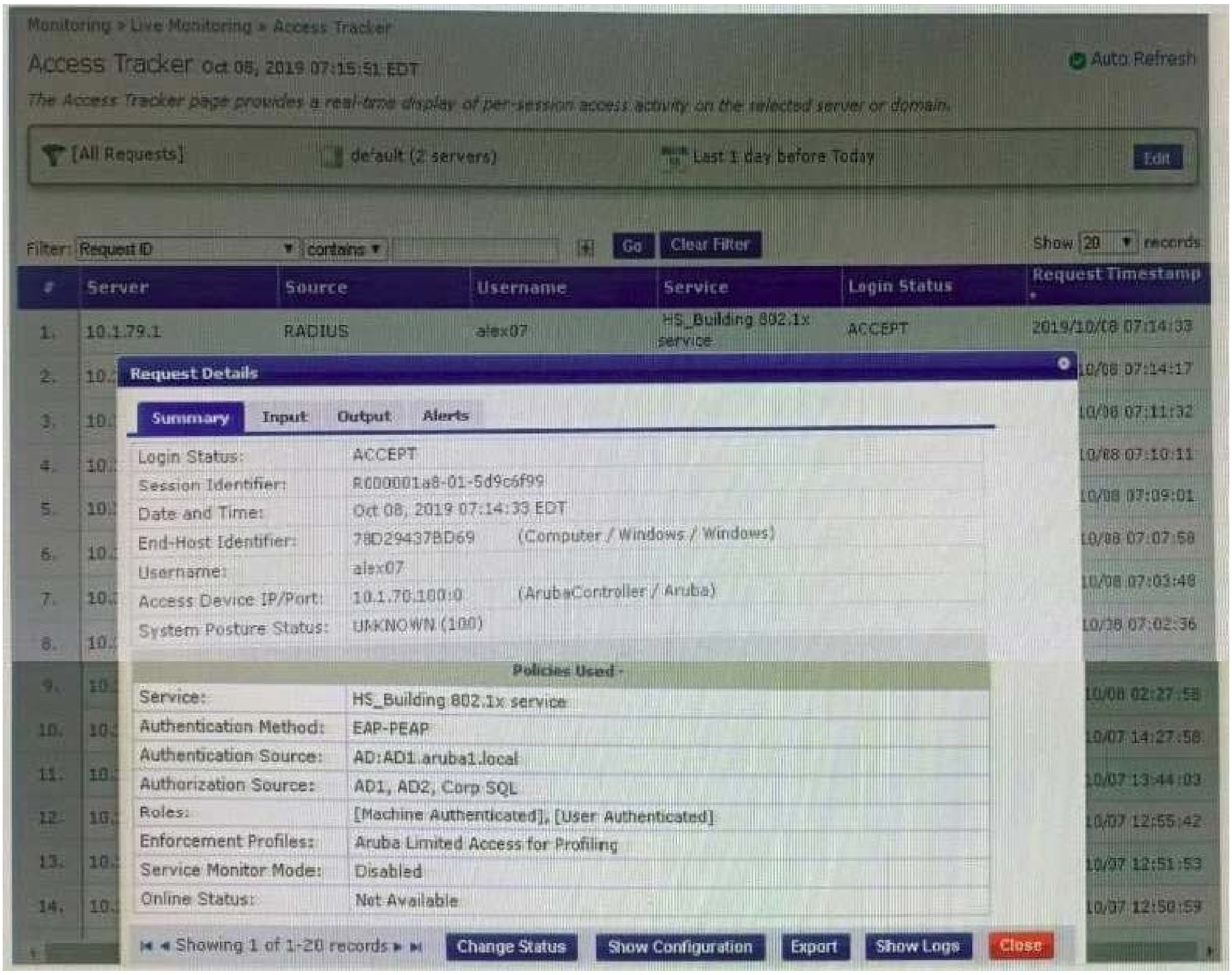
C. insight database

D. ClearPass system cache

Correct Answer: D

QUESTION 4

Refer to the exhibit:



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.

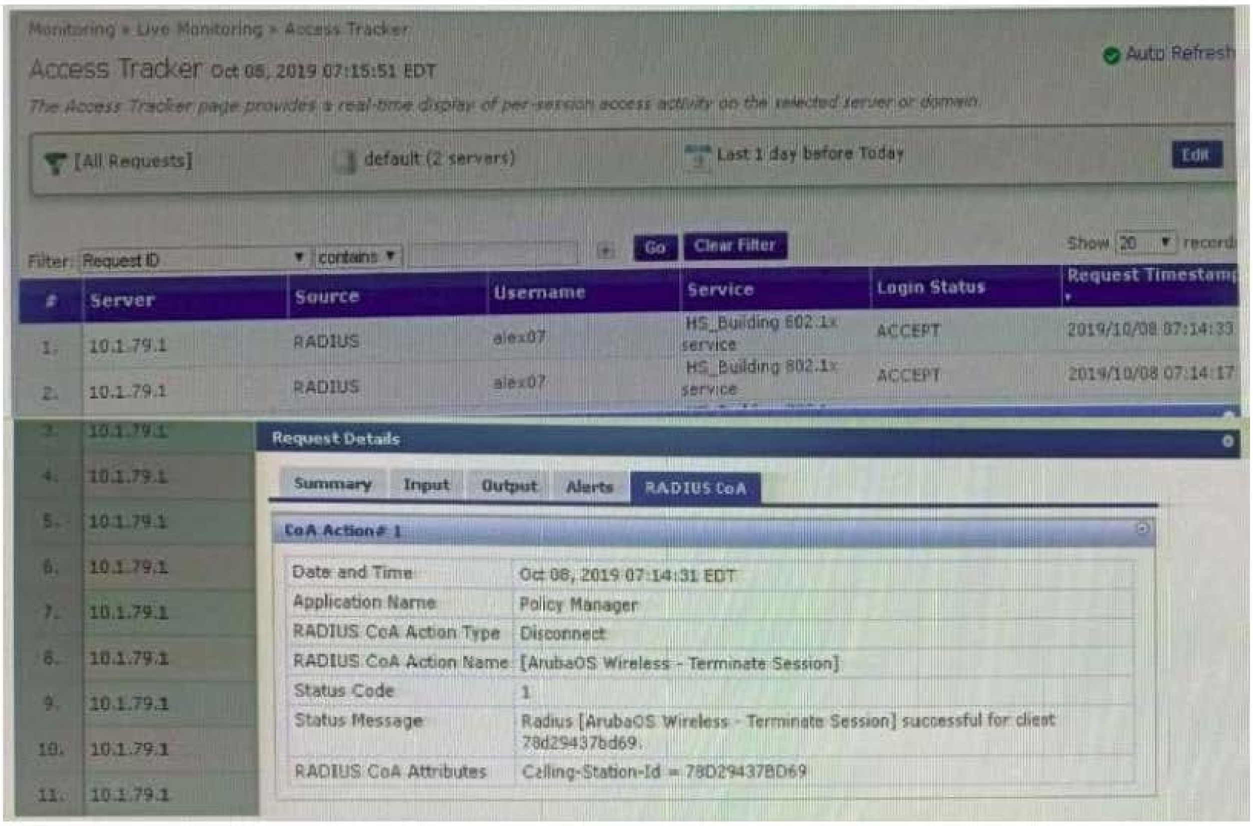
#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.1.79.1	RADIUS	alex07	HS_Building 802.1x service	ACCEPT	2019/10/08 07:14:33
2.	10.					10/08 07:14:17
3.	10.					10/08 07:11:32
4.	10.					10/08 07:10:11
5.	10.					10/08 07:09:01
6.	10.					10/08 07:07:58
7.	10.					10/08 07:03:48
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

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

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

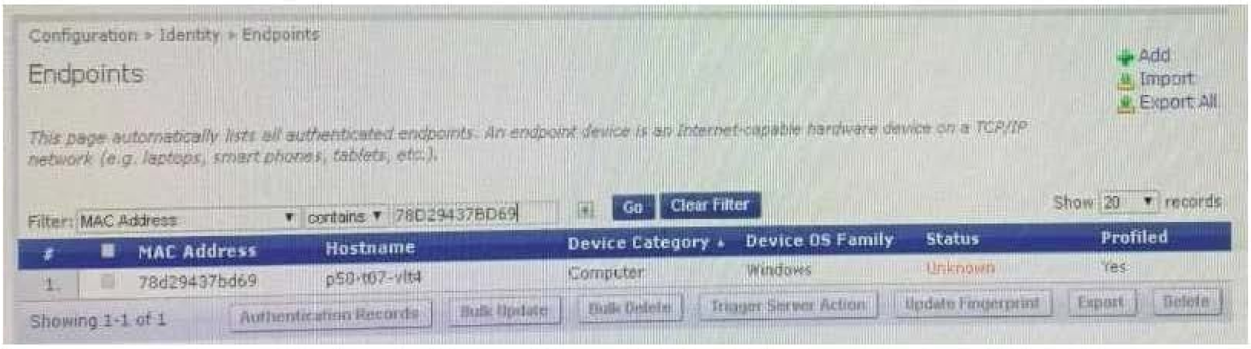
Filter: Request ID ▼ contains ▼ Go Clear Filter Show 20 ▼ records

#	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
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

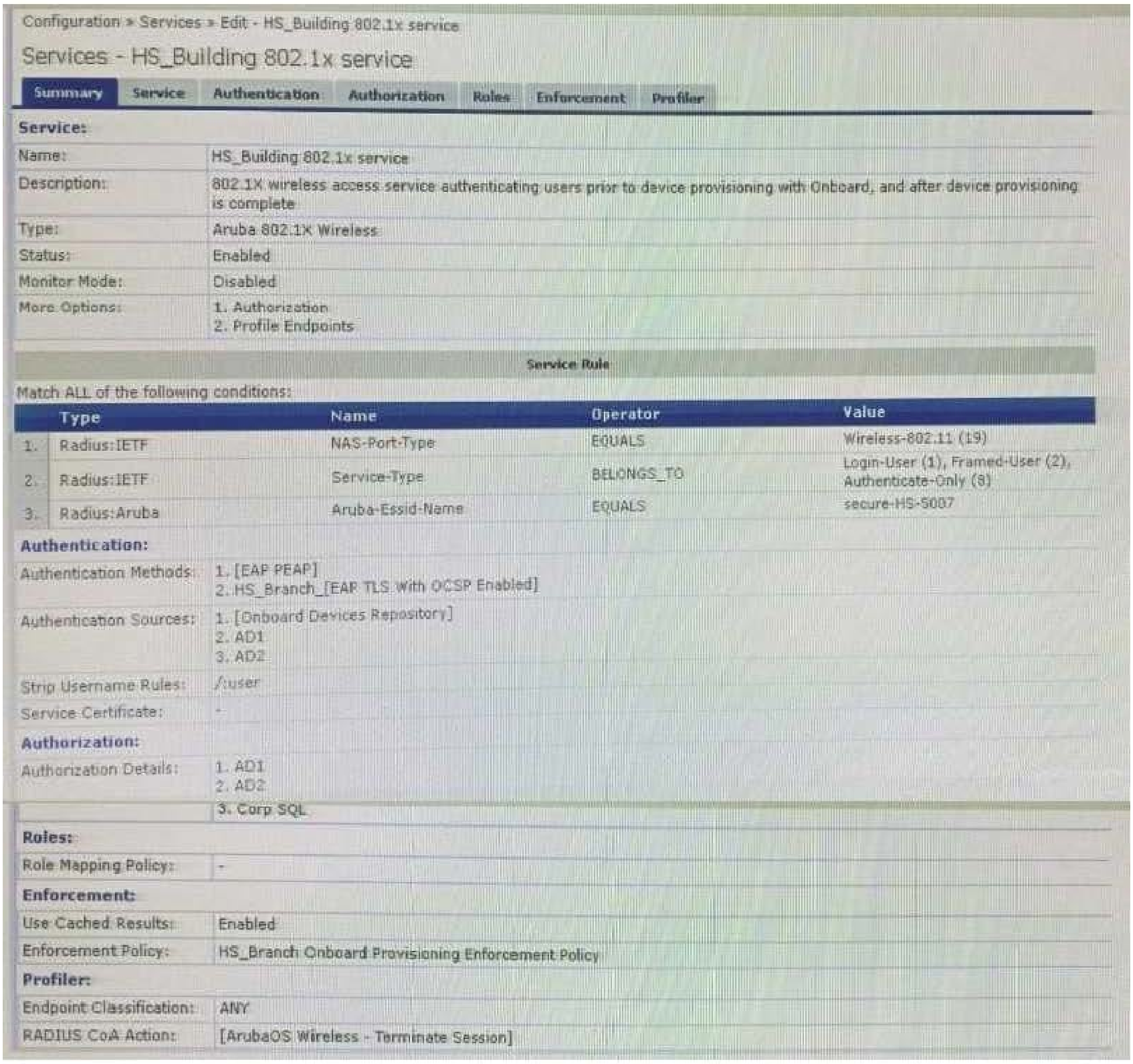
Endpoints

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.).

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



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:

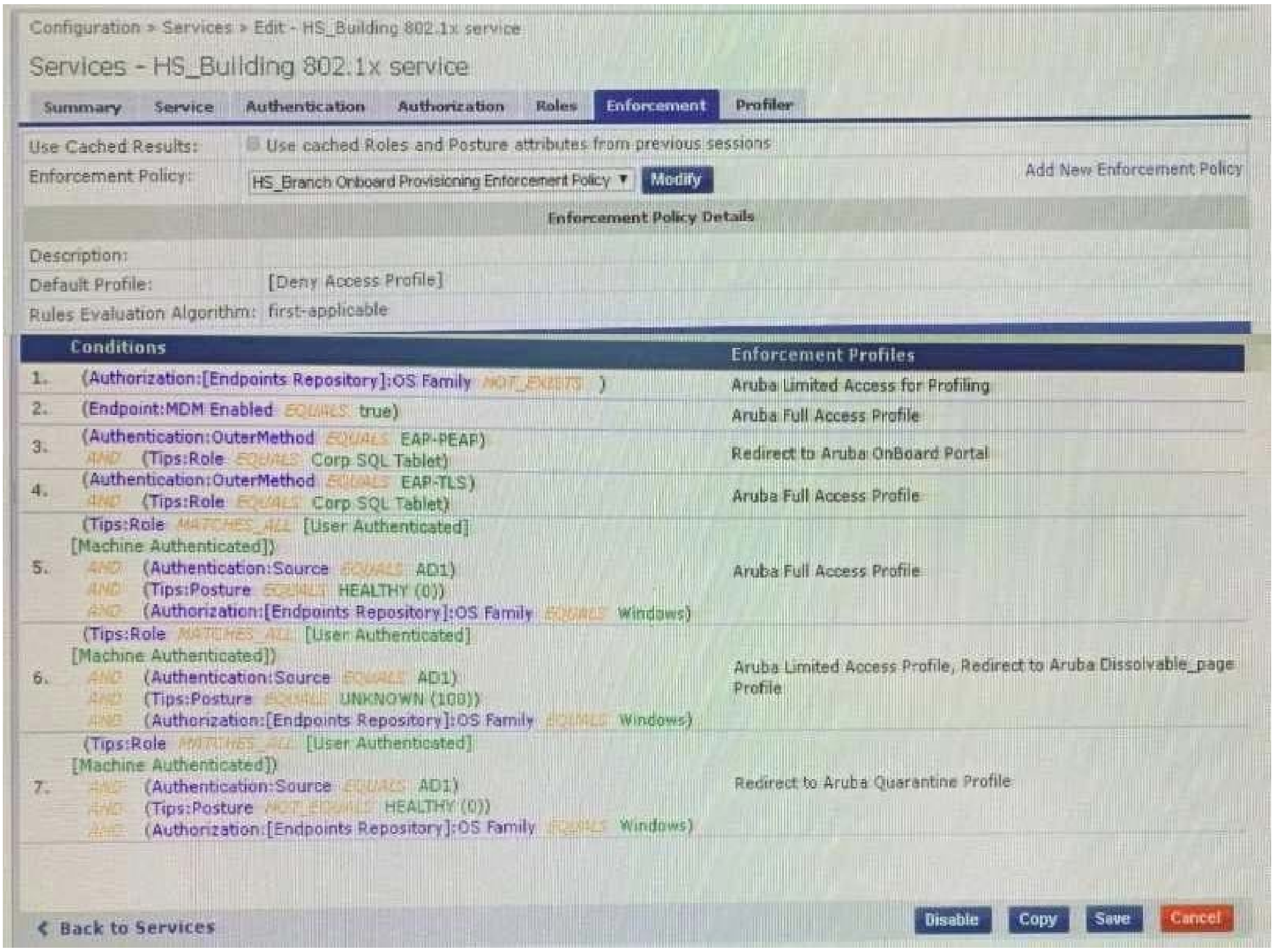
Role Mapping Policy:	-

Enforcement:

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

Profiler:

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



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 ▾

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

QUESTION 5

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