HPE6-A77$^{\text{Q\&As}}$

Aruba Certified ClearPass Expert Written

QUESTION 1

What is the Secure SSID {otherwise referred to as Single SSID) OnBoard deployment service workflow?

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

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

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

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

Correct Answer: A

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}"

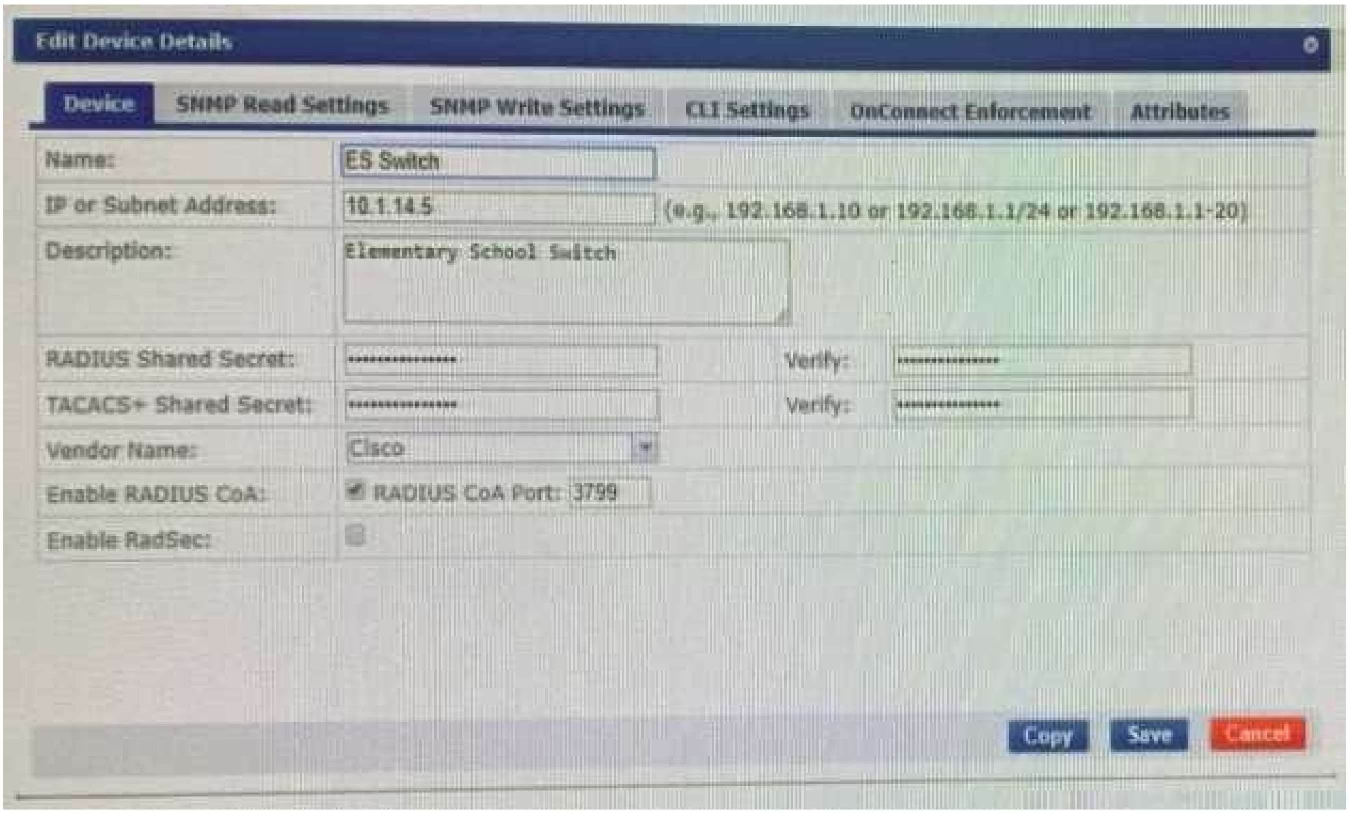
C. Build one Web Login page with vendor settings for controller {company domain)

D. Install multiple public certificates with a different Common Name on each controller

Correct Answer: AB

QUESTION 3

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



Name:	ES Switch		
IP or Subnet Address:	10.1.14.5 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)		
Description:	Elementary School Switch		
RADIUS Shared Secret:	****************	Verify:	****************
TACACS+ Shared Secret:	****************	Verify:	****************
Vendor Name:	Cisco		
Enable RADIUS CoA:	☑ RADIUS CoA Port: 3799		
Enable RadSec:	□		

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.

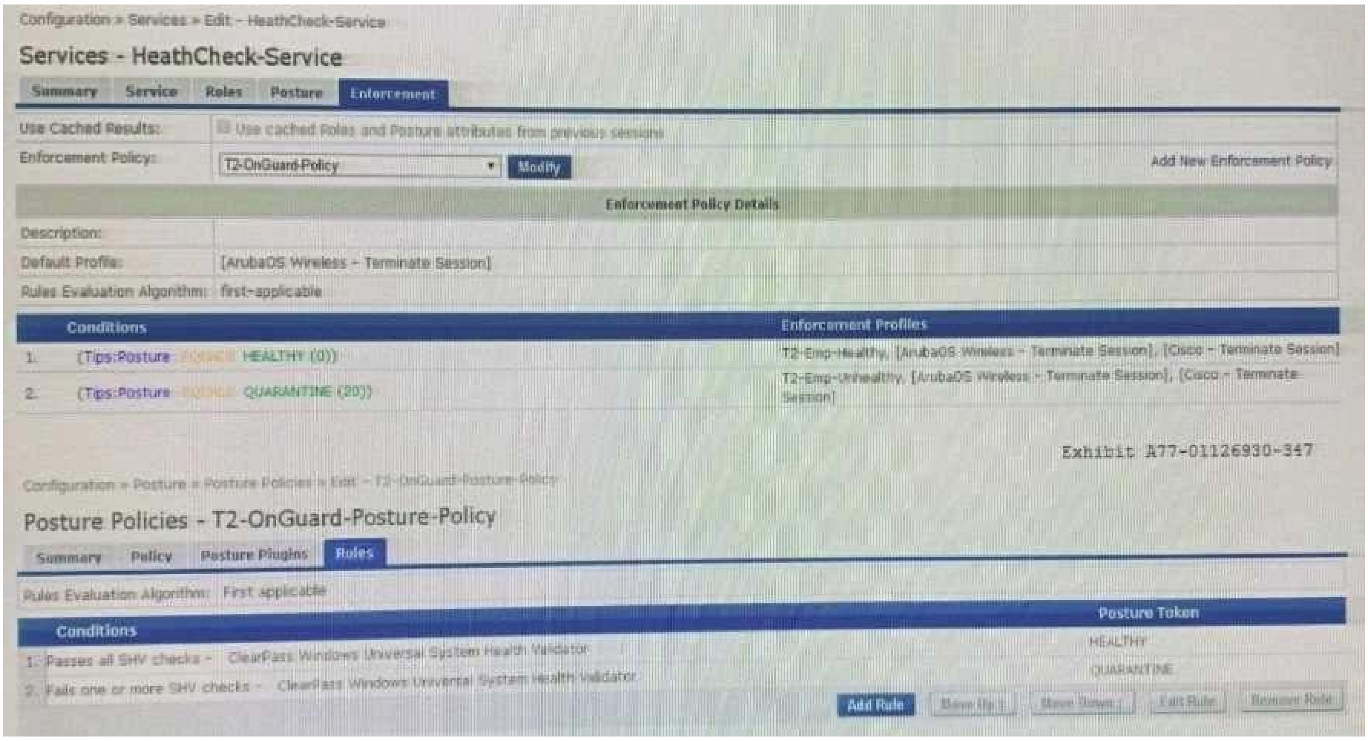
D. On the Attributes tab. you can enable the service to write attributes like Location and Device type based on policy.

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

Correct Answer: DE

QUESTION 4

Refer to the Exhibit:



Configuration » Services » Edit – HeathCheck-Service

Services - HeathCheck-Service

Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	T2-OnGuard-Policy ▾ Modify — Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[ArubaOS Wireless - Terminate Session]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Posture EQUALS HEALTHY (0))	T2-Emp-Healthy, [ArubaOS Wireless - Terminate Session], [Cisco - Terminate Session]
2.	(Tips:Posture EQUALS QUARANTINE (20))	T2-Emp-Unhealthy, [ArubaOS Wireless - Terminate Session], [Cisco - Terminate Session]

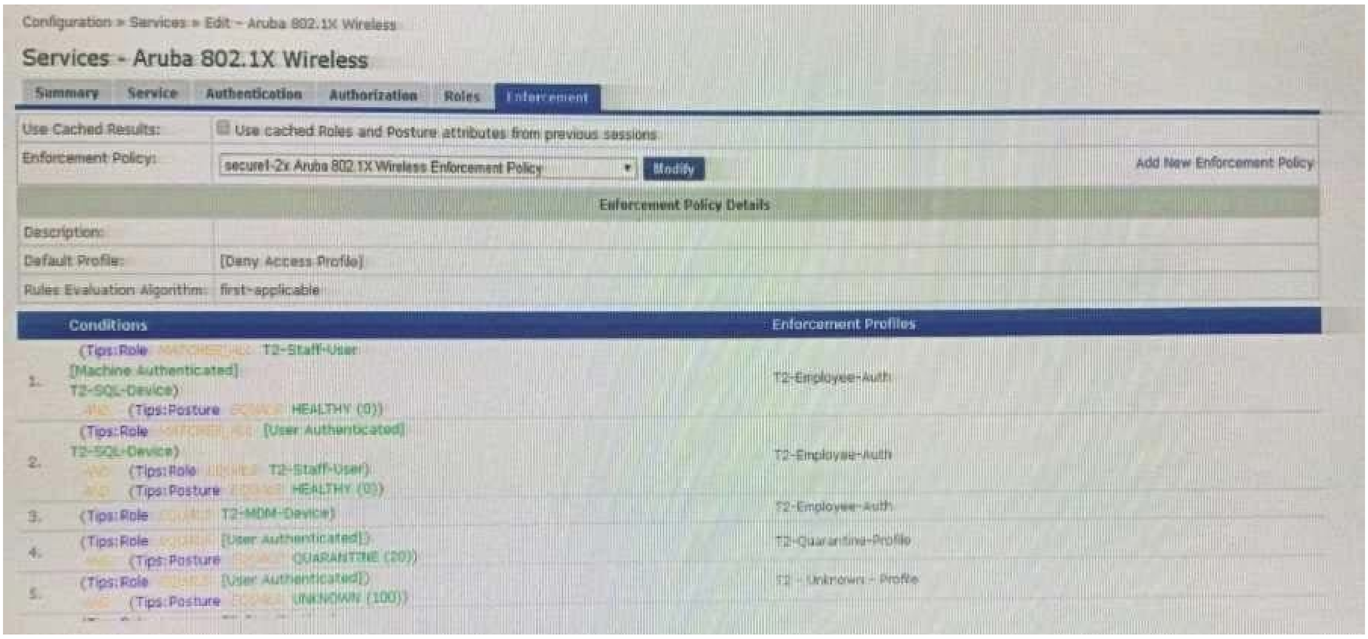
Exhibit A77-01126930-347

Configuration » Posture » Posture Policies » Edit – T2-OnGuard-Posture-Policy

Posture Policies - T2-OnGuard-Posture-Policy

Rules Evaluation Algorithm: First applicable

Conditions	Posture Token
1. Passes all SHV checks - ClearPass Windows Universal System Health Validator	HEALTHY
2. Fails one or more SHV checks - ClearPass Windows Universal System Health Validator	QUARANTINE



Configuration » Services » Edit – Aruba 802.1X Wireless

Services - Aruba 802.1X Wireless

Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	secure1-2x Aruba 802.1X Wireless Enforcement Policy ▾ Modify — Add New Enforcement Policy

Enforcement Policy Details

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

	Conditions	Enforcement Profiles
1.	(Tips:Role MATCHES_ALL T2-Staff-User [Machine Authenticated] T2-SQL-Device) AND (Tips:Posture EQUALS HEALTHY (0))	T2-Employee-Auth
2.	(Tips:Role MATCHES_ALL [User Authenticated] T2-SQL-Device) AND (Tips:Role EQUALS T2-Staff-User) AND (Tips:Posture EQUALS HEALTHY (0))	T2-Employee-Auth
3.	(Tips:Role EQUALS T2-MDM-Device)	T2-Employee-Auth
4.	(Tips:Role EQUALS [User Authenticated]) AND (Tips:Posture EQUALS QUARANTINE (20))	T2-Quarantine-Profile
5.	(Tips:Role EQUALS [User Authenticated]) AND (Tips:Posture EQUALS UNKNOWN (100))	T2 - Unknown - Profile

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

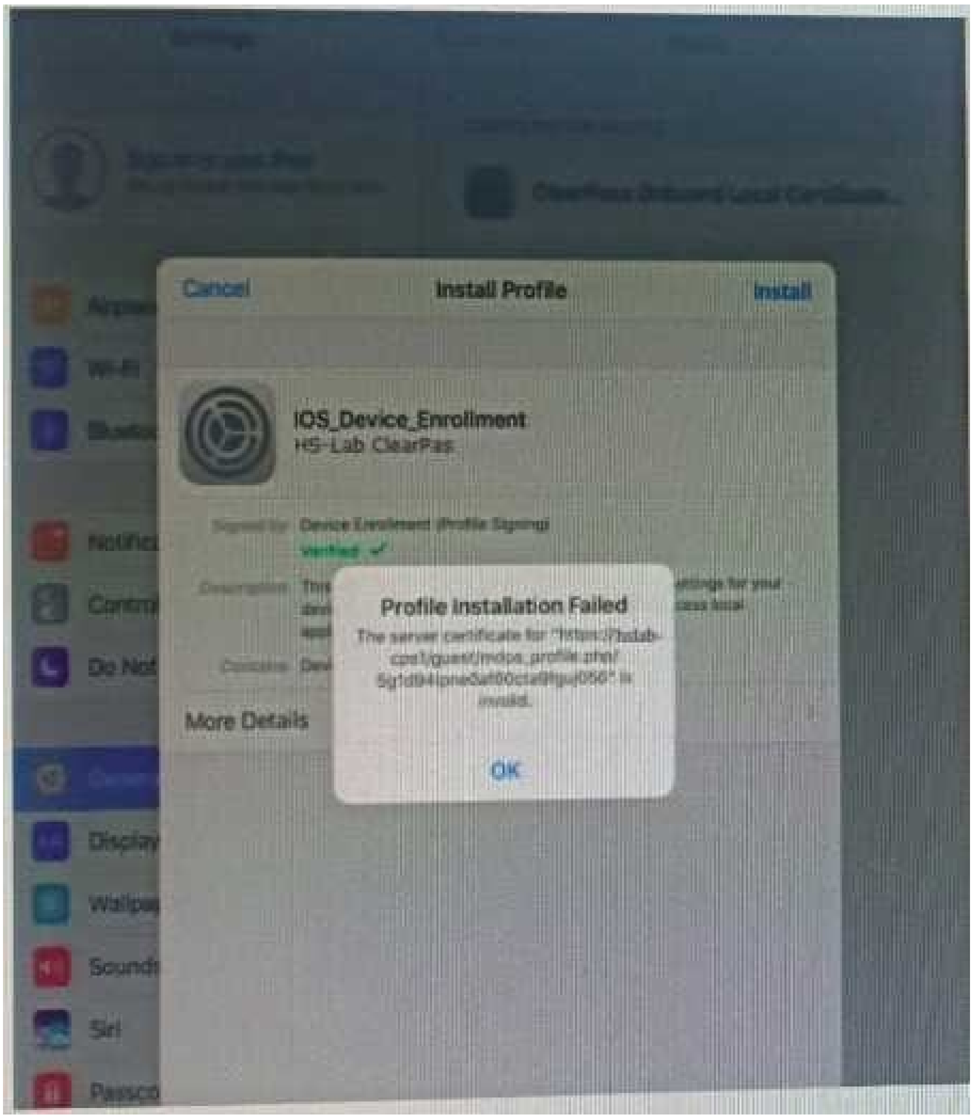
C. RFC-3576 Is not configured correctly on the Aruba Controller and does not update the role.

D. The Enforcement Profile should bounce the connection instead of a Terminate session

Correct Answer: B

QUESTION 5

Refer to the exhibit:



Profile Installation Failed

The server certificate for "https://hslab-cps1/guest/mdps_profile.php/5g1d94lpne3af80cta9fgu050" is invalid.

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 PKl HTTPS certificate for other devices.

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

Correct Answer: AC