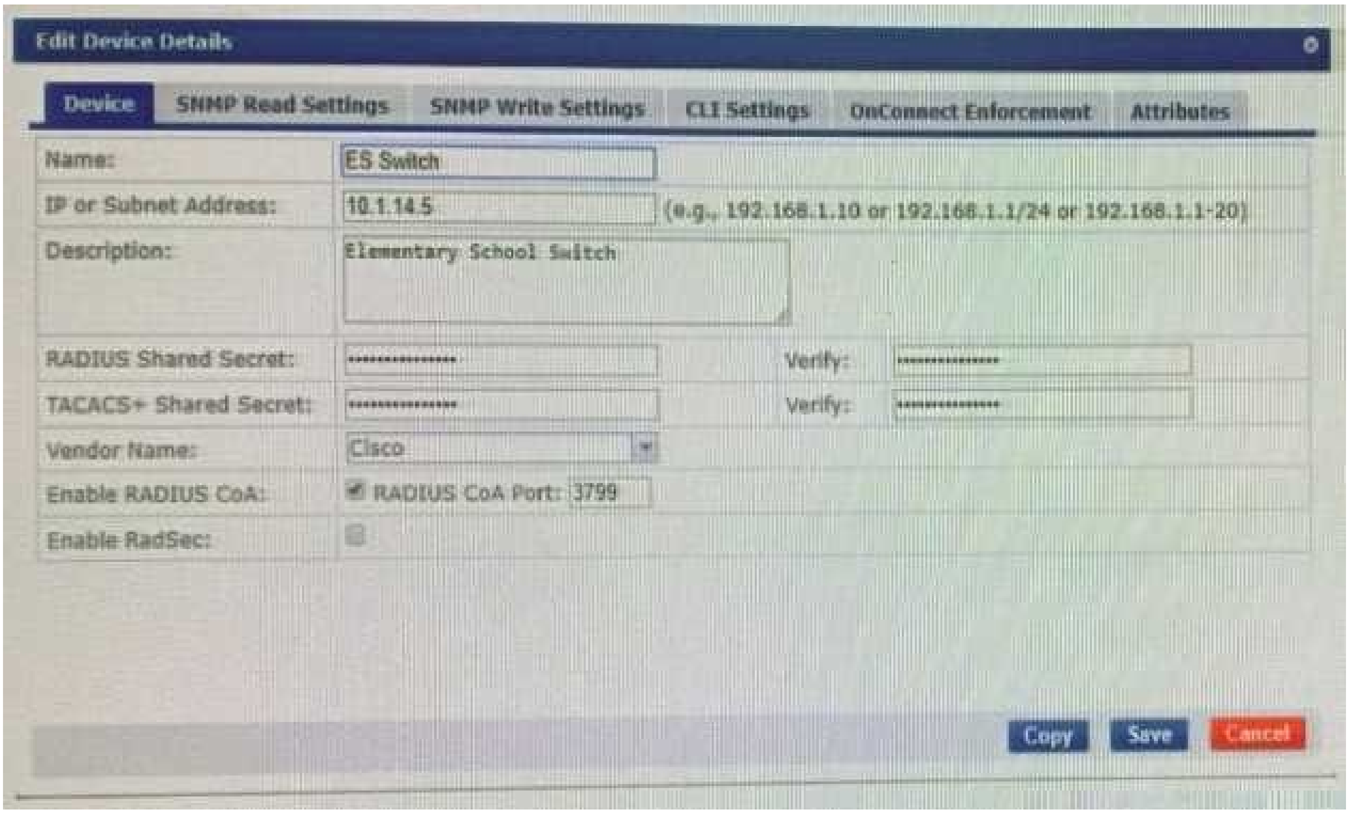
HPE6-A81^Q&As^

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

QUESTION 1

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.

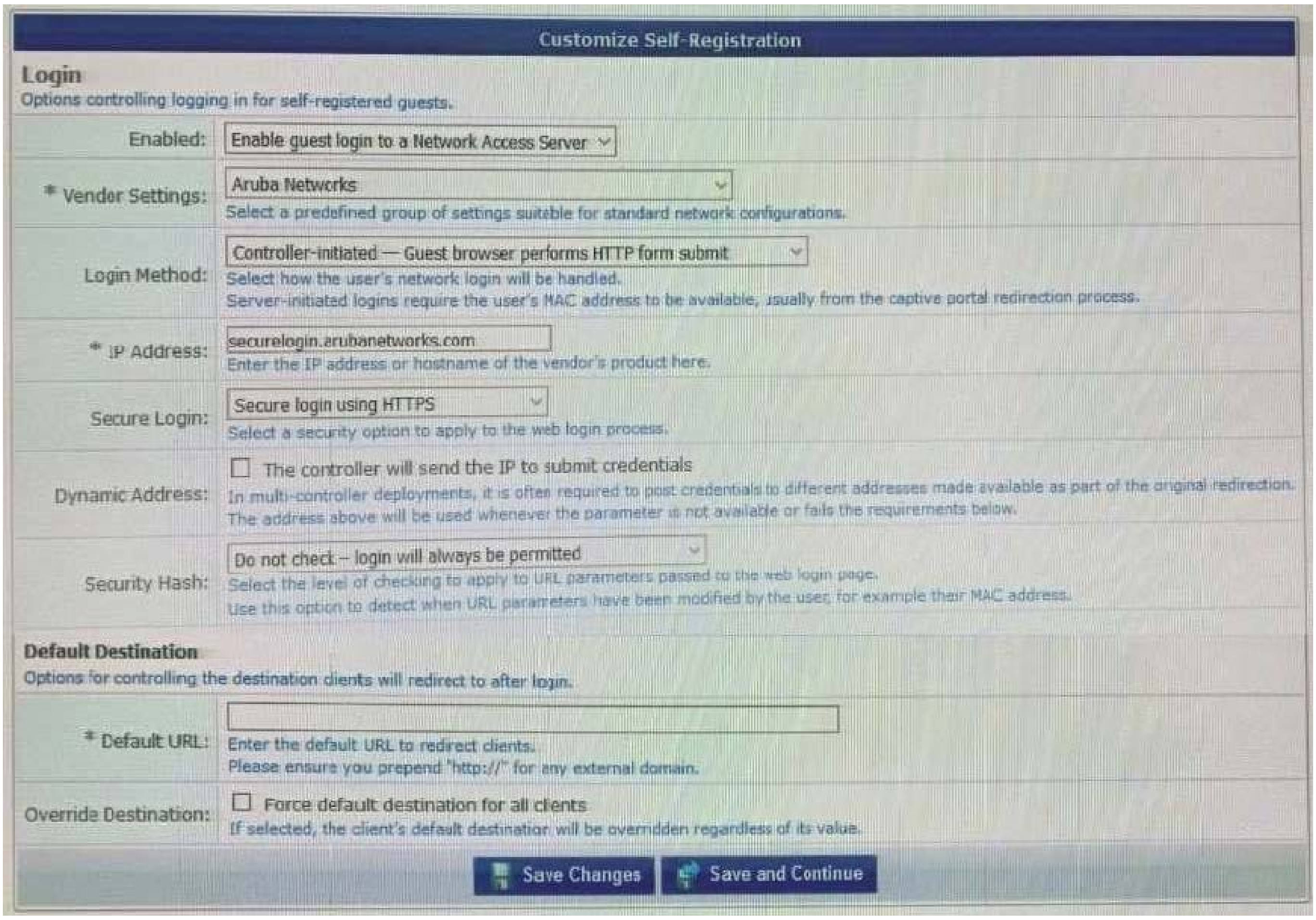
D. On the Attributes tab. you can enable the service to write attributes like Location and Device type based on policy.

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

Correct Answer: DE

QUESTION 2

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".

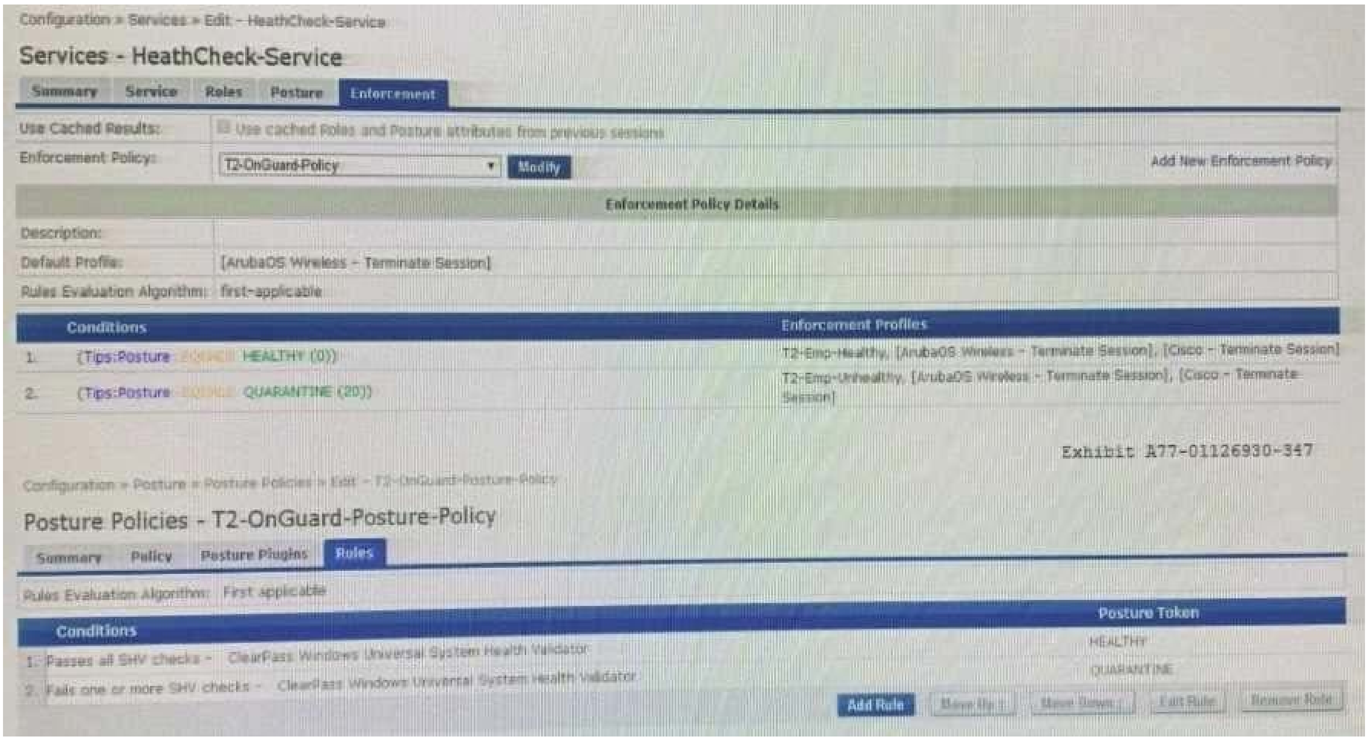
C. Change the "IP Address field to "captiveportal-login.customerdomain.com".

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

Correct Answer: B

QUESTION 3

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

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]

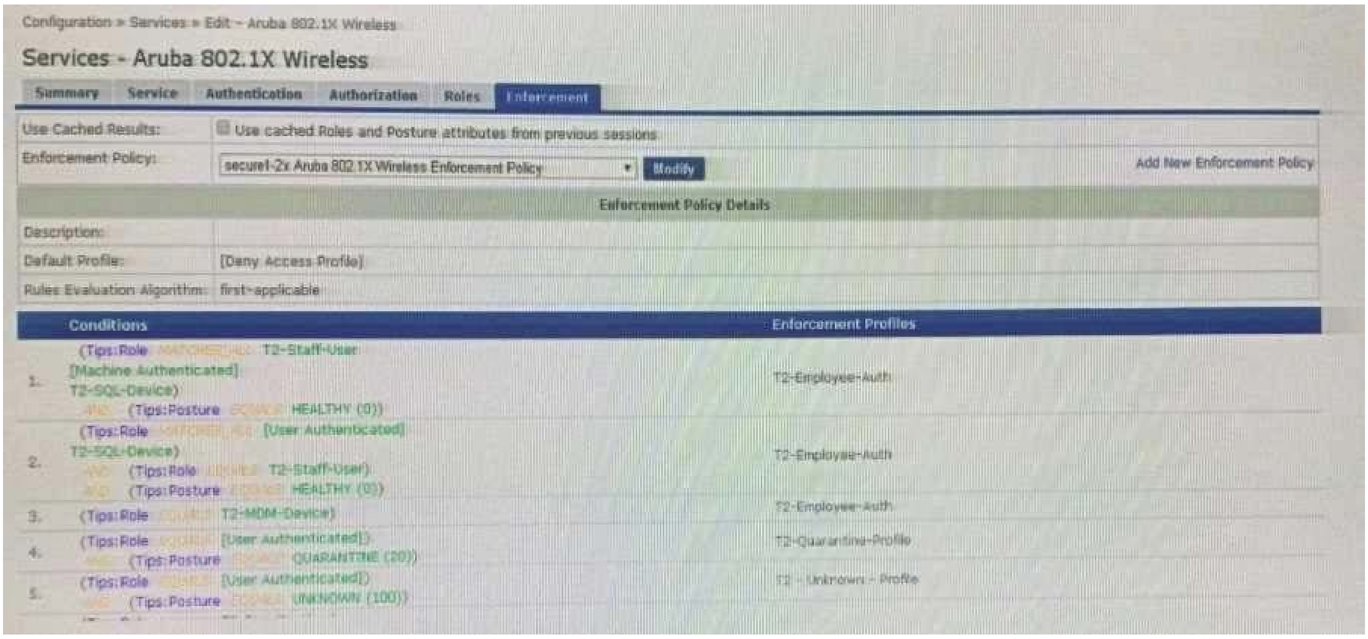
Exhibit A77-01126930-347

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

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 4

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 5

You have Integrated ClearPass Onboard with Active Directory Certificate Services (ADCS) web enrollment to sign the Anal device TLS certificates The Onboard provisioning process completes successfully but when the user finally clicks connect, the user falls to connect to the network with an unknown_ca certificate error. What steps will you follow to complete the requirement?

A. Make sure that the ClearPass servers are using the default self-signed certificates for both SSL and RADIUS server identity

B. Add the ADCS root certificate to both the CPPM Certificate trust list and to the Onboard Certificate Store trust list

C. Make sure both the ClearPass servers have different certificates used for both SSL and RADIUS server identity.

D. Export the self-signed certificate from the ClearPass servers and manually add them as trusted certificates in clients

Correct Answer: A