

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

Refer to the exhibit:

Configuration » Services » Edit - Health-Check

Services - Health-Check

Summary Service Roles **Enforcement**

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

Enforcement Policy: T3-Onguard 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 HEALTHY (0))	T4-Healthy, [ArubaOS Wireless - Terminate Session]
2. (Tips: Posture QUARANTINE (20))	T-4-Unhealthy, [ArubaOS Wireless - Terminate Session]

Posture Policies - Windows

Summary Policy **Posture Plugins** Rules

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
<input checked="" type="checkbox"/> ClearPass Windows Universal System Health Validator	<input type="button" value="Configure"/> <input type="button" value="View"/>	Configured
<input type="checkbox"/> Windows System Health Validator	<input type="button" value="Configure"/> <input type="button" value="View"/>	-
<input type="checkbox"/> Windows Security Health Validator	<input type="button" value="Configure"/> <input type="button" value="View"/>	-

Exhibit: A77-01126930-351

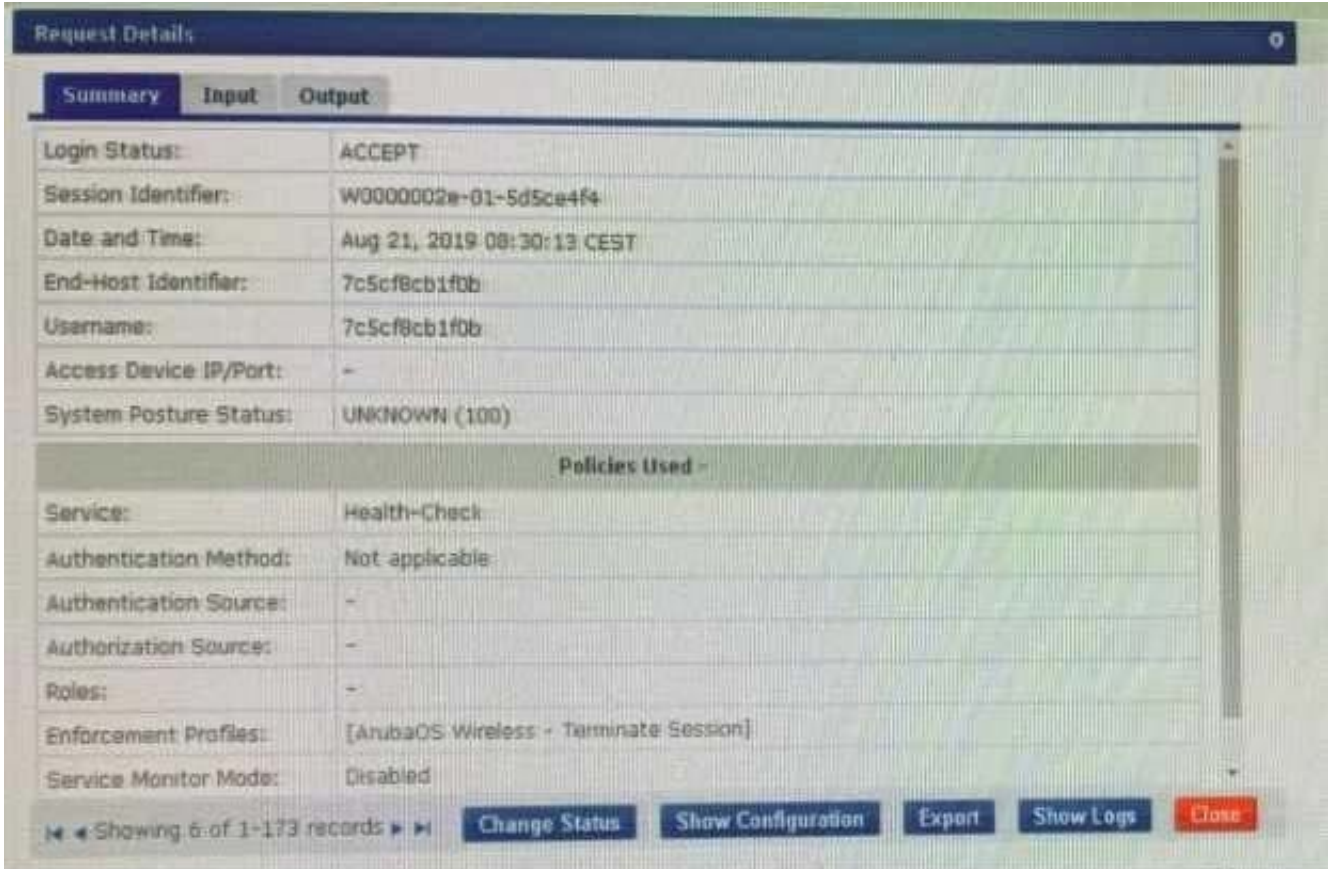
Configuration » Posture » Posture Policies » Edit - Windows

Posture Policies - Windows

Summary Policy Posture Plugins **Rules**

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



What could be causing the error message received on the OnGuard client?

- A. The Service Selection Rules for the service are not configured correctly
- B. The Web-Based Health Check service needs to be configured to use the Posture Policy
- C. There is a firewall policy not allowing the OnGuard Agent to connect to ClearPass
- D. The client's OnGuard Agent has not been configured with the correct Policy Manager Zone

Correct Answer: D

QUESTION 2

Refer to the exhibit: A customer has configured a Guest Self registration page for their Cisco Wireless network with the settings shown. What should be changed in order to successfully authenticate guests users?

Home > Configuration > Pages > Self-Registrations

Customize Self-Registration (Admin-GuestCiscoSelfReg)

Use this form to make changes to the self-registration instance Admin-GuestCiscoSelfReg.

Customize Self-Registration	
Login Options controlling logging in for self-registered guests.	
Enabled:	<input checked="" type="checkbox"/> Enable guest login to a Network Access Server
* Vendor Settings:	Cisco Systems 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:	1.1.1.1 Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default Select a security option to apply to the web login process.
Dynamic Address:	<input checked="" type="checkbox"/> 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.
Username Suffix:	<input type="text"/> The suffix is automatically appended to the username before logging into the NAC.
Default Destination Options for controlling the destination clients will redirect to after login.	
* Default URL:	<input type="text"/> Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input checked="" type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.
<input type="button" value="Save Changes"/> <input type="button" value="Save and Continue"/>	



- A. Secure Login should use HTTP
- B. Change the Vendor Settings to Airespace Networks
- C. Change the IP Address to the Cisco Controller DNS name
- D. Login Method should be Controller-initiated - using HTTPs form submit

Correct Answer: C

QUESTION 3

How does the RadSec improve the RADIUS message exchange? (Select two.)

- A. It can be used on an unsecured network or the Internet.
- B. It builds a TTLS tunnel between the NAD and ClearPass.
- C. Only the NAD needs to trust the ClearPass Certificate.
- D. It encrypts the entire RADIUS message.
- E. It uses UDP to exchange the radius packets.

Correct Answer: DE

QUESTION 4

A customer has configured Onboard with Single SSID provision for Aruba IAP Windows devices work as expected but cannot get the Apple iOS devices to work. The Apple iOS devices automatically get redirected to a blank page and do not get the Onboard portal page. What would you check to fix the issue?

- A. Verify if the checkbox "Enable bypassing the Apple Captive Network Assistant" is checked.
- B. Verify if the Onboard URL is updated correctly in the external captive portal profile.

C. Verify if Onboard Pre-Provisioning enforcement profile sends the correct Aruba user role.

D. Verify if the external captive portal profile is enabled to use HTTPS with port 443.

Correct Answer: B

QUESTION 5

Refer to the exhibit:



Configuration > Services > Edit - ACCX Guest Access

Services - ACCX Guest Access

Summary | Service | Authentication | Roles | Enforcement

Service:

Name:	ACCX Guest Access
Description:	To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.
Type:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator
1.	Radius:IETF	Calling-Station-Id	EXISTS
2.	Connection	Client-Mac-Address	NOT_EQUALS
3.	Radius:Aruba	Aruba-Essid-Name	EQUALS

Authentication:

Authentication Methods:	1. [PAP] 2. [MSCHAP] 3. [CHAP]
Authentication Sources:	[Guest User Repository]
Strip Username Rules:	-
Service Certificate:	-

Roles:

Role Mapping Policy:	[Guest Roles]
----------------------	---------------

Enforcement:

Use Cached Results:	Disabled
---------------------	----------

Home > Configuration > Pages > Web Logins
Web Login (ACCX_LabTest)

Use this form to make changes to the Web Login ACCX_LabTest.

Web Login Editor	
* Name:	ACCX_LabTest <small>Enter a name for this web login page.</small>
Page Name:	ACCX_TestPage <small>Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".</small>
Description:	 <small>Comments or descriptive text about the web login.</small>
* Vendor Settings:	Aruba Networks <small>Select a predefined group of settings suitable for standard network configurations.</small>
Login Method:	Controller-initiated — Guest browser performs HTTP form submit <small>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.</small>
* Address:	securelogin.arubanetworks.com <small>Enter the IP address or hostname of the vendor's product host.</small>
Secure Login:	Use vendor default <small>Select a security option to apply to the web login process.</small>
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials. <small>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.</small>
Page Redirect <small>Options for specifying parameters passed in the initial redirect.</small>	
Security Hash:	Do not check — login will always be permitted <small>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.</small>
Login Form <small>Options for specifying the behaviour and content of the login form.</small>	
Authentication:	Credentials — Require a username and password <small>Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted.</small>

Security Hash:	Do not check — login will always be permitted <small>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.</small>
Login Form <small>Options for specifying the behaviour and content of the login form.</small>	
Authentication:	Credentials — Require a username and password <small>Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set.</small>
Prevent CNA:	<input checked="" type="checkbox"/> Enable bypassing the Apple Captive Network Assistant. <small>The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.</small>
Custom Form:	<input type="checkbox"/> Provide a custom login form <small>If selected, you must supply your own HTML login form in the Header or Footer HTML areas.</small>
Custom Labels:	<input type="checkbox"/> Override the default labels and error messages. <small>If selected, you will be able to alter labels and error messages for the current login form.</small>
* Pre-Auth Check:	App Authentication — check using Aruba Application Authentication <small>Select how the username and password should be checked before proceeding to the RADIUS authentication.</small>
Terms:	<input checked="" type="checkbox"/> Require a Terms and Conditions confirmation. <small>If checked, the user will be forced to accept a Terms and Conditions checkbox.</small>

A year ago, your customer deployed an Aruba ClearPass Policy Manager Server for a Guest SSID hosted in an IAP Cluster. The customer just created a new Web Login Page for the Guest SSID. Even though the previous Web Login

page worked test with the new Web Login Page are failing and the customer has forwarded you the above screenshots.

What recommendation would you give the customer to fix the issue?

- A. The service type configured is not correct. The Guest authentication should be an Application authentication type of service.
- B. The customer should reset the password for the username accx@exam.com using Guest Manage Accounts
- C. The Address filed under the WebLogin Vendor settings is not configured correctly, it should be set to instant.arubanetworks.com
- D. The WebLogin Pre-Auth Check is set to Aruba Application Authentication which requires a separate application service on the policy manager

Correct Answer: A

[Latest HPE6-A77 Dumps](#)

[HPE6-A77 PDF Dumps](#)

[HPE6-A77 Study Guide](#)