

HP

HPE6-A77 Exam

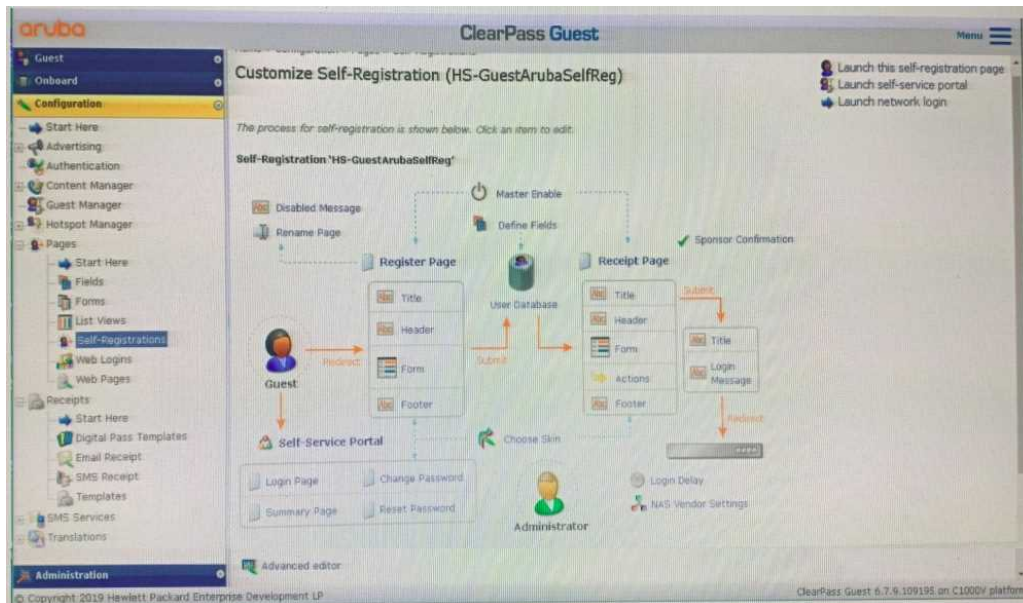
Aruba Certified ClearPass Expert Written Exam

**Questions & Answers
Demo**

Version: 4.0

Question: 1

Refer to the exhibit:



A customer is deploying Guest Self-Registration with Sponsor Approval but does not like the format of the sponsor email. Where can you change the sponsor email?

- A. in the Receipt Page - Actions
- B. in the Sponsor Confirmation section
- C. in me Configuration - Receipts - Email Receipts
- D. in the Configuration - Receipts - Templates

Answer: B

Question: 2

While configuring a guest solution, the customer is requesting that guest user receive access for four hours from their first login. Which Guest Account Expiration would you select?

- A. expire_after
- B. do_expire
- C. expire_time
- D. expire_postlogin

Answer: A

Question: 3

Refer to the exhibit:

The screenshot displays a web interface titled "TACACS+ Session Details". It features three tabs: "Summary", "Request", and "Policies", with "Policies" being the active tab. Below the tabs is a table titled "Policies Used" with the following data:

Policies Used	
Service Name:	[Aruba Device Access Service]
Authentication Source:	[Local User Repository]
Role:	[User Authenticated], [Aruba TACACS read-only Admin]
Profiles:	[ArubaOS Wireless - TACACS Read-Only Access]

At the bottom of the interface, there is a pagination control showing "Showing 2 of 1-2 records" and three buttons: "Export", "Show Logs", and "Close".

The image shows a network configuration interface with two main sections. The top section is titled "Admin Authentication Options" and contains various settings. The bottom section is titled "Auth Servers" and shows a table of servers with a detailed view of the "ClearPass T" server options.

Admin Authentication Options:

- Default role: root
- Enable:
- MSCHAPv2:
- Server group: ClearPass Tacacs
- Management telnet access:
- Login activities persistence period: 0 days
- Login banner text: [Empty text area]
- Banner has to be accepted:
- WEBUI AUTHENTICATION
- Username/password:
- Webui HTTPS port (443) access:
- Client certificate:
- Server certificate: default
- Idle session timeout: 15 minutes
- Re-authentication timeout: [Empty field] minutes

Auth Servers: AAA Profiles | L2 Authentication | L3 Authentication | User Rules | Advanced

NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES
ClearPass T	TACACS	10.1.129.111		

Server Group > ClearPass Tacacs > ClearPass T Server Options:

- Host: 10.1.129.111
- Key: [Redacted]
- Retype key: [Redacted]
- TCP port: 49
- Retransmits: 3
- Timeout: 20
- Mode:
- Session authorization:

```

10.1.120.100 - PuTTY
...
Session Table
-----
ID   User Name   User Role   Connection From   Idle Time   Session Time   Path
-----
1    admin       root        10.1.120.90       00:00:10     00:00:42       /
2    read-only   root        10.1.120.90       00:00:12     00:01:45       /
3    admin       root        10.1.120.90       00:00:12     00:01:44       /

```

A customer has configured the Aruba Controller for administrative authentication using ClearPass as a TACACS server. During testing, the read-only user is getting the root access role. What could be a possible reason for this behavior? (Select two.)

- A. The Controller's Admin Authentication Options Default role is mapped to root.
- B. The ClearPass user role associated to the read-only user is wrong
- C. The Controller Server Group Match Rules are changing the user role
- D. The read-only enforcement profile is mapped to the root role
- E. On the Controller, the TACACS authentication server is not configured for Session authorization

Answer: CE

Question: 4

You have recently implemented a self-registration portal in ClearPass Guest to be used on a Guest SSID broadcast from an Aruba controller. Your customer has started complaining that the users are not able to reliably access the internet after clicking the login button on the receipt page. They tell you that the users will click the login button multiple times and after about a minute they gain access. What could be causing this issue?

- A. The self-registration page is configured with a 1 minute login delay.
- B. The guest client is delayed getting an IP address from the DHCP server.
- C. The guest users are assigned a firewall user role that has a rate limit.
- D. The enforcement profile on ClearPass is set up with an IETF:session delay.

Answer: A

Question: 5

Refer to the exhibit:



The image shows a screenshot of an Aruba network login page. At the top left is the Aruba logo. Below it, there is a message: "Please login to the network using your username and password." followed by "To create a new account click [Create Account](#)." The main login form is titled "Login" and contains the following fields:

- Username:** The input field contains "accx@exam.com" and is highlighted with a red border. Below the field, the text "Invalid username or password" is displayed in red.
- Password:** The input field contains eight black dots representing a masked password.
- Terms:** A checkbox is checked, followed by the text "I accept the terms of use".

At the bottom of the form is a blue "Log In" button. Below the form, there is a message: "Contact a staff member if you are experiencing difficulty logging in."

Exhibit A77-01126930-058

Request Details

Summary
Input
Output
Alerts

Login Status:	REJECT
Session Identifier:	W0000000c-01-5d66e82b
Date and Time:	Sep 23, 2019 11:43:40 EDT
End-Host Identifier:	-
Username:	accx@exam.com
Access Device IP/Port:	-1-
System Posture Status:	-
Policies Used -	
Service:	-
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	-
Enforcement Profiles:	-
Service Monitor Mode:	-
Online Status:	Not Available

Showing 1 of 1-16 records
Show Configuration
Export
Show Logs
Close

Request Details

Summary
Input
Output
Alerts

Error Code:	204
Error Category:	Authentication failure
Error Message:	Failed to classify request to service
Alerts for this Request	
WebAuthService: ServiceClassification failed {No service matched}	

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	Value
1. Radius:IETF	Calling-Station-Id	EXISTS	
2. Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
3. Radius:Aruba	Aruba-Essid-Name	EQUALS	guest-labtest

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>
Descriptions:	 <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 requires 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 here.</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 type="checkbox"/> Enable bypassing the Apple Captive Network Assistant <small>The Apple Captive Network Assistant (CNA) is the pop-up browser shows 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 NAS authentication.</small>
Terms:	<input 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 falling and the customer has forwarded you the above screenshots What recommendation would you give the customer to tix 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 field 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

Answer: A
