HP

HPE6-A77 Exam

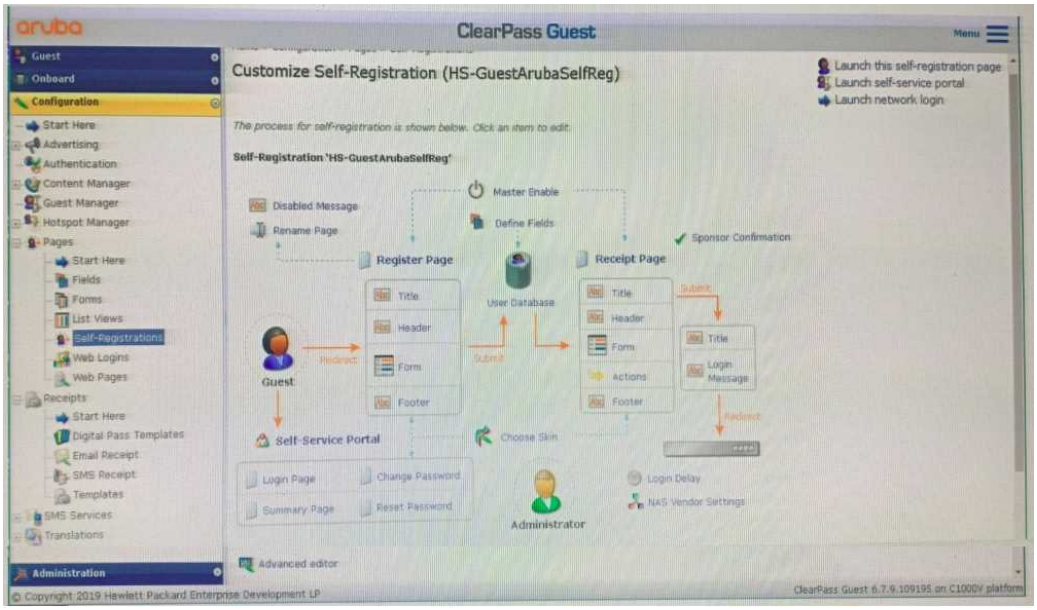
Aruba Certified ClearPass Expert Written Exam

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

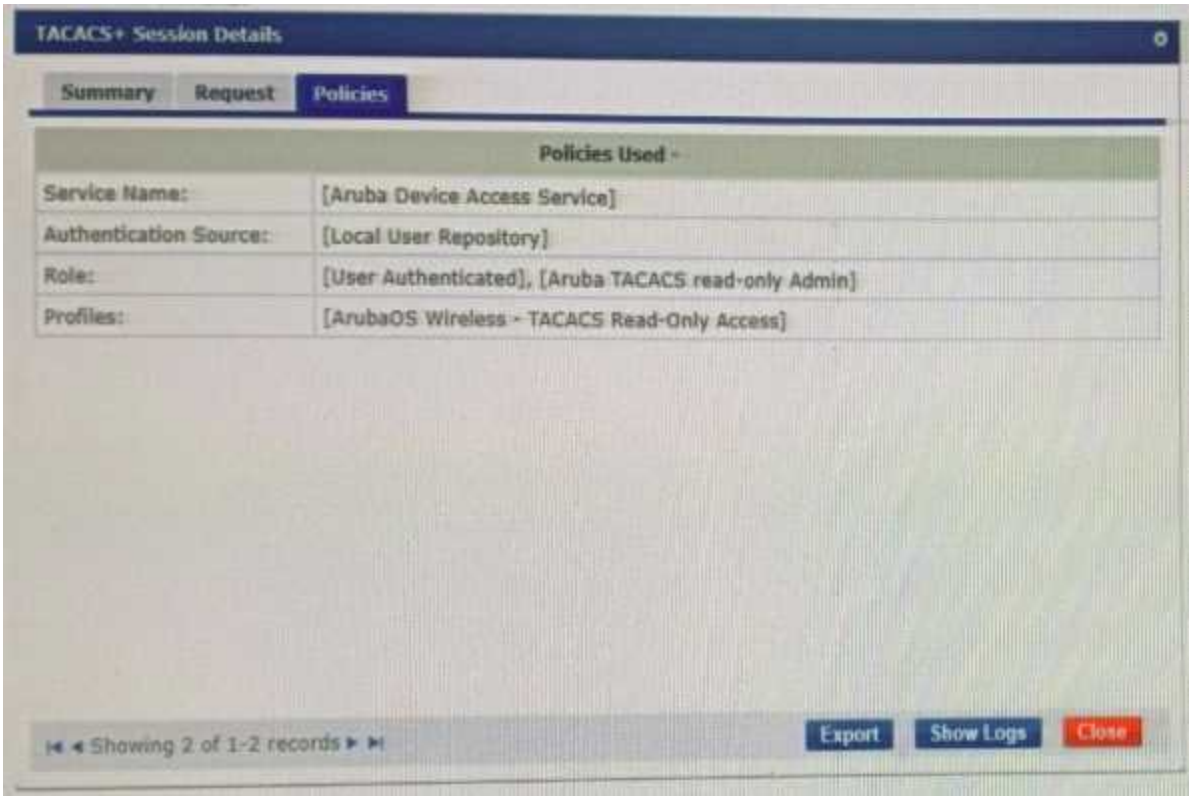
While configuring a guest solution, the customer is requesting that guest user receive access for four hours from their first login. Which Guest Account Expiration would you select?

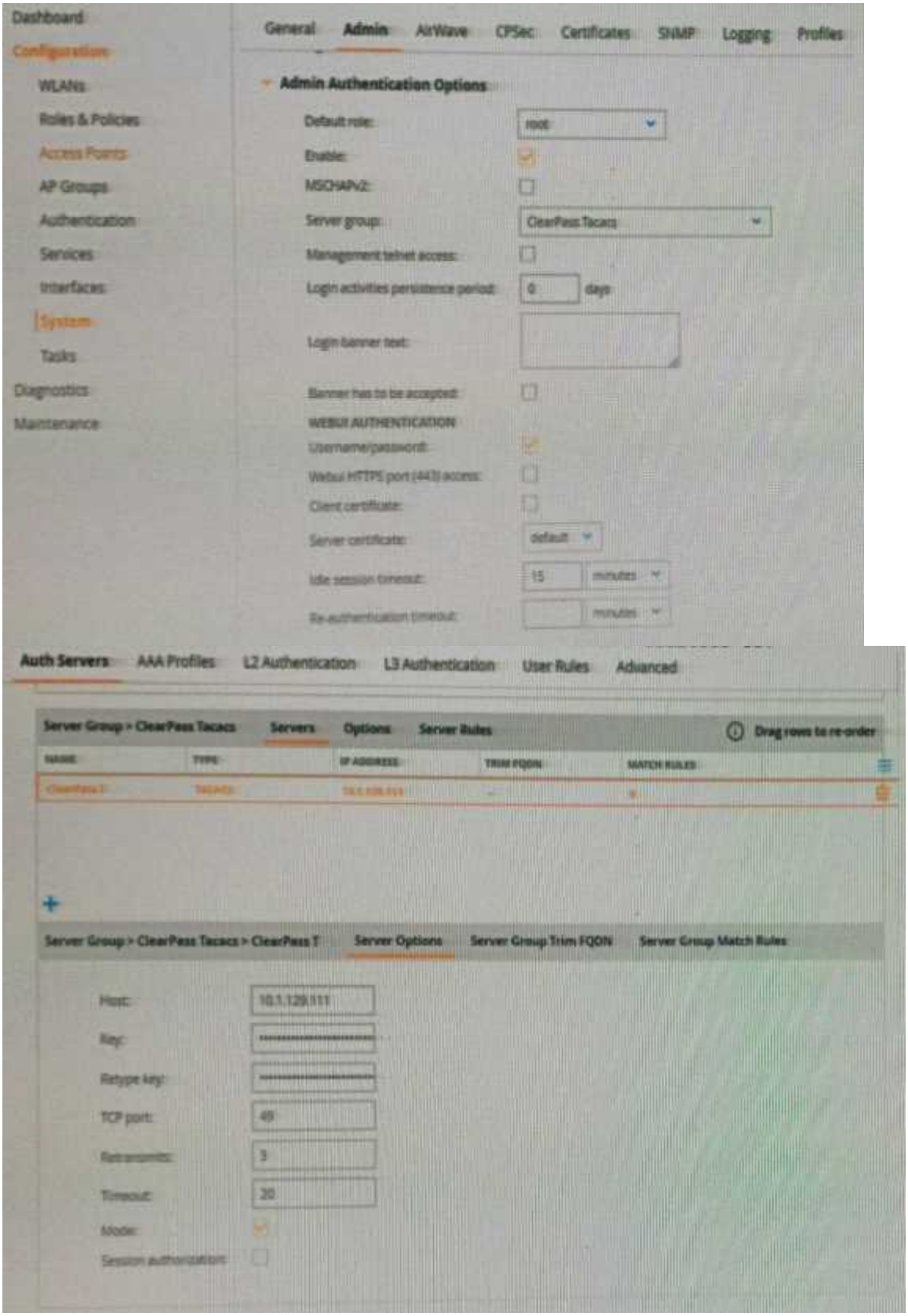
A. expire_after
B. do_expire
C. expire_time
D. expire_ postlogin

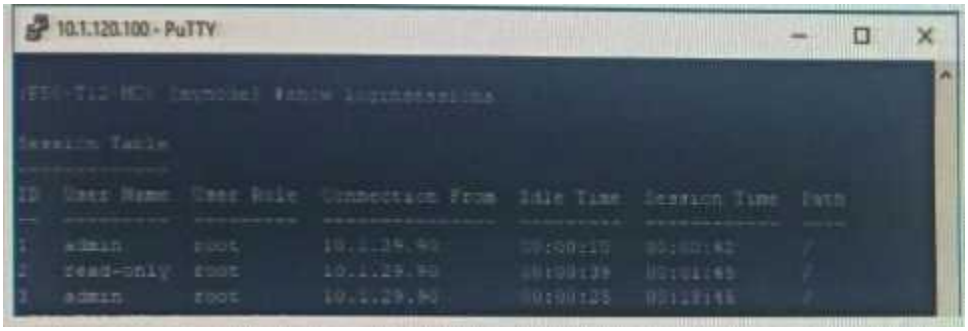
Answer: A

Question: 3

Refer to the exhibit:




Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
System
Tasks
Diagnostics
Maintenance
General
Admin
AirWave
CPSec
Certificates
SNMP
Logging
Profiles
Admin Authentication Options
Default role:
root
Enable:
MSCHAPv2:
Server group:
ClearPass Tacacs
Management telnet access:
Login activities persistence period:
0
days
Login banner text:
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:
minutes
Auth Servers
AAA Profiles
L2 Authentication
L3 Authentication
User Rules
Advanced
Server Group > ClearPass Tacacs
Servers
Options
Server Rules
Drag rows to re-order
NAME
TYPE
IP ADDRESS
TRIM FQDN
MATCH RULES
Server Group > ClearPass Tacacs > ClearPass T
Server Options
Server Group Trim FQDN
Server Group Match Rules
Host:
10.1.129.111
Key:
Retype key:
TCP port:
49
Retransmits:
3
Timeout:
20
Mode:
Session authorization:



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 Controllers Admin Authentication Options Default role is mapped to toot.
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 TACAC$ authentication server Is not configured for Session authorization

Answer: CE

Question: 4

You have recently implemented a serf-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 alter 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 lETF:session delay.

Answer: A

Question: 5

Refer to the exhibit:

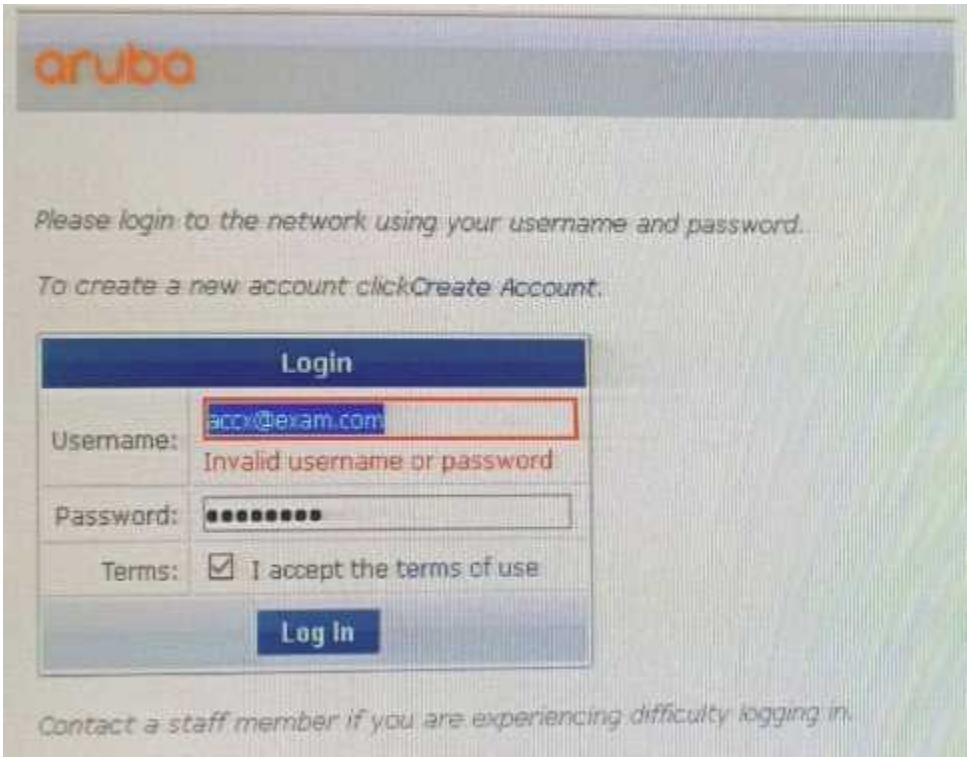

aruba
Please login to the network using your username and password.
To create a new account clickCreate Account.
Login
Username:
accx@exam.com
Invalid username or password
Password:
Terms:
I accept the terms of use
Log In
Contact a staff member if you are experiencing difficulty logging in.

Exhibit A77-01126930-058

Request Details

Summary | Input | Output | Alerts

Login Status:	REJECT
Session Identifier:	W0000000c-01-5d86e82b
Date and Time:	Sep 23, 2019 11:43:40 EDT
End-Host Identifier:	-
Username:	accx@exam.com
Access Device IP/Port:	-:-
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:

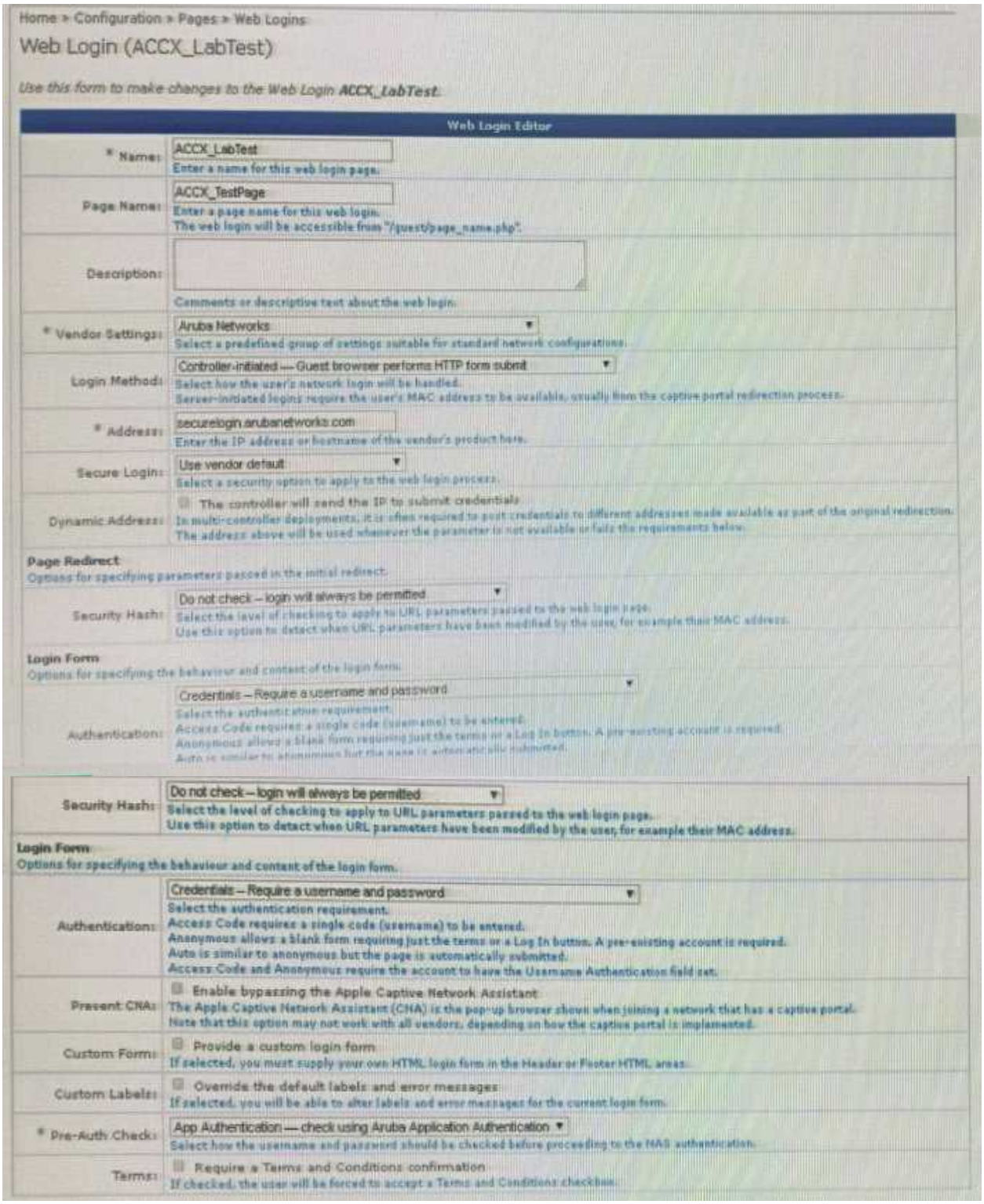
Authentication Methods:	1. [PAP] 2. [MSCHAP] 3. [CHAP]
Authentication Sources:	[Guest User Repository]
Strip Username Rules:	-
Service Certificate:	-

Roles:

Role Mapping Policy:	[Guest Roles]

Enforcement:

Use Cached Results:	Disabled



A year ago, your customer deployed an Aruba ClearPass Policy Manager Server for a Guest SSIC 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 De an Application authentication type of service.
B. The customer should reset the password tor 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

Answer: A