HP

HPE6-A81 Exam

Aruba Certified ClearPass Expert Written

Question: 1

You art deploying Cleat Pass 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 customer's guest solution? (Select two.)

A. Install the same public certificate on all Controllers with the common name "controller.{company domain)

B. Build multiple Web Login pages with vendor settings configured for each controller

C. Build one Web Login page with vendor settings for captiveportal-controller (company domain)

- D. Build one Web Login page with vendor settings for controller (company domain)
- E. Install multiple public certificates with a different Common Name on each controller

Answer: DE

Question: 2

Refer to the exhibit.

Request Deta	sils			1
Summary	Input	Output	Alerts	
Error Code:	3	215		
Error Catego	ory:	Authentica	ation failure	
Error Messa	ge:	TLS sessio	an error	
Alerts for	this Req	uest		
TL	.S Handsh iknown ca	ake failed i	client - unknown_ca n SSL_read with error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert shing TLS session	
H + Showing	1 of 1-20	records .	Show Configuration Export Show Logs Close	

A customer has configured Onboard in a cluster with two nodes. All devices were onboarded in the network through node1 but those clients fail to authenticate through node2 with the error shown What steps would you suggest to make provisioning and authentication work across the entire cluster? (Select three)

A. Configure the Network Settings in Onboard to trust the Policy Manager EAP certificate.

B. Have all of the BYOO clients disconnect and reconnect to the network.

C. Configure the Onboard Root CA to trust the Policy Manager EAP certificate root.

D. Make sure that the EAP certificates on both nodes are issued by one common root Certificate Authority (CA).

Answer: BCD

Question: 3

Refer to the exhibit.

	Customize Self-Registration
Login Options controlling loggin	ig in for self-registered guests.
Enabled:	Enable guest login to a Network Access Server $$
* Vendor Settings:	Aruba Networks v 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 URI, 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 th	e 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.
	Save Changes 🛛 📫 Save and Continue

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.

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

- B. Change the "Secure Login' field to "Use Vendor Default".
- C. Change the 'IP Address field to" securelogin.customerdomain.com
- D. Change the "IP Address field to "captiveportal-login.customerdomain.com".

Answer: D

Question: 4

Refer to the exhibit.

Summary Service	Roles Enforcement			
se Cached Results:	Use cached Poles and Posture	attributes from previous sessions		
forcement Policy:	T-3-Onguard	• Modify		Add New Enforcement Poli
			nt Policy Details	
escription:		Enorceme	it Policy Details	
efault Profile:	(ArubaOS Wireless - Terminate S	ession1		
ules Evaluation Algorithm:				
Conditions			Enforcement Profiles	
. (Tips:Posture EQL	HEALTHY (0))		T4-Healthy, [ArubaOS Wire	less - Terminate Session]
	ALS QUARANTINE (20))			Nireless - Terminate Session]
Configuration > Posture >	Posture Policies » Edit - Windows			
Posture Policies -	Windows			
	Posture Plugins Rules			
elect one/more plugins: Plugin Name			Plugin Configuration	Status
	vs Universal System Health Validato)r	Configure View	Configured
Windows System			Configure View	
Windows Security			Configure View	
	Posture Policies » Edit - Windows			
osture Policies -	Windows			
Summary Policy P	osture Plugins Rules			
ules Evaluation Algorithm:	First applicable			
Conditions				
				Posture Token
Passes all SHV checks	 ClearPass Windows Universal Sy hecks - ClearPass Windows Unive 		Add Rule Mo	Posture Token HEALTHY QUARANTINE ve Up 1 Move Down J Edit Rule Remove Rt
. Passes all SHV checks . Fails one or more SHV c Request Details				HEALTHY QUARANTINE
. Passes all SHV checks . Fails one or more SHV c Request Details	hecks - ClearPass Windows Unive			HEALTHY QUARANTINE
Passes all SHV checks Fails one or more SHV o Request Details Summary Input Login Status: Session Identifier:	Output ACCEPT W0000002e-01-5d5ce4f4			HEALTHY QUARANTINE
Passes all SHV checks Fails one or more SHV of Request Details Summary Input Login Status: Session Identifier: Date and Time:	Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST			HEALTHY QUARANTINE
Passes all SHV checks Fails one or more SHV of Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier:	Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf9cb1f0b			HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username:	Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST			HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c Request Details Summery Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port:	Necks - ClearPass Windows Unive Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b -			HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username:	Necks - ClearPass Windows Unive Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100)	rsal System Health Validator		HEALTHY QUARANTINE
Passes all SHV checks Fails one or more SHV c Request Details Summery Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status:	Necks - ClearPass Windows Unive Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U	rsal System Health Validator		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service:	Necks - ClearPass Windows Unive Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check	rsal System Health Validator		HEALTHY QUARANTINE
Passes all SHV checks Fails one or more SHV of Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method:	Necks - ClearPass Windows Unive Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U	rsal System Health Validator		HEALTHY QUARANTINE
Passes all SHV checks Fails one or more SHV of Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source:	Necks - ClearPass Windows Unive Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check	rsal System Health Validator		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source:	Necks - ClearPass Windows Unive Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check	rsal System Health Validator		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Roles:	becks ClearPass Windows University Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b 7c5cf8cb1f0b OUNKNOWN (100) UNKNOWN (100) Policies U Health-Check Not applicable - - - -	rsal System Health Validator		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Authorization Source: Roles: Enforcement Profiles:	hecks - ClearPass Windows Unive Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check Not applicable [ArubaOS Wireless - Terminate	rsal System Health Validator		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV of Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode:	hecks - ClearPass Windows Unive Output ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check Not applicable - - (ArubaOS Wireless - Terminate Disabled	sed - Session]		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c tequest Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode: I d Showing 6 of 1-173	ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Health-Check Not applicable - Disabled	rsal System Health Validator		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV of Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode:	ACCEPT ACCEPT AUG000020=01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check Not applicable [ArubaOS Wireless - Terminate Disabled records ▶ ▶] Change Status	sed - Session]		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c tequest Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode: I d Showing 6 of 1-173	hecks - ClearPass Windows Unive ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check Not applicable - [ArubaOS Wireless - Terminate Disabled records >) Change Status	sed - Session]		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode: I Service for Jan 200	hecks - ClearPass Windows Unive ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check Not applicable - [ArubaOS Wireless - Terminate Disabled records >) Change Status	sed - Session]		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV checks - Fails one or more SHV checks - Summery Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode: Is Showing 6 of 1–173 ClearPass OnGuard 6710.102 Health Status: Collecti	ACCEPT ACCEPT ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Health-Check Not applicable - [ArubaOS Wireless - Terminate Disabled records > > Change Status	sed - Session]		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV c Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode: I Service for Jan 200	ACCEPT ACCEPT ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Health-Check Not applicable - [ArubaOS Wireless - Terminate Disabled records > > Change Status	sed - Session]		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV checks - Fails one or more SHV checks - Summery Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode: Is Showing 6 of 1–173 ClearPass OnGuard 6710.102 Health Status: Collecti	ACCEPT ACCEPT ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Health-Check Not applicable - [ArubaOS Wireless - Terminate Disabled records > > Change Status ag health information Settings	sed - Session]		HEALTHY
Passes all SHV checks - Fails one or more SHV of Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode: I < Showing 6 of 1-173 I ClearPass OnGuard & 210.100 Health Status: Collecti	AcCEPT ACCEPT AQ 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check Not applicable - [ArubaOS Wireless - Terminate Disabled records ▶ ▶ Change Status 223 Change Status Settrops	sed - Session]		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV of Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode: I < Showing 6 of 1-173 I ClearPass OnGuard & 210.100 Health Status: Collecti	hecks - ClearPass Windows Unive ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check Not applicable - - - - - - - - - - - - -	sed - Session]		HEALTHY QUARANTINE
Passes all SHV checks - Fails one or more SHV of Request Details Summary Input Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: System Posture Status: Service: Authentication Method: Authentication Source: Roles: Enforcement Profiles: Service Monitor Mode: Is a Showing 6 of 1-173 In ClearPass OnGuard 5.710.102 Health Status: Collecti Connection Details Diagnostics	hecks - ClearPass Windows Unive ACCEPT W0000002e-01-5dSce4f4 Aug 21, 2019 08:30:13 CEST 7c5cf8cb1f0b 7c5cf8cb1f0b - UNKNOWN (100) Policies U Health-Check Not applicable - - - - - - - - - - - - -	sed - Session]		HEALTHY 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 Health-Check service does not have Posture Compliance option enabled
- C. The client's OnGuard Agent has not been configured with the correct Policy Manager Zone.
- D. There is a firewall policy not allowing the OnGuard Agent to connect to ClearPass

		Answer: A
Question:	5	
Refer to the	exhibit.	
arubo	L.	
Newsel		
	to the network using your username and password.	
To create a	new account clickCreate Account.	
	Login	
Username:	accx@exam.com	
Username:		
Username: Password:	Invalid username or password	
. 7.774.02700750	Invalid username or password	
Password:	Invalid username or password	

Summary Input	Dutput Alerts
ogin Status:	ABJECT
Session Identifier:	W0000000c-01-5d88e82b
Date and Time:	Sep 23, 2019 11:43:40 EDT
Ind-Host Identifier:	
Jsemame:	ecck@exam.com
Access Device SP/Port:	101
System Posture Status	16 K
	Policies Used -
Service:	
Authentication Hethod:	Not applicable
Authentication Source:	10 C
Authorization Source:	R. Contraction of the second sec
Roles:	6
Inforcement Profiles:	0
Cervice Monitor Mode:	e
Online Status:	Not Available

5	ummary Input	Output Alerts			
Erro	or Code: 204				
Error Category: Authentication failure Error Message: Failed to classify request to service Alerts for this Request					
			ice		
We	ebAuthService Servi	ceClassification failed (No	service matched}		
Con	figuration > Services	+ Edit - ACCX Guest Acce	\$5		
Ser	rvices - ACCX (Guest Access			
Su	mmary Service	Authentication Roles	Enforcement		
ierv	vice:				
Nam	ie:	ACCX Guest Access			
Desc	cription:	To authenticate guest use	ers logging in via captive portal. Gue	sts must re-authenticate after their session (ends.
Type	0	RADIUS Enforcement (0	ieneric)		
Stati		Enabled			
	itor Mode:	Disabled			
More	e Options:	<u>*</u>			
				Service Rule	
tatch	h ALL of the following	conditions:	Name	Decator	Value
	Туре	conditions:	Name Calling-Station-Id	Operator	Value
1.	Type Radius:IETF	a conditions:	Calling-Station-Id	EXISTS	
1. 2.	Type Radius:IETF Connection) conditions:	Calling-Station-Id Client-Mac-Address	EXISTS NOT_EQUALS	%{Radius:IETF:User-Name
1. 2. 3.	Type Radius:IETF Connection Radius:Aruba	; conditions:	Calling-Station-Id	EXISTS	
1. 2. 3.	Type Radius:IETF Connection Radius:Aruba hentication:	1. [PAP] 2. [MSCHAP] 3. [CHAP]	Calling-Station-Id Client-Mac-Address	EXISTS NOT_EQUALS	%{Radius:IETF:User-Name
1. 2. 3. Auth	Type Radius:IETF Connection Radius:Aruba hentication:	1. [PAP] 2. [MSCHAP]	Calling-Station-Id Client-Mac-Address	EXISTS NOT_EQUALS	%{Radius:IETF:User-Name
1. 2. 3. Auth	Type Radius:IETF Connection Radius:Aruba hentication: entication Methods:	1. [PAP] 2. [MSCHAP] 3. [CHAP]	Calling-Station-Id Client-Mac-Address	EXISTS NOT_EQUALS	%{Radius:IETF:User-Name
1. 2. 3. Auth Auth Strip	Type Radius:IETF Connection Radius:Aruba hentication: ientication Methods: mentication Sources:	1. [PAP] 2. [MSCHAP] 3. [CHAP]	Calling-Station-Id Client-Mac-Address	EXISTS NOT_EQUALS	%{Radius:IETF:User-Name
1. 2. 3. Auth Auth Strip Serv	Type Radius:IETF Connection Radius:Aruba hentication: mentication Methods: mentication Sources: b Username Rules: rice Certificate:	1. [PAP] 2. [MSCHAP] 3. [CHAP]	Calling-Station-Id Client-Mac-Address	EXISTS NOT_EQUALS	%{Radius:IETF:User-Name
1. 2. 3. Auth Auth Strip Serv Role	Type Radius:IETF Connection Radius:Aruba hentication: mentication Methods: mentication Sources: b Username Rules: rice Certificate:	1. [PAP] 2. [MSCHAP] 3. [CHAP]	Calling-Station-Id Client-Mac-Address	EXISTS NOT_EQUALS	%{Radius:IETF:User-Name
1. 2. 3. Auth Auth Strip Serv Role	Type Radius:IETF Connection Radius:Aruba hentication: mentication Methods: mentication Sources: b Username Rules: rice Certificate:	1. [PAP] 2. [MSCHAP] 3. [CHAP] [Guest User Repository]	Calling-Station-Id Client-Mac-Address	EXISTS NOT_EQUALS	%{Radius:IETF:User-Name
1. 2. 3. Auth Auth Strip Serv Role Role	Type Radius:IETF Connection Radius:Aruba hentication: entication Methods: mentication Sources: busername Rules: rice Certificate: si Mapping Policy:	1. [PAP] 2. [MSCHAP] 3. [CHAP] [Guest User Repository]	Calling-Station-Id Client-Mac-Address	EXISTS NOT_EQUALS	%{Radius:IETF:User-Name

Web Login (ACCX_LabTest)

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

Web Login (ACCX_LabTest)

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

	Web Login Editor
* Name:	ACCX_LabTest Enter a name for this web login page.
Page Name:	ACCX_TestPage Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	Comments or descriptive text about the web login.
* 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.
* Address:	securelogin.arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login: Page Redirect Options for specifying pa	Use vendor default ~
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.
Login Form Options for specifying th	e behaviour and content of the login form.
Authentication:	Credentials - Require a username and password 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 projure the account to have the Username Authentication field set.
Prevent CNA:	Enable bypassing the Apple Captive Network Assistant 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.
Custom Form:	Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	App Authentication — check using Aruba Application Authentication ~ Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.
Prevent CNA:	Enable bypassing the Apple Captive Network Assistant 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.
Custom Form:	Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	App Authentication — check using Aruba Application Authentication ~ Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

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 customer should reset the password for the username accxCdlexam.com using Guest Manage Accounts.

B. The service type configured is not correct. The Guest authentication should be an Application authentication type of service.

C. The Address filed under the WebLogin Vendor settings is not configured correctly. It should be set to instant, Aruba networks com,

D. The WebLogin Pre-Auth Check is set to Aruba Application Authentication which requires a separate application service on the policy manager

Answer: C