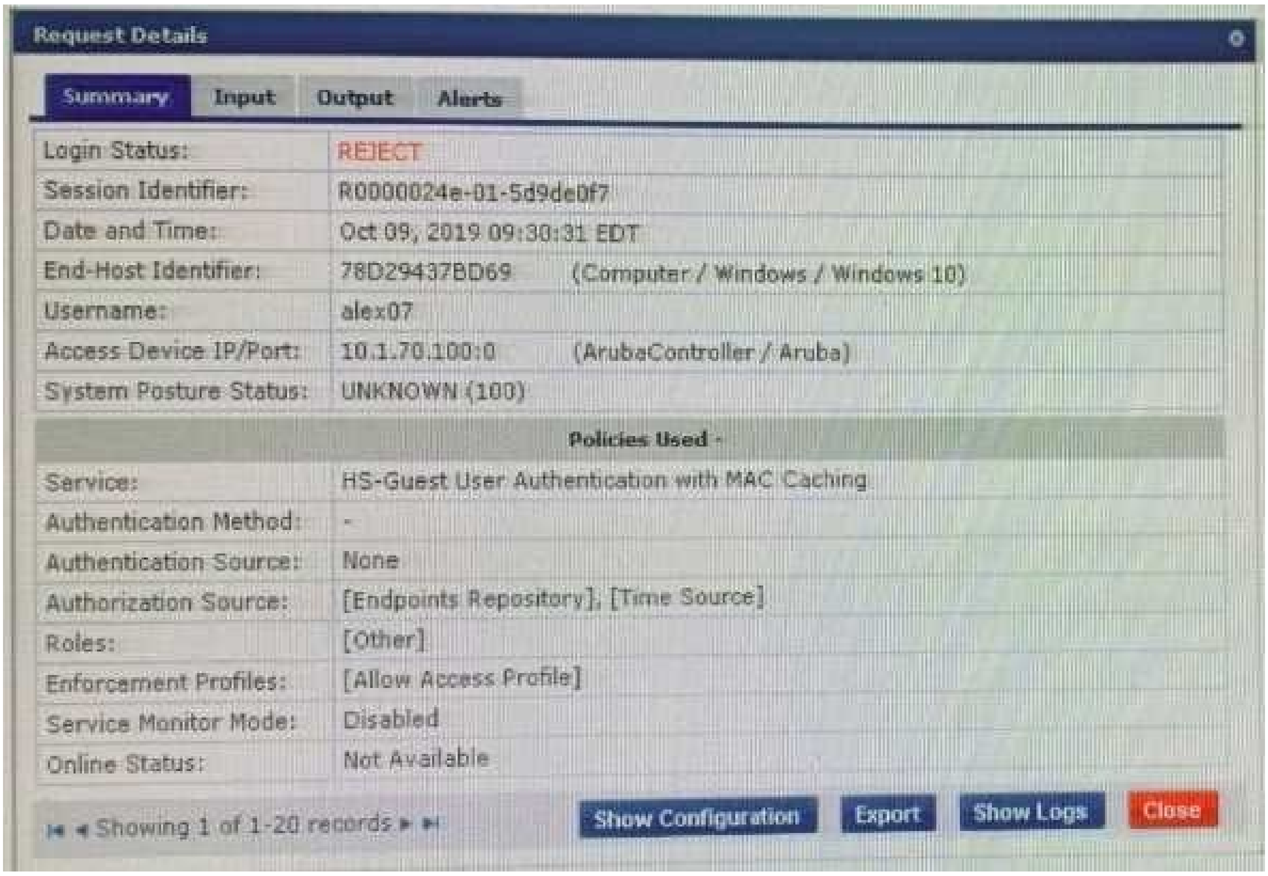
HPE6-A77$^{\text{Q\&As}}$

Aruba Certified ClearPass Expert Written

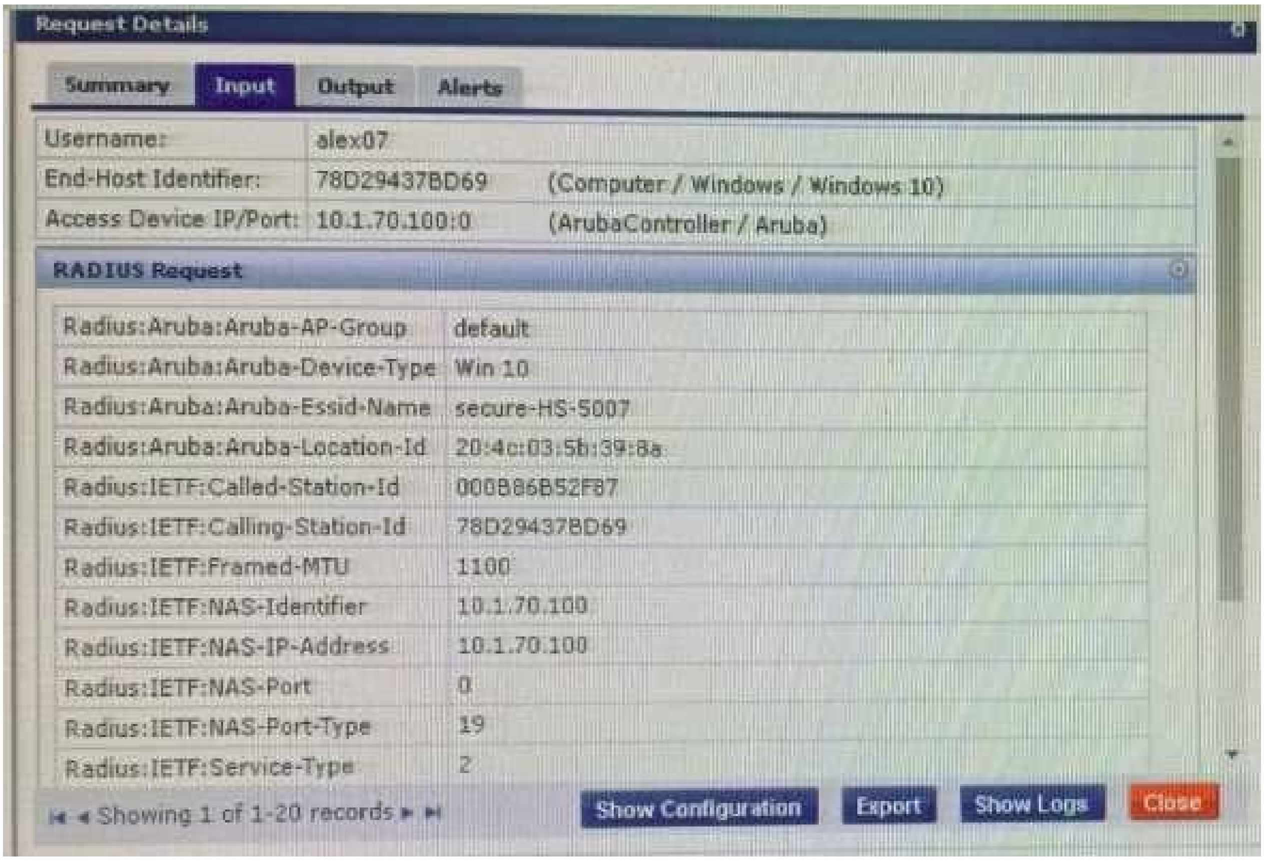
Pass HP HPE6-A77 Exam with 100% Guarantee

QUESTION 1

Refer to the exhibit: Your customer configured a ClearPass server to process the Guest and Secure SSIDs broadcasting from both Aruba and Cisco WLAN controllers When an Employee connects to Aruba or Cisco secure SSID, the authentication hits the guest service causing the client to fail the connection to the network. What change can be implemented to make both the secure and guest services created for Aruba and Cisco devices to work correctly?



Login Status:	REJECT
Session Identifier:	R0000024e-01-5d9de0f7
Date and Time:	Oct 09, 2019 09:30:31 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows 10)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	HS-Guest User Authentication with MAC Caching
Authentication Method:	-
Authentication Source:	None
Authorization Source:	[Endpoints Repository], [Time Source]
Roles:	[Other]
Enforcement Profiles:	[Allow Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Not Available



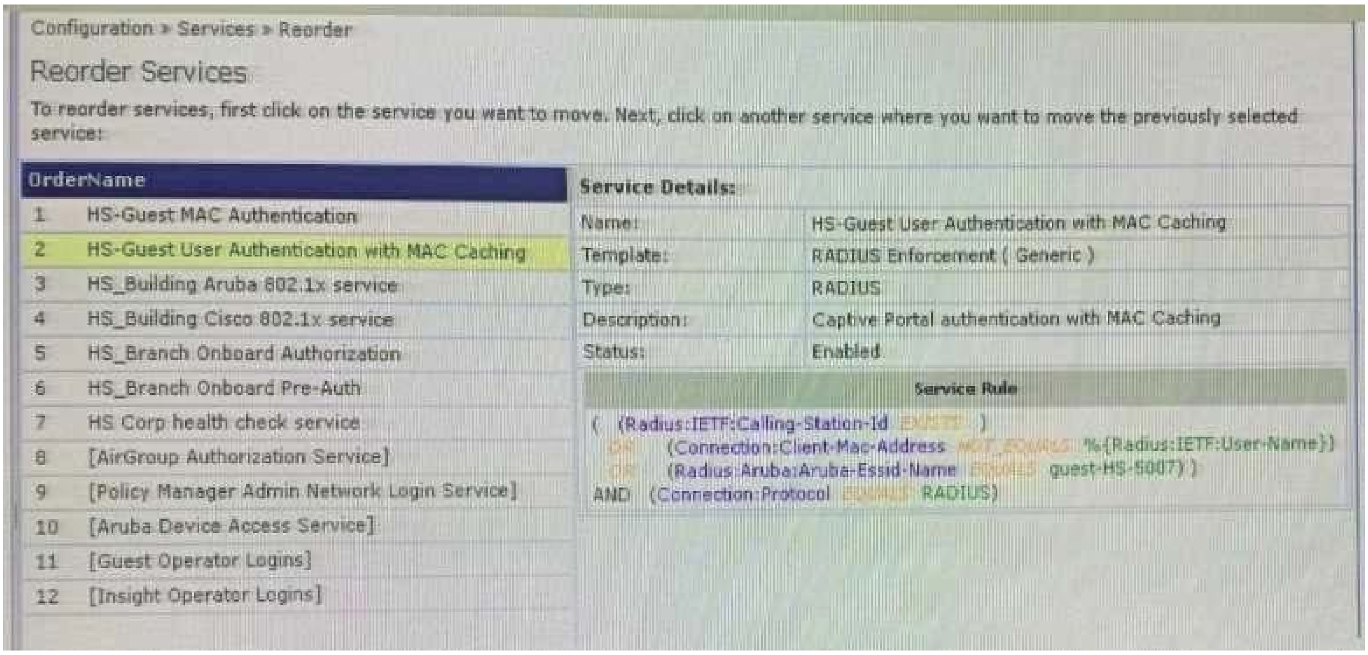
Request Details

Username:	alex07	
End-Host Identifier:	78D29437BD69	(Computer / Windows / Windows 10)
Access Device IP/Port:	10.1.70.100:0	(ArubaController / Aruba)

RADIUS Request

Radius:Aruba:Aruba-AP-Group	default
Radius:Aruba:Aruba-Device-Type	Win 10
Radius:Aruba:Aruba-Essid-Name	secure-HS-5007
Radius:Aruba:Aruba-Location-Id	20:4c:03:5b:39:8a
Radius:IETF:Called-Station-Id	000B86B52F87
Radius:IETF:Calling-Station-Id	78D29437BD69
Radius:IETF:Framed-MTU	1100
Radius:IETF:NAS-Identifier	10.1.70.100
Radius:IETF:NAS-IP-Address	10.1.70.100
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	19
Radius:IETF:Service-Type	2

Showing 1 of 1-20 records



Configuration » Services » Reorder

Reorder Services

To reorder services, first click on the service you want to move. Next, click on another service where you want to move the previously selected service:

Order	Name
1	HS-Guest MAC Authentication
2	HS-Guest User Authentication with MAC Caching
3	HS_Building Aruba 802.1x service
4	HS_Building Cisco 802.1x service
5	HS_Branch Onboard Authorization
6	HS_Branch Onboard Pre-Auth
7	HS Corp health check service
8	[AirGroup Authorization Service]
9	[Policy Manager Admin Network Login Service]
10	[Aruba Device Access Service]
11	[Guest Operator Logins]
12	[Insight Operator Logins]

Service Details:

Name:	HS-Guest User Authentication with MAC Caching
Template:	RADIUS Enforcement (Generic)
Type:	RADIUS
Description:	Captive Portal authentication with MAC Caching
Status:	Enabled

Service Rule

```
(   (Radius:IETF:Calling-Station-Id EXISTS  )
  OR    (Connection:Client-Mac-Address NOT_EQUALS %{Radius:IETF:User-Name})
  OR    (Radius:Aruba:Aruba-Essid-Name EQUALS guest-HS-5007) )
AND  (Connection:Protocol EQUALS RADIUS)
```

A. Move the HS-Guest User Authentication with MAC Caching service to the first position.

B. Modify the service rule matching algorithm to ALL in HS-Guest User Authentication service.

C. Disable HS-Guest User Authentication service and move HS-Guest MAC Authentication to seventh position.

D. Move the HS_Building Aruba 802.1x service to the second position in the service order.

Correct Answer: A

QUESTION 2

You have integrated ClearPass Onboard with Active Directory Certificate Services (ADCS) web enrollment

to sign the final device TLS certificates. The customer would also like to use ADCS for centralized

management of TLS certificates including expiration, revocation, and deletion through ADCS.

What steps will you follow to complete the requirement?

A. Remove the EAP-TLS authentication method and add "EAP-TLS with OCSP Enabled\\' authentication method in the OnBoard Provisioning service. No other configuration changes are required.

B. Copy the [EAP-TLS with OSCP Enabled) authentication method and set the correct ADCS server OCSP URL, remove EAP-TLS and map the custom created method to the Onboard Provisioning Service.

C. Copy the default [EAP-TLS with OSCP Enabled] authentication method and update the correct ADCS server OCSP URL. remove EAP-TLS and map the custom created method to the OnBoard Authorization Service.

D. Edit the [EAP-TLS with OSCP Enabled) authentication method and set the correct ADCS server OCSP URL. remove EAP-TLS and map the [EAP-TLS with OSCP Enabled) method to the Onboard Provisioning Service.

Correct Answer: A

QUESTION 3

A customer is complaining that some of the devices, in their manufacturing network, are not getting profiled while other loT devices from the same subnet have been correctly profiled. The network switches have been configured for DHCP IP helpers and IF-MAP has been configured on the Aruba Controllers. What can the customer do to discover those devices as well? (Select two.)

A. Update the Fingerprints Dictionary to the latest in case new devices have been added.

B. Open a TAC case to help you troubleshoot the DHCP device profile functionality.

C. Add the ClearPass Server IP as an IP helper address on the default gateway as well.

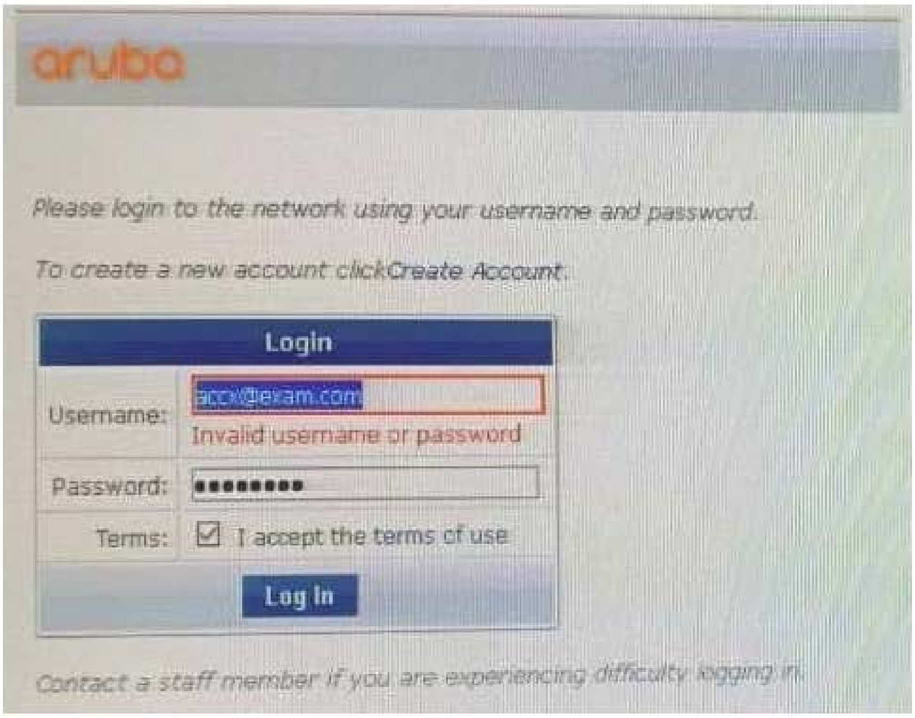
D. Allow time for IF-MAP service on the controller to discover the new devices as well.

E. Manually create a new device fingerprint for the devices that are not being profiled.

Correct Answer: DE

QUESTION 4

Refer to the exhibit:



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

Contact a staff member if you are experiencing difficulty logging in.

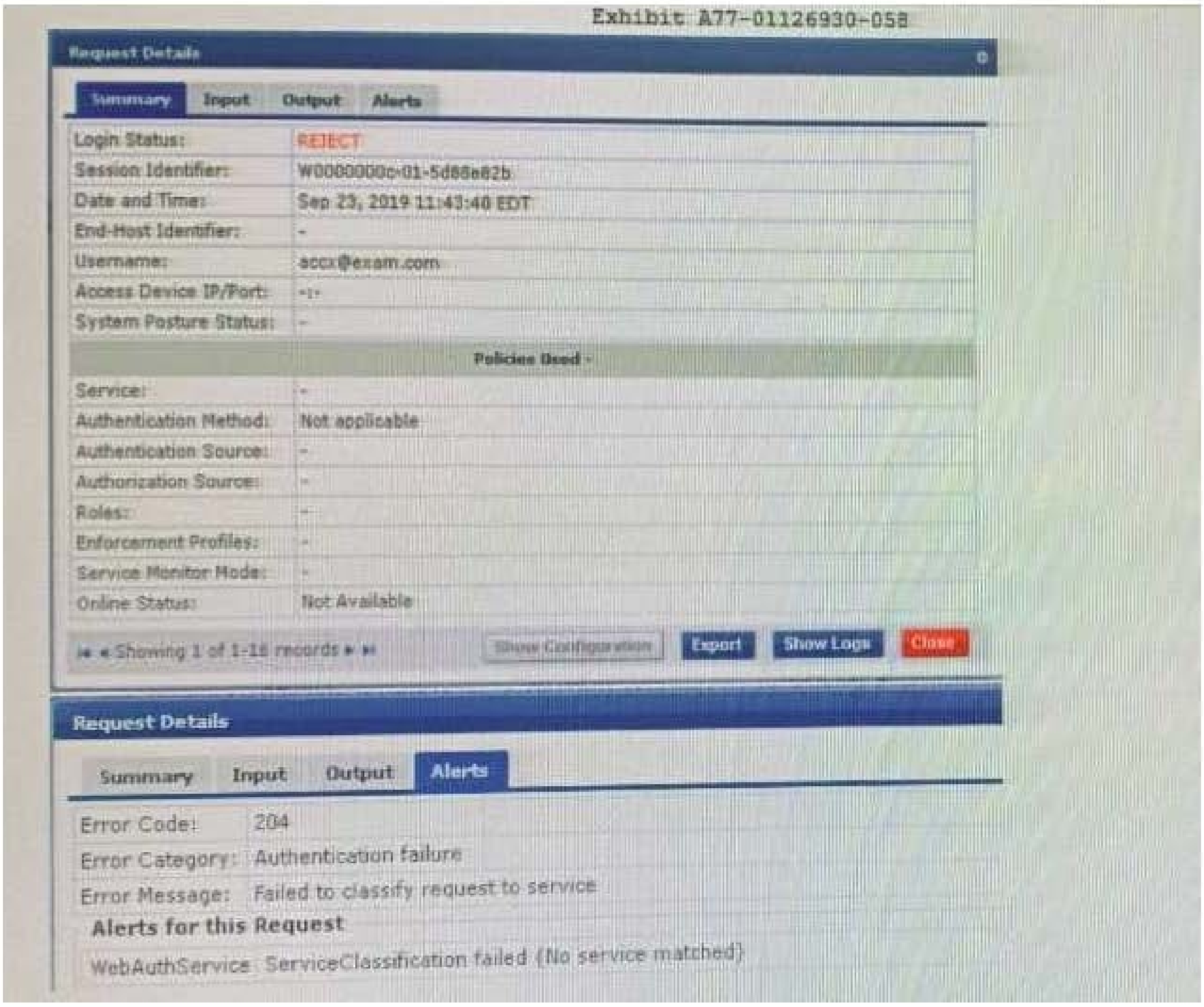


Exhibit A77-01126930-058

Request Details

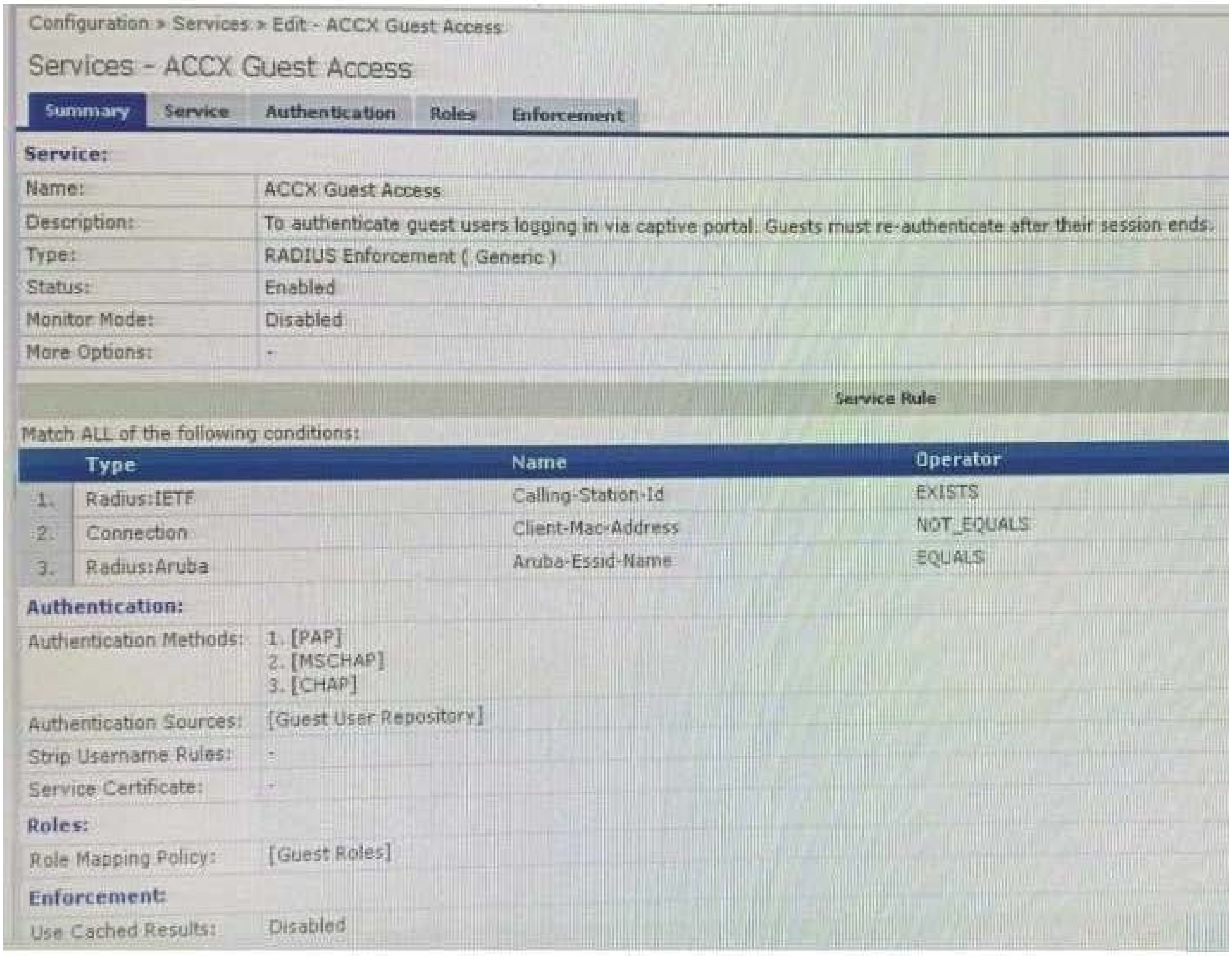
Login Status:	REJECT
Session Identifier:	W0000000c-01-5d88e82b
Date and Time:	Sep 23, 2019 11:43:40 EDT
End-Host Identifier:	-
Username:	accx@exam.com
Access Device IP/Port:	-:-
System Posture Status:	-
Policies Used -	
Service:	-
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	-
Enforcement Profiles:	-
Service Monitor Mode:	-
Online Status:	Not Available

Request Details

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)



Services - ACCX Guest Access

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:

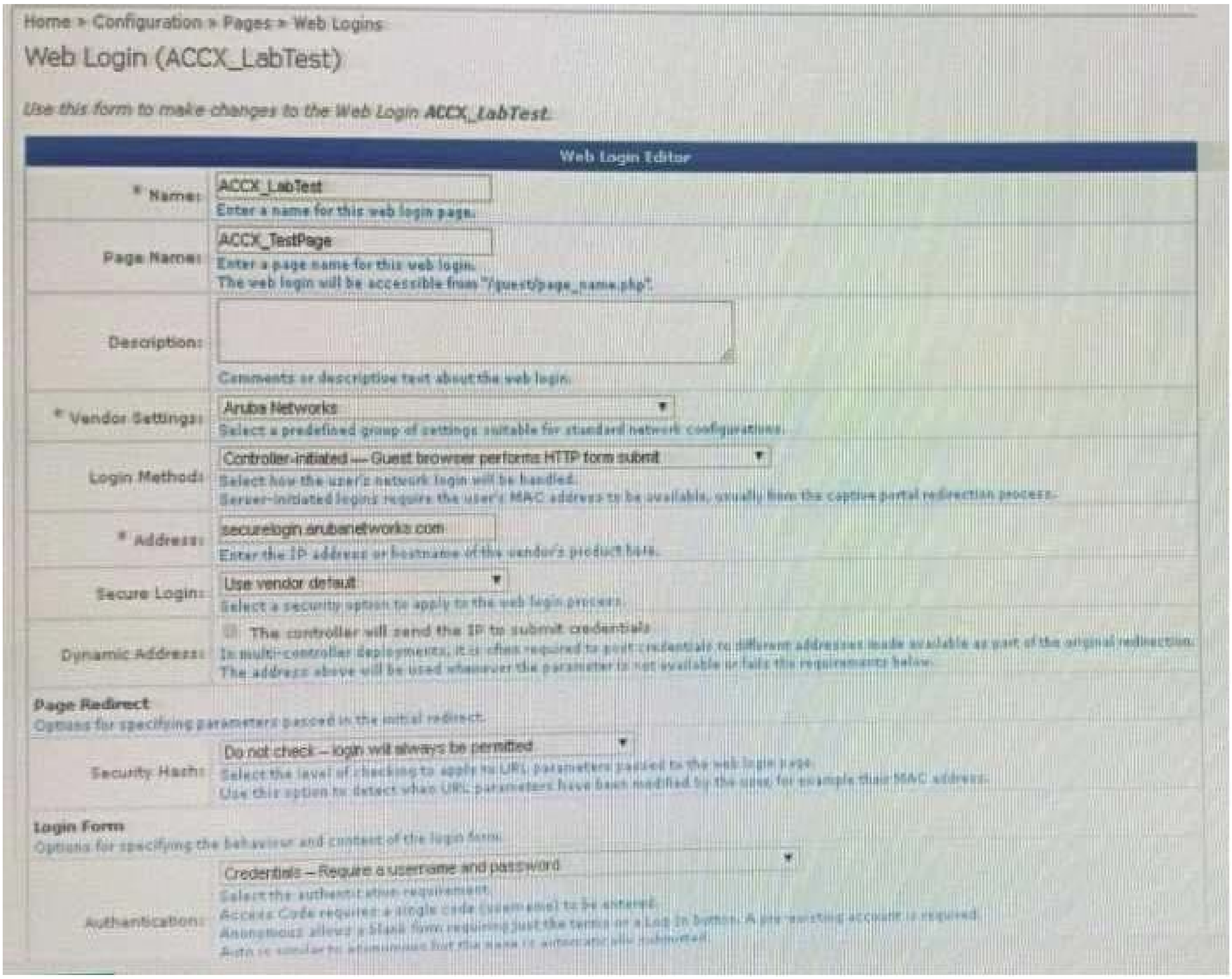
Authentication Methods:	1. [PAP] 2. [MSCHAP] 3. [CHAP]
Authentication Sources:	[Guest User Repository]
Strip Username Rules:	-
Service Certificate:	-

Roles:

Role Mapping Policy:	[Guest Roles]

Enforcement:

Use Cached Results:	Disabled

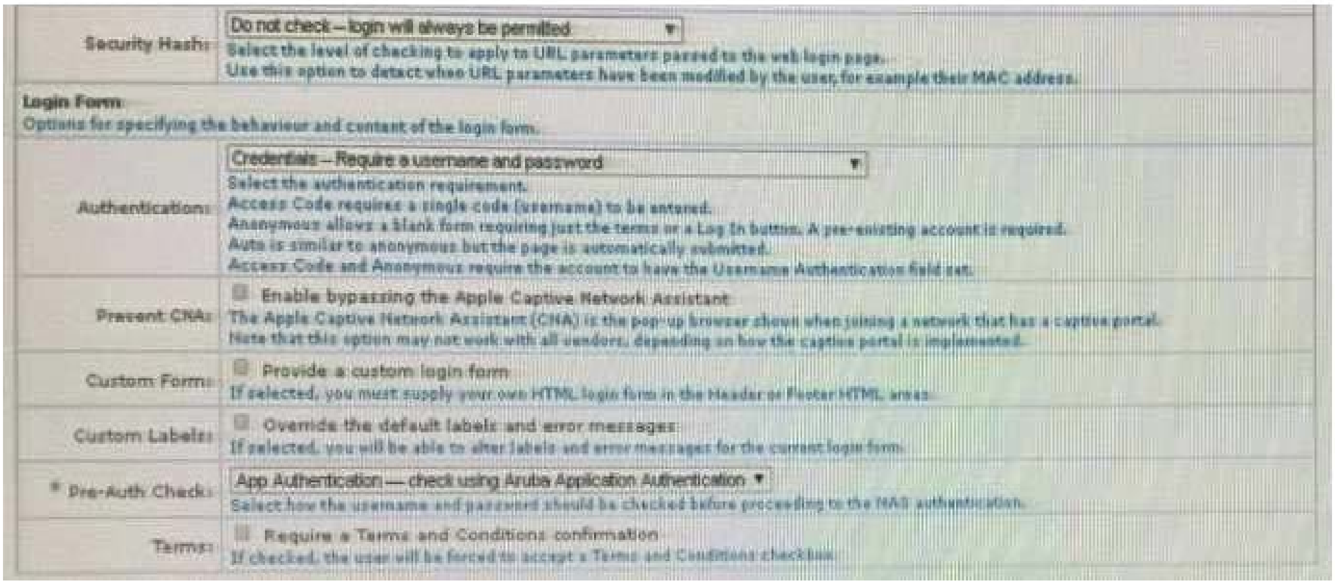


Home » Configuration » Pages » Web Logins

Web Login (ACCX_LabTest)

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

Web Login Editor	
* Name:	ACCX_LabTest 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 description 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:	Use vendor default ▾ 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.
Page Redirect Options for specifying parameters passed in the initial redirect.	
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 the 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.



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 the 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 require 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.

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

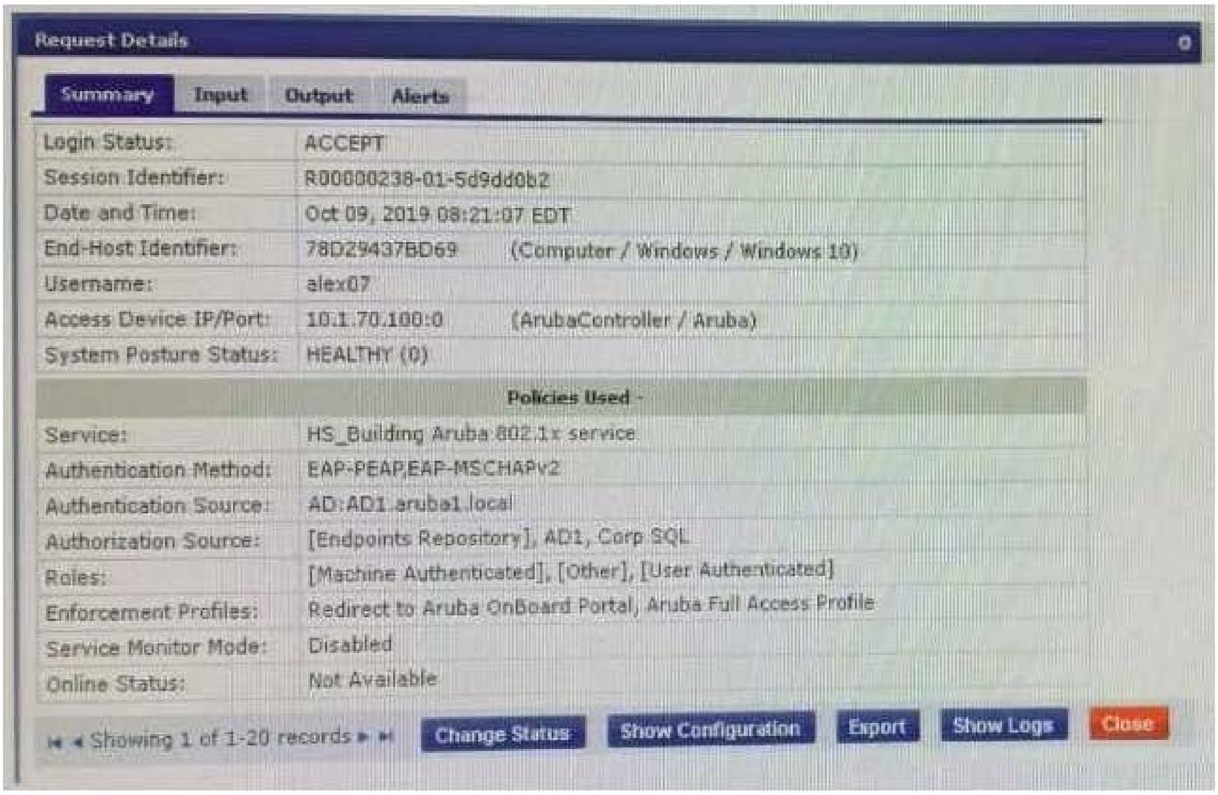
C. The Address filed under the WebLogin Vendor settings is not configured correctly, it should be set to instant arubanetworks.com

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

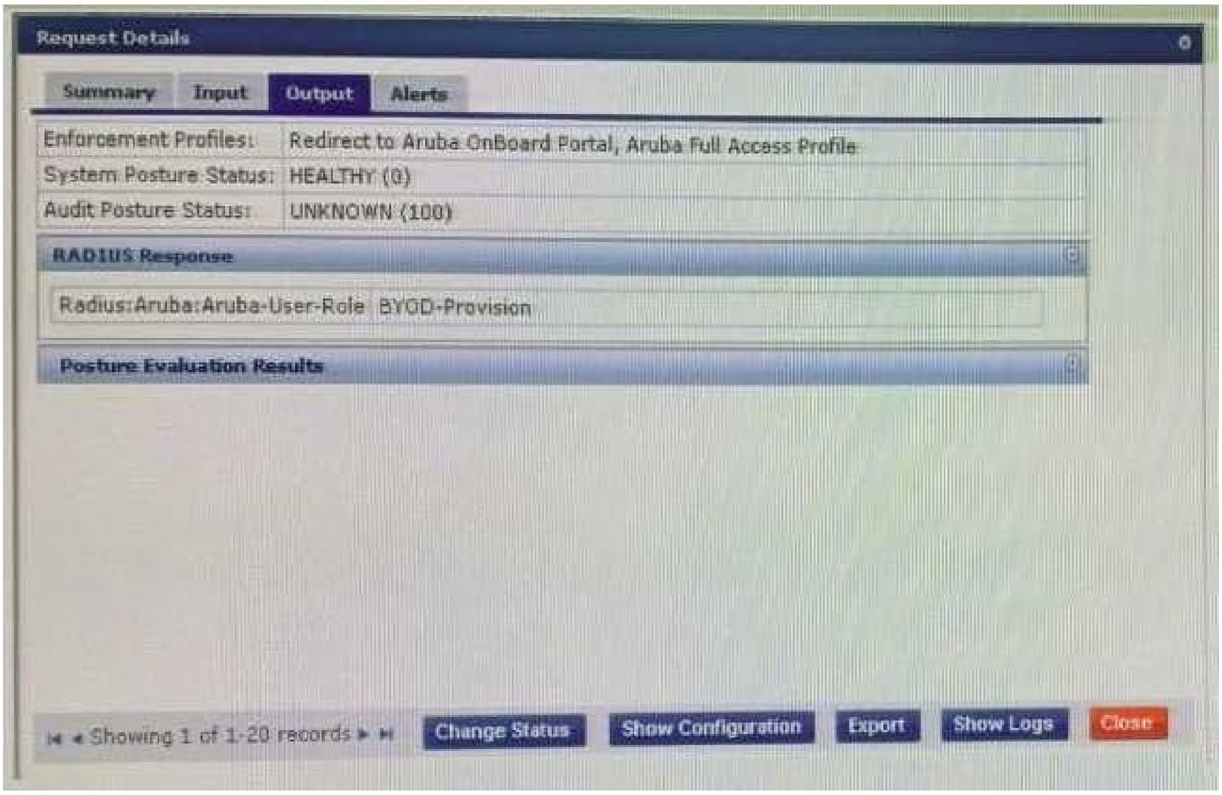
Correct Answer: A

QUESTION 5

Refer to the exhibit:



Login Status:	ACCEPT
Session Identifier:	R00000238-01-5d9dd0b2
Date and Time:	Oct 09, 2019 08:21:07 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows 10)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	HEALTHY (0)
Policies Used -	
Service:	HS_Building Aruba 802.1x service
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	[Endpoints Repository], AD1, Corp SQL
Roles:	[Machine Authenticated], [Other], [User Authenticated]
Enforcement Profiles:	Redirect to Aruba OnBoard Portal, Aruba Full Access Profile
Service Monitor Mode:	Disabled
Online Status:	Not Available

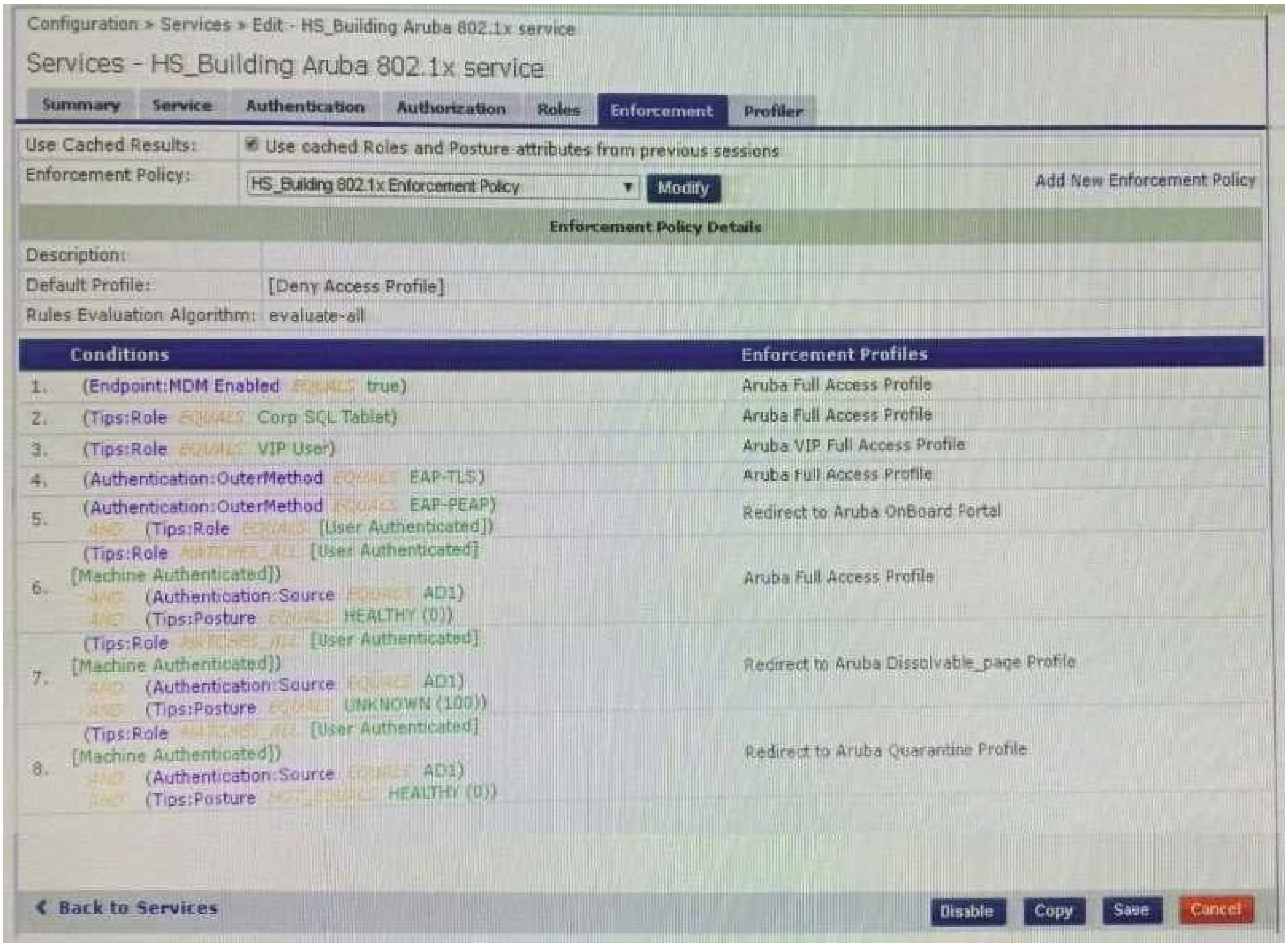


Enforcement Profiles:	Redirect to Aruba OnBoard Portal, Aruba Full Access Profile
System Posture Status:	HEALTHY (0)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role	BYOD-Provision

Posture Evaluation Results



Services - HS_Building Aruba 802.1x service

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

Enforcement Policy: HS_Building 802.1x Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: evaluate-all

	Conditions	Enforcement Profiles
1.	(Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
2.	(Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
3.	(Tips:Role EQUALS VIP User)	Aruba VIP Full Access Profile
4.	(Authentication:OuterMethod EQUALS EAP-TLS)	Aruba Full Access Profile
5.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS [User Authenticated])	Redirect to Aruba OnBoard Portal
6.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0))	Aruba Full Access Profile
7.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100))	Redirect to Aruba Dissolvable_page Profile
8.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	Redirect to Aruba Quarantine Profile

The customer configured an 802.1x service with different enforcement actions for personal and corporate laptops. The corporate laptops are always being redirected to the BYOD Portal. The customer has sent you the above screenshots.

How would you resolve the issue? (Select two)

A. Modify the enforcement policy and change the rule evaluation algorithm to select first match

B. Modify the enforcement policy and re-order the condition with posture not_equals to healthy as the sixth condition

C. Modify the enforcement policy and re-order the EAP-PEAP with [user authenticated] rule to the last condition.

D. Modify the enforcement policy and re-order the condition with Posture - Unknown as the fifth condition

E. Remove the EAP-PEAP with [user authenticated] condition for Onboard and create another service

Correct Answer: CD

HPE6-A77 VCE Dumps HPE6-A77 Study Guide HPE6-A77 Exam Questions