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

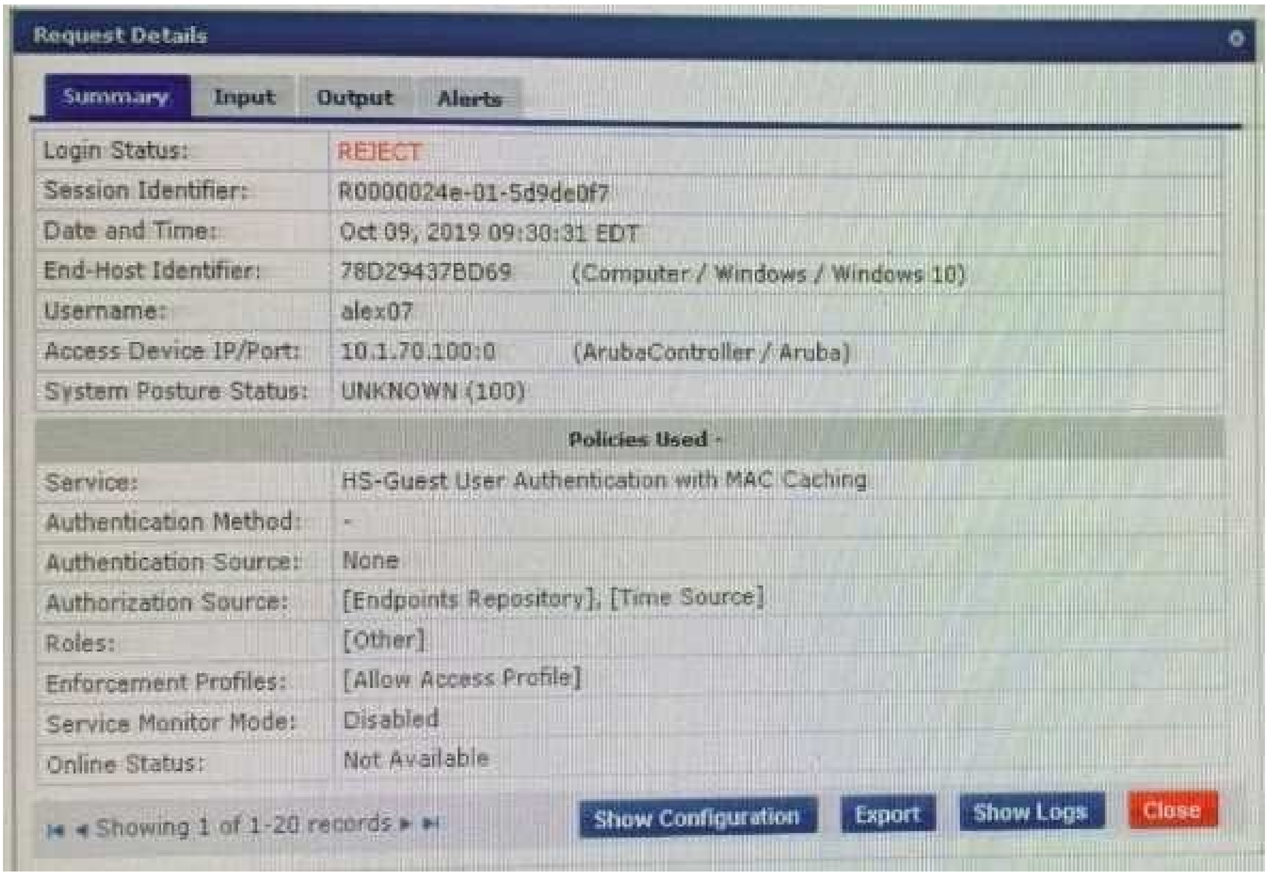
Aruba Certified ClearPass Expert Written

Pass HP HPE6-A77 Exam with 100% Guarantee

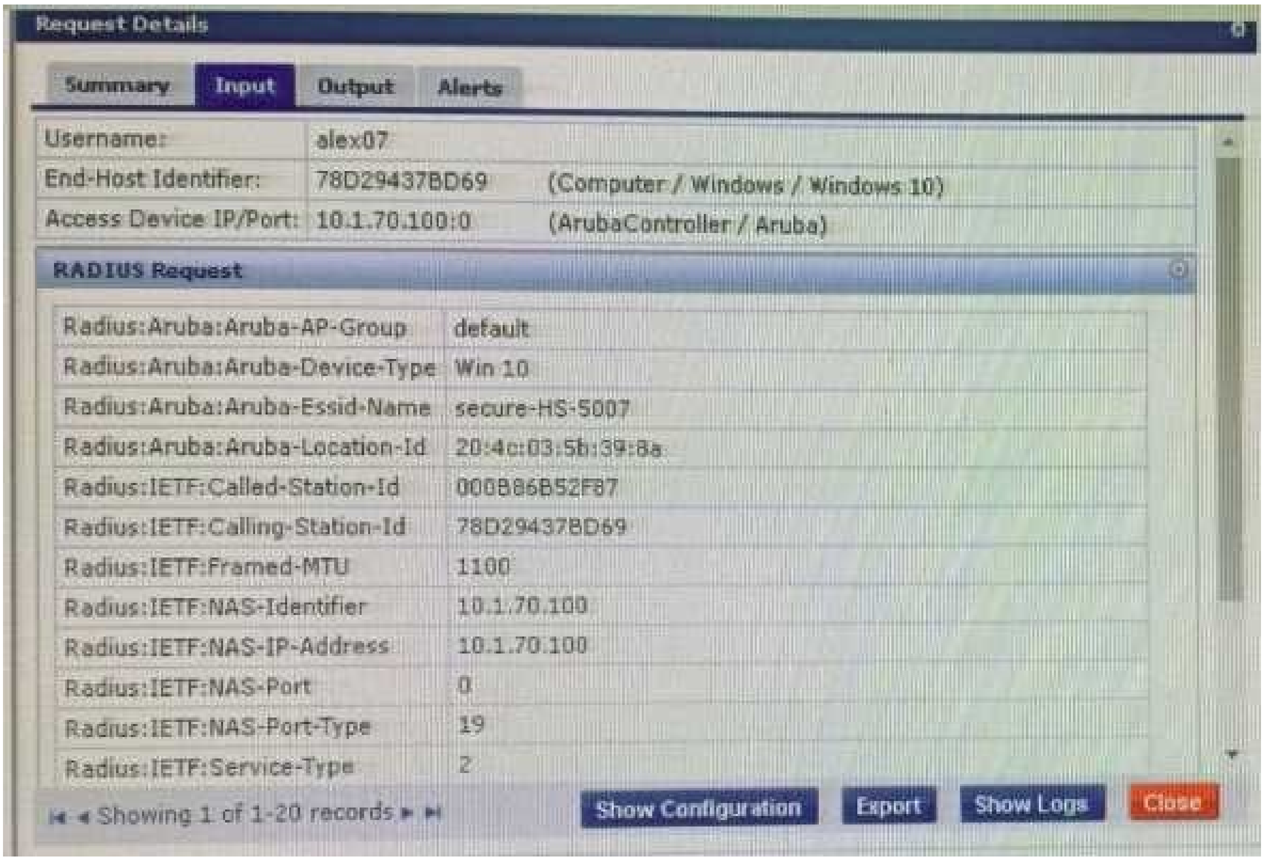
Following Questions and Answers are all new published by HP Official Exam Center

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

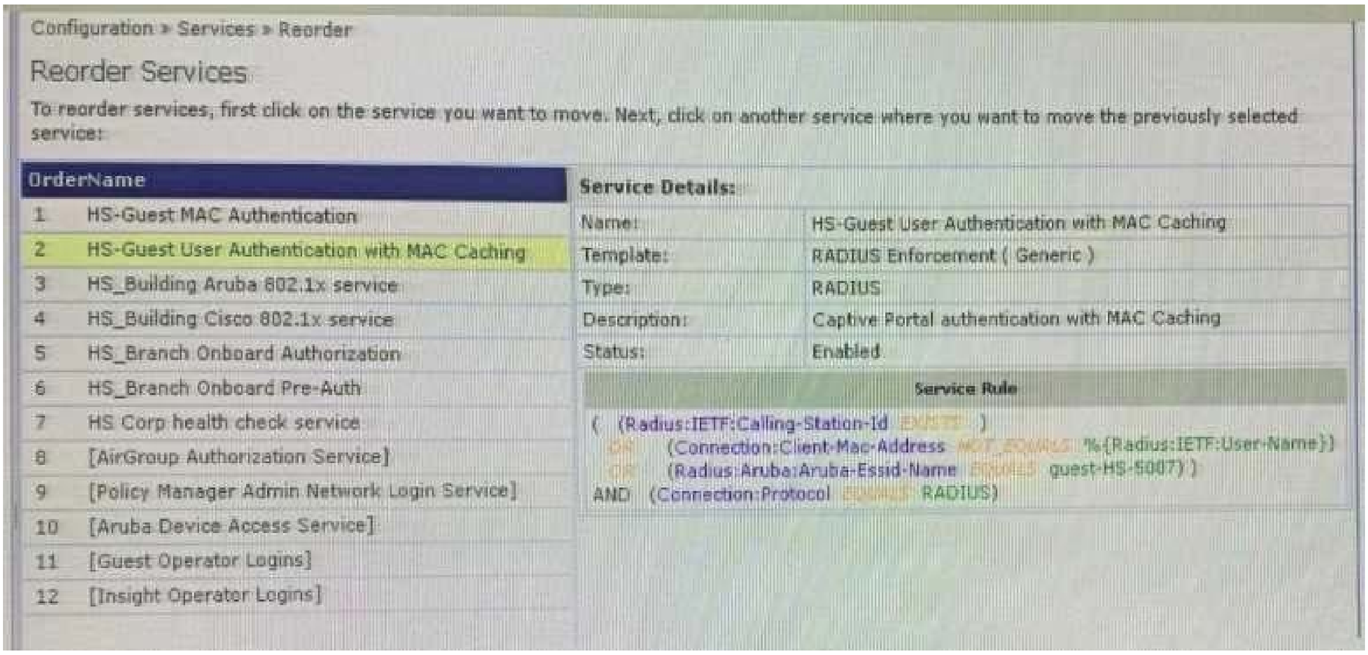


Request Details

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



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.

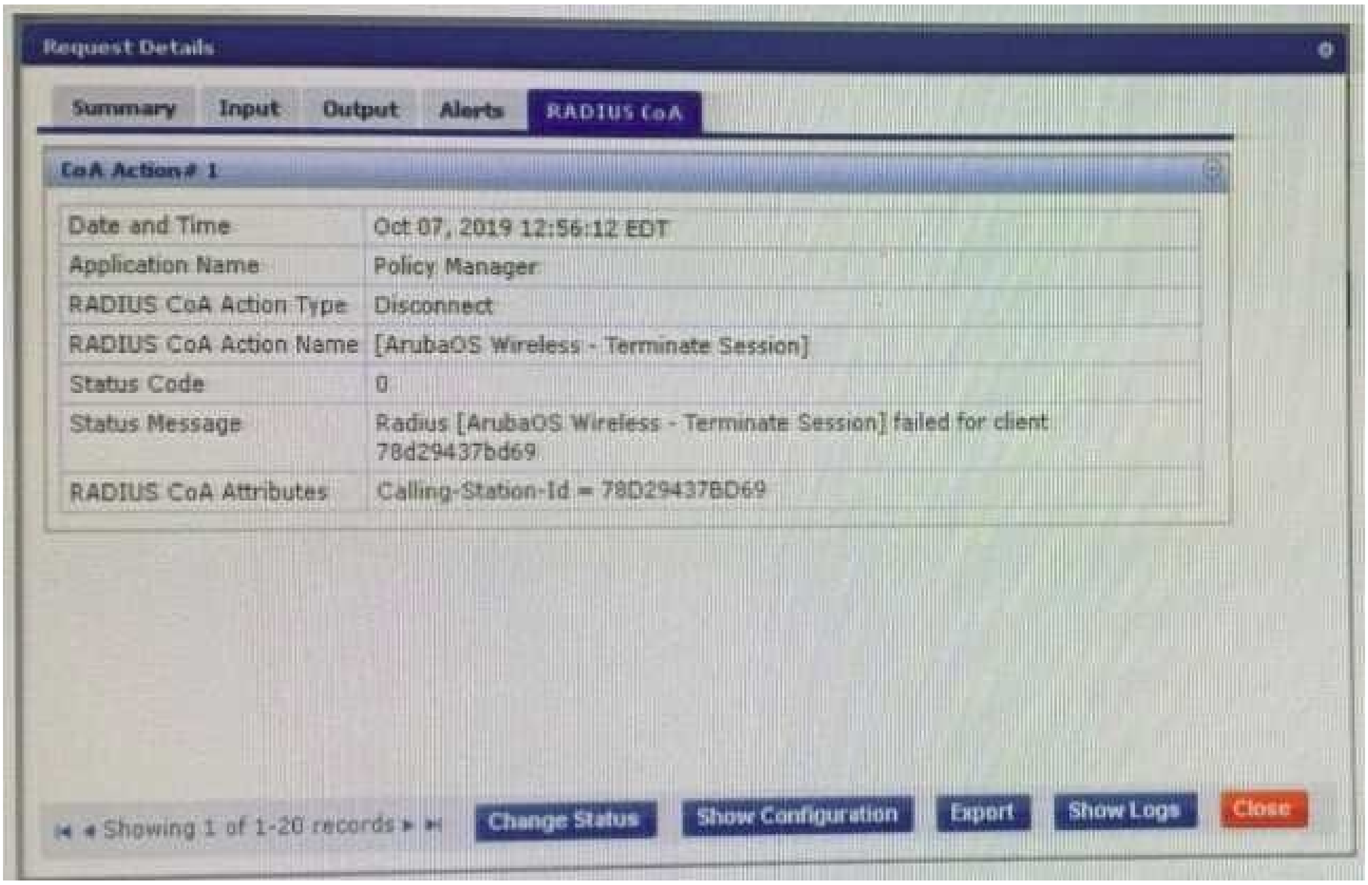
C. Disable HS-Guest User Authentication service and move HS-Guest MAC Authentication to seventh position.

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

Correct Answer: A

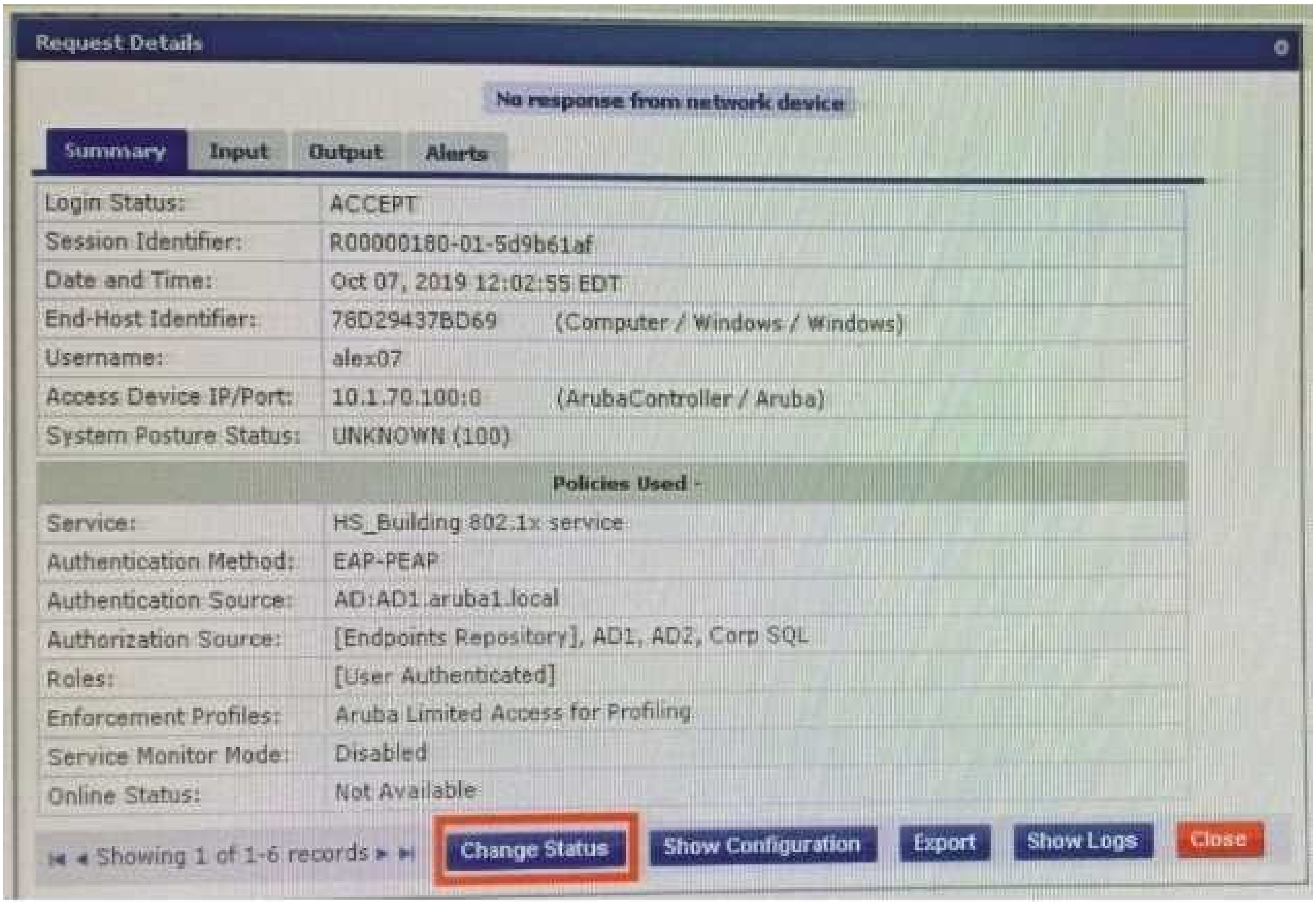
QUESTION 2

Refer to the exhibit: You configuring an 802 1x service endpoint profiling. When the client connects to the network, ClearPass successfully profiles the client and sends Radius Change of Authorization (RCoA) but Radius Change of Authorization {RCoA) fails for the client You manually clicked on the Change Status button in the access tracker to force an RCoA but that failed too. What must you check to ensure that the RCoA will work? (Select two.)



CoA Action# 1

Date and Time	Oct 07, 2019 12:56:12 EDT
Application Name	Policy Manager
RADIUS CoA Action Type	Disconnect
RADIUS CoA Action Name	[ArubaOS Wireless - Terminate Session]
Status Code	0
Status Message	Radius [ArubaOS Wireless - Terminate Session] failed for client 78d29437bd69
RADIUS CoA Attributes	Calling-Station-Id = 78D29437BD69



Login Status:	ACCEPT
Session Identifier:	R00000180-01-5d9b61af
Date and Time:	Oct 07, 2019 12:02:55 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	HS_Building 802.1x service
Authentication Method:	EAP-PEAP
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	[Endpoints Repository], AD1, AD2, Corp SQL
Roles:	[User Authenticated]
Enforcement Profiles:	Aruba Limited Access for Profiling
Service Monitor Mode:	Disabled
Online Status:	Not Available

A. RFC 3576 option is enabled for Aruba Controller under Network device in ClearPass.

B. RFC 3576 server should be mapped in the server group on the Aruba Controller

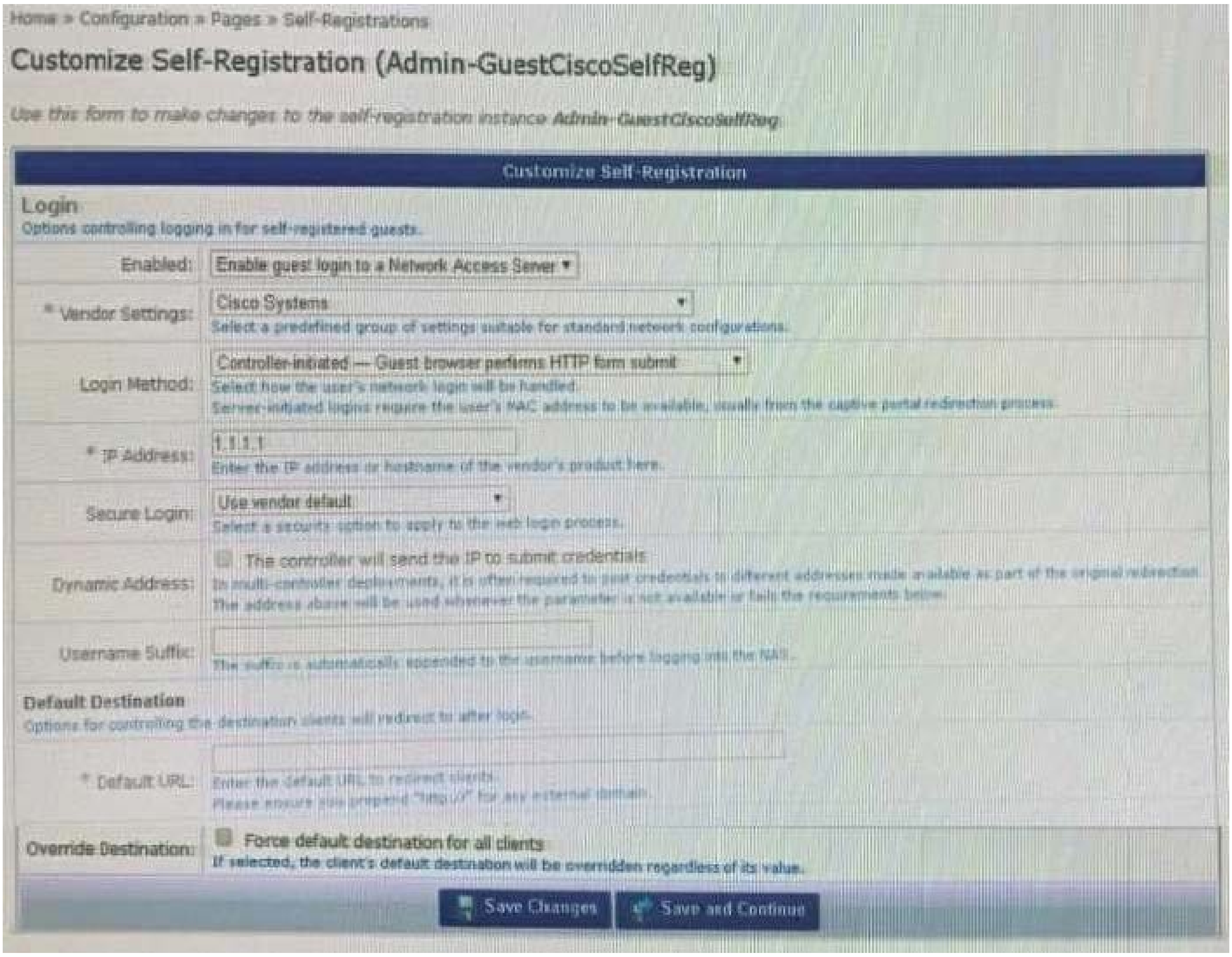
C. The RFC 3576 shared secret on ClearPass should match the Authentication Server shared secret

D. RFC 3576 server IPs and the Authentication server IPs should be same in the AAA profile

Correct Answer: AC

QUESTION 3

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?



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: 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.

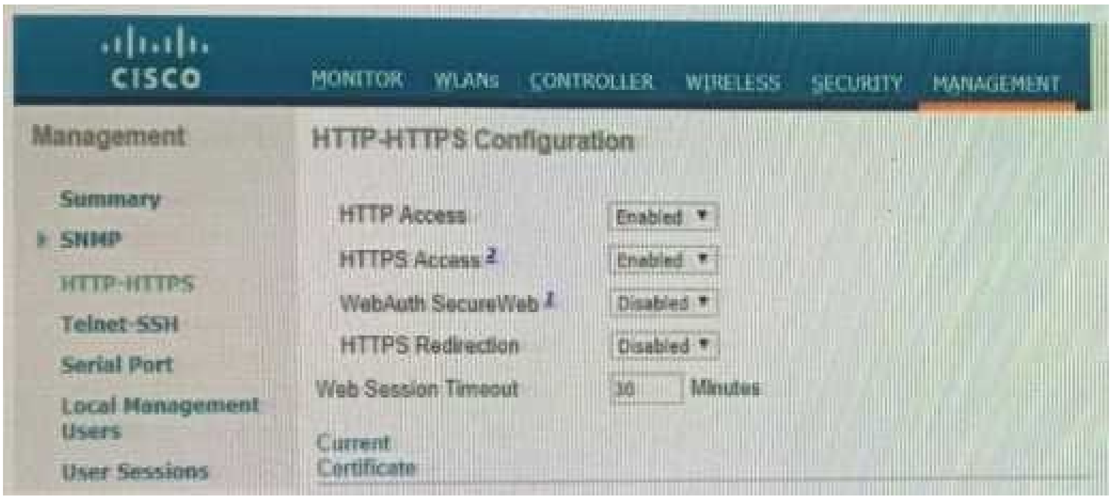
Dynamic Address: □ The controller will send the IP to submit credentials
In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection.
The address above will be used whenever the parameter is not available or fails the requirements below.

Username Suffix:
The suffix is automatically appended to the username before logging into the NAS.

Default Destination
Options for controlling the 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.



HTTP-HTTPS Configuration

HTTP Access: Enabled ▾
HTTPS Access 2: Enabled ▾
WebAuth SecureWeb 1: Disabled ▾
HTTPS Redirection: Disabled ▾
Web Session Timeout: 30 Minutes

Current Certificate

A. Secure Login should use HTTP

B. Change the Vendor Settings to Airespace Networks

C. Change \he IP Address to the Cisco Controller DNS name

D. Login Method should be Controller-initiated - using HTTPs form submit

Correct Answer: C

QUESTION 4

You have configured a Guest SSID with Captive-portal Web Authentication and MAC authentication The MAC caching expiry time set to 12 hours and the Guest Account expiration time is set to 8 hours. What will happen if the guest were to disconnect from the SSID and re-connect 9 hours later?

A. The client will tail the MAC authentication and be denied access to the Guest SSID.

B. The client will successfully pass the mac authentication until the mac caching time expires.

C. The client will successfully pass the MAC authentication but still be redirected to captive portal page.

D. The client will fail the MAC authentication and will be redirected to the Captive-portal login page.

Correct Answer: C

QUESTION 5

What is the Secure SSID {otherwise referred to as Single SSID) OnBoard deployment service workflow?

A. OnBoard Provisioning RADIUS service, OnBoard Authorization RADIUS service. OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

B. OnBoard Provisioning RADIUS service, OnBoard Pre-Auth RADIUS service, OnBoard Authorization Application service. OnBoard Provisioning RADIUS service

C. OnBoard Provisioning RADIUS service, OnBoard Pre-Auth Application service. OnBoard Authorization Application service, OnBoard Provisioning RADIUS service

D. OnBoard Provisioning RADIUS service, OnBoard Authorization Application service, OnBoard Pre- Auth Application service, OnBoard Provisioning RADIUS service

Correct Answer: A

HPE6-A77 Practice Test HPE6-A77 Study Guide HPE6-A77 Braindumps