HPE6-A81 Q&As

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

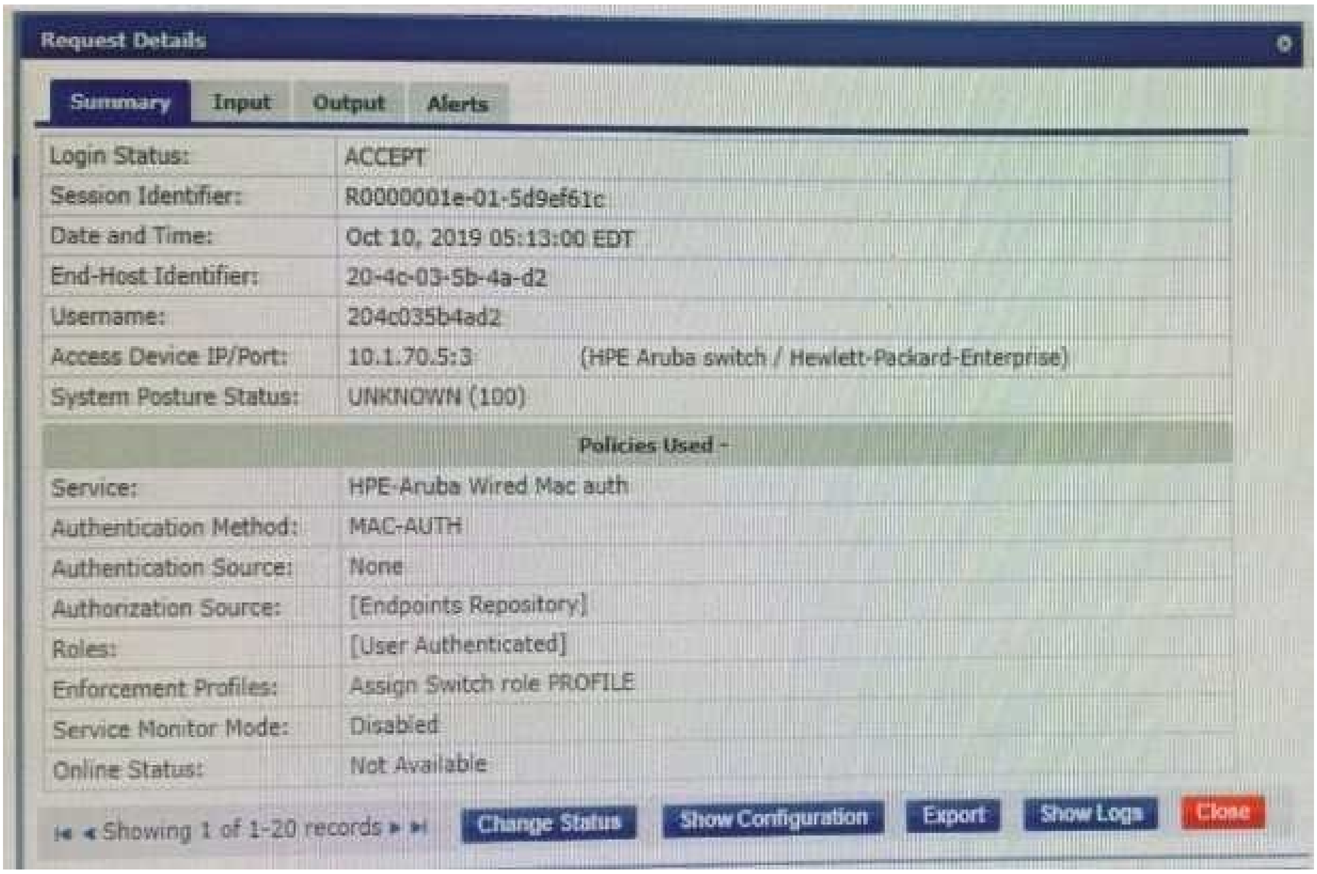
https://www.geekcert.com/hpe6-a81.html

100% Passing Guarantee
100% Money Back Assurance

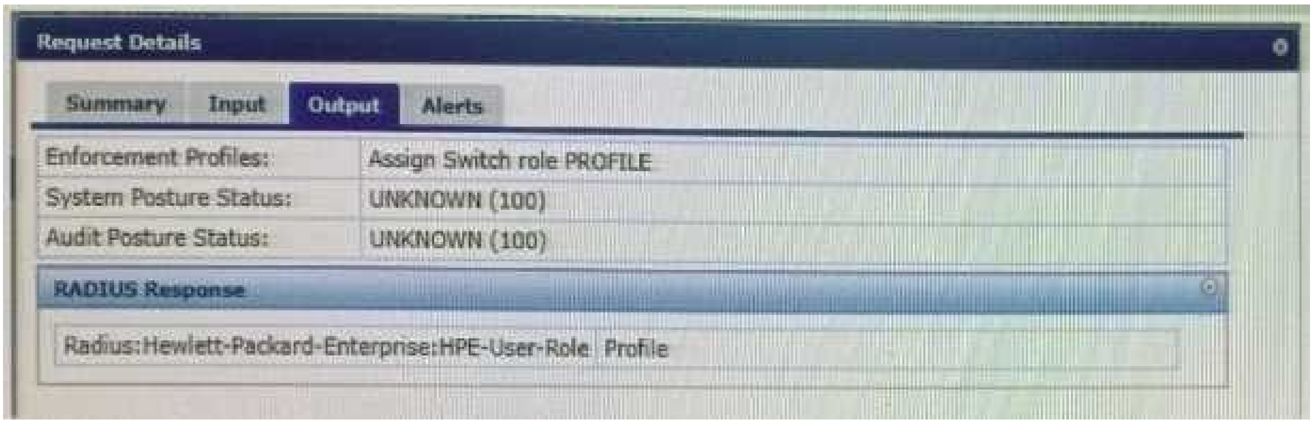
Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

Refer to the exhibit:



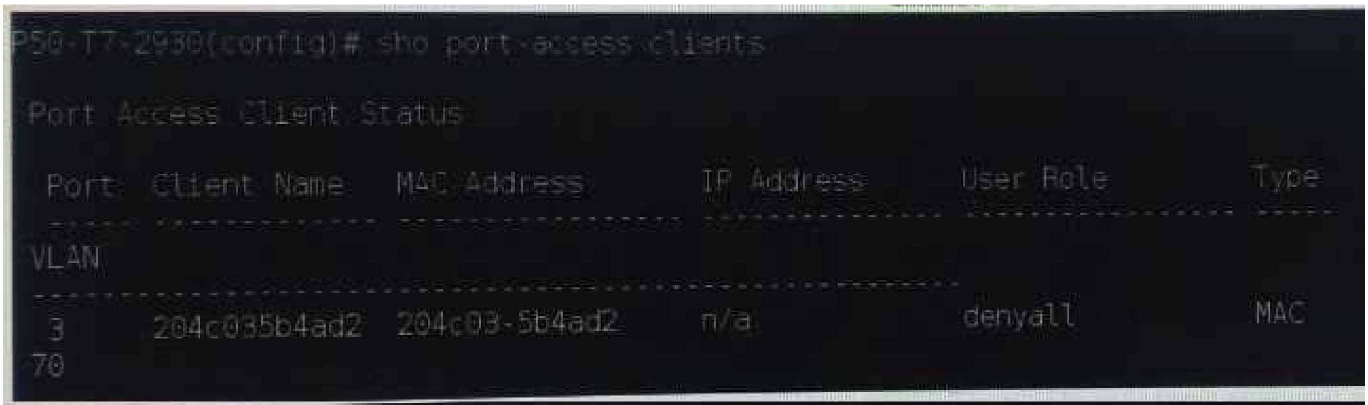
Login Status:	ACCEPT
Session Identifier:	R0000001e-01-5d9ef61c
Date and Time:	Oct 10, 2019 05:13:00 EDT
End-Host Identifier:	20-4c-03-5b-4a-d2
Username:	204c035b4ad2
Access Device IP/Port:	10.1.70.5:3 (HPE Aruba switch / Hewlett-Packard-Enterprise)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	HPE-Aruba Wired Mac auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Endpoints Repository]
Roles:	[User Authenticated]
Enforcement Profiles:	Assign Switch role PROFILE
Service Monitor Mode:	Disabled
Online Status:	Not Available



Enforcement Profiles:	Assign Switch role PROFILE
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

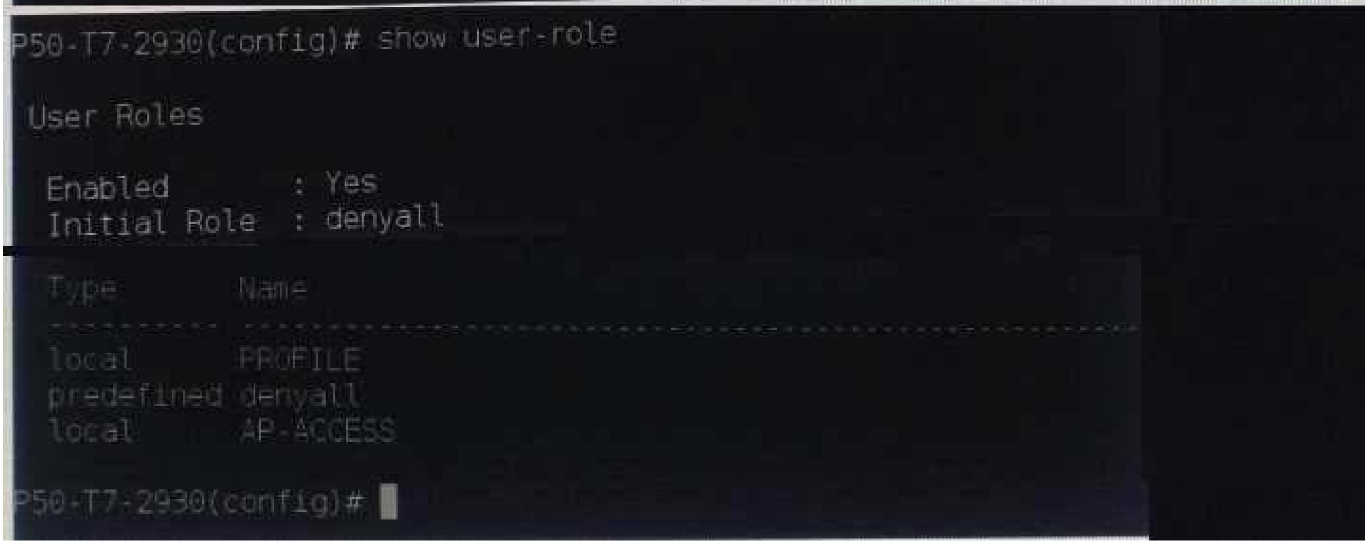
Radius:Hewlett-Packard-Enterprise:HPE-User-Role	Profile



```
P50-T7-2930(config)# sho port-access clients

 Port Access Client Status

  Port  Client Name    MAC Address      IP Address       User Role          Type
  ----- -------------- ---------------- ---------------- ------------------ -----
 VLAN
 ----------------------------------------------------------------------
  3     204c035b4ad2   204c03-5b4ad2    n/a              denyall            MAC
 70
```



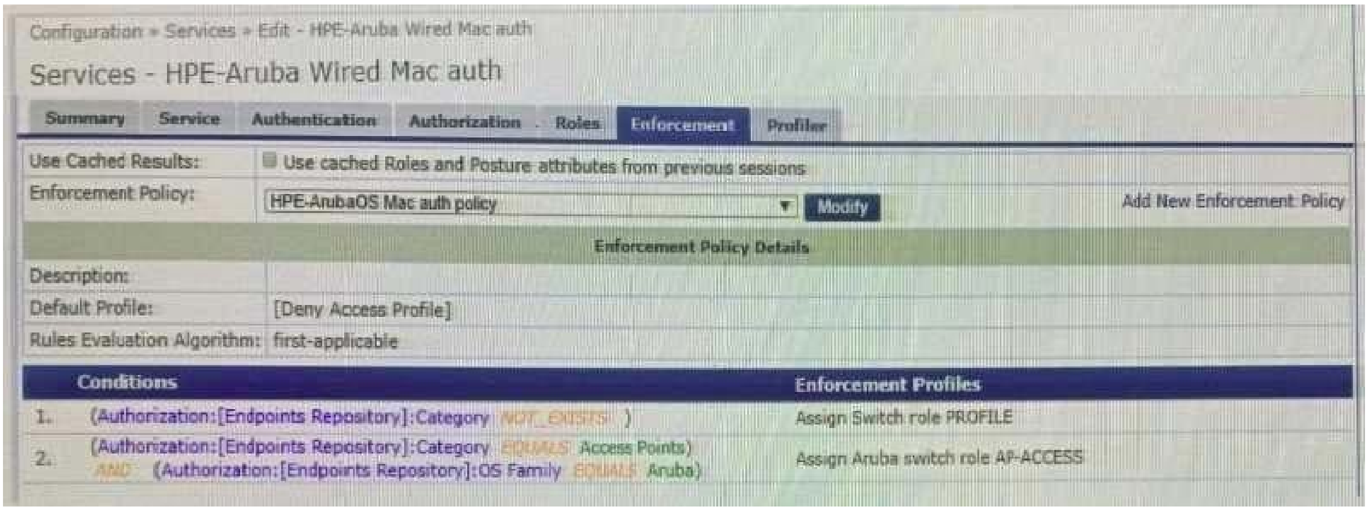
```
P50-T7-2930(config)# show user-role

 User Roles

  Enabled        : Yes
  Initial Role   : denyall

  Type       Name
  ---------- ----------------------------------------------------------
  local      PROFILE
  predefined denyall
  local      AP-ACCESS

P50-T7-2930(config)#
```



Configuration » Services » Edit - HPE-Aruba Wired Mac auth

Services - HPE-Aruba Wired Mac auth

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

Enforcement Policy: HPE-ArubaOS Mac auth policy ▾ Modify Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Category NOT_EXISTS)	Assign Switch role PROFILE
2.	(Authorization:[Endpoints Repository]:Category EQUALS Access Points) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Aruba)	Assign Aruba switch role AP-ACCESS

You have been asked to help a Customer troubleshoot an issue. They have configured an Aruba OS switch (Aruba 2930 with 16.09) to do MAC authentication with profiling using ClearPass as the authentication source. They cannot get it working.

Using the screenshots as a reference, how will you fix the issue?

A. Delete the initial role in the Aruba OS switch to force the device to get the server derived user roles

B. Use a CoA to bounce the switch port to force the port to change to the correct Aruba user role

C. Change the Vendor settings for the Aruba OS switch to "Aruba" so that the enforcement will use the correct VSAs

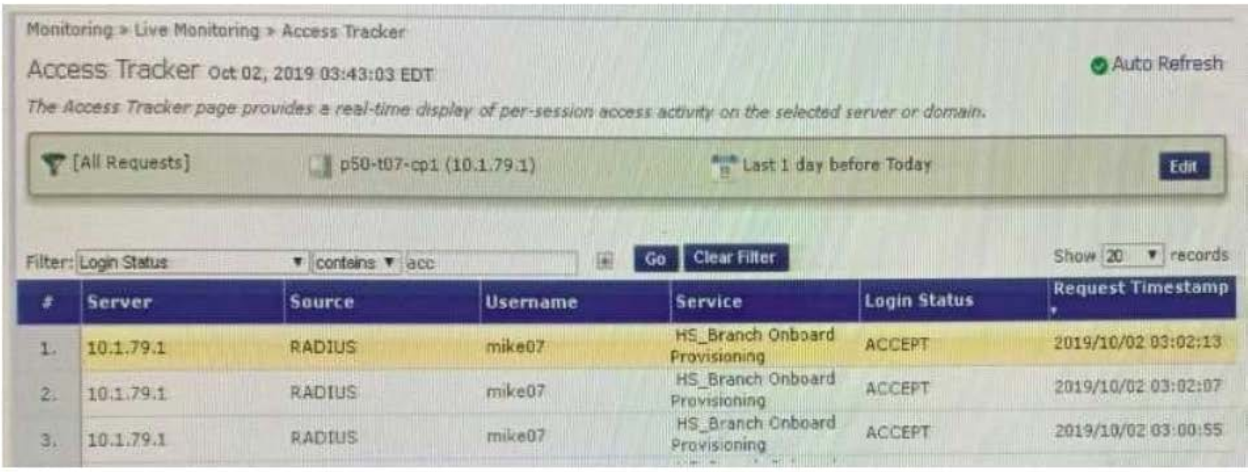
D. Modify the enforcement profile conditions with Aruba Vendor specific attributes and Aruba-user- roles

E. User-roles are case sensitive, update the correct role with correct case in the enforcement profile

Correct Answer: D

QUESTION 2

Refer to the exhibit:



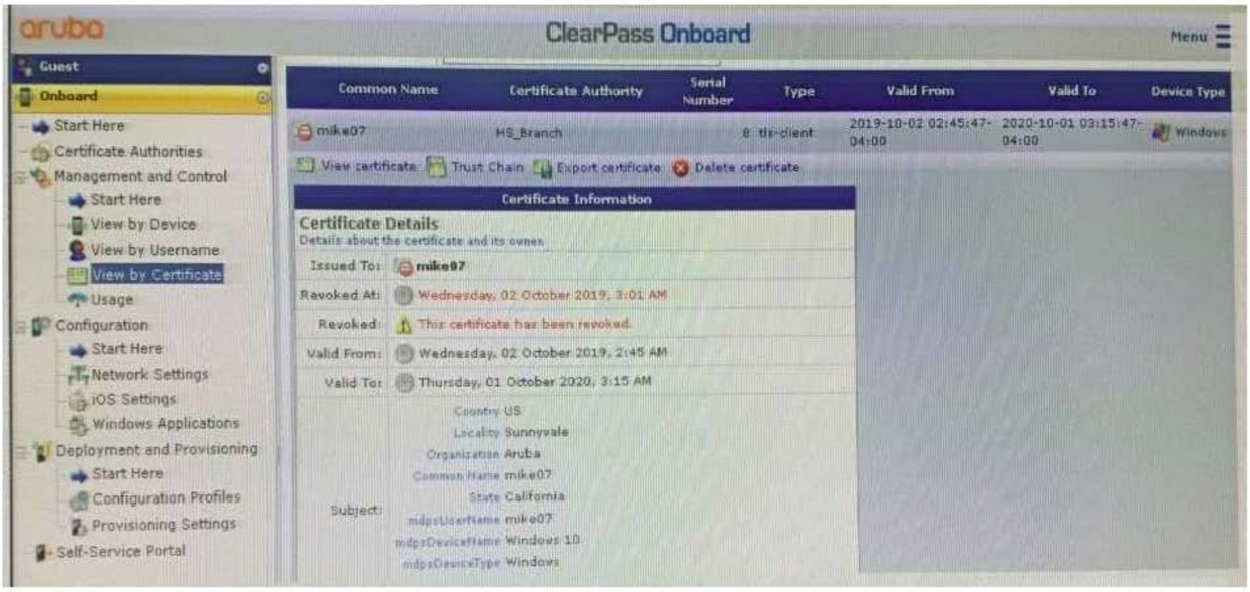
Access Tracker Oct 02, 2019 03:43:03 EDT

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

Filter: Login Status ▾ contains ▾ acc

Show 20 ▾ records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:02:13
2.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:02:07
3.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:00:55



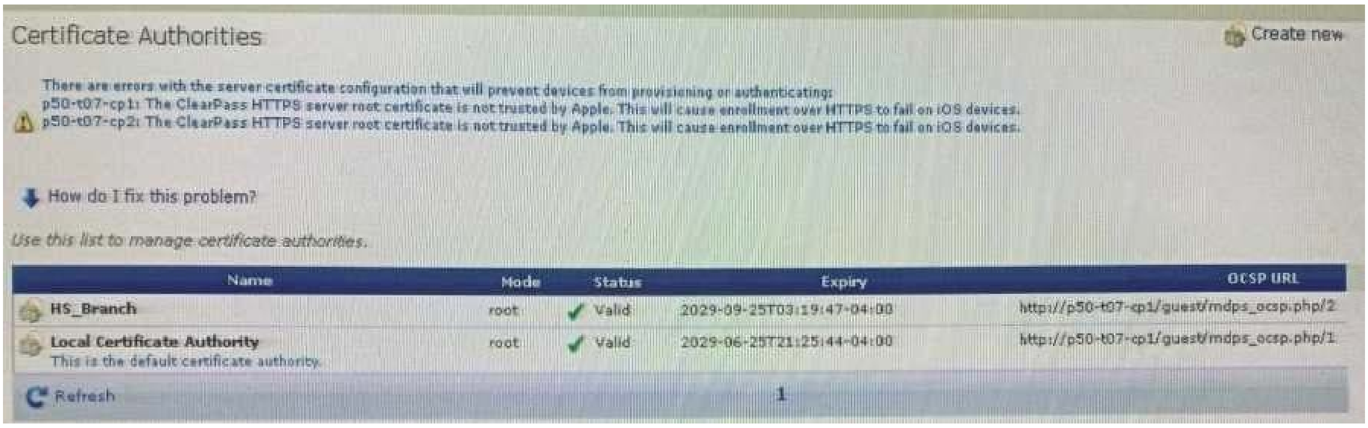
Common Name	Certificate Authority	Serial Number	Type	Valid From	Valid To	Device Type
mike07	HS_Branch	8	tls-client	2019-10-02 02:45:47-04:00	2020-10-01 03:15:47-04:00	Windows

Certificate Information

Certificate Details

Details about the certificate and its owner.

Issued To:	mike07
Revoked At:	Wednesday, 02 October 2019, 3:01 AM
Revoked:	This certificate has been revoked.
Valid From:	Wednesday, 02 October 2019, 2:45 AM
Valid To:	Thursday, 01 October 2020, 3:15 AM
Subject:	Country US Locality Sunnyvale Organization Aruba Common Name mike07 State California mdpsUserName mike07 mdpsDeviceName Windows 10 mdpsDeviceType Windows



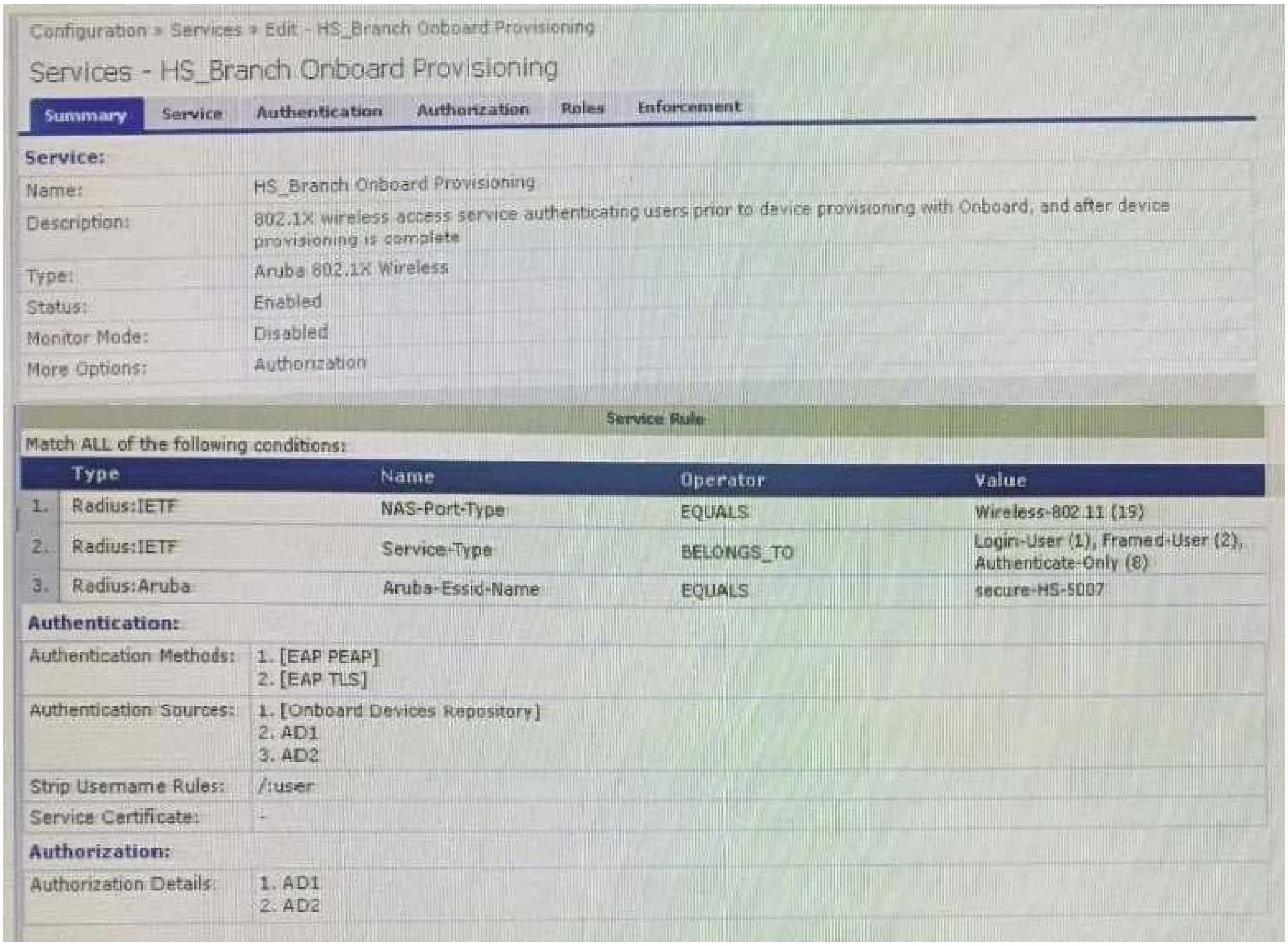
Certificate Authorities

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
p50-t07-cp1: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
p50-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.

How do I fix this problem?

Use this list to manage certificate authorities.

Name	Mode	Status	Expiry	OCSP URL
HS_Branch	root	✓ Valid	2029-09-25T03:19:47-04:00	http://p50-t07-cp1/guest/mdps_ocsp.php/2
Local Certificate Authority This is the default certificate authority.	root	✓ Valid	2029-06-25T21:25:44-04:00	http://p50-t07-cp1/guest/mdps_ocsp.php/1



Configuration » Services » Edit - HS_Branch Onboard Provisioning

Services - HS_Branch Onboard Provisioning

Service:

Name:	HS_Branch Onboard Provisioning
Description:	802.1X wireless access service authenticating users prior to device provisioning with Onboard, and after device provisioning is complete
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Authorization

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:Aruba	Aruba-Essid-Name	EQUALS	secure-HS-5007

Authentication:

Authentication Methods:	1. [EAP PEAP] 2. [EAP TLS]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2
Strip Username Rules:	/:user
Service Certificate:	-

Authorization:

Authorization Details:	1. AD1 2. AD2

After the helpdesk revoked the certificate of a device reported to be lost oy an employee, the lost device

was seen as connected successfully to the secure network. Further testing has shown that device

revocation is not working.

What steps should you follow to make device revocations work?

A. Copy the default [EAP-TLS with OSCP Enabled] authentication method and set The Verify certificate using OSCP option as required then update the correct OSCP URL link of the OnBoard CA. Remove EAP-TLS and map the custom created method to the OnBoard Authorization Service.

B. copy the default [EAP-TLS with OSCP Enabled] authentication method and set the verify certificate using OSCP: option as "required" then configure the correct OSCF URL link for the OnBoard CA. Remove EAP-TLS and map the new [EAP-TLS with OSCP Enabled] method to the 802 1X Radius Service.

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

D. Edit the default [EAP-TLS with OSCP Enabled] authentication method and set the Verify certificate using OSCP option as required then update the correct OSCP URL link of the OnBoard CA Remove EAP-TLS and map the new [EAP-TLS with OSCP Enabled] method to the OnBoard Provisioning Service.

Correct Answer: C

QUESTION 3

A customer has created a Guest Sett-Registration page that they would like to use it as `template\\' for all the new pages that are going to be created from now on. Their goal is to ensure that the header and footer on every page are the same, and any edits made to them are automatically reflected on every Self-Registration Page. What should be configured in order to accomplish this request?

A. Save the "template" page as Master Self-Registration page

B. Create child pages when creating new Self-Registration pages and select the "template" as Parent

C. Save this "template" page as a new Skin to be used on other Self-Registration pages

D. Copy the "template" page and edit it each time a new Self-Registration Page is needed

Correct Answer: C

QUESTION 4

What type of EAP certificate are you able to use on ClearPass? (Select two.)

A. Self signed, when all the clients are Onboarded with the same Root CA as the Self signed certificate.

B. Private signed, when the clients are onboarded or are part of the organization domain.

C. Private signed, when some clients are onboarded and some are not part of the organization.

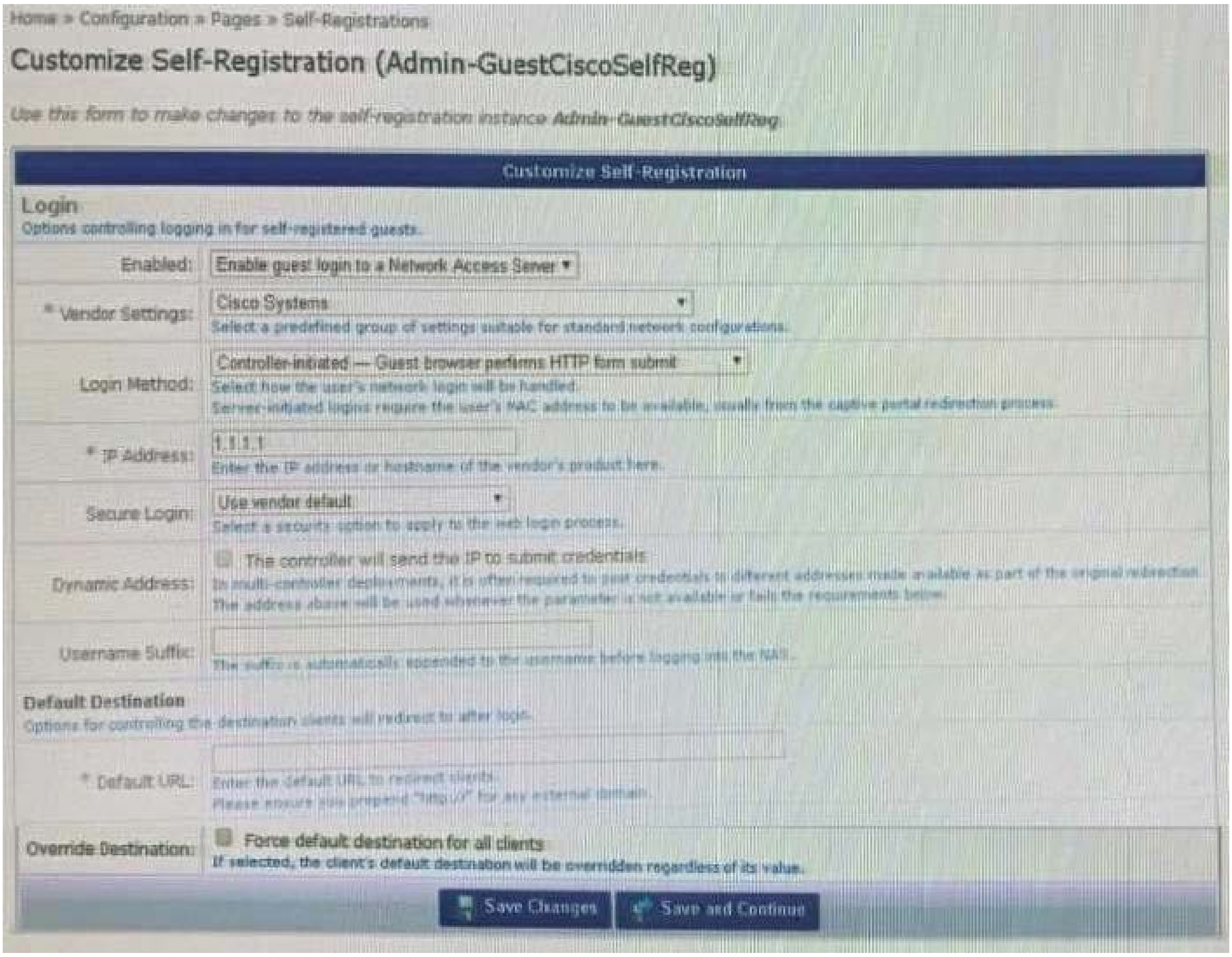
D. Public signed, when not all of the clients are part of the organization domain.

E. Self signed, when all the clients are part of the organization domain.

Correct Answer: CD

QUESTION 5

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?



Home » Configuration » Pages » Self-Registrations

Customize Self-Registration (Admin-GuestCiscoSelfReg)

*Use this form to make changes to the self-registration instance **Admin-GuestCiscoSelfReg***

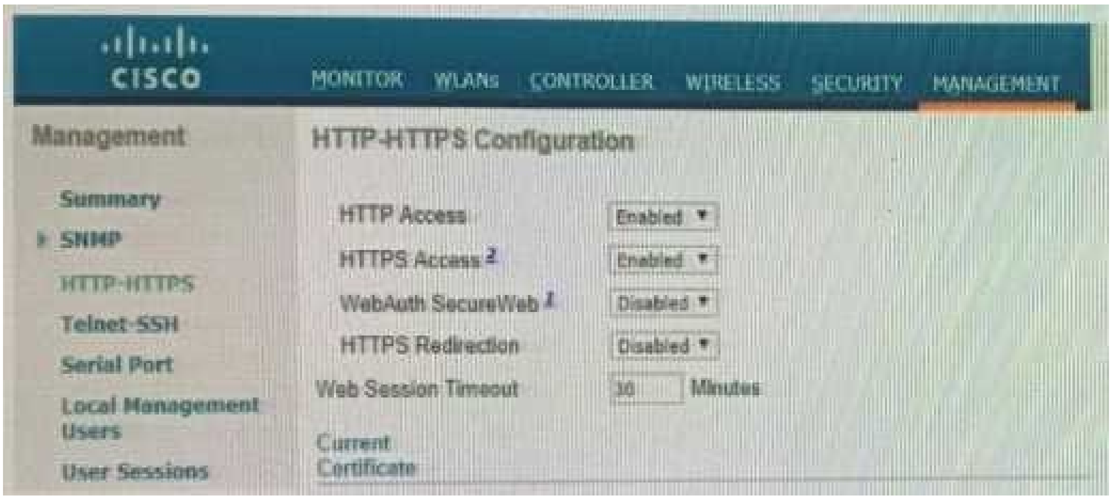
Customize Self-Registration

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 2	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

Latest HPE6-A81 Dumps   HPE6-A81 Exam Questions   HPE6-A81 Braindumps