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

A customer would like to allow only the AD users with the "Manager" title from the "HQ" location to

Onboard their personal devices. Any other AD users should not be authorized to pass beyond the initial

device provisioning page.

Which Onboard service will you use to implement this requirement?

A. Onboard CP login service

B. Onboard Authorization service

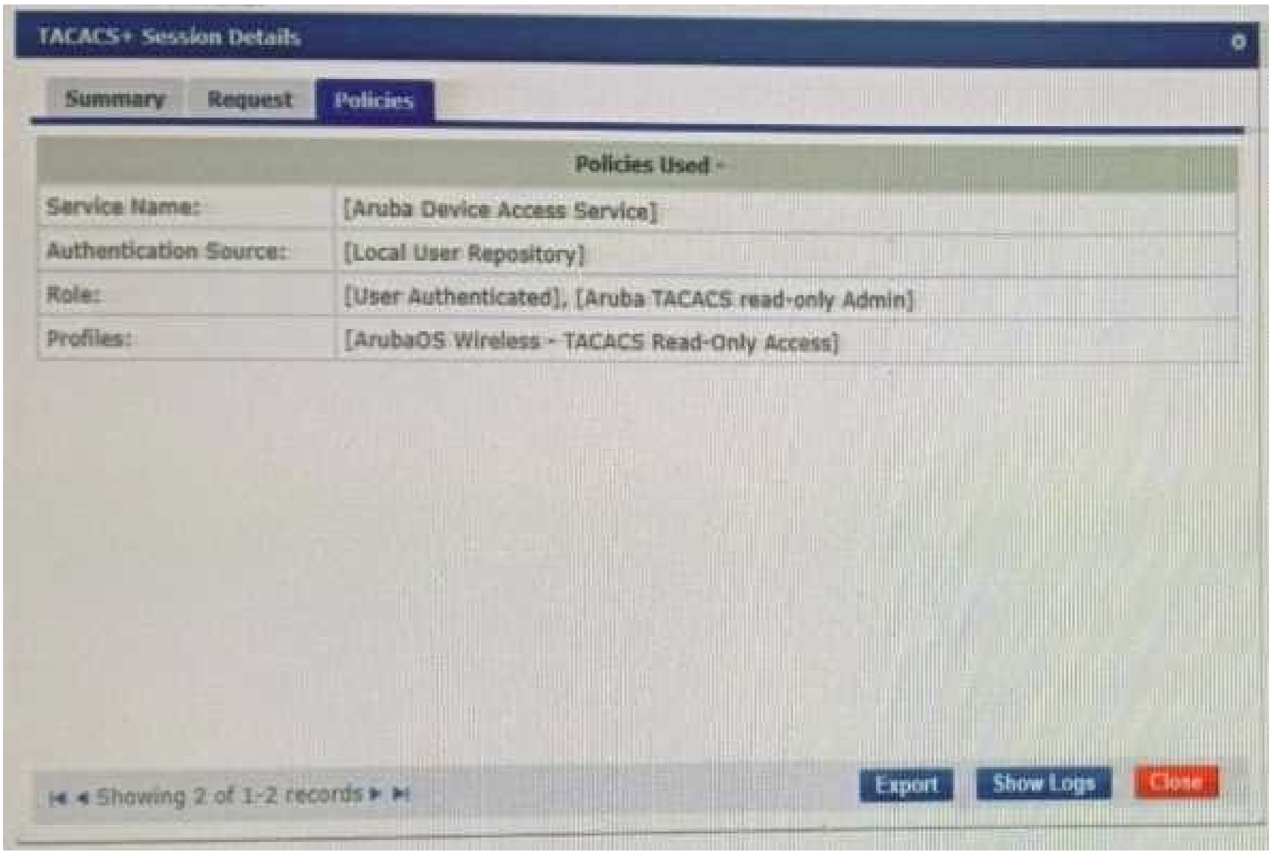
C. Onboard Provisioning service

D. Onboard Pre-Auth service

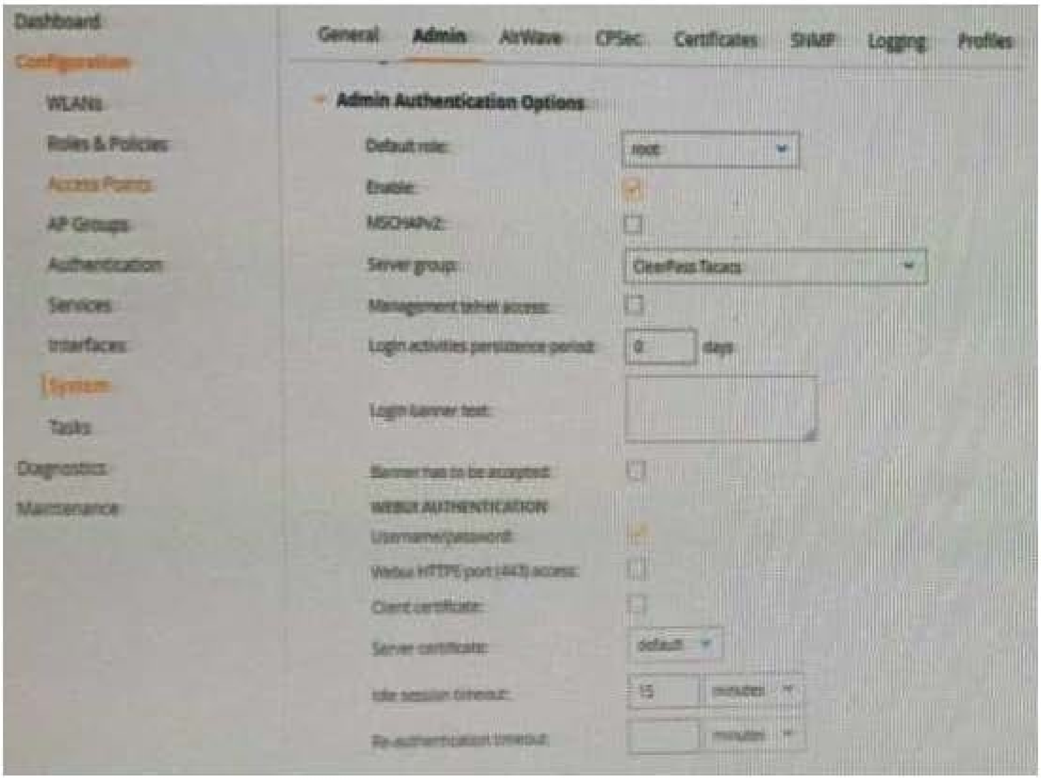
Correct Answer: A

QUESTION 2

Refer to the exhibit:



Policies Used -	
Service Name:	[Aruba Device Access Service]
Authentication Source:	[Local User Repository]
Role:	[User Authenticated], [Aruba TACACS read-only Admin]
Profiles:	[ArubaOS Wireless - TACACS Read-Only Access]



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: ☑

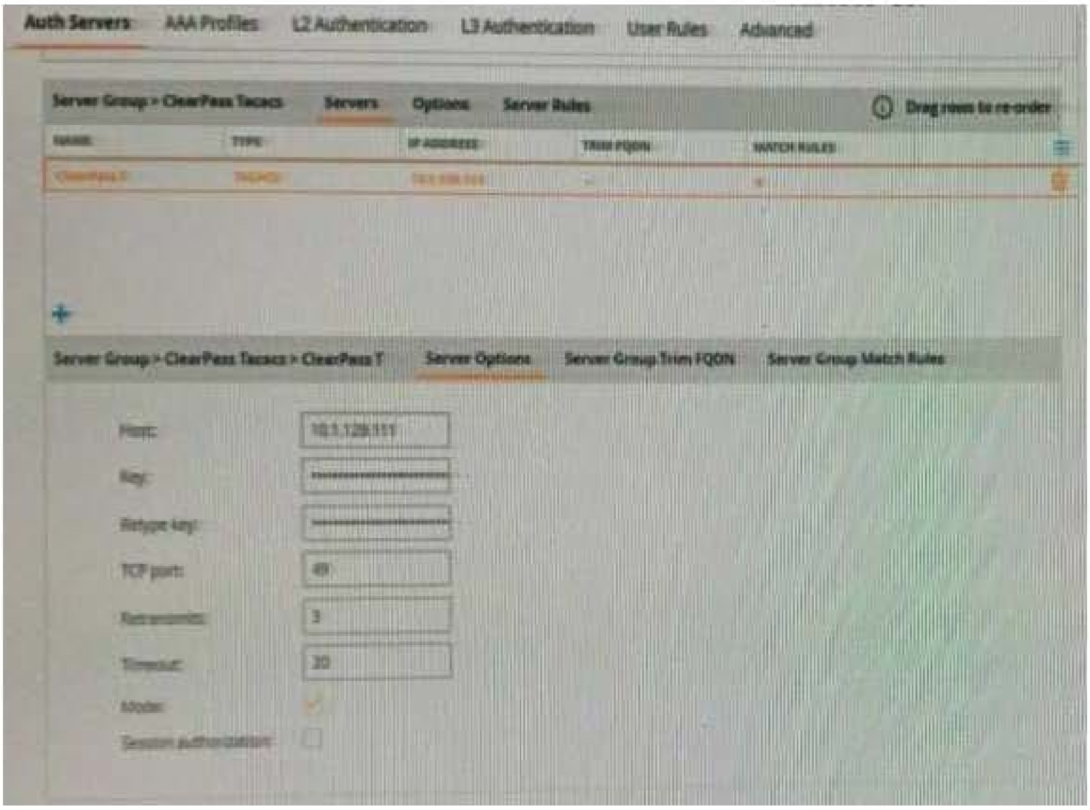
Webui HTTPS port (443) access: □

Client certificate: □

Server certificate: default

Idle session timeout: 15 minutes

Re-authentication timeout: minutes



Server Group > ClearPass Tacacs

NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES
ClearPass T	TACACS	[illegible]	-	✓

Server Group > ClearPass Tacacs > ClearPass T

Host: 10.1.128.111

Key: ••••••••••••••••••••••••

Retype key: ••••••••••••••••••••••••

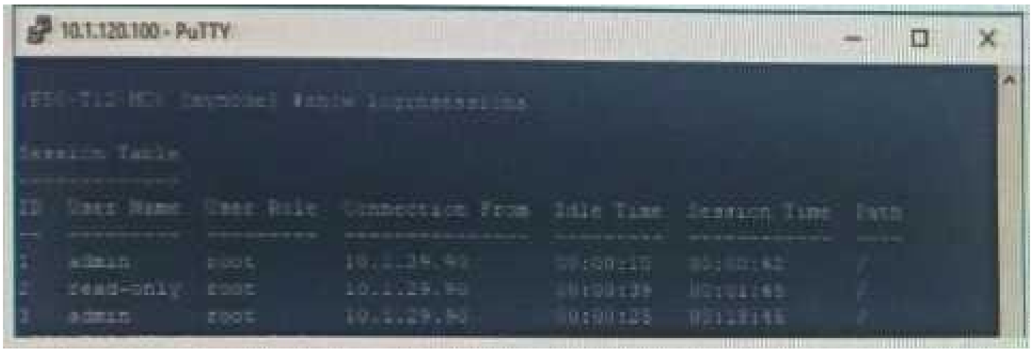
TCP port: 49

Retransmits: 3

Timeout: 20

Mode: ☑

Session authorization: □



```
([illegible]) [mynode] #show loginsessions

Session Table
-------------
ID  User Name  User Role  Connection From  Idle Time  Session Time  Path
--  ---------  ---------  ---------------  ---------  ------------  ----
1   admin      root       10.1.29.90       00:00:15   00:00:42      /
2   read-only  root       10.1.29.90       00:00:19   00:01:45      /
3   admin      root       10.1.29.90       00:00:25   00:12:16      /
```

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

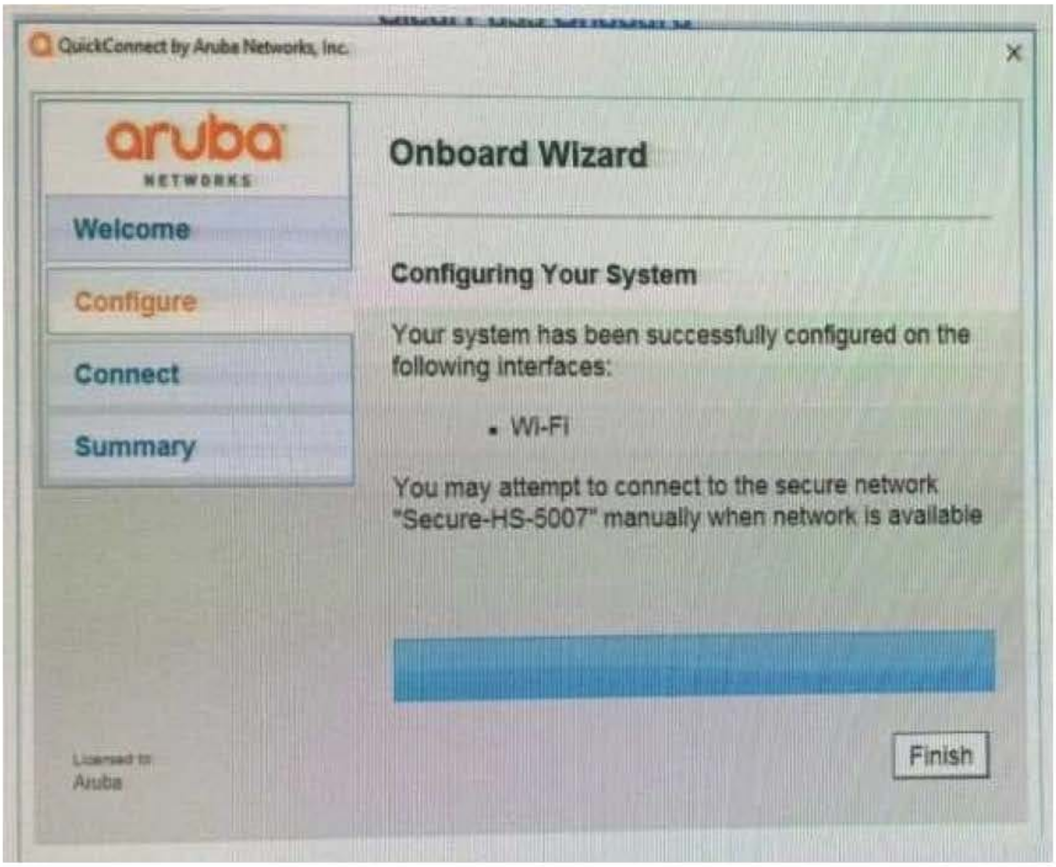
D. The read-only enforcement profile is mapped to the root role

E. On the Controller, the TACAC$ authentication server Is not configured for Session authorization

Correct Answer: CE

QUESTION 3

Refer to the exhibit:



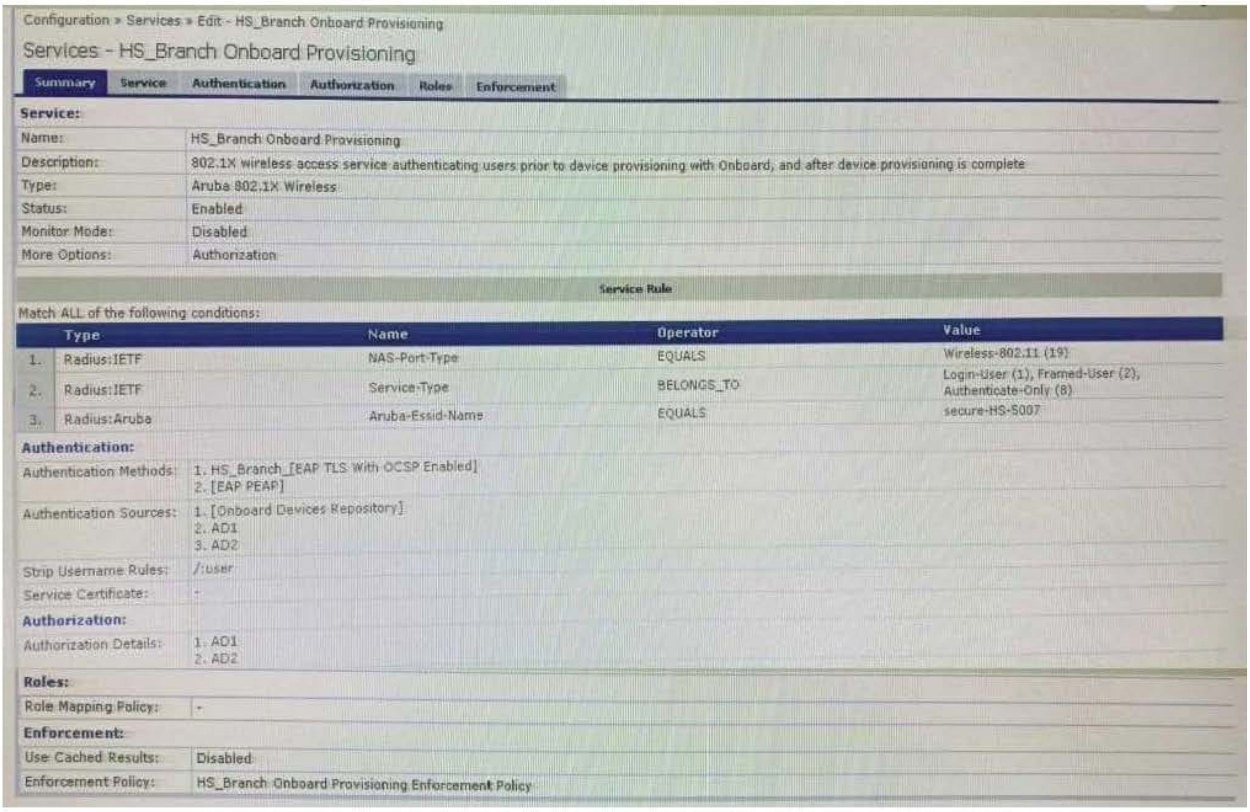
Onboard Wizard

Configuring Your System

Your system has been successfully configured on the following interfaces:

- Wi-Fi

You may attempt to connect to the secure network "Secure-HS-5007" manually when network is available


Configuration » Services » Edit - HS_Branch Onboard Provisioning
Summary
Service
Authentication
Authorization
Roles
Enforcement

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

Authorization:

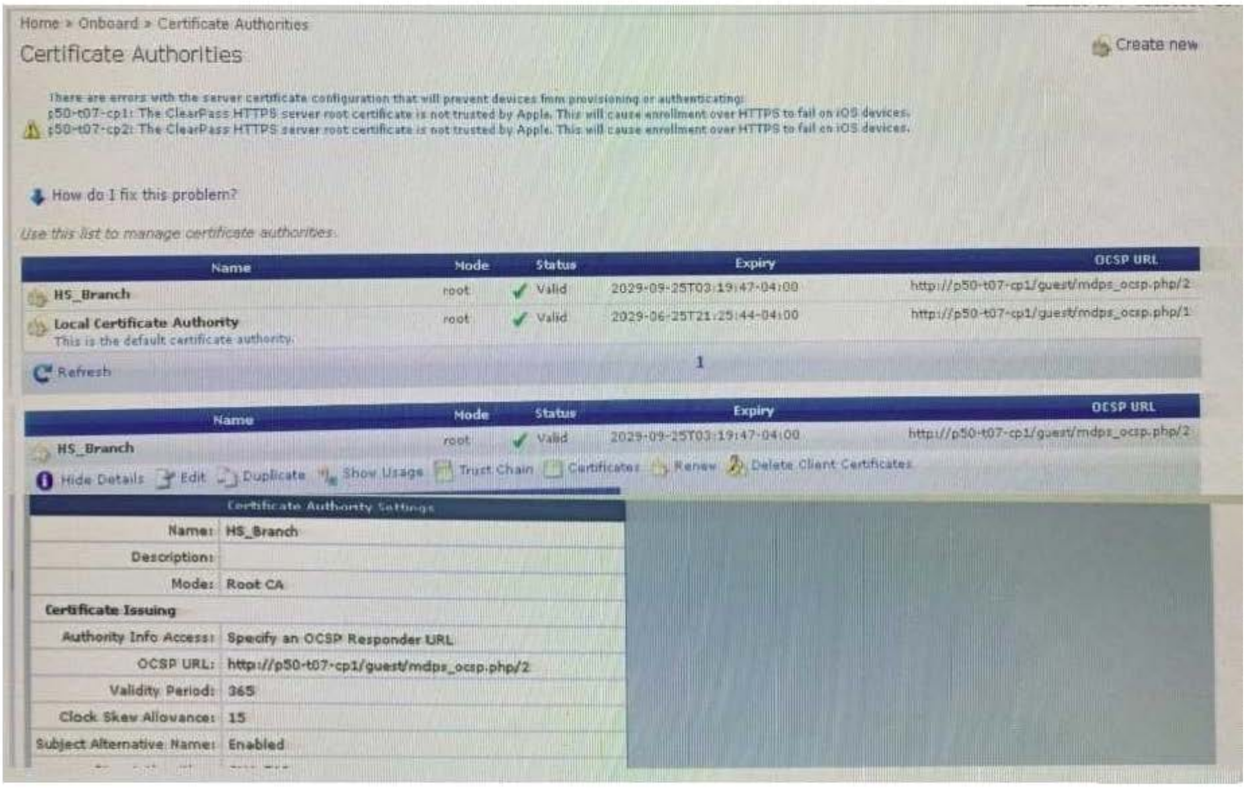
Authorization Details:	1. AD1 2. AD2

Roles:

Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	HS_Branch Onboard Provisioning Enforcement Policy



Home » Onboard » Certificate Authorities

Certificate Authorities

Create new

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

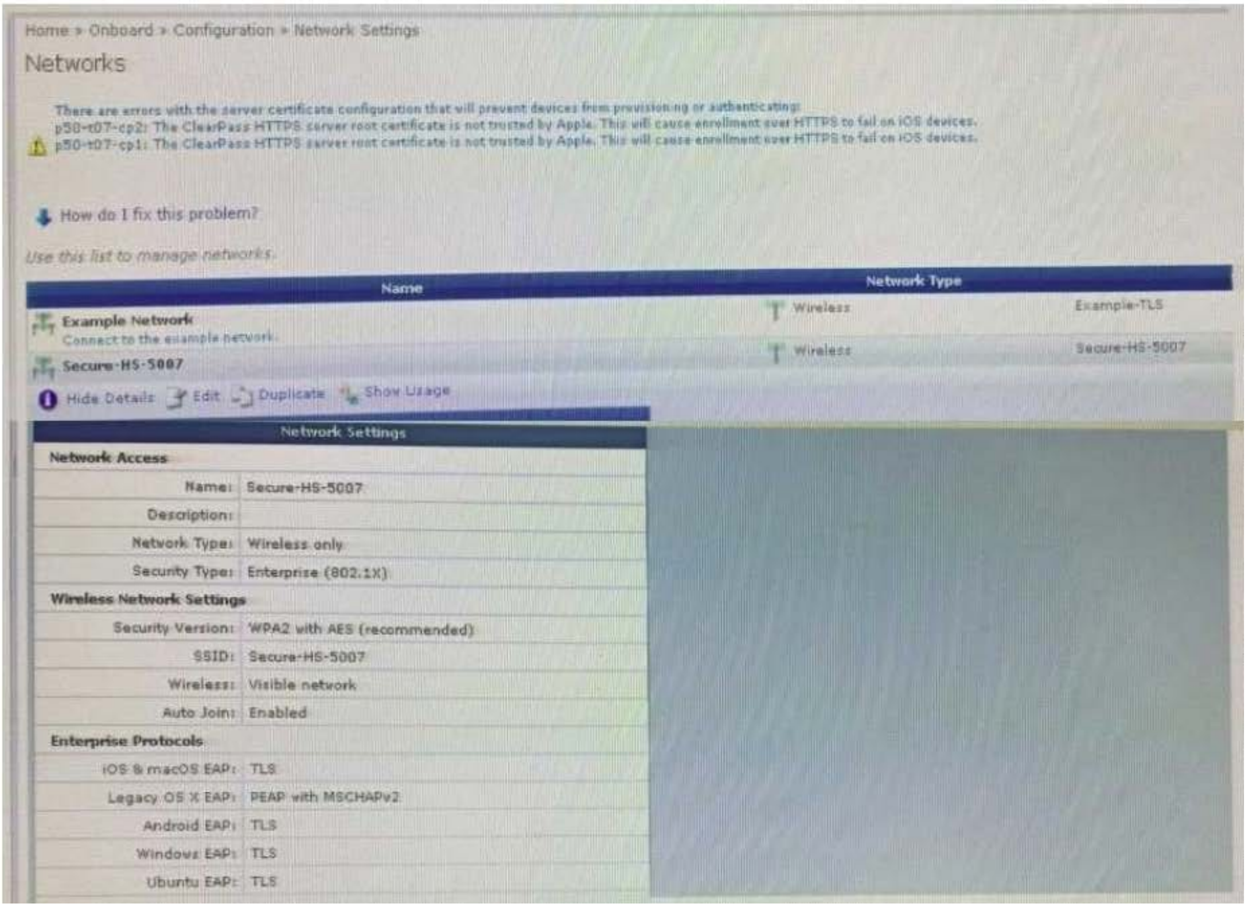
Refresh 1

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

Hide Details | Edit | Duplicate | Show Usage | Trust Chain | Certificates | Renew | Delete Client Certificates

Certificate Authority Settings

Name:	HS_Branch
Description:	
Mode:	Root CA
Certificate Issuing	
Authority Info Access:	Specify an OCSP Responder URL
OCSP URL:	http://p50-t07-cp1/guest/mdps_ocsp.php/2
Validity Period:	365
Clock Skew Allowance:	15
Subject Alternative Name:	Enabled



Home » Onboard » Configuration » Network Settings

Networks

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
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.
⚠ 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.

How do I fix this problem?

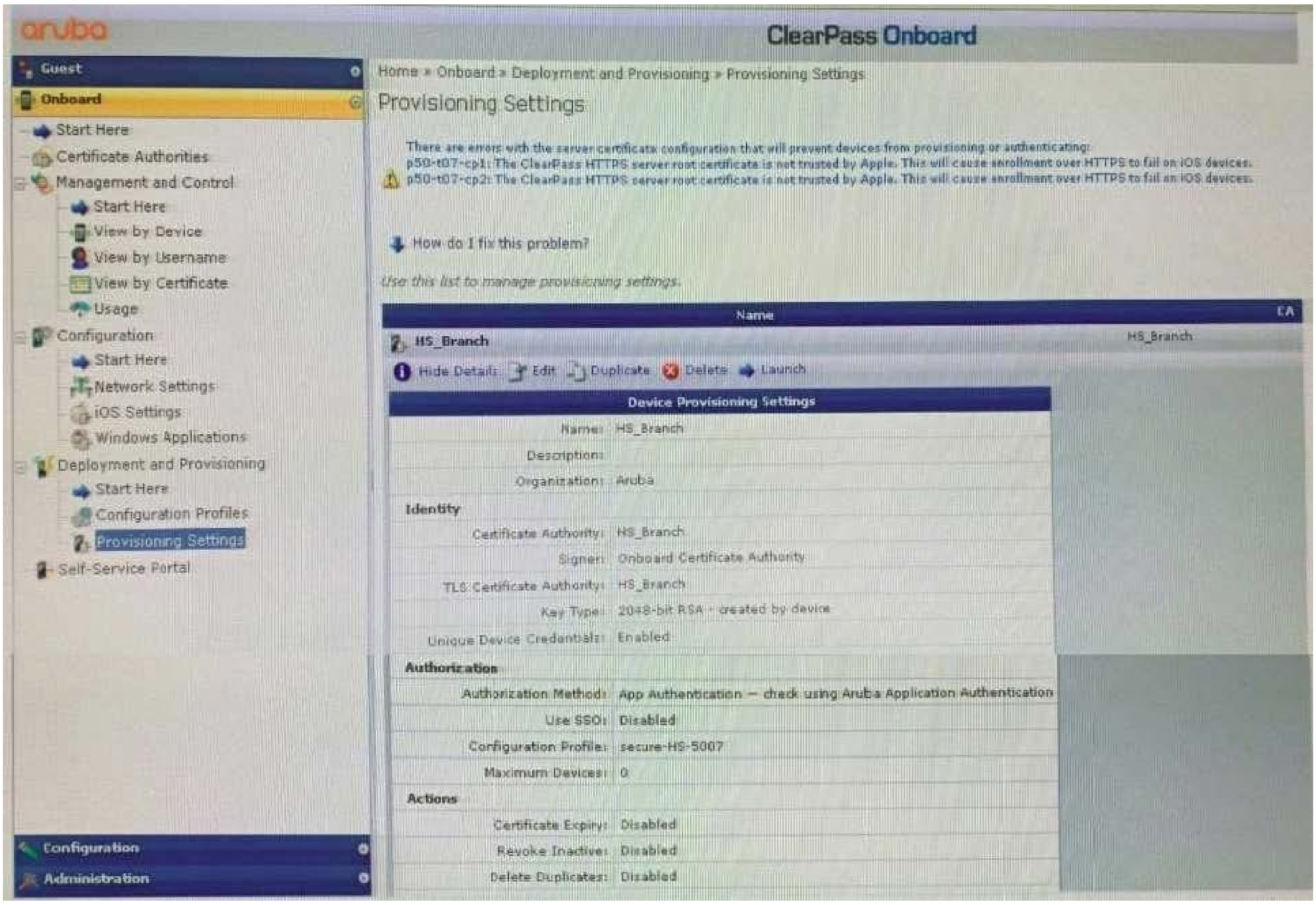
Use this list to manage networks.

Name	Network Type	
Example Network Connect to the example network.	Wireless	Example-TLS
Secure-HS-5007	Wireless	Secure-HS-5007

Hide Details | Edit | Duplicate | Show Usage

Network Settings

Network Access	
Name:	Secure-HS-5007
Description:	
Network Type:	Wireless only
Security Type:	Enterprise (802.1X)
Wireless Network Settings	
Security Version:	WPA2 with AES (recommended)
SSID:	Secure-HS-5007
Wireless:	Visible network
Auto Join:	Enabled
Enterprise Protocols	
iOS & macOS EAP:	TLS
Legacy OS X EAP:	PEAP with MSCHAPv2
Android EAP:	TLS
Windows EAP:	TLS
Ubuntu EAP:	TLS



Home » Onboard » Deployment and Provisioning » Provisioning Settings

Provisioning Settings

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 provisioning settings.

Name	CA
HS_Branch	HS_Branch

Device Provisioning Settings	
Name:	HS_Branch
Description:	
Organization:	Aruba
Identity	
Certificate Authority:	HS_Branch
Signer:	Onboard Certificate Authority
TLS Certificate Authority:	HS_Branch
Key Type:	2048-bit RSA - created by device
Unique Device Credentials:	Enabled
Authorization	
Authorization Method:	App Authentication — check using Aruba Application Authentication
Use SSO:	Disabled
Configuration Profile:	secure-HS-5007
Maximum Devices:	0
Actions	
Certificate Expiry:	Disabled
Revoke Inactive:	Disabled
Delete Duplicates:	Disabled

You have configured an Onboard portal for single SSID provision. During testing you notice that the QuickConnect Application did not display the "Connect" button, only the finish button. To get connected the test user had to manually connect to the secure-HS-5007 SSID but was prompted for a username and password. Using the screenshots as a reference, how would you fix this issue?

A. Check the network settings for the correct SSID name spelling.

B. Change the network settings to use EAP-TLS for the authentication protocol.

C. Install a public signed HTTPs web server certificate on the ClearPass server.

D. Configure the SSID to support both EAP-PEAP and EAP-TLS authentication method.

Correct Answer: A

QUESTION 4

What is used to validate the EAP Certificate? (Select three.)

A. Common Name

B. Date

C. Key usage

D. Server Identity

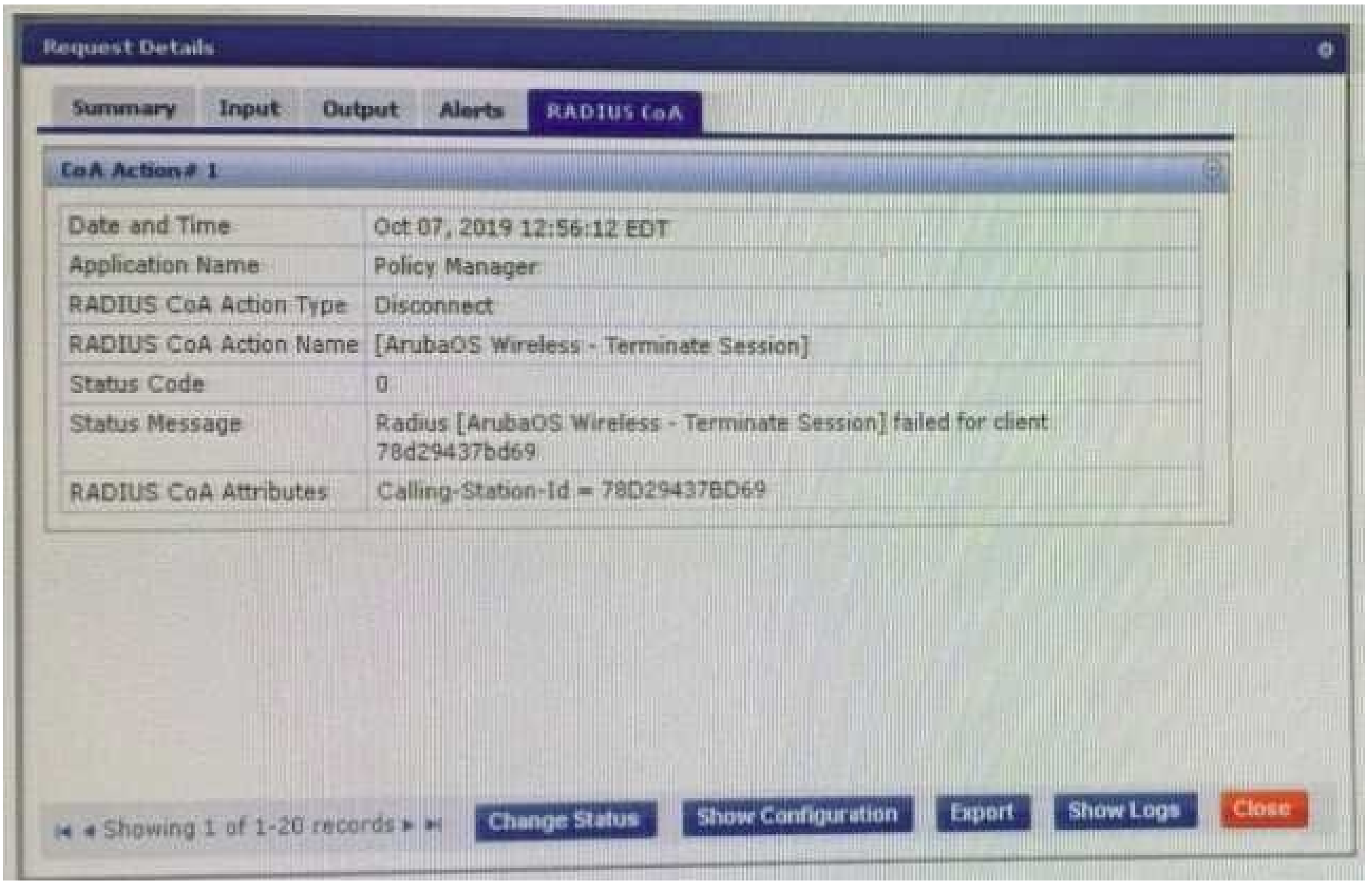
E. SAN entries

F. Trust chain

Correct Answer: ACF

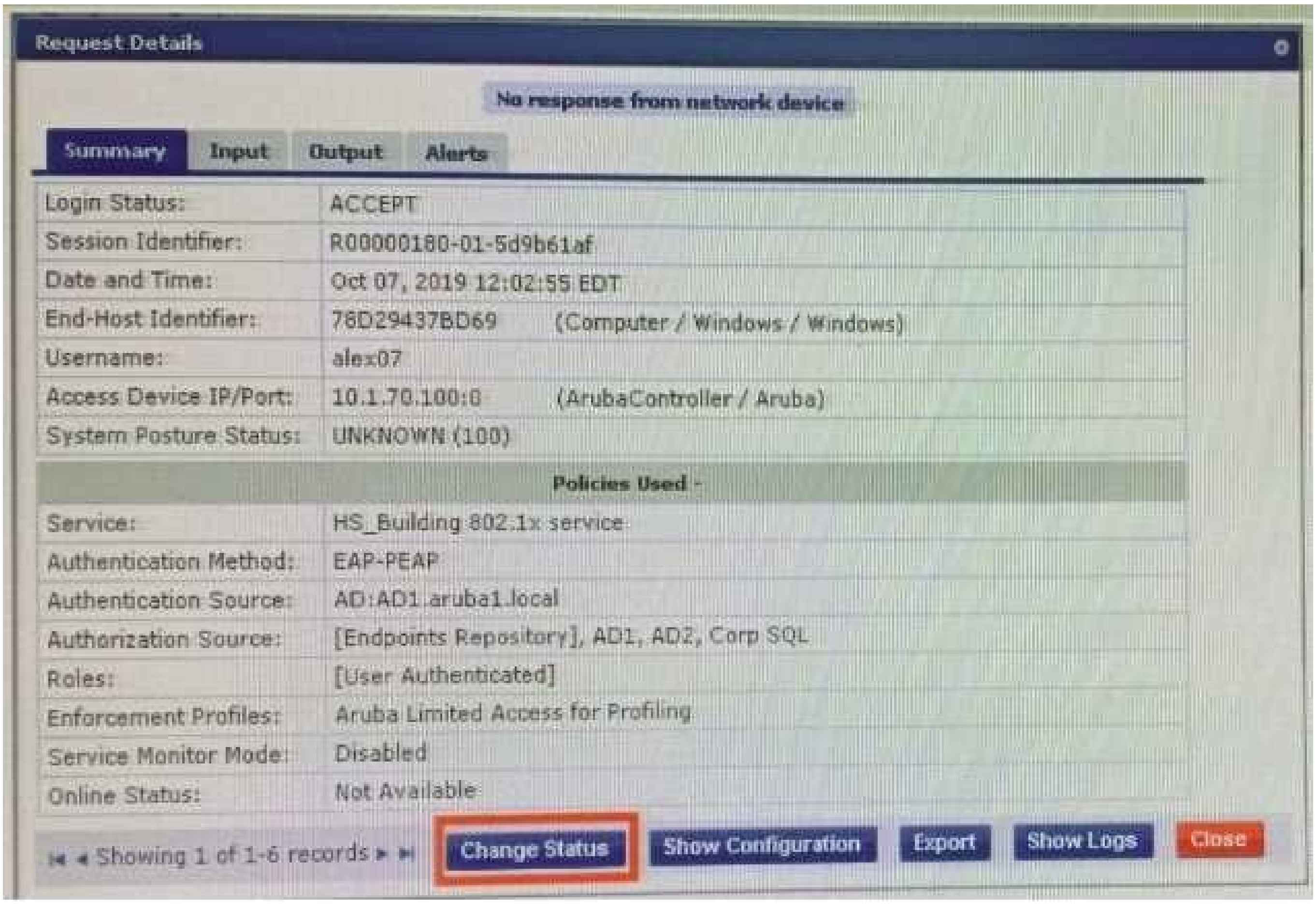
QUESTION 5

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 6

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.

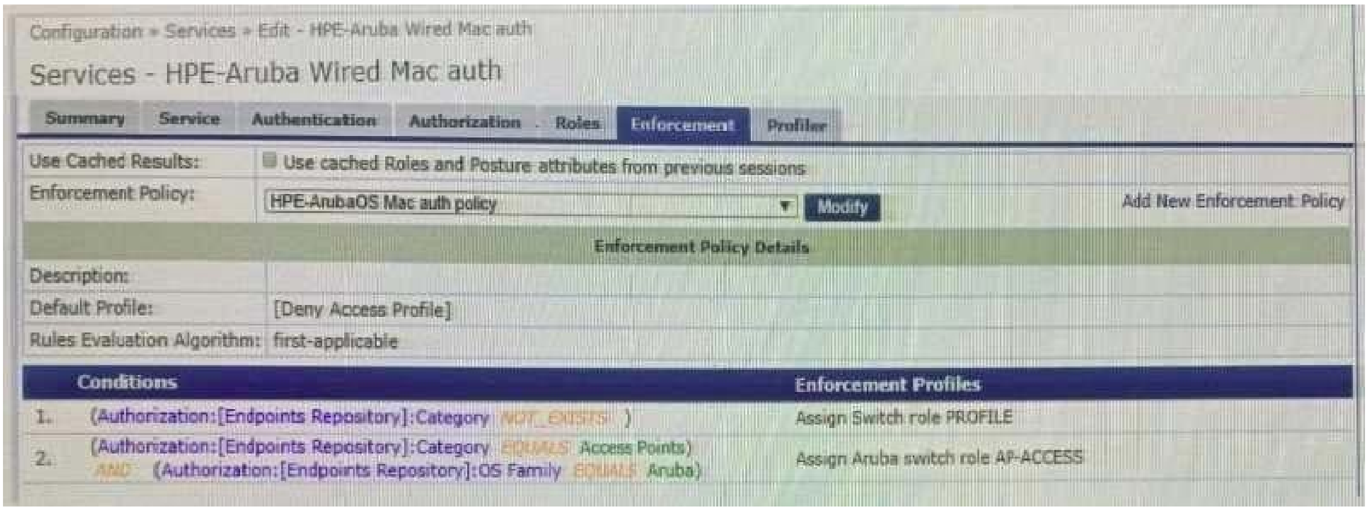
C. The guest users are assigned a firewall user role that has a rate limit.

D. The enforcement profile on ClearPass is set up with an IETF:session delay.

Correct Answer: A

QUESTION 7

Refer to the exhibit: You are doing a ClearPass PoC at a customer site with a single Aruba Mobility Controller. The customer asked for a demonstration of a simple Web Login functionality. You used a service template to create the guest services. During testing, the user gets redirected back to the weblogin page with an Authentication failed message. The guest configurations on the Aruba Mobility Controller are configured correctly. Why would the guest fail to authenticate successfully?



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

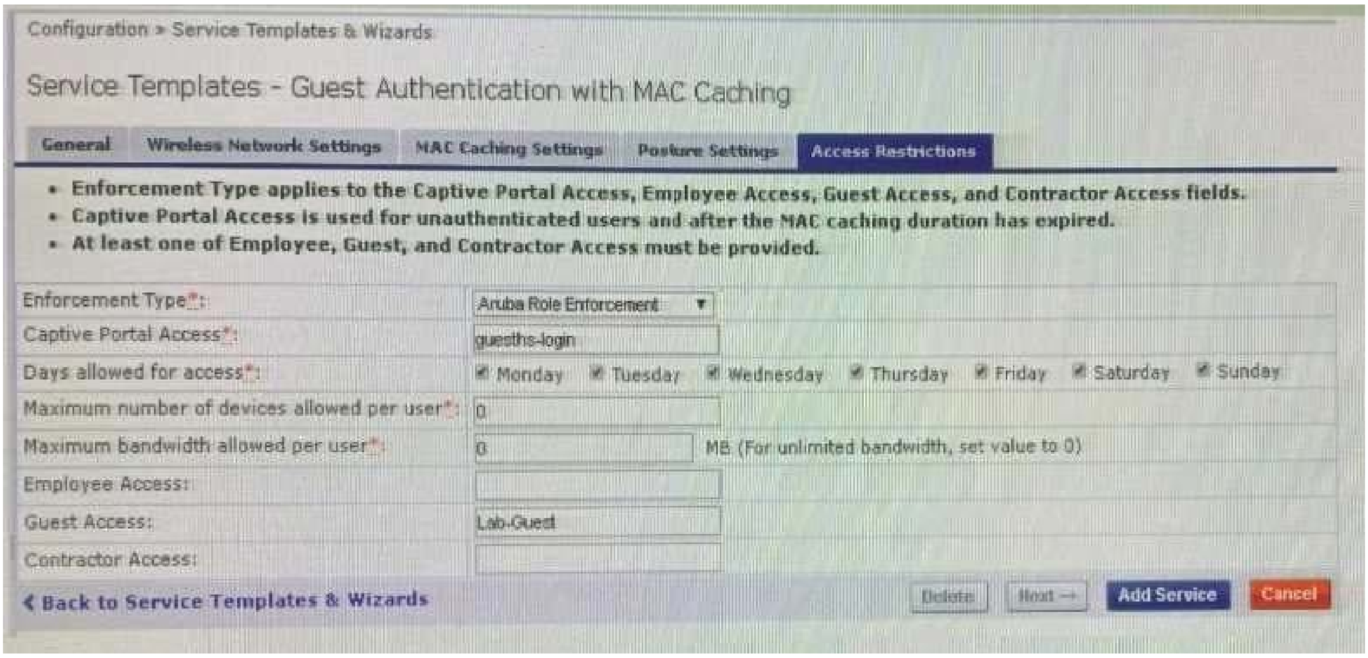
Services - HPE-Aruba Wired Mac auth

Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	HPE-ArubaOS Mac auth policy ▾

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

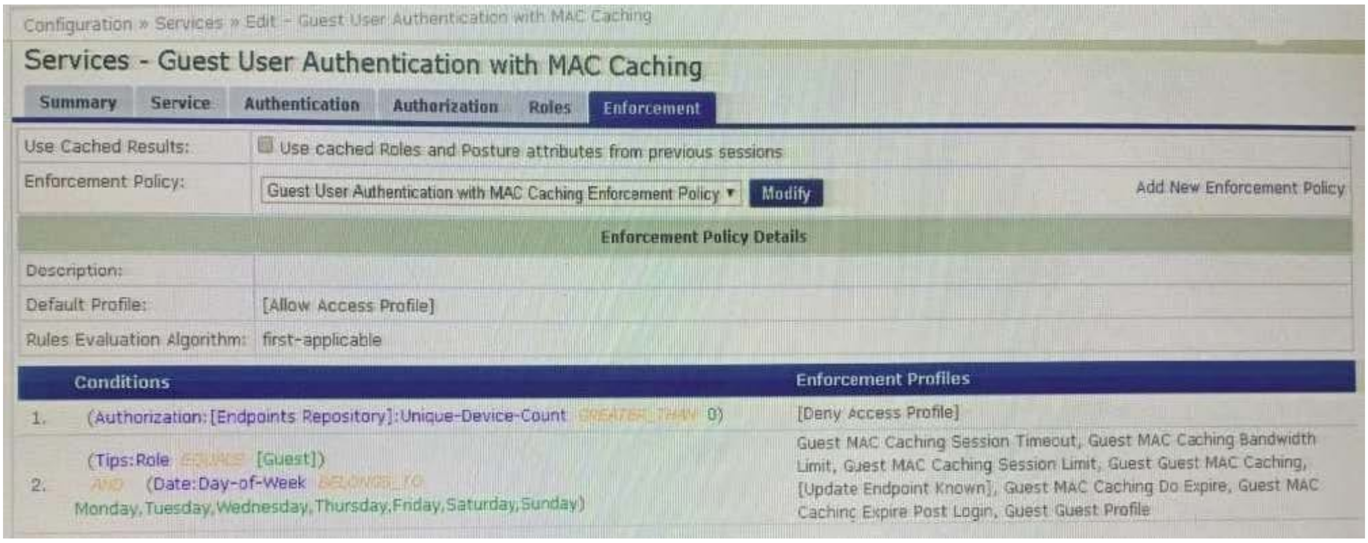


Configuration » Service Templates & Wizards

Service Templates - Guest Authentication with MAC Caching

- Enforcement Type applies to the Captive Portal Access, Employee Access, Guest Access, and Contractor Access fields.
- Captive Portal Access is used for unauthenticated users and after the MAC caching duration has expired.
- At least one of Employee, Guest, and Contractor Access must be provided.

Enforcement Type*:	Aruba Role Enforcement ▾
Captive Portal Access*:	guesths-login
Days allowed for access*:	☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday
Maximum number of devices allowed per user*:	0
Maximum bandwidth allowed per user*:	0 MB (For unlimited bandwidth, set value to 0)
Employee Access:	
Guest Access:	Lab-Guest
Contractor Access:	



Configuration » Services » Edit - Guest User Authentication with MAC Caching

Services - Guest User Authentication with MAC Caching

Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	Guest User Authentication with MAC Caching Enforcement Policy ▾

Enforcement Policy Details

Description:	
Default Profile:	[Allow Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 0)	[Deny Access Profile]
2.	(Tips:Role EQUALS [Guest]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	Guest MAC Caching Session Timeout, Guest MAC Caching Bandwidth Limit, Guest MAC Caching Session Limit, Guest Guest MAC Caching, [Update Endpoint Known], Guest MAC Caching Do Expire, Guest MAC Cachinc Expire Post Login, Guest Guest Profile

A. The authentication source mapped in the service is incorrect, it should be mapped as (Guest Device Repository] [Local SQL DB].

B. The username and/or password used for authentication is incorrect Re-enter the correct password on the weblogin page.

C. The username used for authentication does not exist in the Guest User Database Create a new user and authenticate again.

D. The Unique-Device-Count does not allow any Client devices. Update the Enforcement policy condition: Unique-Device-Count.

Correct Answer: A

QUESTION 8

Where is the following information stored in ClearPass?

1.

Roles and Posture for Connected Clients

2.

System Health for OnGuard

3.

Machine authentication State

4.

CoA session info

5.

Mapping of connected clients to NAS/NAD

A. Multi-Master cache

B. Endpoint database

C. insight database

D. ClearPass system cache

Correct Answer: D

QUESTION 9

What is the Open SSID (otherwise referred to as Dual SSID) Onboard deployment service workflow?

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

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

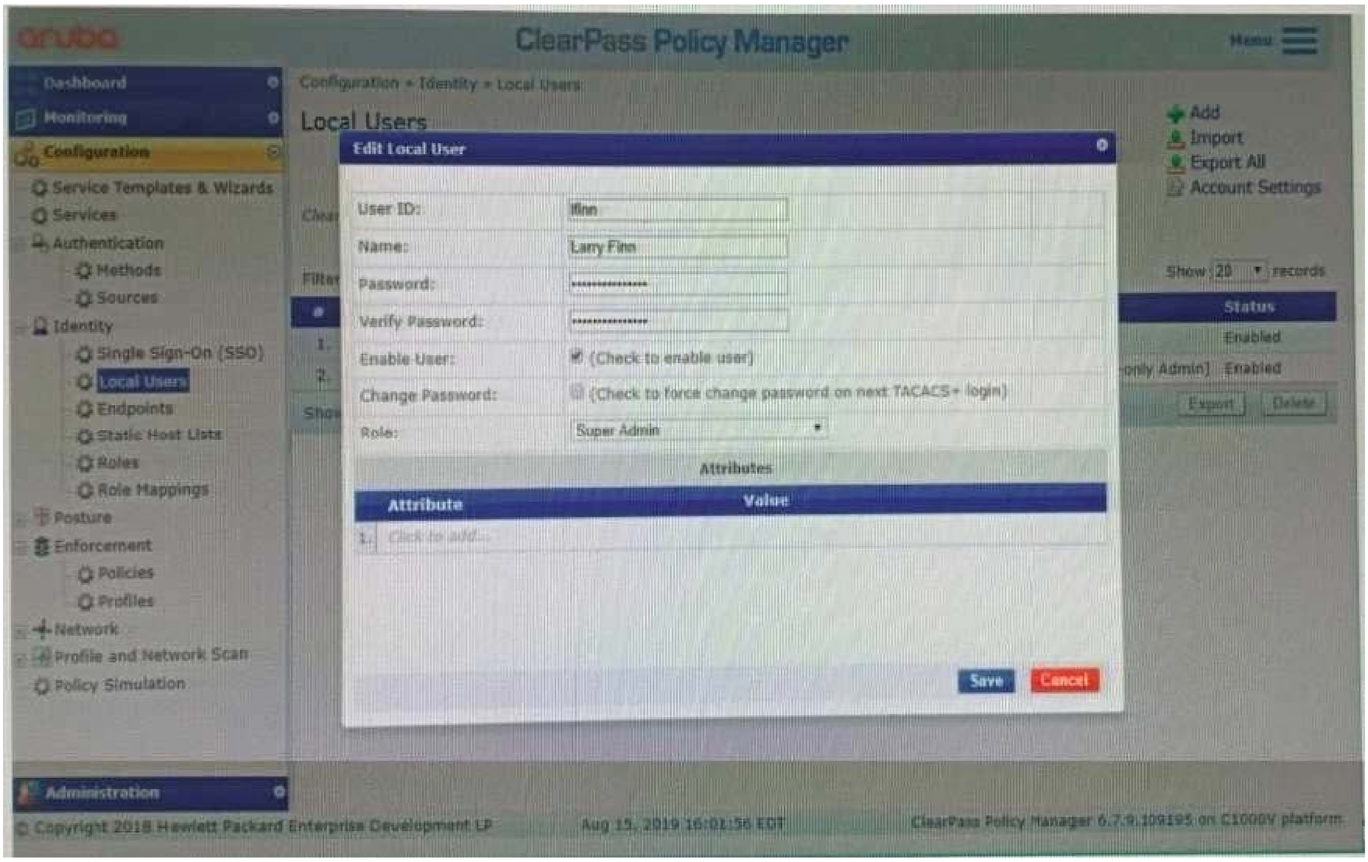
C. OnBoard Authorization Application service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

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

Correct Answer: C

QUESTION 10

Refer to the exhibit:



User ID:	lfinn
Name:	Larry Finn
Password:	•••••••••••••••
Verify Password:	•••••••••••••••
Enable User:	☑ (Check to enable user)
Change Password:	□ (Check to force change password on next TACACS+ login)
Role:	Super Admin

Attributes

	Attribute	Value
1.	Click to add...	

The customer complains that the user shown cannot log into the ClearPass Server as an administrator using the [Policy Manager Admin Network Login Service]. What could be the reason for this?

A. The user might be used for a TACACS authentication

B. The account created does not fit this purpose.

C. The mapping on the role should be changed to [RADIUS Super Admin]

D. The local user authentication might be disabled

Correct Answer: B

[Latest HPE6-A77 Dumps](https://www.certbus.com/hpe6-a77.html) [HPE6-A77 Practice Test](https://www.certbus.com/hpe6-a77.html) [HPE6-A77 Study Guide](https://www.certbus.com/hpe6-a77.html)