HPE6-A77^Q&As^

Aruba Certified ClearPass Expert Written

Pass HP HPE6-A77 Exam with 100% Guarantee

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

https://www.pass4itsure.com/hpe6-a77.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A customer is planning to implement machine and user authentication on infrastructure with one Aruba

Controller and a single ClearPass Server.

What should the customer consider while designing this solution? (Select three.)

A. The Windows User must log off, restart or disconnect their machine to initiate a machine authentication before the cache expires.

B. The machine authentication status is written in the Multi-master cache on the ClearPass Server for 24 hrs.

C. Onboard must be used to install the Certificates on the personal devices to do the user and machine authentication.

D. The Customer should enable Multi-Master Cache Survivability as the Aruba Controller will not cache the machine state.

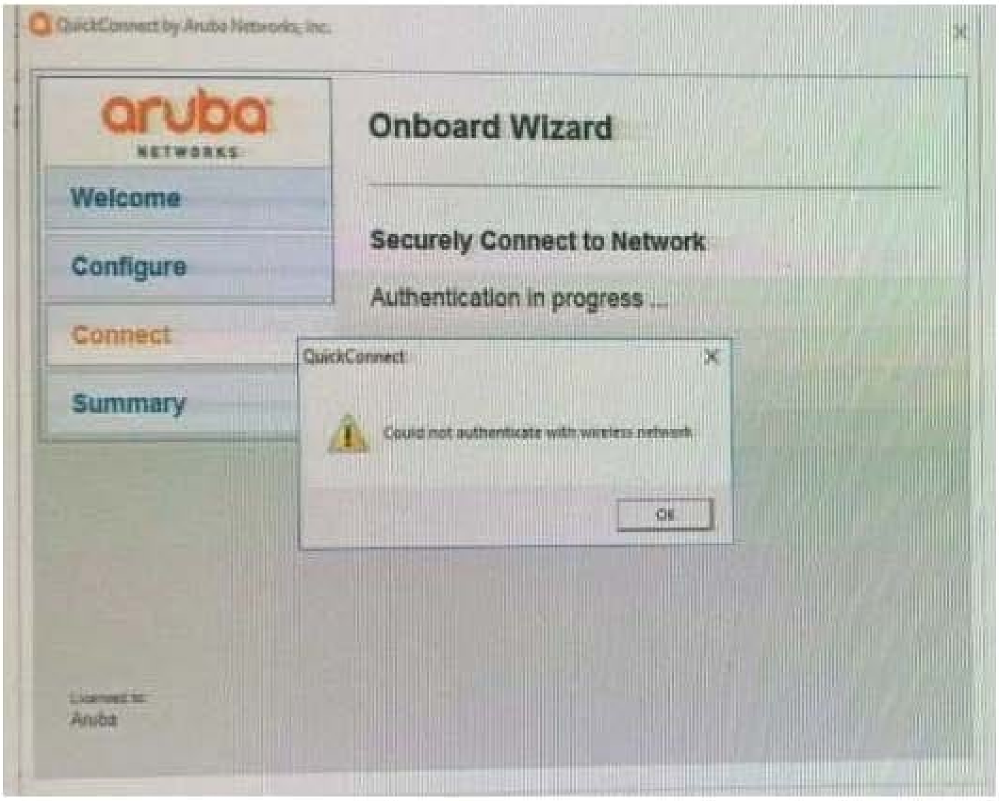
E. Machine Authentication only uses EAP TLS, as such a PKI infrastructure should be in place for machine authentication.

F. The customer does not need to worry about Multi-Master Cache Survivability because the Controller will also cache the machine state.

Correct Answer: BCE

QUESTION 2

Refer to the exhibit:



QuickConnect by Aruba Networks, Inc.

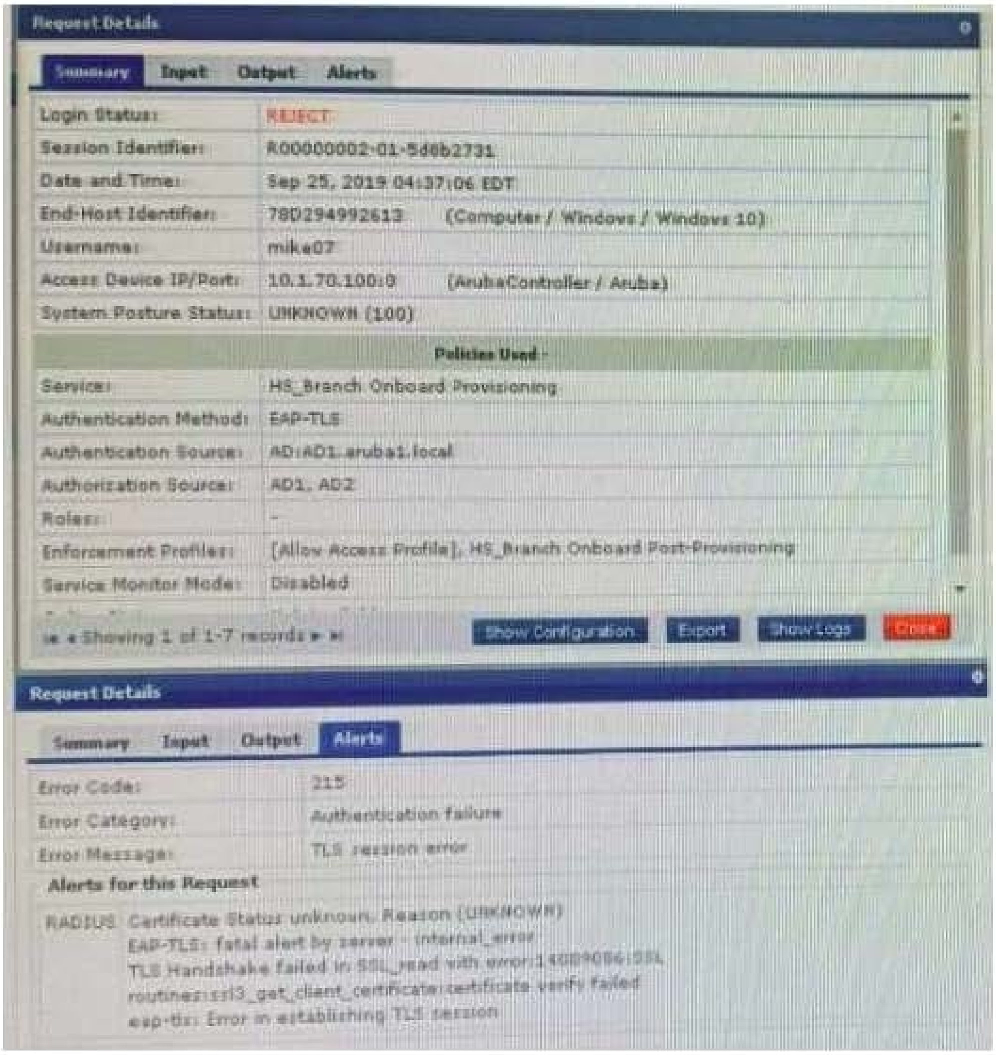
Onboard Wizard

Securely Connect to Network

Authentication in progress ...

QuickConnect

Could not authenticate with wireless network

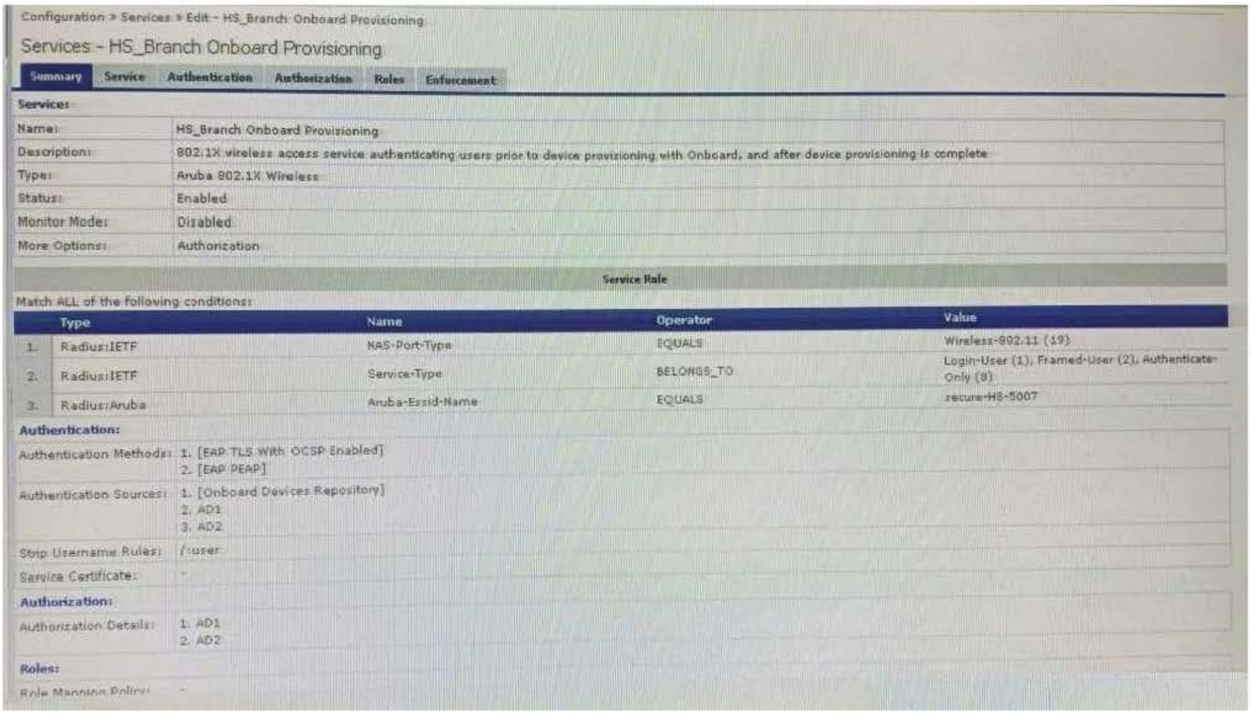


Login Status:	REJECT
Session Identifier:	R00000002-01-5d8b2731
Date and Time:	Sep 25, 2019 04:37:06 EDT
End-Host Identifier:	78D294992613 (Computer / Windows / Windows 10)
Username:	mike07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	HS_Branch Onboard Provisioning
Authentication Method:	EAP-TLS
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	AD1, AD2
Roles:	-
Enforcement Profiles:	[Allow Access Profile], HS_Branch Onboard Post-Provisioning
Service Monitor Mode:	Disabled

Error Code:	215
Error Category:	Authentication failure
Error Message:	TLS session error

Alerts for this Request

```
RADIUS  Certificate Status unknown, Reason (UNKNOWN)
        EAP-TLS: fatal alert by server - internal_error
        TLS Handshake failed in SSL_read with error:14089086:SSL
        routines:ssl3_get_client_certificate:certificate verify failed
        eap-tls: Error in establishing TLS session
```



Configuration » Services » Edit - HS_Branch Onboard Provisioning

Services - HS_Branch Onboard Provisioning

Services:

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:

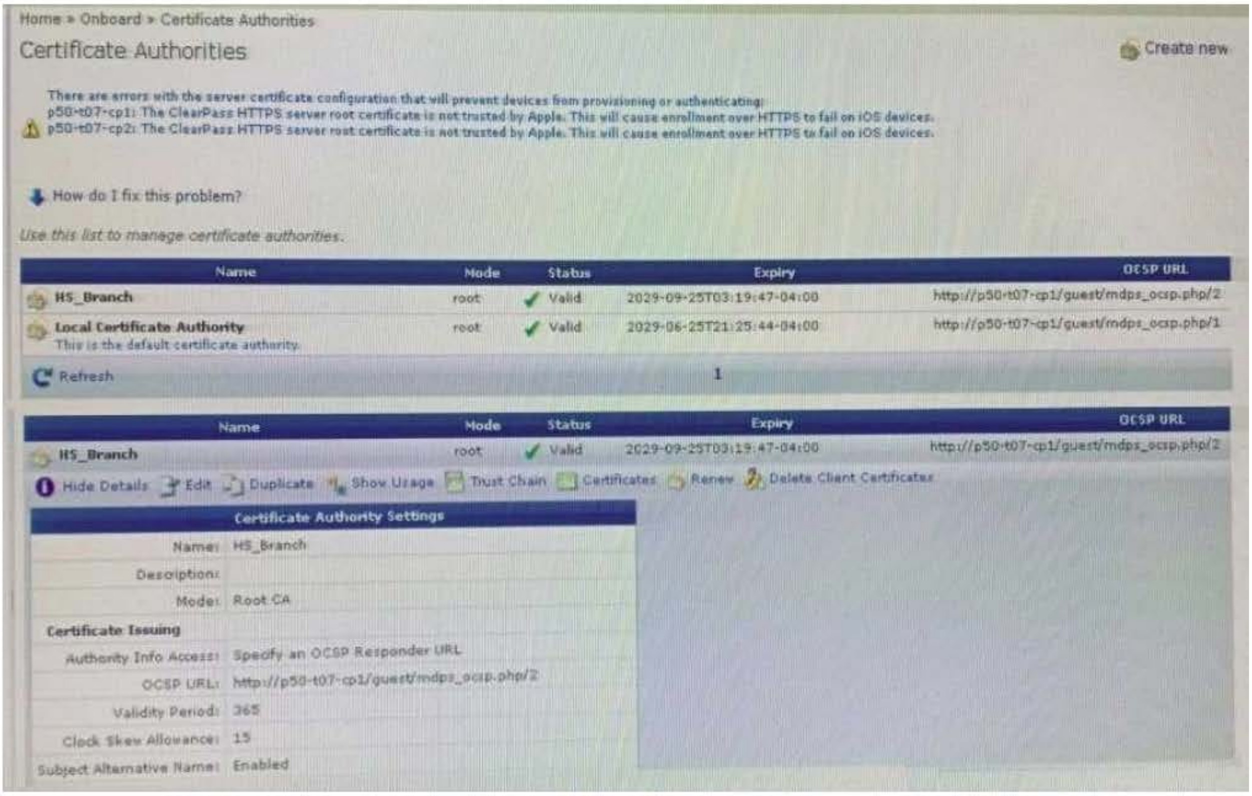
Authentication Methods:	1. [EAP TLS With OCSP Enabled] 2. [EAP PEAP]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2
Strip Username Rules:	/:user
Service Certificate:	-

Authorization:

Authorization Details:	1. AD1 2. AD2

Roles:

Role Mapping Policy: -



Home » Onboard » Certificate Authorities

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?

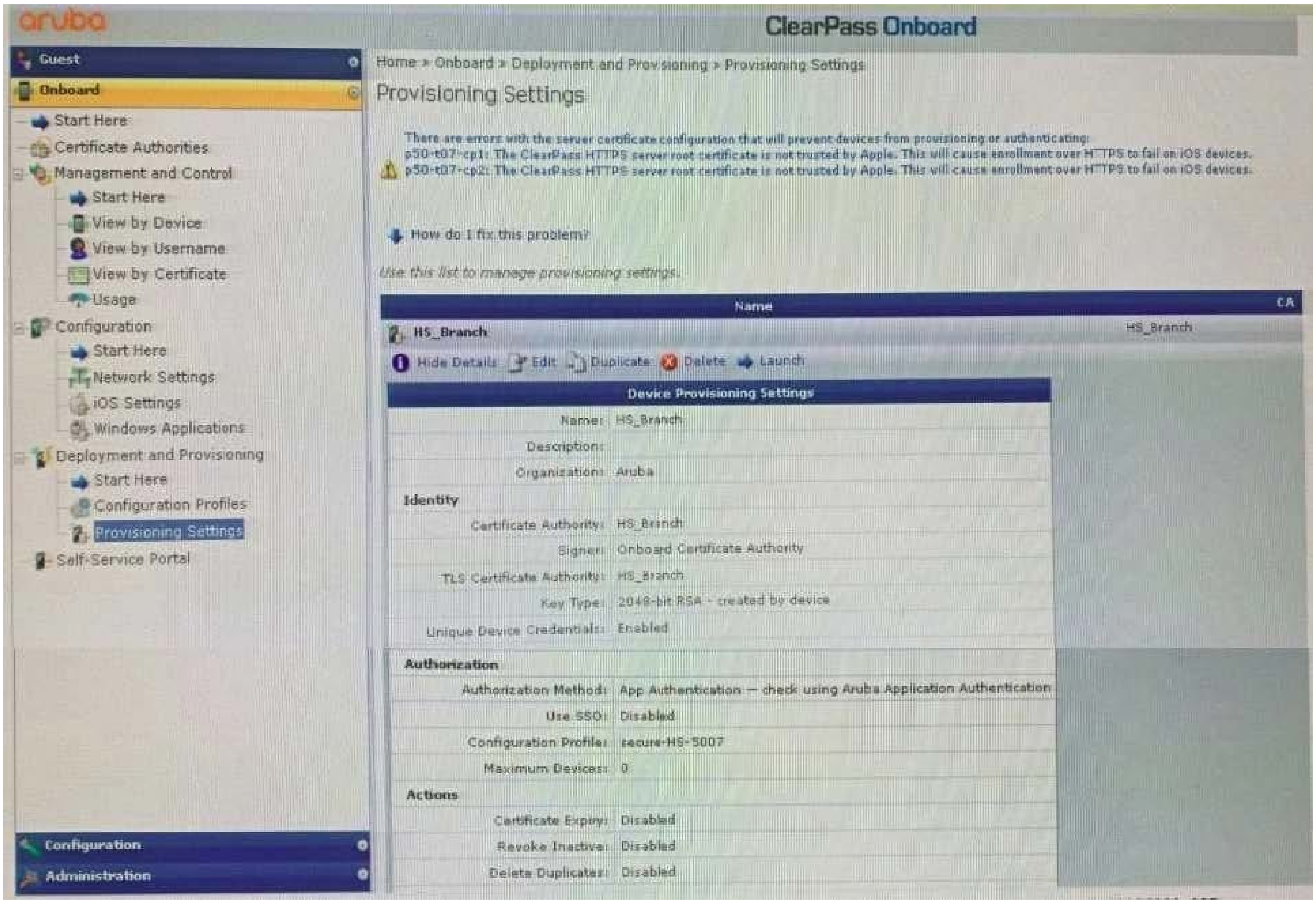
Use this list to manage certificate authorities.

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

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

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



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 Onboard and cannot get it working The customer has sent you the above

screenshots.

How would you resolve the issue?

A. Re-provision the client by running the QuickConnect application as Administrator

B. Install a public signed server authentication certificate on the ClearPass server for EAP

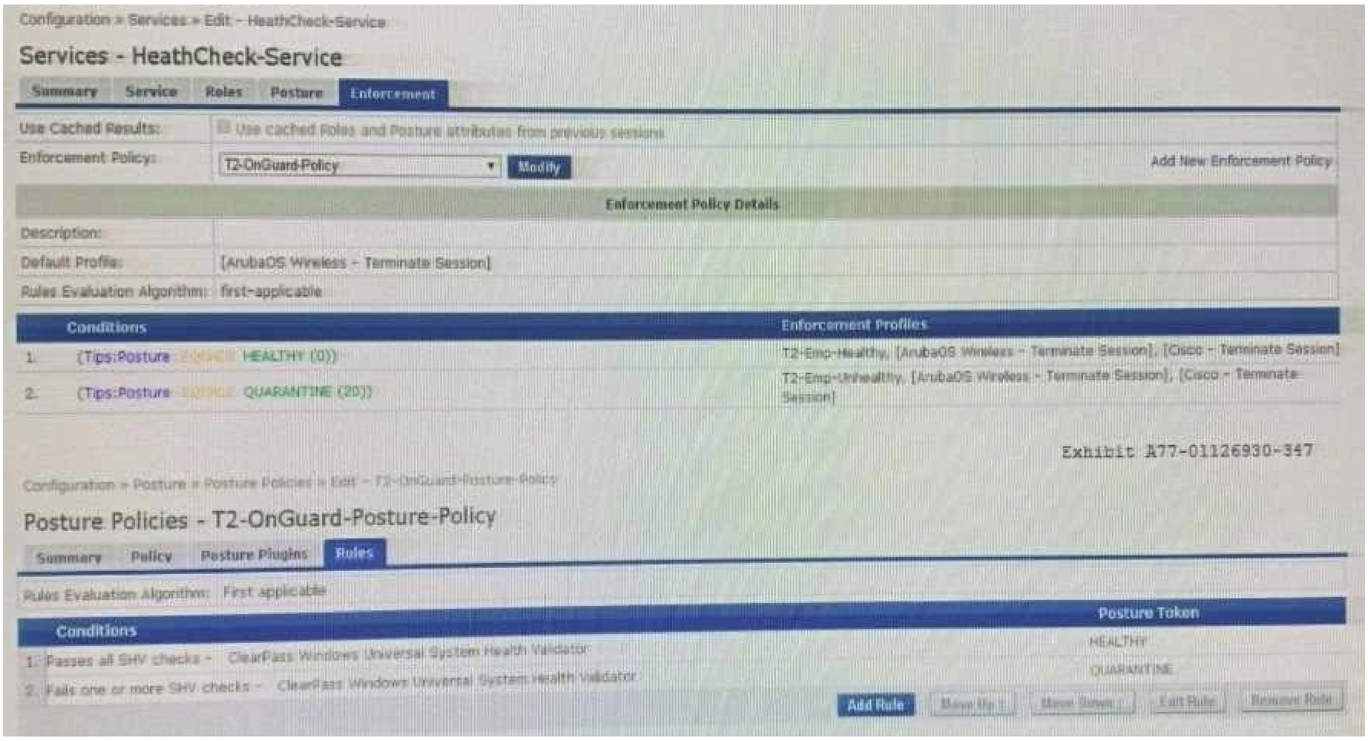
C. Reconnect the client and select the correct certificate when prompted

D. Copy the [EAP-TLS with OSCP Enabled] authentication method and set the correct OCSP URL

Correct Answer: A

QUESTION 3

Refer to the Exhibit:



Configuration » Services » Edit – HeathCheck-Service

Services - HeathCheck-Service

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

Enforcement Policy: T2-OnGuard-Policy

Enforcement Policy Details

Description:	
Default Profile:	[ArubaOS Wireless – Terminate Session]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Posture EQUALS HEALTHY (0))	T2-Emp-Healthy, [ArubaOS Wireless – Terminate Session], [Cisco – Terminate Session]
2.	(Tips:Posture EQUALS QUARANTINE (20))	T2-Emp-Unhealthy, [ArubaOS Wireless – Terminate Session], [Cisco – Terminate Session]

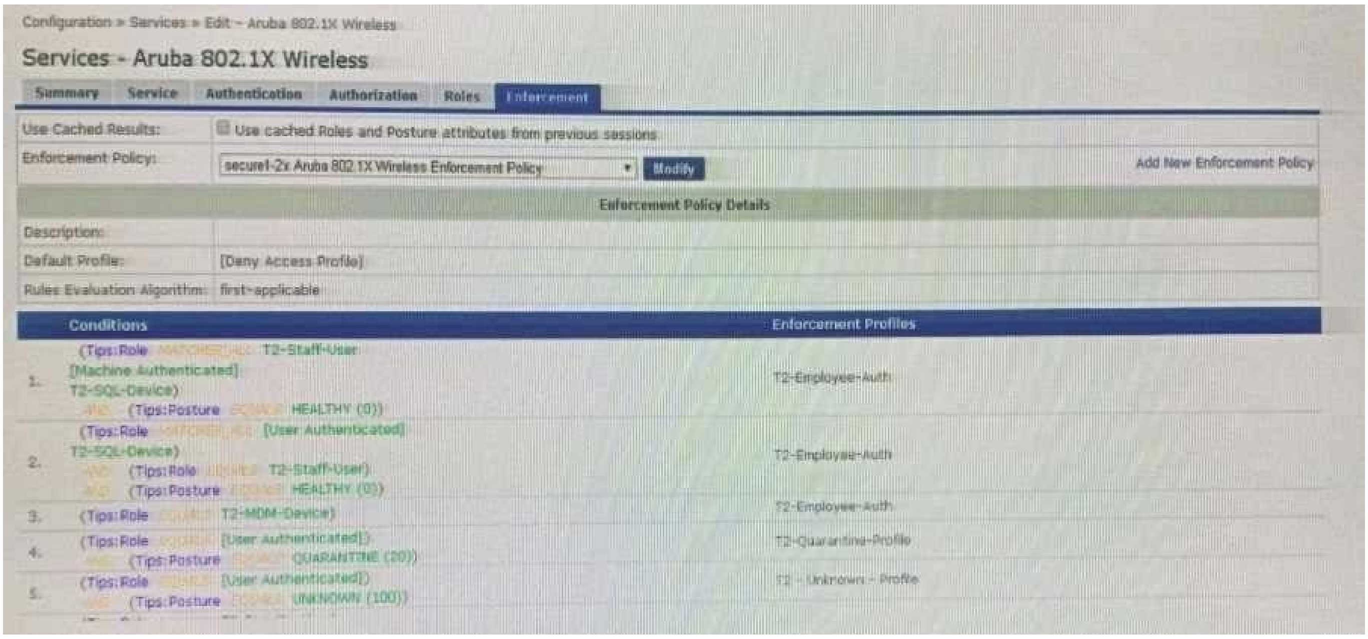
Exhibit A77-01126930-347

Configuration » Posture » Posture Policies » Edit – T2-OnGuard-Posture-Policy

Posture Policies - T2-OnGuard-Posture-Policy

Rules Evaluation Algorithm: First applicable

	Conditions	Posture Token
1.	Passes all SHV checks - ClearPass Windows Universal System Health Validator	HEALTHY
2.	Fails one or more SHV checks - ClearPass Windows Universal System Health Validator	QUARANTINE



Configuration » Services » Edit – Aruba 802.1X Wireless

Services - Aruba 802.1X Wireless

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

Enforcement Policy: secure1-2x Aruba 802.1X Wireless Enforcement Policy

Enforcement Policy Details

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

	Conditions	Enforcement Profiles
1.	(Tips:Role MATCHES_ALL T2-Staff-User [Machine Authenticated] T2-SQL-Device) AND (Tips:Posture EQUALS HEALTHY (0))	T2-Employee-Auth
2.	(Tips:Role MATCHES_ALL [User Authenticated] T2-SQL-Device) AND (Tips:Role EQUALS T2-Staff-User) AND (Tips:Posture EQUALS HEALTHY (0))	T2-Employee-Auth
3.	(Tips:Role EQUALS T2-MDM-Device)	T2-Employee-Auth
4.	(Tips:Role EQUALS [User Authenticated]) AND (Tips:Posture EQUALS QUARANTINE (20))	T2-Quarantine-Profile
5.	(Tips:Role EQUALS [User Authenticated]) AND (Tips:Posture EQUALS UNKNOWN (100))	T2 – Unknown – Profile

A customer wants to integrate posture validation into an Aruba Wireless 802.1X authentication service

During testing, the client connects to the Aruba Employee Secure SSID and is redirected to the Captive Portal page where the user can download the OnGuard Agent After the Agent is installed, the client receives the Healthy token the client remains connected to the Captive Portal page ClearPass is assigning the endpoint the following roles: T2-Staff-User. (Machine Authenticated! and T2-SOL-Device. What could cause this behavior?

A. The Enforcement Policy conditions for rule 1 are not configured correctly.

B. Used Cached Results: has not been enabled In the Aruba 802.1X Wireless Service

C. RFC-3576 Is not configured correctly on the Aruba Controller and does not update the role.

D. The Enforcement Profile should bounce the connection instead of a Terminate session

Correct Answer: B

QUESTION 4

You are integrating a Postgres SQL server with the ClearPass Policy Manager. What steps will you follow to complete the integration process? (Select three)

A. Click on the default filter name with pre-defined filter queries and check box to enable as role.

B. Specify a new filter with filter queries to fetch authentication and authorization attributes.

C. Attribute Name under filter configuration must match one of the columns being requested from the database table.

D. Create a new Endpoint context server and add the SQL server IP, credentilas and the database name.

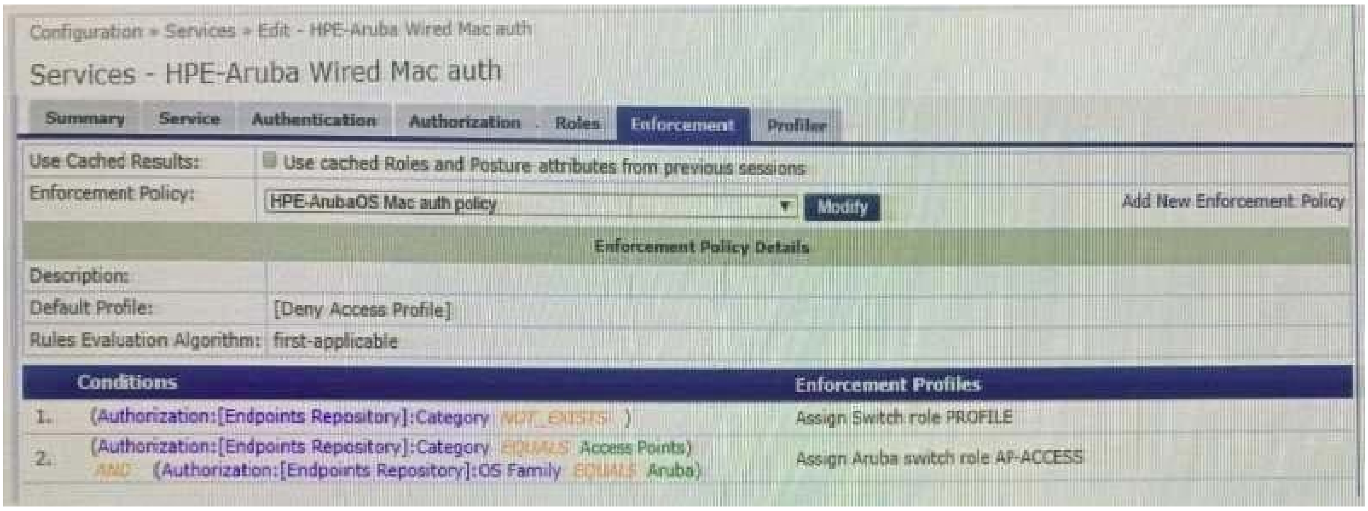
E. Alias Name under filter configuration must match one of the columns being requested from the database table.

F. Create a new authentication source and add the SQL server IP, credentials and the database name.

Correct Answer: BDF

QUESTION 5

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?



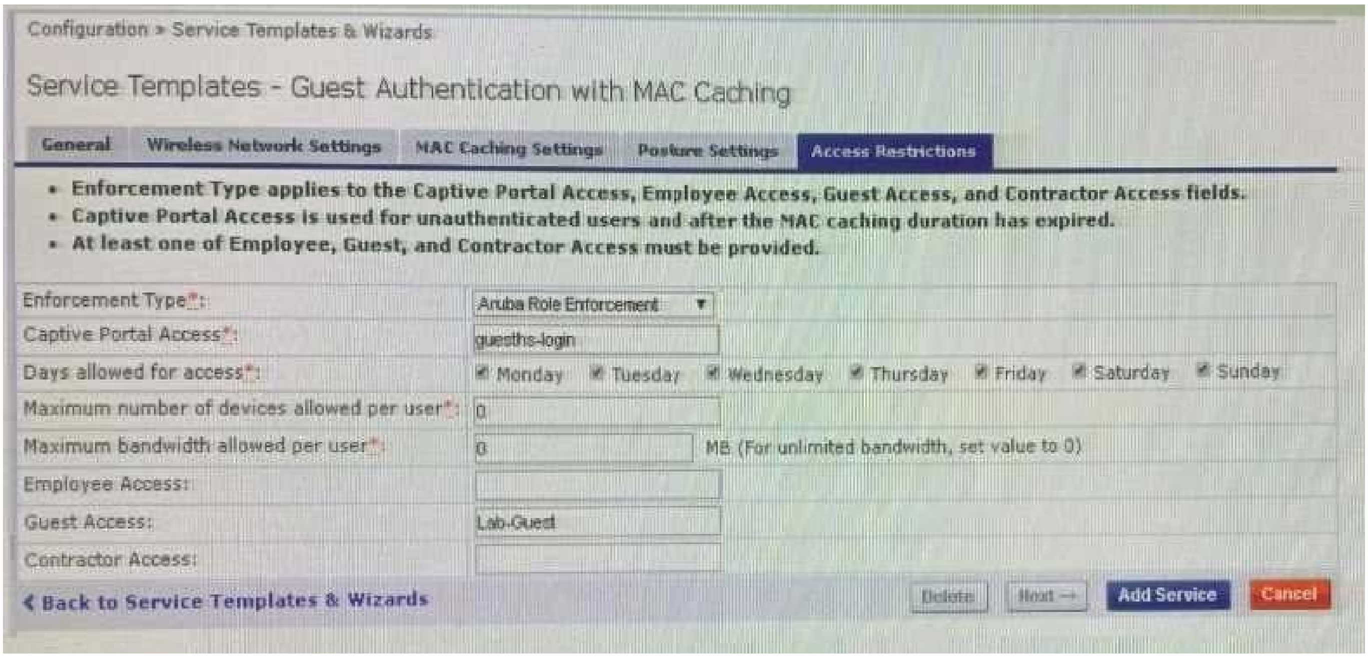
Services - HPE-Aruba Wired Mac auth

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

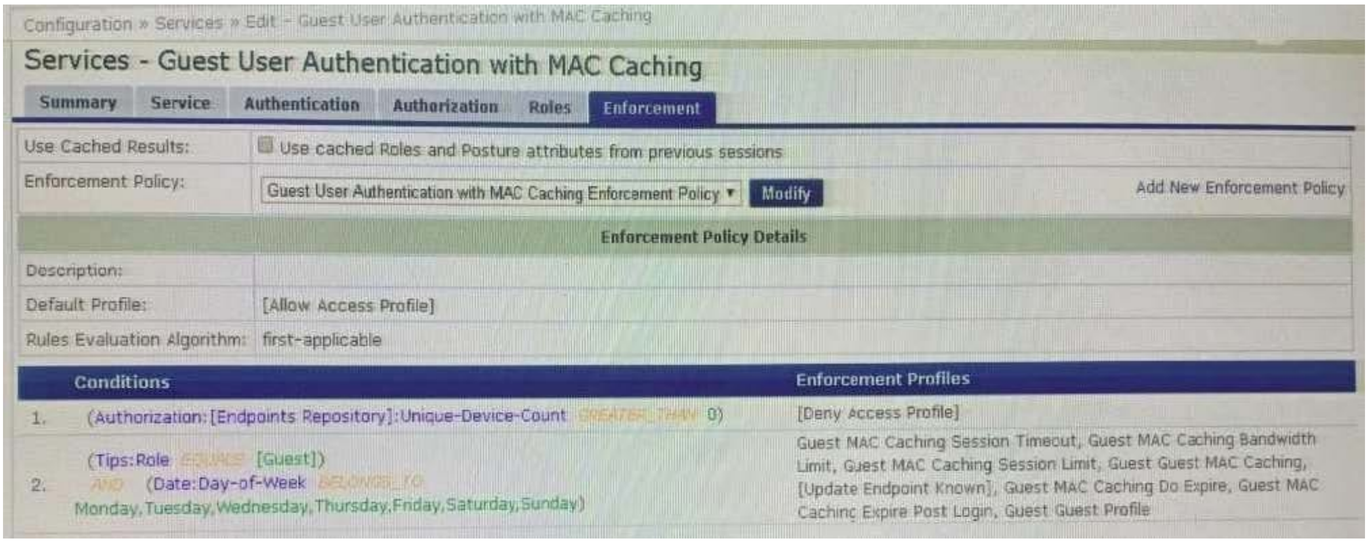


Configuration » Service Templates & Wizards

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 ▾ Modify

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 Caching 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

HPE6-A77 PDF Dumps HPE6-A77 VCE Dumps HPE6-A77 Exam Questions