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.passapply.com/hpe6-a77.html

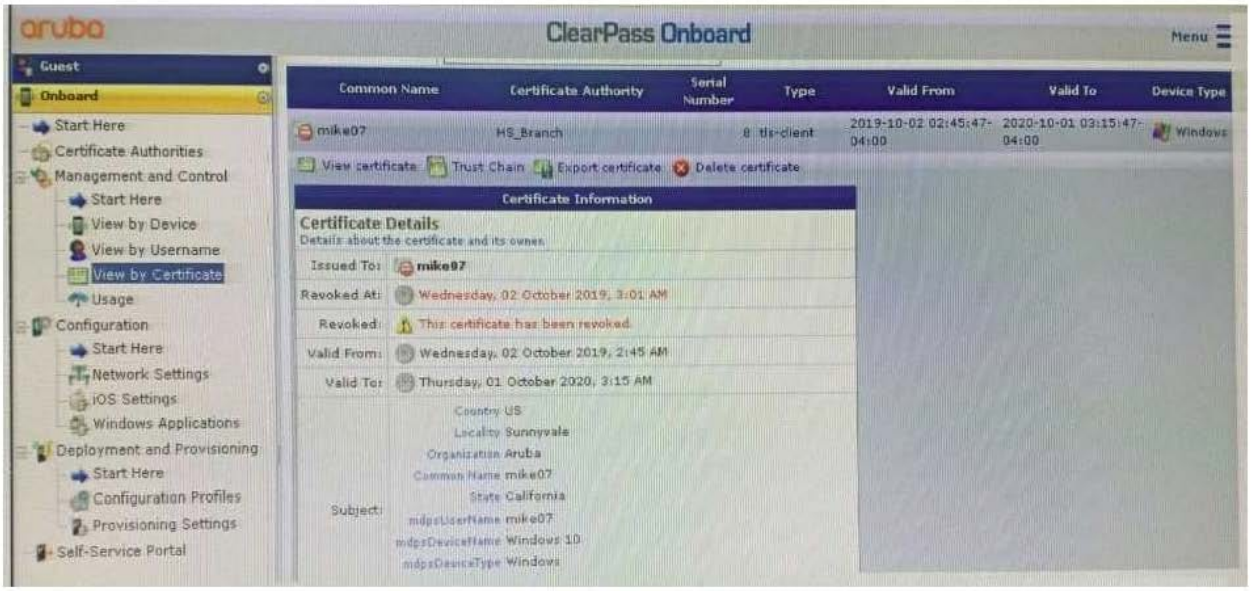
100% Passing Guarantee
100% Money Back Assurance

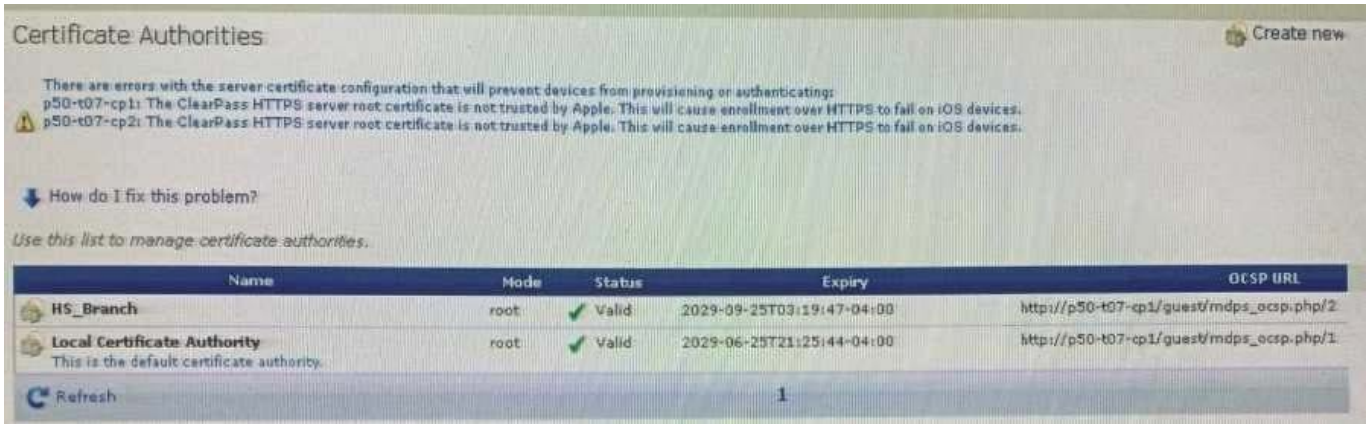
Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

Refer to the exhibit:


Monitoring » Live Monitoring » Access Tracker
Access Tracker Oct 02, 2019 03:43:03 EDT
Auto Refresh
The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.
[All Requests]
p50-t07-cp1 (10.1.79.1)
Last 1 day before Today
Edit
Filter: Login Status contains acc
Go
Clear Filter
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


aruba
ClearPass Onboard
Menu
Guest
Onboard
Start Here
Certificate Authorities
Management and Control
Start Here
View by Device
View by Username
View by Certificate
Usage
Configuration
Start Here
Network Settings
iOS Settings
Windows Applications
Deployment and Provisioning
Start Here
Configuration Profiles
Provisioning Settings
Self-Service Portal
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
View certificate Trust Chain Export certificate Delete certificate
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Revoked: This certificate has been revoked.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

Create new

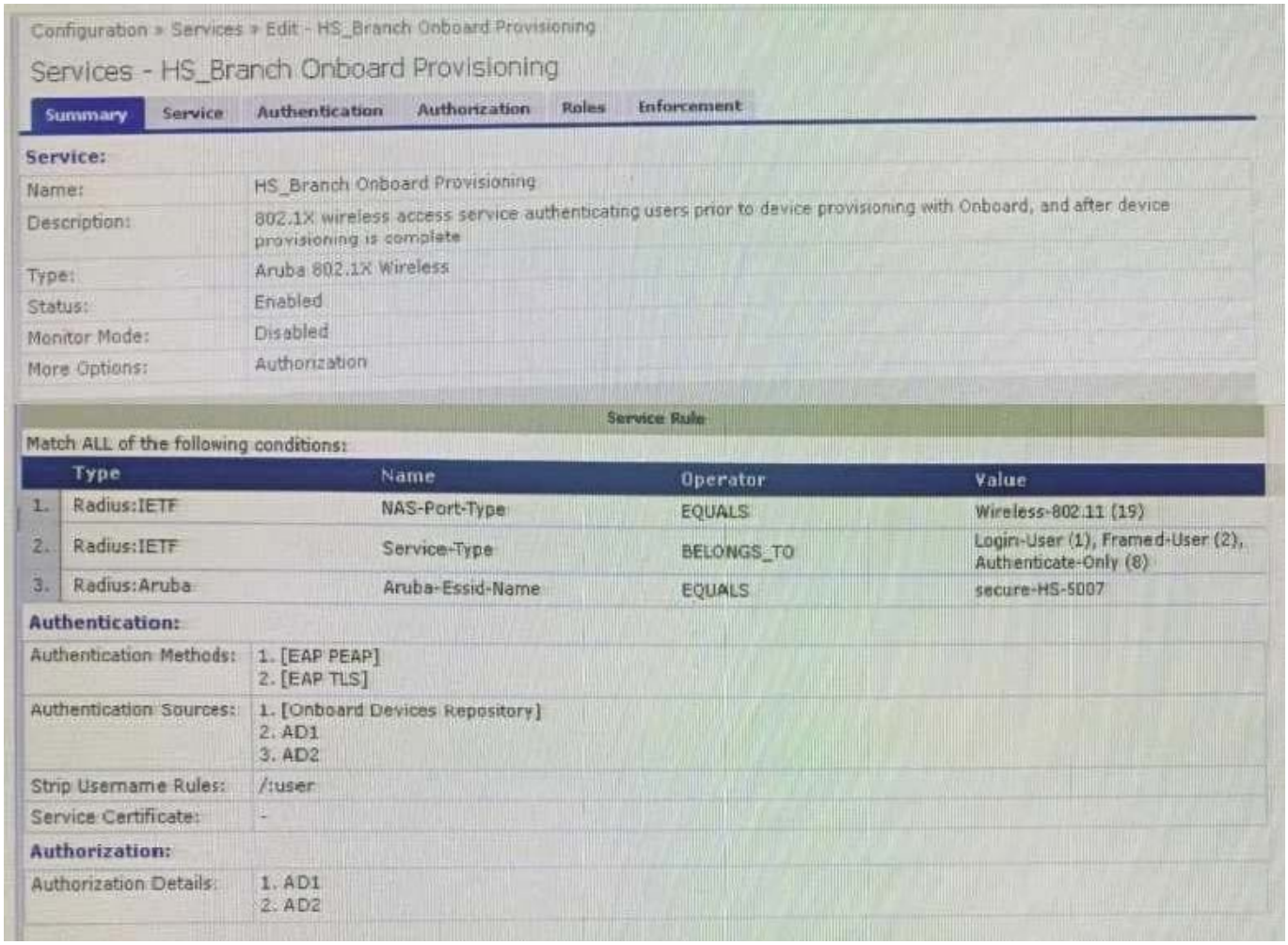
There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
p50-t07-cp1: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
p50-t07-cp2: The ClearPass HTTPS server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


Configuration » Services » Edit - HS_Branch Onboard Provisioning

Services - HS_Branch Onboard Provisioning

Summary | Service | Authentication | Authorization | Roles | Enforcement

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.

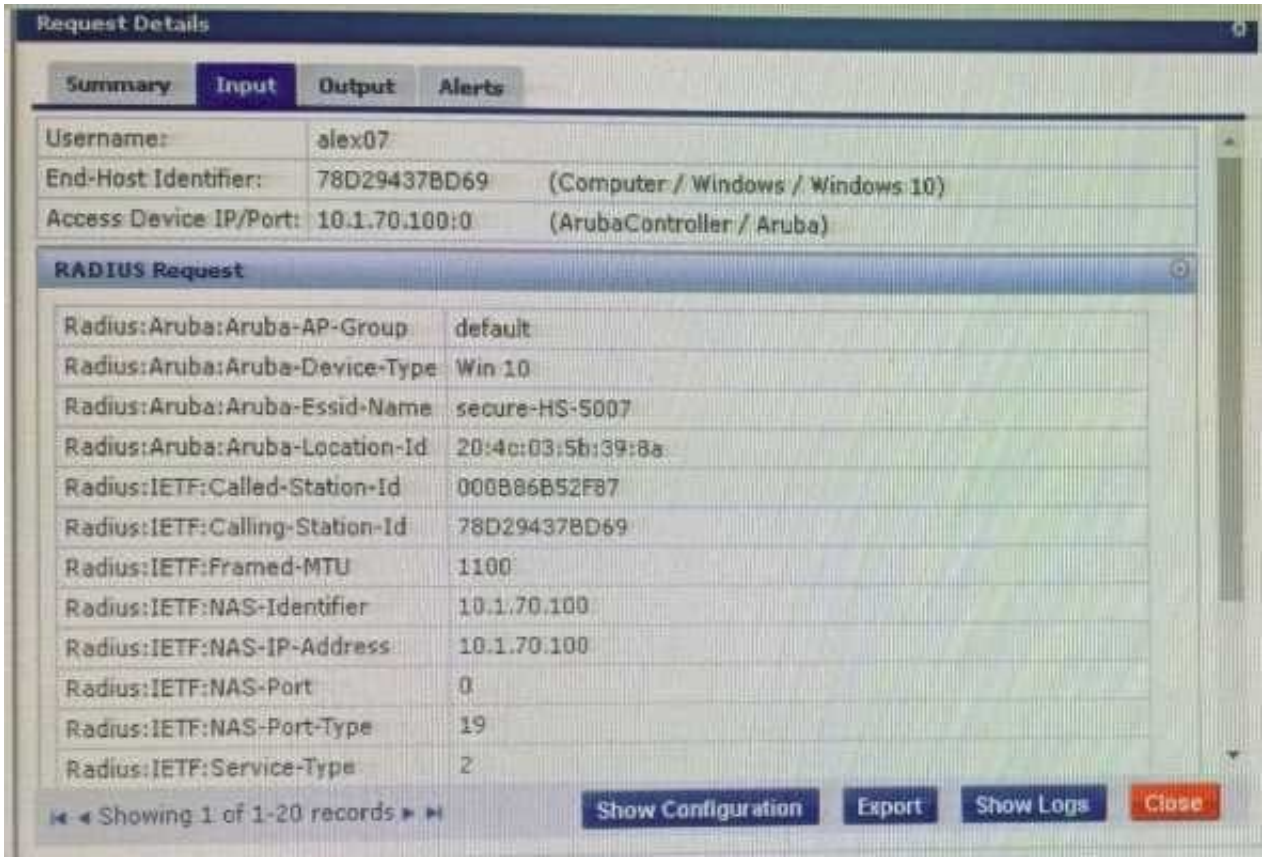
C. Remove the EAP-TLS authentication method configuration changes are required and add "EAP-TLS with OCSP Enabled" authentication method in the OnBoard Provisioning service. No other configuration changes are required.

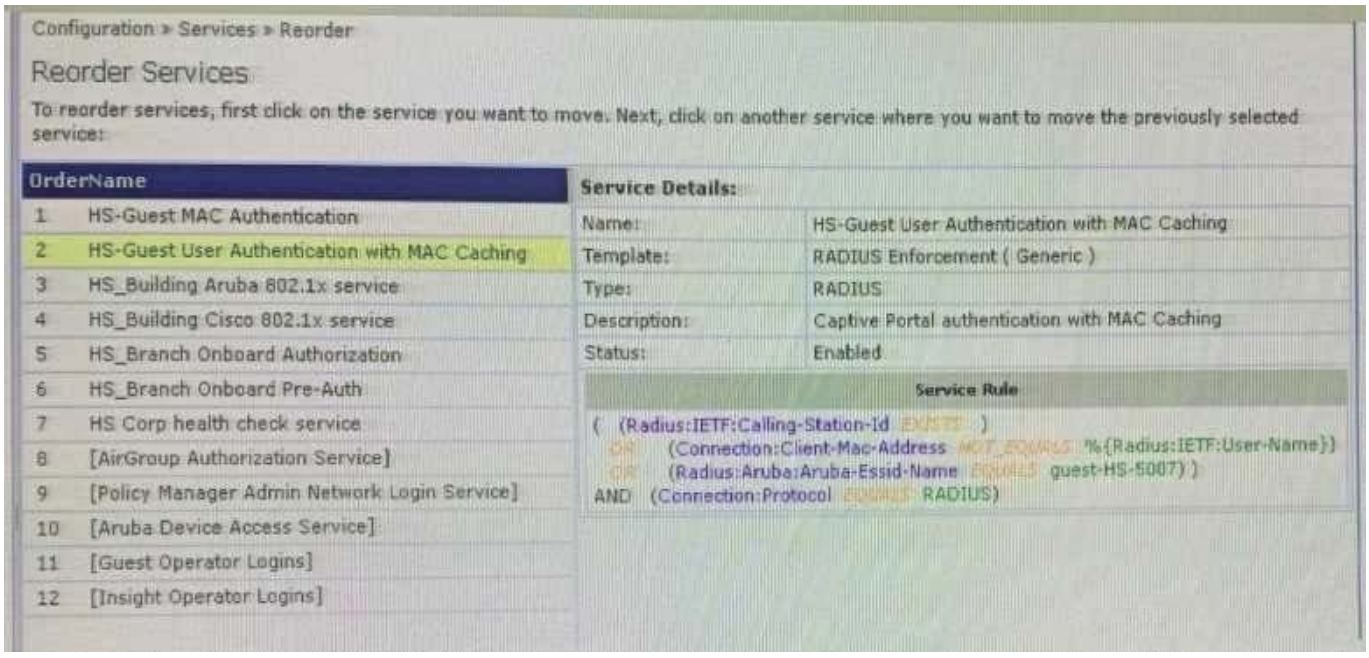
D. Edit the default [EAP-TLS with OSCP Enabled] authentication method and set the Verify certificate using OSCP option as required then update the correct OSCP URL link of the OnBoard CA Remove EAP-TLS and map the new [EAP-TLS with OSCP Enabled] method to the OnBoard Provisioning Service.

Correct Answer: C

QUESTION 2

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?





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 3

A customer has acquired another company that has its own Active Directory infrastructure The 802 1X authentication works with the customers original Active Directory servers but the customer would like to authenticate users from the acquired company as well. What steps are required, in regards to the Authentication Sources, in order to support this request? (Select two.)

A. Create a new Authentication Source, type Active Directory.

B. Join the ClearPass server(s) to the new AD domain.

C. Add the new AD server(s) as backup into the existing Authentication Source.

D. There is no need to Join ClearPass to the new AD domain.

E. Create a new Authentication Source, type Generic LDAP.

Correct Answer: BD

QUESTION 4

Refer to the exhibit:

A customer with multiple Aruba Controllers has just installed a new certificate for "*.customerdomain com" on all Aruba Controllers. While testing the existing guest Self-Registration page the customer noticed that the logins are failing. While troubleshooting they are finding no entries in the Event Viewer or Access Tracker for the tests. Suspecting that the Aruba Controllers may not be properly posting the credentials from the guest browser, they open the NAS Vendor Settings for the Guest Self-Registration Page. From the screen shown, how can you fix the errors?

A. Change the "IP Address: field to" securelogin.customerdomain.com.

B. Change the "Secure Login:" field to "Use Vendor Default".

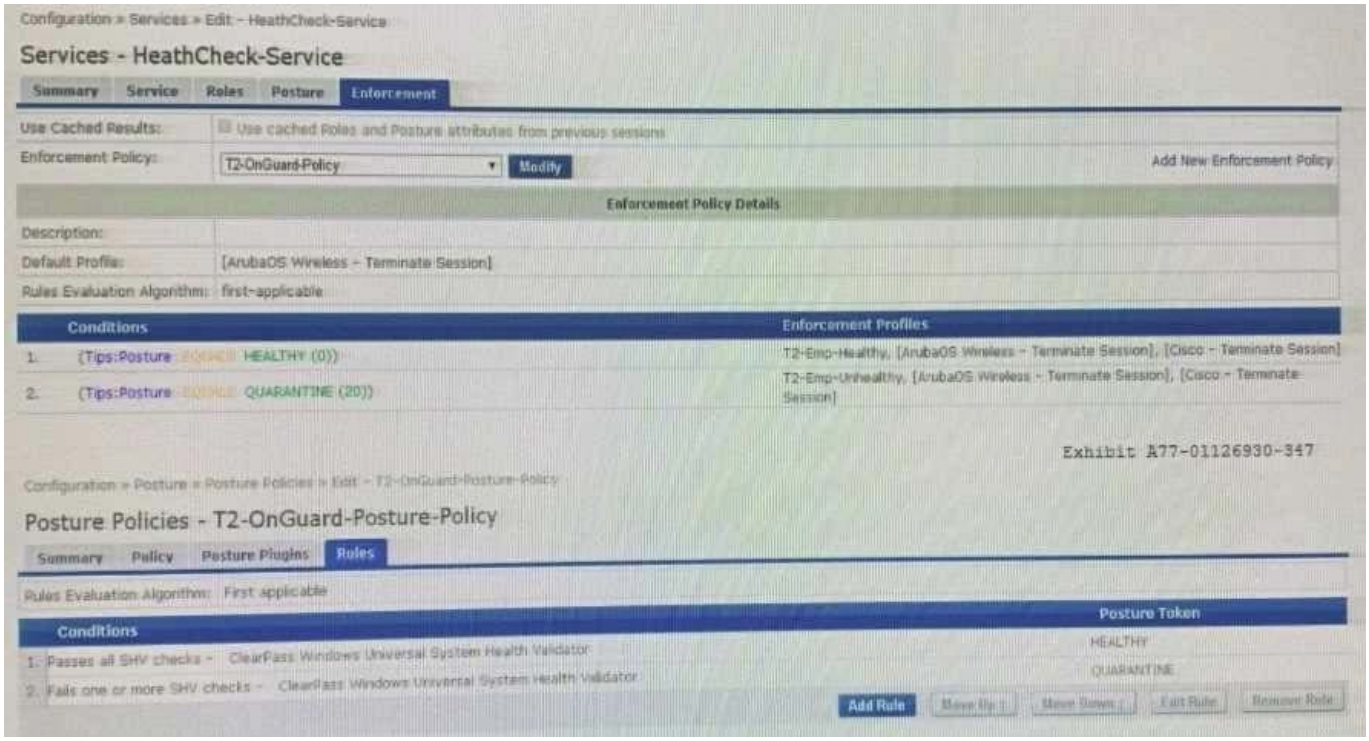
C. Change the "IP Address field to "captiveportal-login.customerdomain.com".

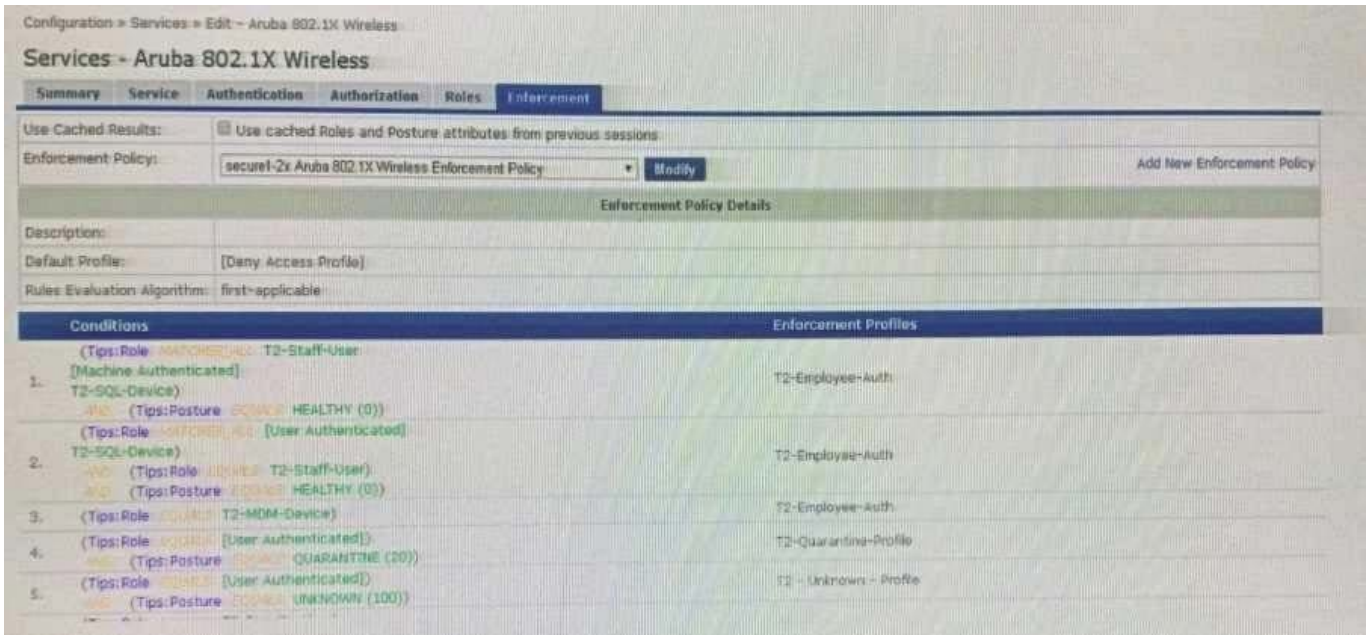
D. Add PTR records on the DNS server for "securelogin.arubanetworks.com".

Correct Answer: B

QUESTION 5

Refer to the Exhibit:





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