HPE6-A81$^{\text{Q\&As}}$

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

QUESTION 1

There is an Aruba Controller configured to send Guest AAA requests to ClearPass. If the customer would like the most effective way to ensure the lowest license usage counts, how should the controller be configured?

A. Aruba Controller will send stop messages only if EAP termination and Interim accounting are enabled.

B. Aruba Controller will send stop messages if RADIUS Accounting Server Group is defined in the authentication profile.

C. Aruba Controller will send stop messages only if both accounting and interim accounting are enabled.

D. Configure EAP Termination on the Aruba Controller and the client will send a stop message.

Correct Answer: D

QUESTION 2

You have integrated ClearPass Onboard with Active Directory Certificate Services (ADCS) web enrollment

to sign the final device TLS certificates. The customer would also like to use ADCS for centralized

management of TLS certificates including expiration, revocation, and deletion through ADCS.

What steps will you follow to complete the requirement?

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

B. Copy the [EAP-TLS with OSCP Enabled) authentication method and set the correct ADCS server OCSP URL, remove EAP-TLS and map the custom created method to the Onboard Provisioning Service.

C. Copy the default [EAP-TLS with OSCP Enabled] authentication method and update the correct ADCS server OCSP URL. remove EAP-TLS and map the custom created method to the OnBoard Authorization Service.

D. Edit the [EAP-TLS with OSCP Enabled) authentication method and set the correct ADCS server OCSP URL. remove EAP-TLS and map the [EAP-TLS with OSCP Enabled) method to the Onboard Provisioning Service.

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.

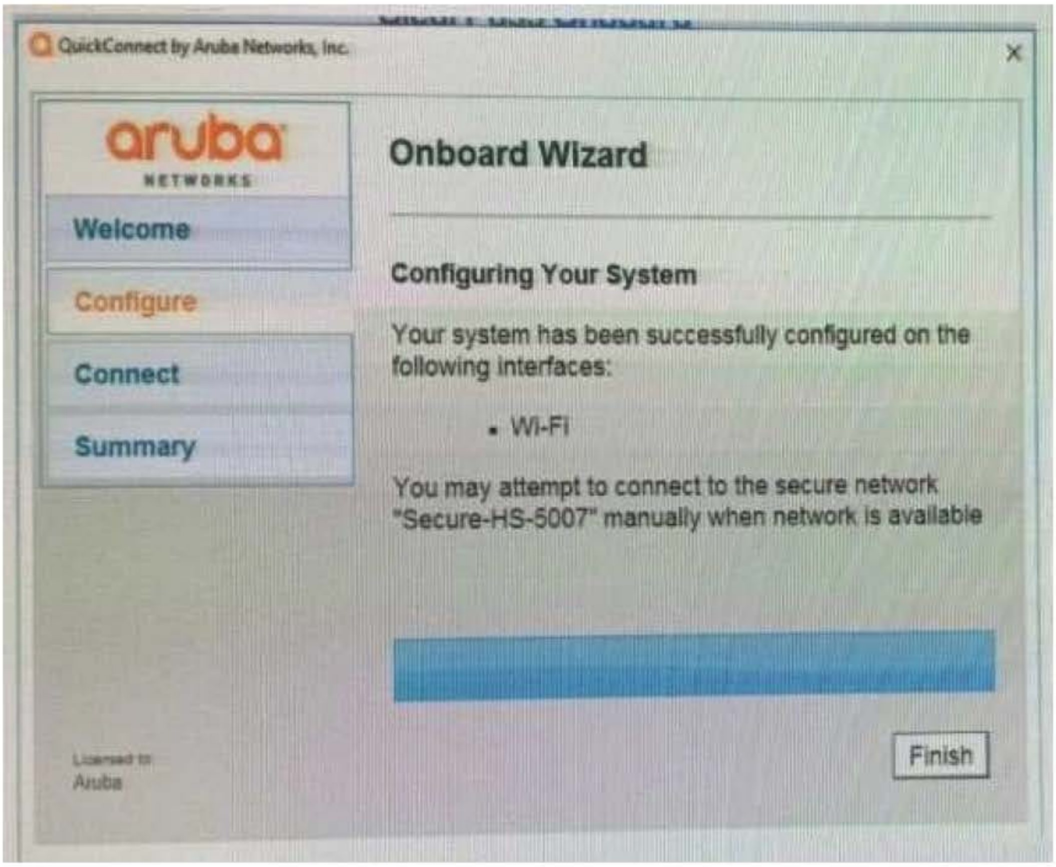
D. There is no need to Join ClearPass to the new AD domain.

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

Correct Answer: BD

QUESTION 4

Refer to the exhibit:



QuickConnect by Aruba Networks, Inc.

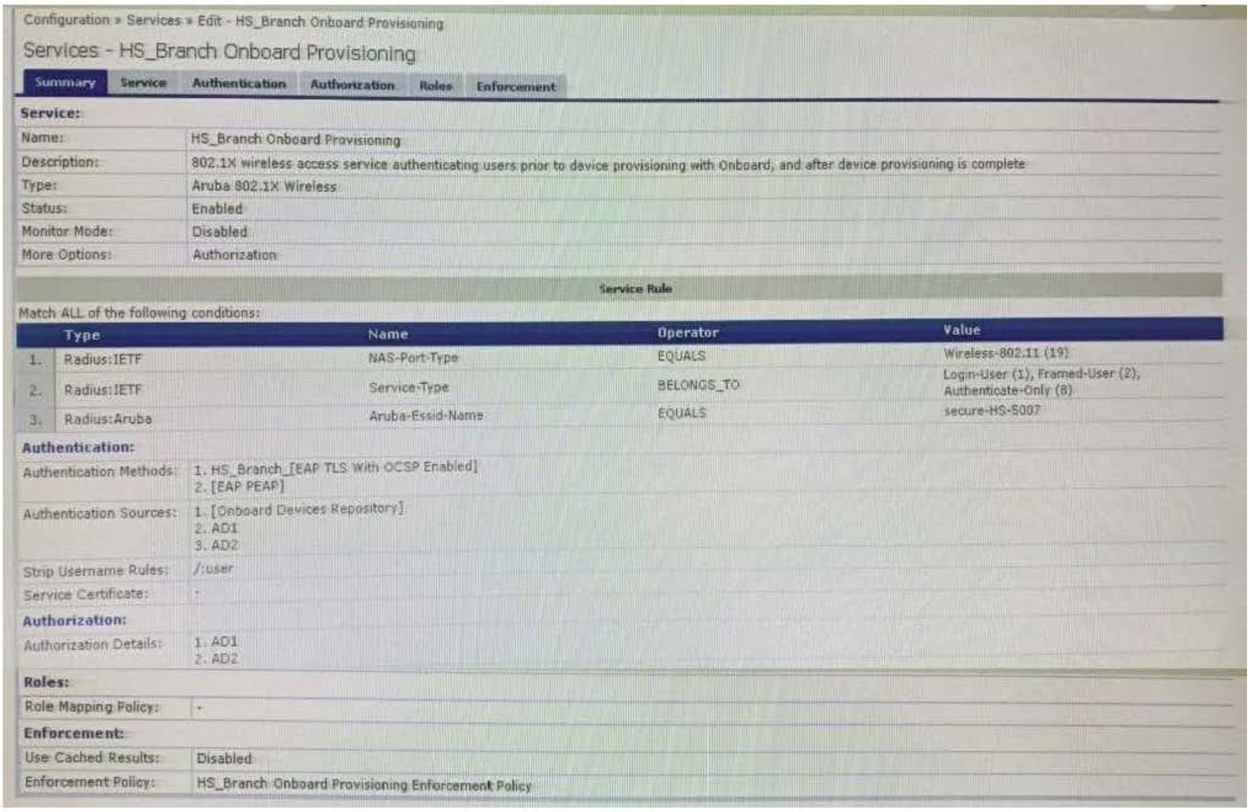
Onboard Wizard

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

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:

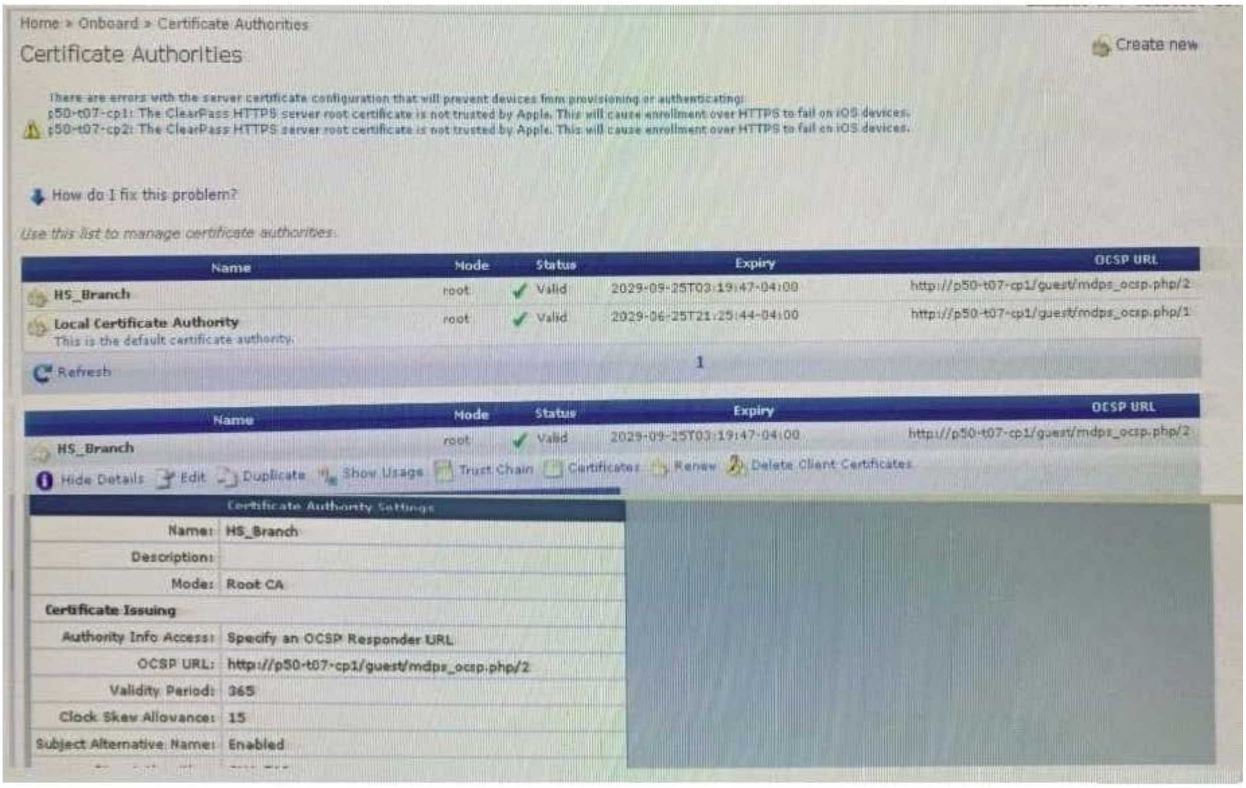
Authorization Details:	1. AD1 2. AD2

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.

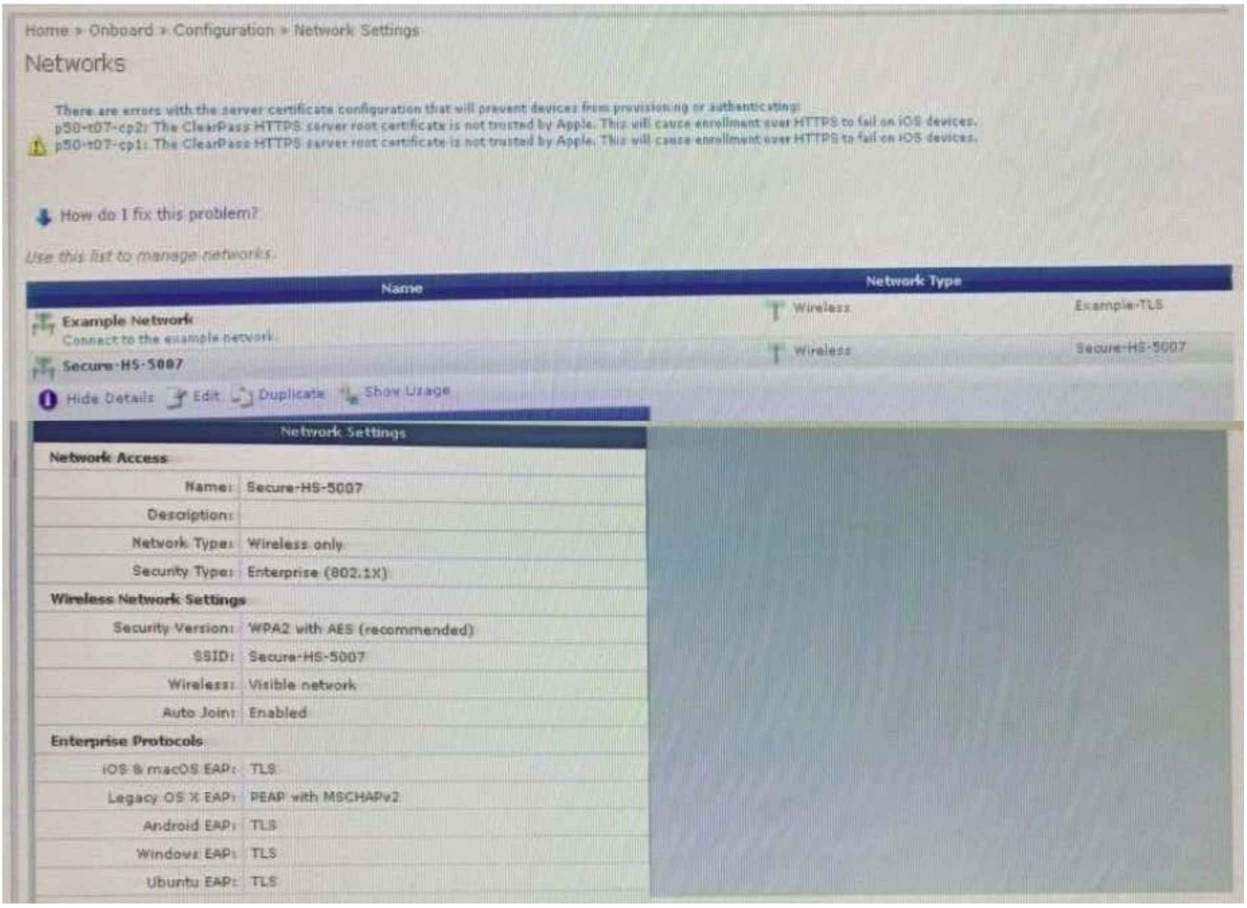
Name	Mode	Status	Expiry	OCSP URL
HS_Branch	root	✓ Valid	2029-09-25T03:19:47-04:00	http://p50-t07-cp1/guest/mdps_ocsp.php/2
Local Certificate Authority This is the default certificate authority.	root	✓ Valid	2029-06-25T21:25:44-04:00	http://p50-t07-cp1/guest/mdps_ocsp.php/1

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.

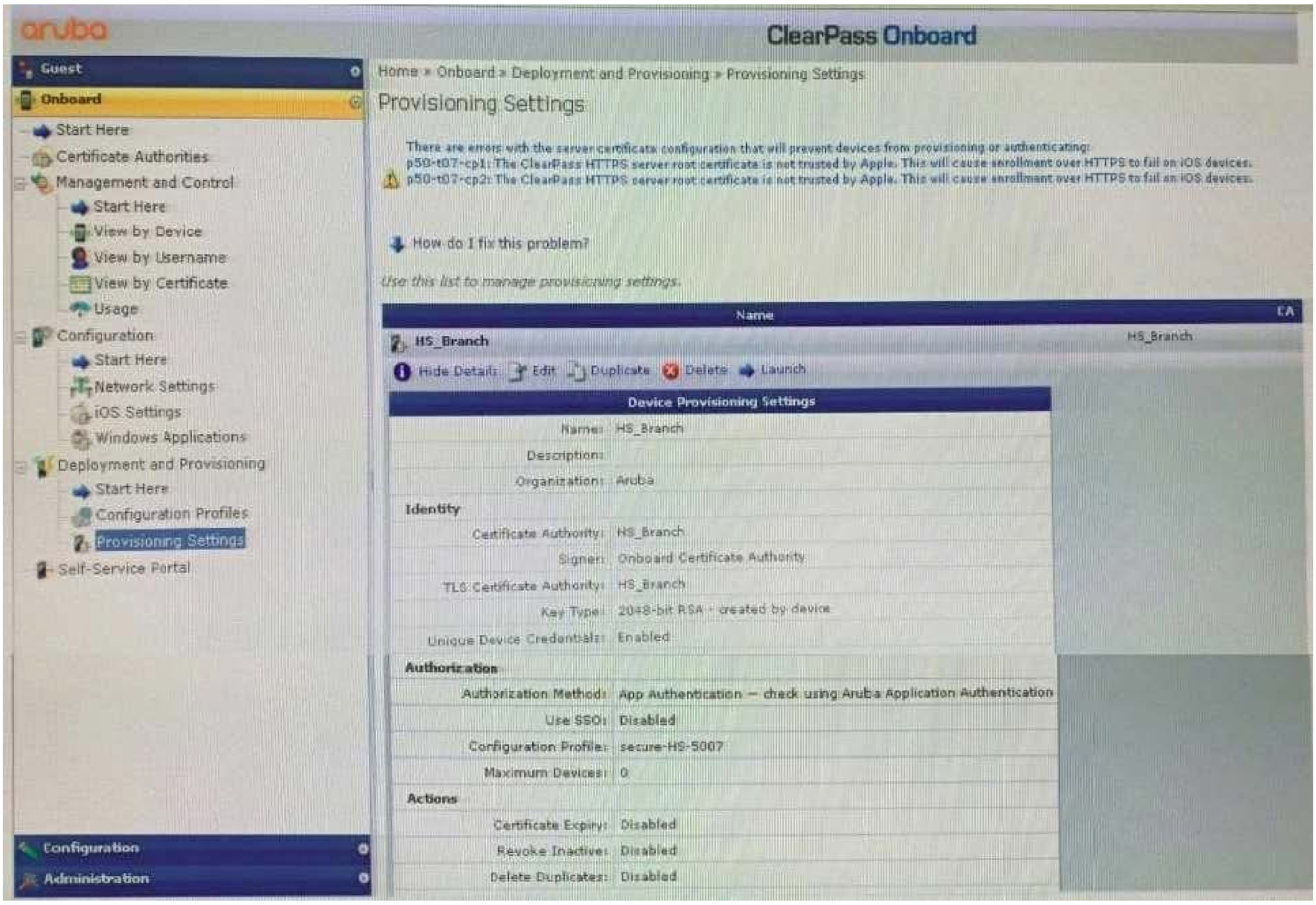
How do I fix this problem?

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 5

A customer has deployed an OnGuard Solution to all the corporate devices using a group policy rule to push the OnGuard Agents. The network administrator is complaining that some of the agents are communicating to the ClearPass server that is located in a DMZ, outside the firewall The network administrator wants all of the agents System Health Validation traffic to stay inside the Management subnets. What can the ClearPass administrator do to move the traffic only to the ClearPass Management Ports?

A. Edit the agent.conf file being deployed to the clients to use the ClearPass Management Port for SHV updates.

B. Select the correct OnGuard Agent installer, and use the one configured for Management Port for the clients.

C. Configure a Policy Manager Zone mapping so the OnGuard agent will use the Management Port IP.

D. Filter TCP port 6658 on the firewall, forcing the OnGuard agent to use the ClearPass Management port.

Correct Answer: C