# 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.pass2lead.com/hpe6-a81.html**

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

**QUESTION 1**

A customer has configured Onboard with Single SSID provision for Aruba IAP Windows devices work as expected but cannot get the Apple iOS devices to work. The Apple iOS devices automatically get redirected to a blank page and do not get the Onboard portal page. What would you check to fix the issue?

A. Verify if the checkbox "Enable bypassing the Apple Captive Network Assistant" is checked.

B. Verify if the Onboard URL is updated correctly in the external captive portal profile.

C. Verify if Onboard Pre-Provisioning enforcement profile sends the correct Aruba user role.

D. Verify if the external captive portal profile is enabled to use HTTPS with port 443.

Correct Answer: B

**QUESTION 2**

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 3**

A customer is complaining that some of the devices, in their manufacturing network, are not getting profiled while other loT devices from the same subnet have been correctly profiled. The network switches have been configured for DHCP IP helpers and IF-MAP has been configured on the Aruba Controllers. What can the customer do to discover those devices as well? (Select two.)

A. Update the Fingerprints Dictionary to the latest in case new devices have been added.

B. Open a TAC case to help you troubleshoot the DHCP device profile functionality.

C. Add the ClearPass Server IP as an IP helper address on the default gateway as well.

D. Allow time for IF-MAP service on the controller to discover the new devices as well.

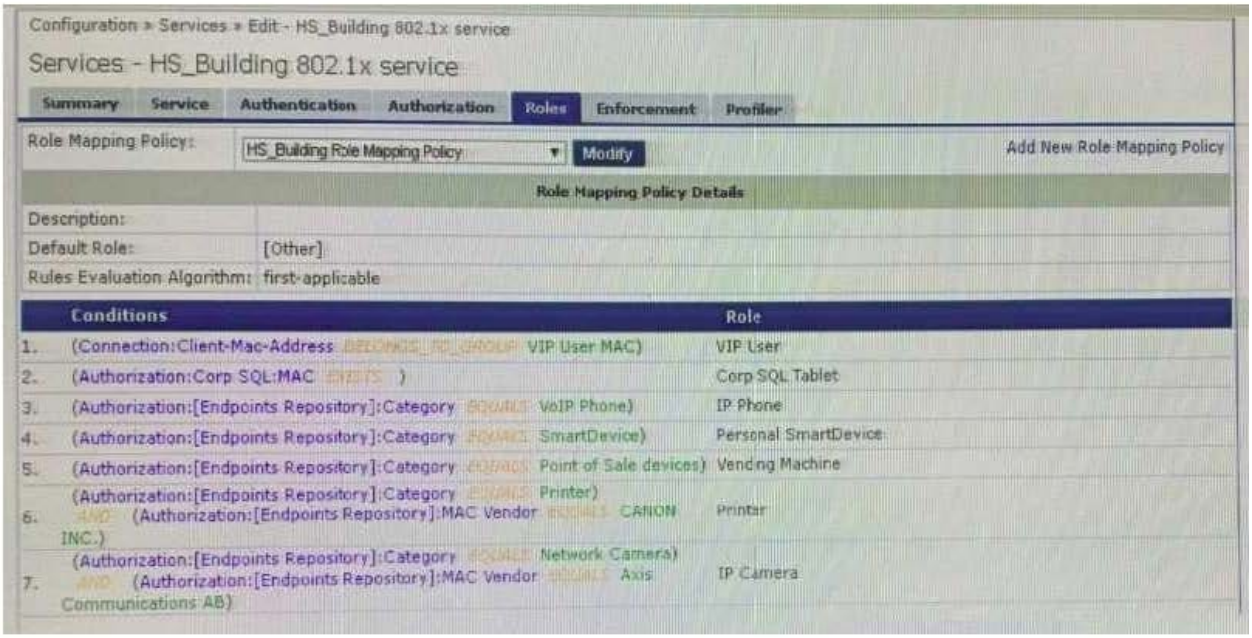
E. Manually create a new device fingerprint for the devices that are not being profiled.

Correct Answer: DE

**QUESTION 4**

Refer to the exhibit:


Request Details
Summary
Input
Output
Alerts
Login Status: ACCEPT
Session Identifier: R000001ae-01-5d9cb453
Date and Time: Oct 08, 2019 12:07:47 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,EAP-MSCHAPv2
Authentication Source: AD:AD1.aruba1.local
Authorization Source: [Endpoints Repository], AD1, AD2, Corp SQL
Roles: VIP User, [Machine Authenticated], [User Authenticated]
Enforcement Profiles: Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
Service Monitor Mode: Disabled
Online Status: Not Available
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Configuration » Services » Edit - HS_Building 802.1x service
Services - HS_Building 802.1x service
Summary
Service
Authentication
Authorization
Roles
Enforcement
Profiler
Role Mapping Policy:
HS_Building Role Mapping Policy
Modify
Add New Role Mapping Policy
Role Mapping Policy Details
Description:
Default Role: [Other]
Rules Evaluation Algorithm: first-applicable
Conditions
Role
1. (Connection:Client-Mac-Address VIP User MAC) VIP User
2. (Authorization:Corp SQL:MAC ) Corp SQL Tablet
3. (Authorization:[Endpoints Repository]:Category VoIP Phone) IP Phone
4. (Authorization:[Endpoints Repository]:Category SmartDevice) Personal SmartDevice
5. (Authorization:[Endpoints Repository]:Category Point of Sale devices) Vending Machine
6. (Authorization:[Endpoints Repository]:Category Printer) AND (Authorization:[Endpoints Repository]:MAC Vendor CANON INC.) Printer
7. (Authorization:[Endpoints Repository]:Category Network Camera) AND (Authorization:[Endpoints Repository]:MAC Vendor Axis Communications AB) IP Camera


The customer created a new enforcement policy condition to allow VIP Users access without additional security compliance checks hut cannot gel it working. The customer has sent you the above screenshots. How would you resolve the issue?

A. Ask the VIP user to complete the one time web health check to get the VIP profile.

B. Set the Enforcement Policy rules evaluation algorithm to evaluate all.

C. Include VIP User role along with the Healthy posture enforcement condition.

D. Modify the Enforcement Policy and re-order the VIP user condition to the lop.

Correct Answer: C

**QUESTION 5**

A customer has completed all the required configurations in the Windows server in order for Active Directory Certificate Services (ADCS) to sign Onboard device TLS certificates. The Onboard portal and the Onboard services are also configured. Testing shows that the Client certificates ate still signed by the Onboard Certificate Authority and not ADCS. How can you help the customer with the situation?

A. Educate the customer that, when integrating with Active Directory Certificate Services (ADCS) the Onboard CA will the same authority used for signing me final TLS certificate of the device.

B. Configure the identity certificate signer as Active Directory Certificate Services and enter the ADCS URL http://ADCSVVeoEnrollmentServemostname/certsrv in the OnBoard Provisioning settings.

C. Enable access to EST servers from the Certificate Authority to make ClearPass Onboard to use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

D. Enable access to SCEP servers from the Certificate Authority to make ClearPass Onboard to use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

Correct Answer: C