



# HPE6-A81<sup>Q&As</sup>

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.passapply.com/hpe6-a81.html>

100% Passing Guarantee  
100% Money Back Assurance

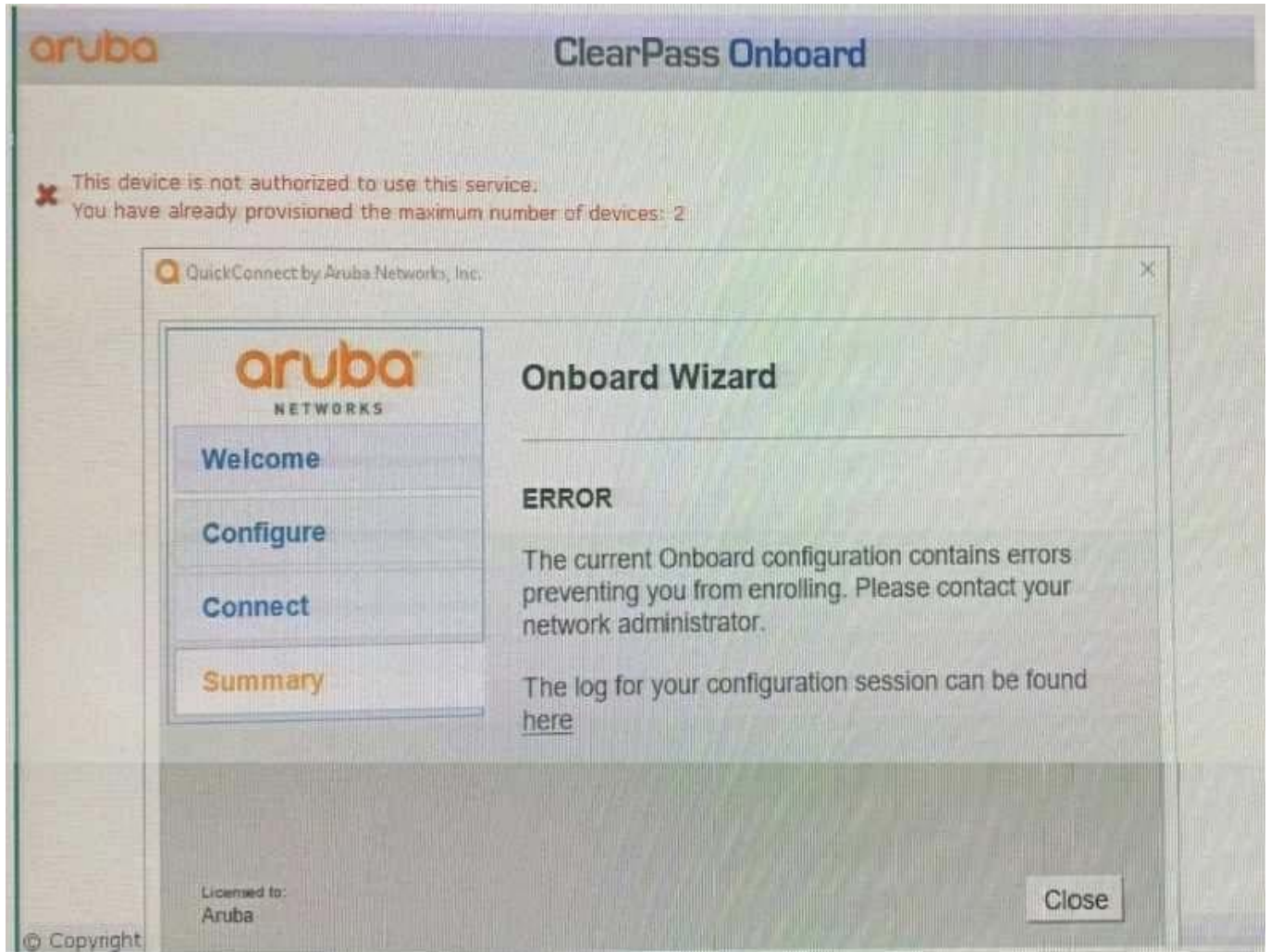
Following Questions and Answers are all new published by HP Official Exam Center

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



**QUESTION 1**

Refer to the exhibit: You have configured Onboard but the customer could not onboard one of his devices and has sent you the above screenshots. How could you resolve the issue?



- A. Instruct the user to delete the profile on one of their other BYOD devices.
- B. Instruct the user to run the Quick connect application in Sponsor Mode.
- C. Increase the maximum number of devices allowed by the individual user account.
- D. Increase the maximum number of devices that all users can provision to 3.

Correct Answer: D

**QUESTION 2**

Refer to the exhibit: A customer has configured a service with the Onboard Devices Repository as an Authentication Source and an Active Directory Domain Server as an Authorization Source. What will happen if the client certificate is



still valid and the user account associated with the certificate is disabled in Active Directory?

Configuration » Services » Edit - My\_organization\_ Onboard Provisioning

### Services - My\_organization\_ Onboard Provisioning

Summary Service Authentication Authorization Roles Enforcement

**Service:**

Name: My\_organization\_ 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	Home_SSID

**Authentication:**

Authentication Methods: [EAP-TLS With OCSP Enabled]

Authentication Methods: [EAP-TLS With OCSP Enabled]

Authentication Sources: [Onboard Devices Repository]

Strip Username Rules: /:user

Service Certificate: -

**Authorization:**

Authorization Details: AD1

**Roles:**

Role Mapping Policy: -

**Enforcement:**

Use Cached Results: Disabled

Enforcement Policy: My\_organization\_ Onboard Provisioning Enforcement Policy

◀ Back to Services

Disable Copy Save Cancel

- A. ClearPass will not process the request
- B. Enforcement will apply the [Deny Access Profile]
- C. ClearPass will redirect the client to Onboard again
- D. ClearPass will block network access to the device
- E. ClearPass will allow the device to access the network.

Correct Answer: D

### QUESTION 3

A customer has acquired another company that has its own Active Directory infrastructure. The 802.1X authentication works with the customer's 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

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 5

Refer to the exhibit:





**Customize Self-Registration**

**Login**  
Options controlling logging in for self-registered guests.

Enabled:

\* Vendor Settings:   
Select a predefined group of settings suitable for standard network configurations.

Login Method:   
Select how the user's network login will be handled.  
Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.

\* IP Address:   
Enter the IP address or hostname of the vendor's product here.

Secure Login:   
Select a security option to apply to the web login process.

Dynamic Address: ☐ The controller will send the IP to submit credentials  
In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

Security Hash:   
Select the level of checking to apply to URL parameters passed to the web login page.  
Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

**Default Destination**  
Options for controlling the destination clients will redirect to after login.

\* Default URL:   
Enter the default URL to redirect clients.  
Please ensure you prepend 'http://' for any external domain.

Override Destination: ☐ Force default destination for all clients  
If selected, the client's default destination will be overridden regardless of its value.

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

[Latest HPE6-A81 Dumps](#)

[HPE6-A81 PDF Dumps](#)

[HPE6-A81 Exam Questions](#)