

➤ **Vendor: HP**➤ **Exam Code: HPE6-A68**➤ **Exam Name: Aruba Certified ClearPass Professional Exam**➤ **New Updated Questions from [Braindump2go](#) (Updated in [April/2020](#))****Visit Braindump2go and Download Full Version HPE6-A68 Exam Dumps****QUESTION 11**

Refer to the exhibit. A user who is tagged with the ClearPass roles of Role\_Engineer and developer, but not testqa, connects to the network with a corporate Windows laptop.

Summary	Enforcement	Rules
<b>Enforcement:</b>		
Name:	Handled_Wireless_Access_Policy	
Description:	Enforcement policy for handled wireless access	
Enforcement Type:	RADIUS	
Default Profile:	WIRELESS_CAPTIVE_NETWORK	
<b>Rules:</b>		
Rules Evaluation Algorithm:	First applicable	
Conditions	Actions	
1. (Tips: Role MATCHES_ANY [guest])	WIRELESS_GUEST_NETWORK	
2. (Endpoint:Os Version CONTAINS Android)	WIRELESS_HANDLED_NETWORK	
(Tips: Role MATCHES_ANY conferencelaptop developer	WIRELESS_EMPLOYEE_NETWORK	
3. senior_mgmt		
testqa		
Role_Engineer)		

Which Enforcement Profile is applied?

- A. WIRELESS\_GUEST\_NETWORK
- B. WIRELESS\_CAPTIVE\_NETWORK
- C. WIRELESS\_HANDHELD\_NETWORK
- D. WIRELESS\_EMPLOYEE\_NETWORK

**Answer: D**

**QUESTION 12**

Which statement is true about the databases in ClearPass?

- A. Entries in the guest user database do not expire.
- B. A Static host list can only contain a list of IP addresses.
- C. Entries in the guest user database can be deleted.
- D. Entries in the local user database cannot be modified.
- E. The endpoints database can only be populated by manually adding MAC addresses to the

[HPE6-A68 Exam Dumps](#) [HPE6-A68 Exam Questions](#) [HPE6-A68 PDF Dumps](#) [HPE6-A68 VCE Dumps](#)

<https://www.braindump2go.com/hpe6-a68.html>

table.

**Answer: A**

**QUESTION 13**

Refer to the exhibit. When configuring a Web Login Page in Clear Pass Guest, the information shown is displayed.

Home » Configuration » Web Logins

## RADIUS Web Login

Use this form to make changes to the RADIUS Web Login **Guest Network**.

RADIUS Web Login Editor	
* Name:	<input style="width: 90%;" type="text" value="GuestNetwork"/> <small>Enter a name for this web login page.</small>
Page Name:	<input style="width: 90%;" type="text" value="Aruba_login"/> <small>Enter a name for this web login page. The web login will be accessible from "/guest/page_name.php".</small>
Description:	<div style="border: 1px solid #ccc; height: 30px; width: 100%;"></div> <small>Comments or descriptive text about the web login.</small>
* Vendor Settings:	<div style="border: 1px solid #ccc; padding: 2px;">Aruba Networks ▼</div> <small>Select a predefined group of settings suitable for standard network configurations.</small>
Address:	<input style="width: 90%;" type="text" value="securelogin.arubanetworks.com"/> <small>Enter the IP address or hostname of the vendor's product here.</small>
Secure Login:	<div style="border: 1px solid #ccc; padding: 2px;">Use Vendor default ▼</div> <small>Select a security option to apply to the web login process.</small>
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials <small>In multi-controller deployments, it is often required to post credentials to different add The address above will be used whenever the parameter is not available or fails the r</small>

What is the page name field used for?

- A. For Administrators to access the PHP page, but not guests.
- B. For forming the Web Login Page URL.
- C. For forming the Web Login Page URL where Administrators add guest users.
- D. For Administrators to reference the page only.
- E. For forming the Web Login Page URL and the page name that guests must configure on their laptop wireless supplicant.

**Answer: B**

**QUESTION 14**

Refer to the exhibit. Based on the configuration for the client's certificate private key as shown, which statements accurately describe the settings? (Choose two.)

Device Provisioning Settings	
General	Web Login
iOS	iOS & OS X
Legacy OS X	Windows
Android	Onboard Client
*Name:	Local Device Provisioning <small>Enter a name for this configuration set.</small>
Description:	This is the default configuration set for device provisioning. <small>Enter a description for the configuration set.</small>
*Organization:	Example Organization <small>Enter an organization name for this configuration set. The organization name is displayed by the device during provisioning.</small>
<b>Identity</b> <small>These options control the generation of device credentials</small>	
* Certificate Authority:	Local Certificate Authority <small>Select the certificate authority that will be used to sign profiles and messages.</small>
* Signer:	Onboard Certificate Authority <small>Select the source that will be use to sign TLS client certificates.</small>
* Key Type:	1024-bit RSA - created by device <small>Select the type of private key to use for TLS certificates.</small>
* Unique Device Credentials:	<input checked="" type="checkbox"/> Include the username in unique device credentials <small>When checked, the username is prefixed to the device's PEAP credentials. This unique set of credentials is used to identify the user and device on the network.</small>

- A. More bits in the private key will increase security.
- B. The private key for TLS client certificates is not created.
- C. The private key is stored in the ClearPass server.
- D. More bits in the private key will reduce security.
- E. The private key is stored in the user device.

**Answer:** AE

**QUESTION 15**

Refer to the exhibit. A user logged in to the Self-Service Portal as shown.

**ARUBA**  
networks

ClearPass

## Customer Service

ClearPass

Welcome to the visitor portal, guest1.



Username: **guest1@abc.com**



**Your account has expired.**



Your IP address: **172.16.199.168**



Last network login: **2013-03-08 03:33**



Traffic received: **94.7 KB**

**MB**



Traffic sent: **51.2 KB**

**MB**



[Change your password](#)



[Log out of self-service](#)

What does the traffic received and sent statistics present?

- A. These show the total amount of traffic the guest transmitted, as seen through RADIUS CoA packets from the NAD to ClearPass.
- B. These show the total amount of traffic the NAD transmitted to ClearPass, as seen through RADIUS accounting messages from the NAD to ClearPass.
- C. These show the total amount of traffic the guest transmitted after account expiration, as seen through RADIUS accounting messages sent from the NAD to ClearPass.

[HPE6-A68 Exam Dumps](#) [HPE6-A68 Exam Questions](#) [HPE6-A68 PDF Dumps](#) [HPE6-A68 VCE Dumps](#)

<https://www.braindump2go.com/hpe6-a68.html>

- D. These show the total amount of traffic the guest transmitted, as seen through RADIUS CoA packets from the client to ClearPass.
- E. These show the total amount of traffic the guest transmitted, as seen through RADIUS accounting messages sent from the NAD to ClearPass.

**Answer: E**

**QUESTION 16**

A University wants to deploy ClearPass with the Guest module. They have two types of users that need to use web login authentication. The first type of users are students whose accounts are in Active Directory server. The second type of user are friends of students who need to self-register to access the network. How should the service be setup in the Policy Manager for this Network?

- A. Either the Guest User Repository or Active Directory server should be the single authentication source.
- B. Guest User Repository as the authentication source, and Guest User Repository and Active Directory server as authentication sources.
- C. Guest User Repository as the authentication source and the Active Directory server as authentication source.
- D. Active Directory server as authentication source and the Guest User Repository as the authentication source.
- E. Guest User Repository and Active Directory server both as authentication sources.

**Answer: E**

**QUESTION 17**

Refer to the exhibit. What does the Cache Timeout Value refer to?



## Authentication Sources - remotelab AD

Summary	General	Primary	Attributes
Name:	retemotelab AD		
Description:			
Type:	Active Directory		
User for Authorization:	<input checked="" type="checkbox"/> Enable to use this authentication source to		
Authorization Sources:	<div></div> <div>-- Select --</div>		
Server Timeout:	10	seconds	
Cache Timeout:	36000	seconds	
Backup Servers Priority:			

- A. The amount of time the Policy Manager caches the user credentials stored in the Active Directory.
- B. The amount of time the Policy Manager waits for a response from the Active Directory before checking the backup authentication source.
- C. The amount of time the Policy Manager caches the user attributes fetched from Active Directory.
- D. The amount of time the Policy Manager waits for response from the Active Directory before sending a timeout message to the Network Access Device.
- E. The amount of time the Policy Manager caches the user's client certificate.

**Answer: C**

### QUESTION 18

Which components of a ClearPass is mandatory?

- A. Authorization Source
- B. Enforcement
- C. Profiler
- D. Role Mapping Policy
- E. Posture

**Answer: B**

**QUESTION 19**

Which is a valid policy simulation types in ClearPass? (Choose three.)

- A. Enforcement Policy
- B. Posture token derivation
- C. Role Mapping
- D. Endpoint Profiler
- E. Chained simulation

**Answer:** ACE

**QUESTION 20**

Which needs to be validated for a successful EAP-TLS authentication? (Choose two.)

- A. WPA2-PSK
- B. Username and Password
- C. Client Certificate
- D. Server Certificate
- E. Pre-shared key

**Answer:** CD