

ACCP-V6.2^{Q&As}

Aruba Certified Clearpass Professional v6.2

Pass Aruba ACCP-V6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/accp-v6-2.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



QUESTION 1

Which of the following devices support Apple over-the-air provisioning? (Choose 2)

- A. Laptop running Mac OS X 10.6
- B. Laptop running Mac OS X 10.8
- C. iOS 5
- D. Android 2.2
- E. Windows XP

Correct Answer: BC

QUESTION 2

Refer to the screen capture below: Based upon Endpoint information shown here, which collectors were used to profile the device as Apple iPad? (Choose 2)

View Endpoint			
MAC Address	98b8e362fddf	IP Address	192.168.1.252
Description		Static IP	FALSE
Status	Unknown	Hostname	
Added by	Policy Manager	MAC Vendor	Apple
		Category	SmartDevice
		OS Family	Apple
		Device Name	Apple iPad
		Updated At	Apr 10, 2013 19:47:28 UTC
		Show Fingerprint	<input checked="" type="checkbox"/>

Endpoint Fingerprint Details	
Host User Agent	Mozilla/5.0 (iPad; CPU OS 6_0_2 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A8500 Safari/8536.25
DHCP Option55	["1,3,6,15,119,252"]
DHCP Options	["53,55,57,61,50,51,12"]

- A. OnGuard Agent
- B. HTTP User-Agent
- C. DHCP fingerprinting
- D. SNMP
- E. SmartDevice

Correct Answer: BC

QUESTION 3

What must be configured to enable RADIUS authentication with Clearpass on a network access device (NAD)? (Choose 2)

- A. An NTP server needs to be set up on the NAD.
- B. A bind username and bind password must be provided.
- C. A shared secret must be configured on the Clearpass server and NAD.
- D. The Clearpass server must have the network device added as a valid NAD.
- E. The Clearpass server certificate must be installed on the NAD.

Correct Answer: CD

QUESTION 4

Refer to the screen capture below: Based on the Enforcement Policy configuration, if a user connects to the network using an Apple iphone, what Enforcement Profile is applied?

Summary	Enforcement	Rules
Enforcement:		
Name:	Handheld_Wireless_Access_Policy	
Description:	Enforcement policy for handheld wireless access	
Enforcement Type:	RADIUS	
Default Profile:	WIRELESS_CAPTIVE_NETWORK	
Rules:		
Rules Evaluation Algorithm:	First applicable	
Conditions		Actions
1.	(Tips:Role MATCHES_ANY [guest])	WIRELESS_GUEST_NETWORK
2.	(Endpoint:OS Version CONTAINS Android)	WIRELESS_HANDHELD_NETWORK
3.	(Tips:Role MATCHES_ANY conferencelaptop developer senior_mgmt testqa Role_Engineer)	WIRELESS_EMPLOYEE_NETWORK

- A. WIRELESS_CAPTIVE_NETWORK
- B. WIRELESS_HANDHELD_NETWORK
- C. WIRELESS_GUEST_NETWORK
- D. WIRELESS_EMPLOYEE_NETWORK
- E. Deny Access

Correct Answer: A

QUESTION 5

Below is a screenshot of a client connecting to a Guest SSID:



Based on the image shown above, which of the following best describes the client's state?

- A. The client authenticated through the web login page first before it was able to obtain an IP address.
- B. The client does not have an IP address, but they have authenticated through the web login page.
- C. The client does not have an IP address because they have not authenticated through the web login page yet.
- D. We can't tell from the image above.

Correct Answer: D

QUESTION 6

Which of the following is TRUE of dual-SSID onboarding?

- A. The device connects to the secure SSID for provisioning
- B. The Onboard Authorization service is triggered when the user connects to the secure SSID
- C. The Onboard Provisioning service is triggered when the user connects to the Provisioning SSID

D. The Onboard Authorization service is triggered during the Onboarding process

E. The Onboard Authorization service is never triggered

Correct Answer: D

QUESTION 7

Which of the following components of a Policy Service is mandatory?

A. Enforcement

B. Posture

C. Profiler

D. Role Mapping Policy

E. Authorization Source

Correct Answer: A

QUESTION 8

Refer to the screenshot in the diagram below, as seen when configuring a Web Login Page in ClearPass Guest:

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 type="text" value="Guest Network"/> Enter a name for this web login page.
Page Name:	<input type="text" value="Aruba_login"/> Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	<input type="text"/> Comments or descriptive text about the web login.
* Vendor Settings:	<input type="text" value="Aruba Networks"/> Select a predefined group of settings suitable for standard network configurations.
Address:	<input type="text" value="securelogin.arubanetworks.com"/> Enter the IP address or hostname of the vendor's product here.
Secure Login:	<input type="text" value="Use vendor default"/> Select a security option to apply to the web login process.
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials 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

What is the page name field used for?

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

Correct Answer: C

QUESTION 9

An Android device goes through the single-ssid onboarding process and successfully connects using EAPTLS to the secure network. What is the order in which services are triggered?

- A. Onboard Provisioning, Onboard Authorization

B. Onboard Provisioning, Onboard Authorization, Onboard Provisioning

C. Onboard Authorization, Onboard Provisioning

D. Onboard Authorization, Onboard Provisioning, Onboard Authorization

E. Onboard Provisioning

Correct Answer: B

QUESTION 10

Refer to the screenshot below: Which of the following statements is correct regarding the above configuration for the private key? (Choose 2)

Device Provisioning Settings	
<div> General Web Login iOS iOS & OS X Legacy OS X Windows Android Onboard Client </div>	
* 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>
Identity <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 used 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. The private key is stored in the user device.

B. The private key is stored in the ClearPass server.

C. More bits in the private key will reduce security, hence smallest private key size is used.

D. More bits in the private key will increase the processing time, hence smallest private key size is used.

E. The private key for TLS client certificates is not created.

Correct Answer: AD

QUESTION 11

Which of the following information is NOT required while building a Policy Service for 802.1X authentication?

- A. Network Access Device used
- B. Authentication Method used
- C. Authentication Source used
- D. Posture Token of the client
- E. Profiling information of the client

Correct Answer: D

QUESTION 12

Refer to the screenshot below:



Which of the following statements is correct regarding the above configuration for '\\maximum devices\\'?

- A. It limits the total number of Onboarded devices connected to the network.
- B. It limits the total number of devices that can be provisioned by ClearPass.
- C. It limits the number of devices that a single user can Onboard.
- D. It limits the number of devices that a single user can connect to the network.
- E. With this setting, the user cannot Onboard any devices.

Correct Answer: C

QUESTION 13

Refer to the screen capture below: 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. What Enforcement Profile is applied?

Summary	Enforcement	Rules
Enforcement:		
Name:	Handheld_Wireless_Access_Policy	
Description:	Enforcement policy for handheld wireless access	
Enforcement Type:	RADIUS	
Default Profile:	WIRELESS_CAPTIVE_NETWORK	
Rules:		
Rules Evaluation Algorithm:	First applicable	
Conditions	Actions	
1. (Tips:Role MATCHES_ANY [guest])	WIRELESS_GUEST_NETWORK	
2. (Endpoint:OS Version CONTAINS Android)	WIRELESS_HANDHELD_NETWORK	
(Tips:Role MATCHES_ANY conferencelaptop developer		
3. senior_mgmt	WIRELESS_EMPLOYEE_NETWORK	
testqa		
Role_Engineer)		

- A. WIRELESS_CAPTIVE_NETWORK
- B. WIRELESS_HANDHELD_NETWORK
- C. WIRELESS_GUEST_NETWORK
- D. WIRELESS_EMPLOYEE_NETWORK
- E. Deny Access

Correct Answer: D

QUESTION 14

Describe the purpose of the Aruba TACACS+ dictionary as shown here:

Administration » Dictionaries » TACACS+ Services

TACACS+ Services Dictionaries

TACACS+ Service Dictionary Attributes				
Display Name:		Aruba:Common		
#	Name	Display Name	Type	Allowed Values
1.	Aruba-Admin-Role	Aruba-Admin-Role	String	root, read-only, location-api-mgmt, network-operations, guest-provisioning, no-access
Close				

- A. The Aruba-Admin-Role attribute is used to assign different privileges to clients during 802.1X authentication.
- B. The Aruba-Admin-Role attribute is used by ClearPass to assign TIPS roles to clients during 802.1X authentication.
- C. The Aruba-Admin-Role attribute is used to assign different privileges to administrators logging into an Aruba NAD device.
- D. The Aruba-Admin-Role attribute is used to assign different privileges to administrators logging into ClearPass.
- E. The Aruba-Admin-Role on the controller is applied to users using TACACS+ to login to the Policy Manager.

Correct Answer: C

QUESTION 15

Which of the following options is the correct order of steps of a Policy Service request?

- 1) Clearpass tests the request against Service Rules to select a Policy Service.
- 2) Clearpass applies the Enforcement Policy.
- 3) Negotiation of the Authentication Method occurs between the NAD and Clearpass.

4) Clearpass sends the Enforcement Profile attributes to the NAD.

5) NAD forwards authentication request to Clearpass.

A. 1, 3, 2, 4, 5

B. 5, 1, 3, 2, 4

C. 5, 1, 3, 4, 2

D. 1, 2, 3, 4, 5

E. 2, 3, 4, 5, 1

Correct Answer: B

[ACCP-V6.2 PDF Dumps](#)

[ACCP-V6.2 Exam
Questions](#)

[ACCP-V6.2 Braindumps](#)