



# ACCP-V6.2<sup>Q&As</sup>

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.pass4itsure.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

Refer to the screen capture below:

Configuration » Enforcement » Policies » Edit - Onboard Provisioning - Aruba

#### Enforcement Policies - Onboard Provisioning - Aruba

Summary	Enforcement	Rules
<b>Enforcement:</b>		
Name:	Onboard Provisioning - Aruba	
Description:	Enforcement policy controlling network access for device provisioning	
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	
<b>Rules:</b>		
Rules Evaluation Algorithm:	First applicable	
Conditions	Actions	
1. (Authentication:OuterMethod EQUALS EAP-TLS)	[Allow Access Profile], Onboard Post-Provisioning - Aruba	
2. (Authentication:Source EQUALS [Onboard Devices Repository])	[Allow Access Profile], Onboard Post-Provisioning - Aruba	
3. (Authentication:Source NOT_EQUALS [Onboard Devices Repository])	[Allow Access Profile], Onboard Pre-Provisioning - Aruba	

Based on the Enforcement Policy configuration shown in the capture, what Enforcement Profile will an employee connecting an iOS device to the network for the first time receive using EAP- PEAP?

- A. Deny Access Profile
- B. Onboard Post-Provisioning - Aruba
- C. Onboard Pre-Provisioning Aruba
- D. Cannot be determined
- E. Onboard Device Repository

Correct Answer: C

### QUESTION 2

The screenshot here from the Event Viewer in ClearPass shows an error when a user does an EAP-TLS authentication to ClearPass through an Aruba Controller's Wireless Network.



Monitoring » Event Viewer  
Event Viewer

5

Filter: Source contains RADIUS + Go Clear Filter

#	Source	Level	Category
1.	RADIUS	ERROR	Authentication

**System Event Details**

Source	RADIUS
Level	ERROR
Category	Authentication
Action	Unknown
Timestamp	May 09, 2013 23:29:31 UTC
Description	Received packet from 10.8.10.100 with invalid Message-Authenticator! (Shared secret is incorrect.)

Close

What is the cause of this error?

- A. The client has sent an incorrect shared secret for the 802.1X authentication.
- B. The controller has sent an incorrect shared secret for the RADIUS authentication.
- C. The client's shared secret used during the certificate exchange is incorrect.
- D. The controller's shared secret used during the certificate exchange is incorrect.
- E. The NAS source interface IP is incorrect.

Correct Answer: B

**QUESTION 3**

Which of the following statements is NOT true about the configuration of Active Directory (AD) as an External Authentication Server in Clearpass?

- A. Clearpass should join the AD domain when PEAP and MSCHAPv2 are used as the authentication type.
- B. The bind DN for an AD can be in the administrator@domain format.
- C. Clearpass cannot be a member of more than one AD domain.



- D. The list of attributes fetched from the AD can be customized.
- E. Clearpass nodes in a cluster can join different AD domains.

Correct Answer: C

---

#### QUESTION 4

If a client's authentication is failing and there are no entries in the Clearpass's Access Tracker, which of the following is a possible reason for the authentication failure?

- A. The client used a wrong password.
- B. The user is not found in the database.
- C. The shared secret between Network Access Device and Clearpass does not match.
- D. The user account has expired.
- E. The user's certificate is invalid.

Correct Answer: C

---

#### QUESTION 5

Refer to the screenshot below:



The screenshot displays the 'Network Settings' configuration page for a mobile device. The left-hand navigation pane is expanded to 'Network Settings'. The main content area is titled 'Network Settings >> Network Access' and contains the following configuration details:

- Network Access Section:**
  - Name:** Employee\_Secure
  - Description:** Connect to the example network.
  - Network Type:** Wireless only
  - Security Type:** Enterprise (802.1X)
- Wireless Network Settings Section:**
  - Security Version:** WPA2 with AES (recommended)
  - SSID:** secure\_emp
  - Hidden network:**

Which of the following statements is true regarding the above configuration for network settings? (Choose 2)

- A. Onboarded devices will connect to Employee\_Secure SSID after provisioning.
- B. Onboarded devices will connect to secure\_emp SSID after provisioning.
- C. Users will connect to Employee\_Secure SSID for provisioning their devices.
- D. Users must enter a Pre-shared key to connect to the network.
- E. Users will do 802.1X authentication when connecting to the SSID.

Correct Answer: BE

### QUESTION 6

Which of the following CLI commands is used to upgrade the image of a ClearPass server?

- A. Upgrade image
- B. System upgrade
- C. Upgrade software
- D. Reboot





E. System update

Correct Answer: B

---

### QUESTION 7

Refer to the screenshot below: Based on the above configuration, which of the following statements is true?

## Certificate Authority Trust Chain

✓ Imported certificate(s) for use as Onboard CA.

 **arubatraining-REMOTELABSERVER-CA** (self-signed)

↓ Show certificate

 **ClearPass Onboard Local Certificate Authority**

Aruba Networks ↓ Show certificate

A. ClearPass is configured as a Root CA.

B. ClearPass is configured as the Intermediate CA.

C. ClearPass has an expired server certificate.

D. The arubatraining-REMOTELABSERVER-CA will issue client certificates during Onboarding.

E. This is not a valid trust chain since the arubatraining-REMOTELABSERVER-CA has a self-signed certificate.

Correct Answer: B

---

### QUESTION 8

Which of the following ways are used by Clearpass to assign roles to the client? (Choose 2)

A. Through a role mapping policy.

B. Roles can be derived from the Aruba Network Access Device.

C. From the attributes configured in Active Directory.

D. From the attributes configured in a Network Access Device.



E. From the server derivation rule in the Aruba Controller server group for the client.

Correct Answer: AC

## QUESTION 9

Refer to the screen capture below:

### Authentication Sources - remotelab AD

Summary	General	Primary	Attributes
Name:	remotelab AD		
Description:			
Type:	Active Directory		
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this authentication source to		
Authorization Sources:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="border: 1px solid #ccc; padding: 2px;">-- Select --</div>		
Server Timeout:	10	seconds	
Cache Timeout:	36000	seconds	
Backup Servers Priority:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: right; background-color: #0056b3; color: white; padding: 2px 5px; font-weight: bold;">Add Backup</div>		

What does the Cache Timeout Value refer to?

- 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 caches the user attributes fetched from Active Directory.
- C. The amount of time the Policy Manager waits for a response from the Active Directory before sending a timeout message to the Network Access Device.
- D. The amount of time the Policy Manager waits for a response from the Active Directory before checking the backup authentication source.



E. The amount of time the Policy Manager caches the user's client certificate.

Correct Answer: B

**QUESTION 10**

Shown here is a AAA profile in the Aruba Controller.

AAA Profile > p8t1guest Show Reference

Initial role	guest8-1_initial	MAC Authentication Default Role	guest
802.1X Authentication Default Role	guest	L2 Authentication Fail Through	<input type="checkbox"/>
RADIUS Interim Accounting	<input type="checkbox"/>	User derivation rules	--NONE--
Wired to Wireless Roaming	<input checked="" type="checkbox"/>	SIP authentication role	--NONE--
Device Type Classification	<input checked="" type="checkbox"/>	Enforce DHCP	<input type="checkbox"/>

- MAC Authentication Profile
- MAC Authentication Server Group
- 802.1X Authentication Profile
- 802.1X Authentication Server Group
- RADIUS Accounting Server Group Clearpass
- XML API server
- RFC 3576 server

According to the configuration shown here, what would we expect to see in the ClearPass Policy Manager?

- A. RADIUS accounting start-stop messages
- B. RADIUS interim accounting messages
- C. RADIUS interim and start-stop messages
- D. No accounting messages will be seen
- E. RADIUS accounting messages will be sent from the Client to the Controller

Correct Answer: A

**QUESTION 11**

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
<b>Enforcement:</b>		
Name:	Handheld_Wireless_Access_Policy	
Description:	Enforcement policy for handheld 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) (Tips:Role MATCHES_ANY conferencelaptop developer)	WIRELESS_HANDHELD_NETWORK	
3. 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 12

An employee authenticates using their corporate laptop and runs the dissolvable onguard agent to send a health check back the Policy Manager. Based on the health of the device a VLAN is assigned to the corporate laptop.

Which licenses are consumed in this scenario?

- A. 1 Policy Manager license, 1 Onboard License.
- B. 1 Policy Manager license, 1 OnGuard License.
- C. 2 Policy Manager licenses, 1 OnGuard License.
- D. 1 Policy Manager license, 1 Profile License.
- E. 2 Policy Manager licenses, 2 Onguard licenses.

Correct Answer: B

### QUESTION 13



What is RADIUS CoA used for?

- A. To authenticate users or devices before granting them access to a network.
- B. To force the client to re-authenticate upon roaming to a new Controller.
- C. To apply firewall policies based on authentication credentials.
- D. To validate a host MAC against a white and a black list.
- E. To transmit messages to the NAD/NAS to modify a user's session status.

Correct Answer: E

#### QUESTION 14

Refer to the screen capture below: An employee connects a corporate laptop to the network and authenticates for the first time using EAP-TLS. Based on the above Enforcement Policy configuration, what Enforcement Profile will be sent in this scenario?

Configuration » Enforcement » Policies » Edit - Onboard Provisioning - Aruba

#### Enforcement Policies - Onboard Provisioning - Aruba

Summary	Enforcement	Rules
<b>Enforcement:</b>		
Name:	Onboard Provisioning - Aruba	
Description:	Enforcement policy controlling network access for device provisioning	
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	
<b>Rules:</b>		
Rules Evaluation Algorithm:	First applicable	
Conditions	Actions	
1. (Authentication:OuterMethod EQUALS EAP-TLS)	[Allow Access Profile], Onboard Post-Provisioning - Aruba	
2. (Authentication:Source EQUALS [Onboard Devices Repository])	[Allow Access Profile], Onboard Post-Provisioning - Aruba	
3. (Authentication:Source NOT_EQUALS [Onboard Devices Repository])	[Allow Access Profile], Onboard Pre-Provisioning - Aruba	

- A. Deny Access Profile
- B. Onboard Post-Provisioning - Aruba
- C. Onboard Pre-Provisioning Aruba
- D. Cannot be determined
- E. Onboard Device Repository

Correct Answer: B

#### QUESTION 15

Which of the following statements is NOT true about the configuration of a generic LDAP server as an External



Authentication Server in Clearpass?

- A. The bind DN can be in the administrator@domain format.
- B. The list of attributes fetched from an LDAP server can be customized.
- C. An LDAP Browser can be used to search the Base DN.
- D. Multiple LDAP servers cannot be configured as authentication sources.
- E. Generic LDAP servers can be used as authentication sources.

Correct Answer: A

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

[ACCP-V6.2 Practice Test](#)

[ACCP-V6.2 Braindumps](#)