

# 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.certbus.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

Below is an Enforcement Profile that has been created in the Policy Manager: What is the action that is taken by this Enforcement Profile?

Configuration » Enforcement » Profiles » Add Enforcement Profile

#### Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Radius:IETF	Session-Timeout (27)	= 600
2. Click to add...		

- A. ClearPass will count down 600 seconds and send a RADIUS CoA message to the NAD device to end the user's session after this time is up.
- B. ClearPass will send the Session-Timeout attribute in the RADIUS Access-Accept packet to the User and the user's session will be terminated after 600 seconds.
- C. ClearPass will send the Session-Timeout attribute in the RADIUS Access-Accept packet to the NAD device and the NAD will end the user's session after 600 seconds.
- D. ClearPass will send the Session-Timeout attribute in the RADIUS Access-Request packet to the NAD device and the NAD will end the user's session after 600 seconds.

Correct Answer: C

### QUESTION 2

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 gray; height: 60px;"></div> <div style="border: 1px solid gray; padding: 2px;">-- Select --</div>		
Server Timeout:	10	seconds	
Cache Timeout:	36000	seconds	
Backup Servers Priority:	<div style="border: 1px solid gray; height: 40px;"></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 3

Which of the following is true about Data and Management ports on the ClearPass appliance? (Choose 2)

- A. Configuration of the data port is optional.
- B. Configuration of the data port is mandatory.
- C. Configuration of the management port is optional.
- D. Configuration of the management port is mandatory.
- E. Static IP addresses are only allowed on the management port.

Correct Answer: AD

---

#### QUESTION 4

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 5

A hotel chain recently deployed ClearPass Guest. A guest enters the hotel and connects to the Guest SSID. They launch their web browser and type in [www.google.com](http://www.google.com), but they're unable to immediately see the web login page.

Which of the following could be causing this? (Choose 2):

- A. The DNS server is not replying with an IP address for [www.google.com](http://www.google.com).
- B. The guest is using a Linux laptop which doesn't support web login.
- C. The ClearPass server has a server certificate issued by Verisign.
- D. The ClearPass server has a server certificate issued by the internal Microsoft Certificate Server.
- E. The ClearPass server does not recognize the client's certificate.

Correct Answer: AD

---

#### QUESTION 6

Refer to the screen capture below:

Configuration » Posture » Posture Policies » Edit - Employee Posture Policy  
**Posture Policies - Employee Posture Policy**

Summary	Policy	Posture Plugins	Rules
Policy Name:	Employee Posture Policy		
Description:			
Posture Agent:	<input type="radio"/> NAP Agent <input checked="" type="radio"/> OnGuard Agent (Persistent or Dissolvable)		
Host Operating System:	<input checked="" type="radio"/> Windows <input type="radio"/> Linux <input type="radio"/> Mac OS X		

Based on the Posture Policy configuration shown above, which of the following statements is true?

- A. This Posture Policy can be applied to an 802.1x wired service.
- B. This Posture Policy checks the health status of devices running Windows, Linux and Mac OS
- C. This Posture Policy can use either the persistent or dissolvable OnGuard agent to obtain the statement of health.
- D. This Posture Policy checks for presence of a firewall application in Windows devices.
- E. This Posture Policy checks with a Windows NPS server for posture tokens.

Correct Answer: C

**QUESTION 7**

Which of the following statements is true based on the Access Tracker output shown below?

Monitoring & Reporting » Live Monitoring » Access Tracker

**Access Tracker** Jul 12, 2012 10:26:39 PDT

Data Filter: [All Requests] Server: Clearpass6 (10.254.1.176)  
 Date Range: Last 1 day before Today

Filter: Type contains [ ] + Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date
10.254.1.176	RADIUS	BC705A065CF0		REJECT	2012/0

**Request Details**

Summary Input Output Alerts

Error Code: 204  
 Error Category: Authentication failure  
 Error Message: Failed to classify request to service

**Alerts for this Request**

RADIUS Service Categorization failed

- A. The client wireless profile is incorrectly setup.
- B. Clearpass does not have a service enabled for MAC authentication.
- C. The client MAC address is not present in the Endpoints table in the Clearpass database.
- D. The client used incorrect credentials to authenticate to the network.
- E. The RADIUS client on the Windows server failed to categorize the service correctly.

Correct Answer: B

**QUESTION 8**

Which of following is true for both the persistent and dissolvable versions of OnGuard? (Choose 2)

- A. Ability to bounce the endpoint
- B. Auto-remediation is available
- C. Gather statement of health information for network authorization
- D. Supports Windows, Mac OS X devices
- E. They need to be installed on the client devices.

Correct Answer: CD

**QUESTION 9**

A Search was performed using Insight and the following is displayed:

**Search**

Search Type	<input checked="" type="radio"/> Search All Records <input type="radio"/> Search Reports <input type="radio"/> Search Alerts				
Select Template	RADIUS Failed Authentications				<a href="#">Create Report</a>
Rules	<input checked="" type="radio"/> AND <input type="radio"/> OR				
	Type	Name	Operator	Value	+/-
	Auth	Protocol	EQUALS	RADIUS	
	Auth	Error Code	NOT_EQUALS	0	- +
Select date range	From : 2013-05-20 18:38:52		To : 2013-05-29 18:38:51		<a href="#">Search</a>
Show 10 entries					
Auth.Username	Auth.Host MAC Address	Auth.Network Device	Auth.Service	CppmErrorCode.Error Code Details	CppmAlert.Alerts
0024d665b61a	0024d665b61a	10.8.10.100		Failed to classify request to service	
0024d665b61a	0024d665b61a	10.8.10.100		Failed to classify request to service	

What could be a possible reason for the ErrorCode '\\Failed to classify request to service\\' shown above?

- A. The user failed authentication.
- B. ClearPass couldn't match the authentication request to a service, but the user passed authentication.

- C. ClearPass service rules were not configured correctly.
- D. ClearPass service authentication sources were not configured correctly.
- E. The NAD device didn't send the authentication request.

Correct Answer: C

---

#### QUESTION 10

What does a client need for it to perform EAP-TLS successfully? (Choose 2)

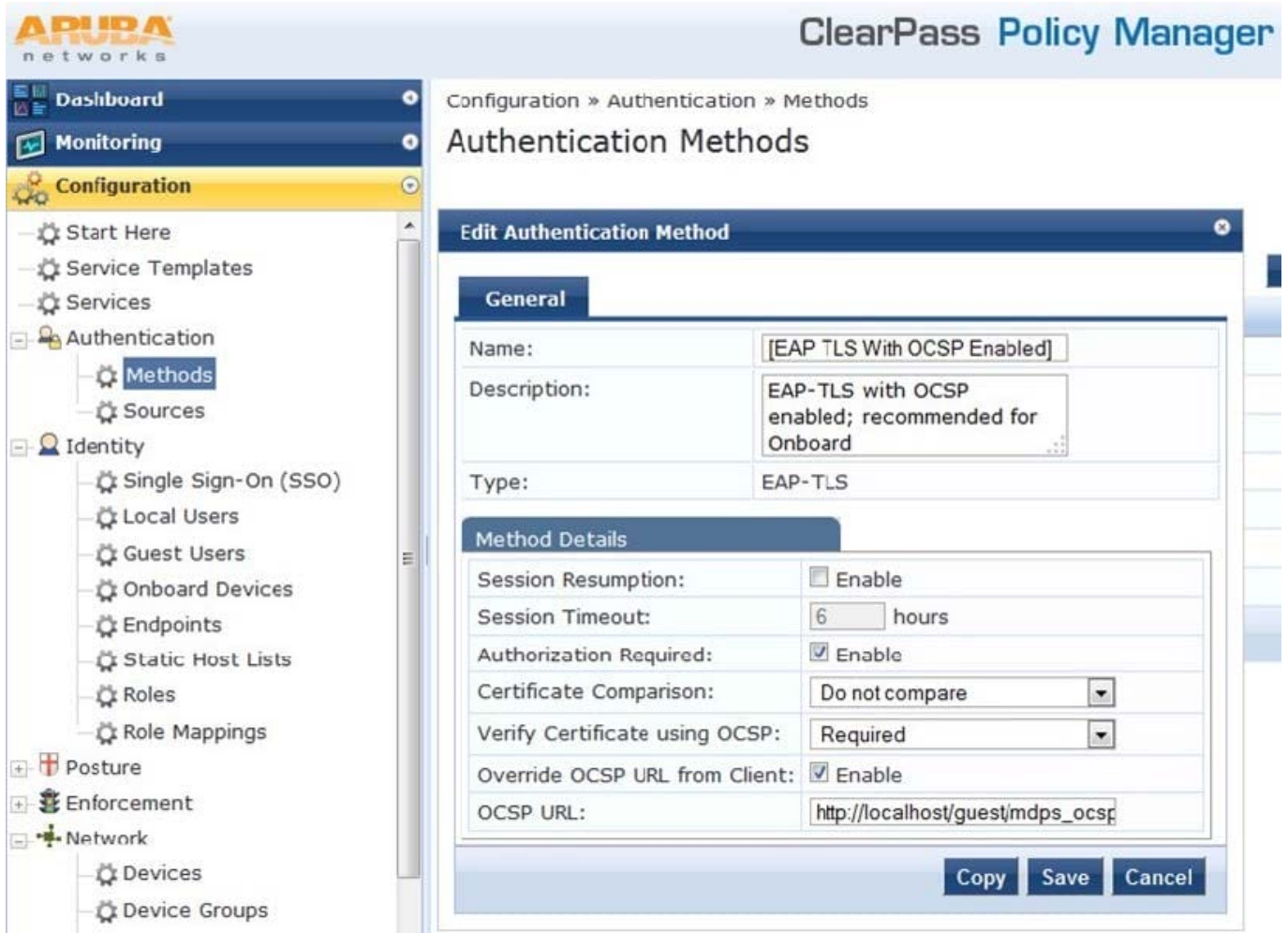
- A. Username and Password
- B. Client Certificate
- C. Pre-shared key
- D. Certificate Authority
- E. Server Certificate

Correct Answer: BE

---

#### QUESTION 11

What is the certificate format PKCS #7, or .p7b, used for?



- A. Certificate chain
- B. Certificate Signing Request
- C. Certificate with an encrypted private key
- D. Binary encoded X.509 certificate
- E. Binary encoded X.509 certificate with public key

Correct Answer: A

**QUESTION 12**

Refer to the screenshot in the diagram below, as seen when a Web Login Page is configured 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 Address field value '\\securelogin.arubanetworks.com\\' used for?

- A. For appending to the Web Login URL, before the page name.
- B. For ClearPass to POST the user credentials to the NAD device.
- C. For ClearPass to send a RADIUS request to the NAD device.
- D. For ClearPass to send a TACACS+ request to the NAD device.
- E. For appending to the Web Login URL, after the page name.

Correct Answer: B

### QUESTION 13

What types of files are stored in the Local Shared Folders database in Clearpass? (Choose 2)

- A. Backup Files
- B. Software image

- C. Log files
- D. Generated Reports
- E. Device fingerprint dictionaries

Correct Answer: AC

---

#### QUESTION 14

What are Operator Profiles used for?

- A. To assign ClearPass roles to guest users.
- B. To enforce role based access control for ClearPass Guest operator users.
- C. To enforce role based access control for ClearPass Policy Manager admin users.
- D. To map AD attributes to admin privilege levels in ClearPass Guest.
- E. To enforce role based access control for Aruba Controllers.

Correct Answer: B

---

#### QUESTION 15

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

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

[ACCP-V6.2 Study Guide](#)

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