Aruba Certified Clearpass Professional 6.7

HP HPE6-A68

Version Demo

Total Demo Questions: 10

Total Premium Questions: 121

QUESTION NO: 1

A customer would like to deploy ClearPass with these requirements:

➢ every day, 100 employees need to authenticate with their corporate laptops using EAP-TLS

➢ every Friday, a meeting with business partners takes place and an additional 50 devices need to authenticate using Web Login Guest Authentication

What should the customer do regarding licenses? (Select two.)

A. When counting policy manager licenses, include the additional 50 business partner devices.

B. When counting policy manager licenses, exclude the additional 50 business partner devices.

C. Purchase Onboard licenses.

D. Purchase guest licenses.

E. Purchase Onguard licenses.

ANSWER: A C

QUESTION NO: 2

What are Operator Profiles used for?

A. to enforce role based access control for Aruba Controllers

B. to enforce role based access control for ClearPass Policy Manager admin users

C. to enforce role based access control for ClearPass Guest Admin users

D. to assign ClearPass roles to guest users

E. to map AD attributes to admin privilege levels in ClearPass Guest

ANSWER: C

Explanation:

An operator profile determines what actions an operator is permitted to take when using ClearPass Guest.

References:

http://www.arubanetworks.com/techdocs/ClearPass/CPGuest_UG_HTML_6.5/Content/OperatorLogins/Operato

QUESTION NO: 3

Based on the Local User repository in ClearPass shown, which Aruba firewall role will be assigned to “mike” when this user authenticates Aruba Controller?

A. We can’t know this from the screenshot above.

B. mike

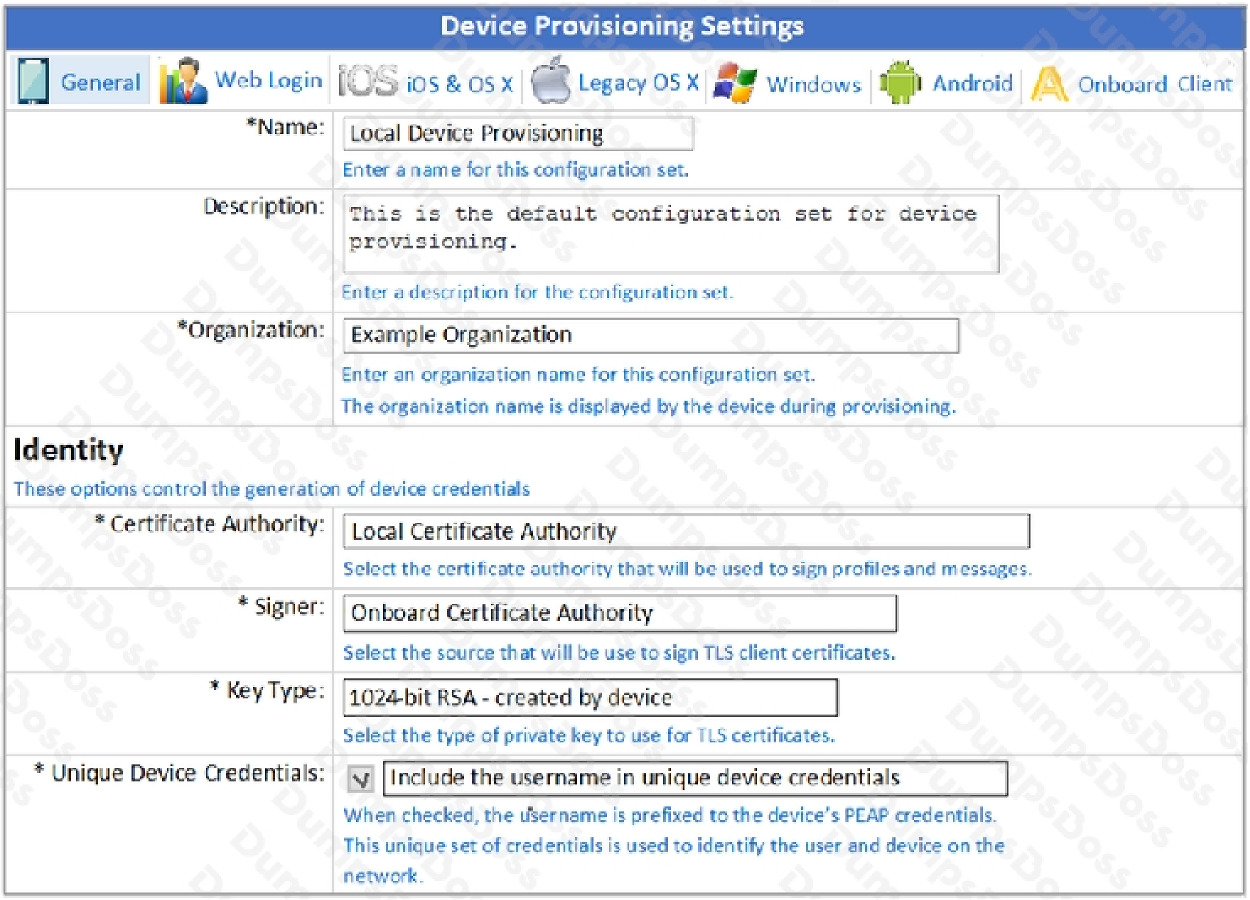
C. Employee

D. john

ANSWER: A

QUESTION NO: 4

Refer to the exhibit.



*Name:	Local Device Provisioning Enter a name for this configuration set.
Description:	This is the default configuration set for device provisioning. Enter a description for the configuration set.
*Organization:	Example Organization Enter an organization name for this configuration set. The organization name is displayed by the device during provisioning.

Identity

These options control the generation of device credentials

* Certificate Authority:	Local Certificate Authority Select the certificate authority that will be used to sign profiles and messages.
* Signer:	Onboard Certificate Authority Select the source that will be use to sign TLS client certificates.
* Key Type:	1024-bit RSA - created by device Select the type of private key to use for TLS certificates.
* Unique Device Credentials:	☑ Include the username in unique device credentials 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.

Based on the configuration for the client’s certificate private key as shown, which statements accurately describe the settings? (Select two.)

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

B. The private key is stored in the user device.

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

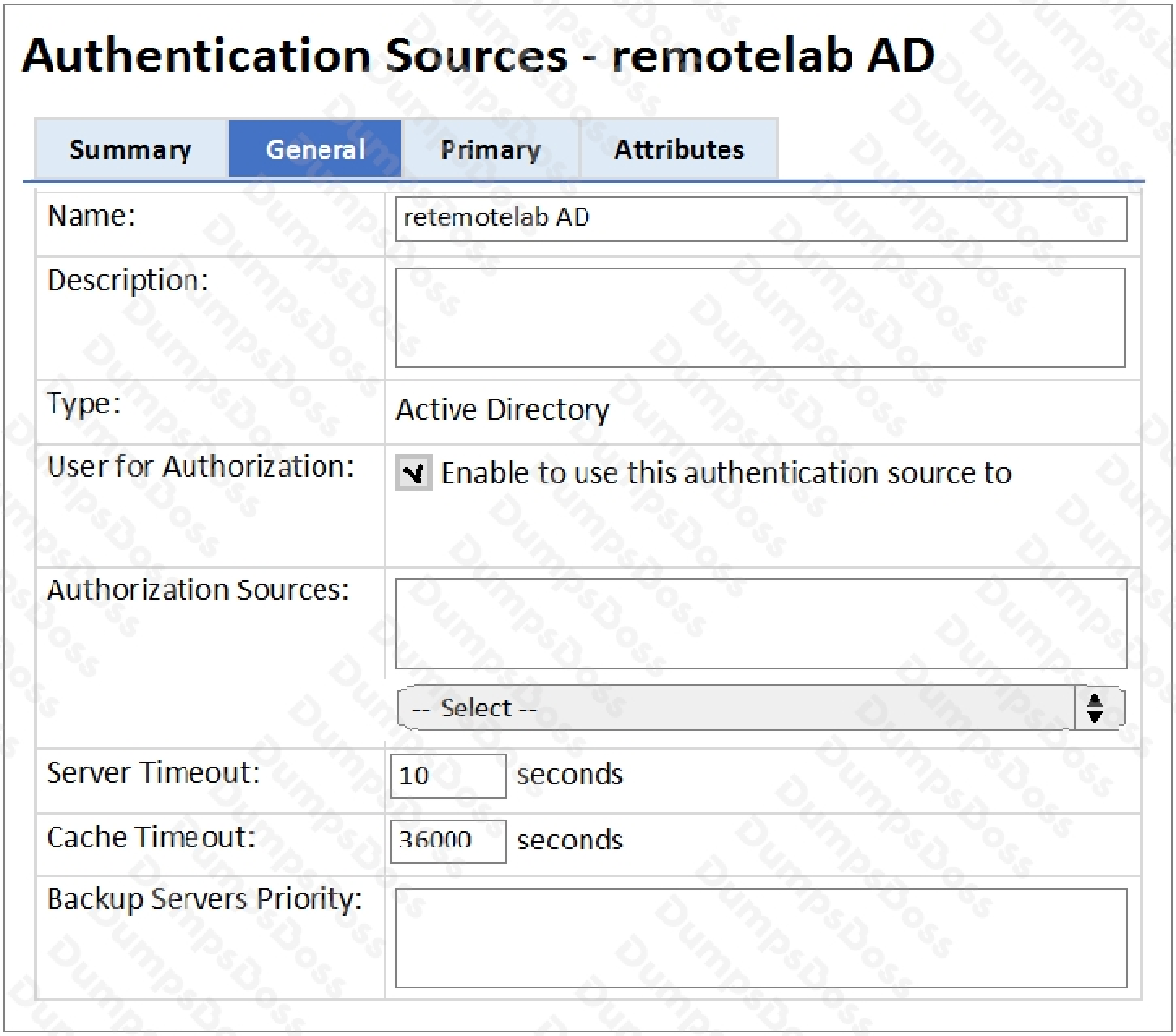
D. More bits in the private key will increase security.

E. More bits in the private key will reduce security.

ANSWER: B D

QUESTION NO: 5

Refer to the exhibit.



Authentication Sources - remotelab AD

Name:	retemotelab AD
Description:	
Type:	Active Directory
User for Authorization:	☑ Enable to use this authentication source to
Authorization Sources:	-- Select --
Server Timeout:	10 seconds
Cache Timeout:	36000 seconds
Backup Servers Priority:	

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 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 NO: 6

A guest self-registered through a Publisher’s Register page.

Which statement accurately describes how the guest’s account will be stored?

A. It will be stored in the Publisher’s guest user repository and the Subscriber’s Onboard user repository.

B. It will be stored in the Publisher’s local user repository and the Subscriber’s guest user repository.

C. It will be stored in the Publisher’s guest user repository permanently, but only for 14 days in the Subscriber’s guest user repository,

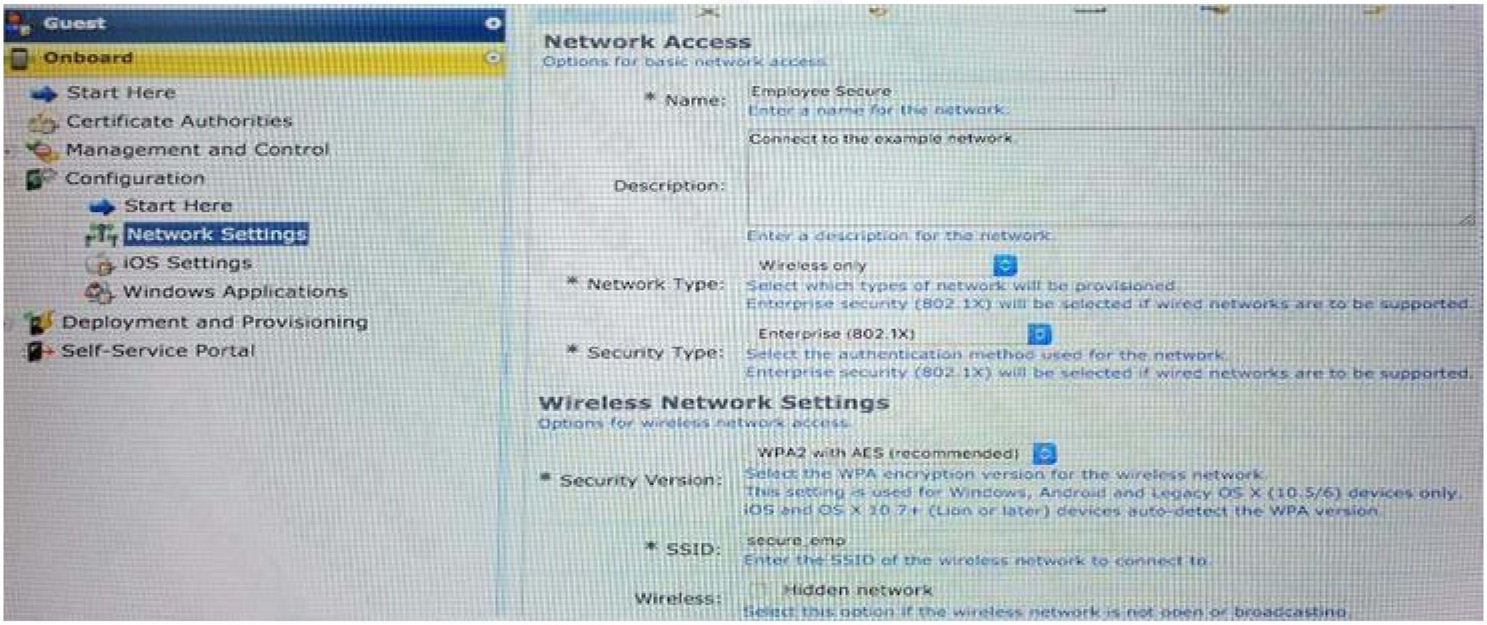
D. It will be stored in both the Publisher’s guest user repository and the Subscriber’s guest user repository.

E. It will be stored in the Publisher’s guest user repository, but not the Subscriber’s.

ANSWER: D

QUESTION NO: 7

Refer to the exhibit.



Network Access
Options for basic network access.

* Name: Employee Secure
Enter a name for the network.

Description: Connect to the example network
Enter a description for the network.

* Network Type: Wireless only
Select which types of network will be provisioned.
Enterprise security (802.1X) will be selected if wired networks are to be supported.

* Security Type: Enterprise (802.1X)
Select the authentication method used for the network.
Enterprise security (802.1X) will be selected if wired networks are to be supported.

Wireless Network Settings
Options for wireless network access.

* Security Version: WPA2 with AES (recommended)
Select the WPA encryption version for the wireless network.
This setting is used for Windows, Android and Legacy OS X (10.5/6) devices only.
iOS and OS X 10.7+ (Lion or later) devices auto-detect the WPA version.

* SSID: secure_emp
Enter the SSID of the wireless network to connect to.

Wireless: □ Hidden network
Select this option if the wireless network is not open or broadcasting.

Which statements accurately describe the status of the Onboarded devices in the configuration for the network settings shown? (Select two.)

A. They will connect to Employee_Secure SSID after provisioning.

B. They will connect to Employee_Secure SSID for provisioning their devices.

C. They will use WPA2-PSK with AES when connecting to the SSID.

D. They will connect to secure_emp SSID after provisioning.

E. They will perform 802.1X authentication when connecting to the SSID.

ANSWER: D E

QUESTION NO: 8

Which authorization servers are supported by ClearPass? (Select two.)

A. Aruba Controller

B. LDAP server

C. Cisco Controller

D. Active Directory

E. Aruba Mobility Access Switch

ANSWER: B D

Explanation:

Authentication Sources can be one or more instances of the following examples:

* Active Directory

* LDAP Directory

* SQL DB

* Token Server

* Policy Manager local DB

References:

ClearPass Policy Manager 6.5 User Guide (October 2015), page 114
https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%

QUESTION NO: 9

Which steps are required to use ClearPass as a TACACS+ Authentication server for a network device? (Select two.)

A. Configure a TACACS Enforcement Profile on ClearPass for the desired privilege level.

B. Configure a RADIUS Enforcement Profile on ClearPass for the desired privilege level.

C. Configure ClearPass as an Authentication server on the network device.

D. Configure ClearPass roles on the network device.

E. Enable RADIUS accounting on the NAD.

ANSWER: A C

Explanation:

You need to make sure you modify your policy (Configuration » Enforcement » Policies » Edit - [Admin Network Login Policy]) and add your AD group settings in to the corresponding privilege level.

QUESTION NO: 10

What does Authorization allow users to do in a Policy Service?

A. To use attributes in databases in role mapping and Enforcement.

B. To use attributes stored in databases in Enforcement only, but not role mapping.

C. To use attributes stored in external databases for Enforcement, but not internal databases.

D. To use attributes stored in databases in role mapping only, but not Enforcement.

E. To use attributes sored in internal databases for Enforcement, but not external databases.

ANSWER: A