HPE6-A15$^{\text{Q\&As}}$

Aruba Certified Clearpass Professional 6.5

Pass HP HPE6-A15 Exam with 100% Guarantee

QUESTION 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.

Correct Answer: AC

QUESTION 2

Why can the Onguard posture check not be performed during 802.1x authentication?

A. Health Checks cannot be used with 802.1x.

B. Onguard uses RADIUS, so an additional service must be created.

C. Onguard uses HTTPS, so an additional service must be created.

D. Onguard uses TACACS, so an additional service must be created.

E. 802.1x is already secure, so Onguard is not needed.

Correct Answer: C

OnGuard uses HTTPS to send posture information to the ClearPass appliance. For OnGuard to use HTTPS, it must have access to the network. If a customer requires 802.1x authentication on the wired switch, a separate 802.1x authentication must be used prior to the OnGuard posture check. In this example, an 802.1x PEAP-EAP-MSCHAPv2 authentication is completed first. A separate WebAuth service must be setup with posture checks to use the OnGuard agent.

References: MAC Authentication and OnGuard Posture Enforcement using Dell WSeries ClearPass and Dell Networking Switches (August 2013), page 21

QUESTION 3

A client\\'s authentication is failing and there are no entries in the ClearPass Access tracker. What is a possible reason for the authentication failure?

A. The user account has expired.

B. The client used a wrong password.

C. The shared secret between the NAD and ClearPass does not match.

D. The user\\'s certificate is invalid.

E. The user is not found in the database.

Correct Answer: C

QUESTION 4

When a third party Mobile Device Management server is integrated with ClearPass, where is the endpoint information from the MDM server stored in ClearPass?

A. Endpoints repository

B. Onboard Device repository

C. MDM repository

D. Guest User repository

E. Local User repository

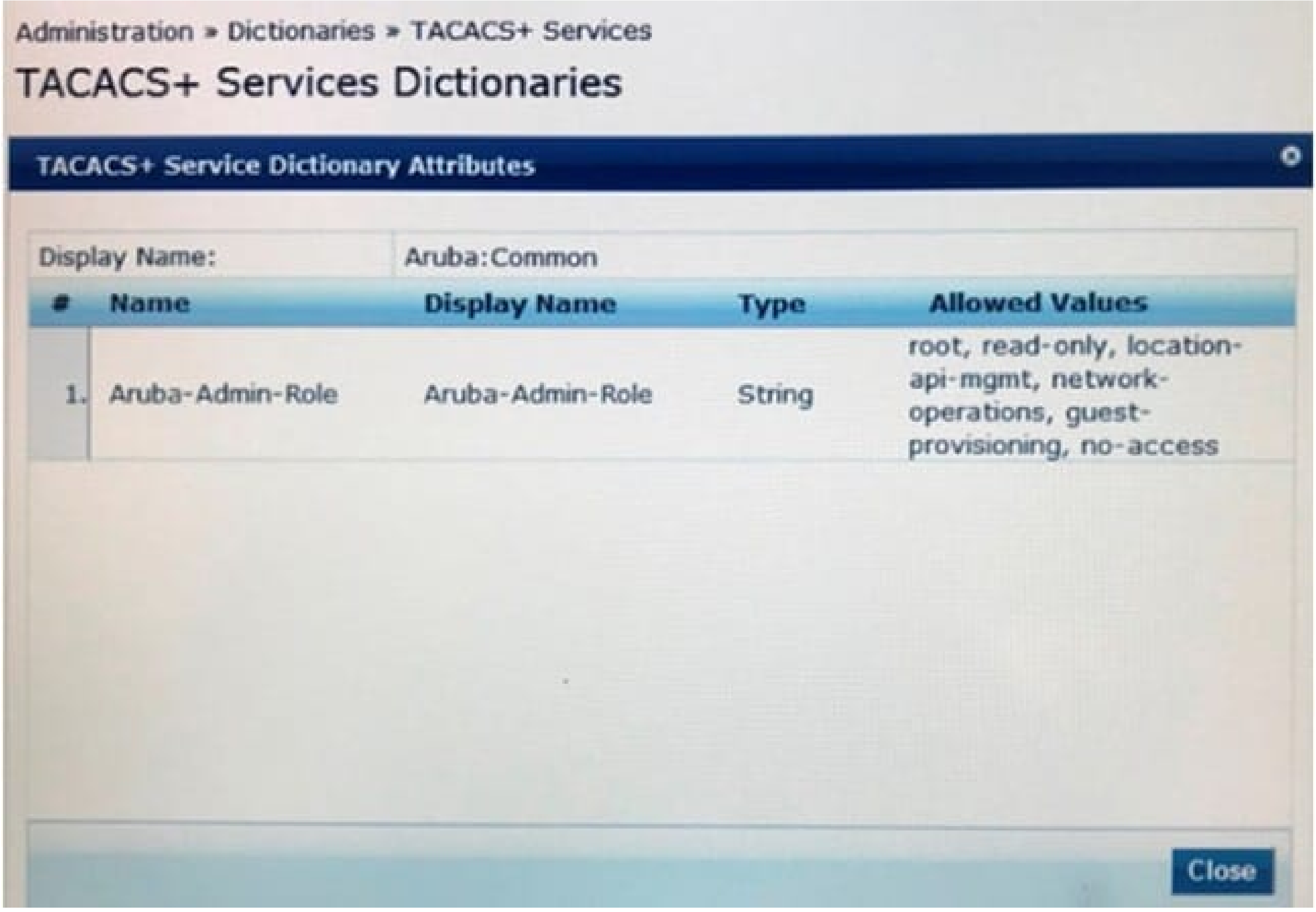
Correct Answer: A

A service running in CPPM periodically polls MDM servers using their exposed APIs. Device attributes obtained from MDM are added as endpoint tags. Profiler related attributes are send to profiler which uses these attributes to derive final profile.

References: ClearPass Profiling TechNote (2014), page 23 https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%20TechNote.pdf

QUESTION 5

Refer to the exhibit.



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

Based on the Aruba TACACS+ dictionary shown, how is the Aruba-Role attribute used?

A. The Aruba-Admin-Role on the controller is applies to users using TACACS+ to login to the Policy Manager

B. To assign different privileges to clients during 802.1X authentication

C. To assign different privileges to administrators logging into an Aruba NAD

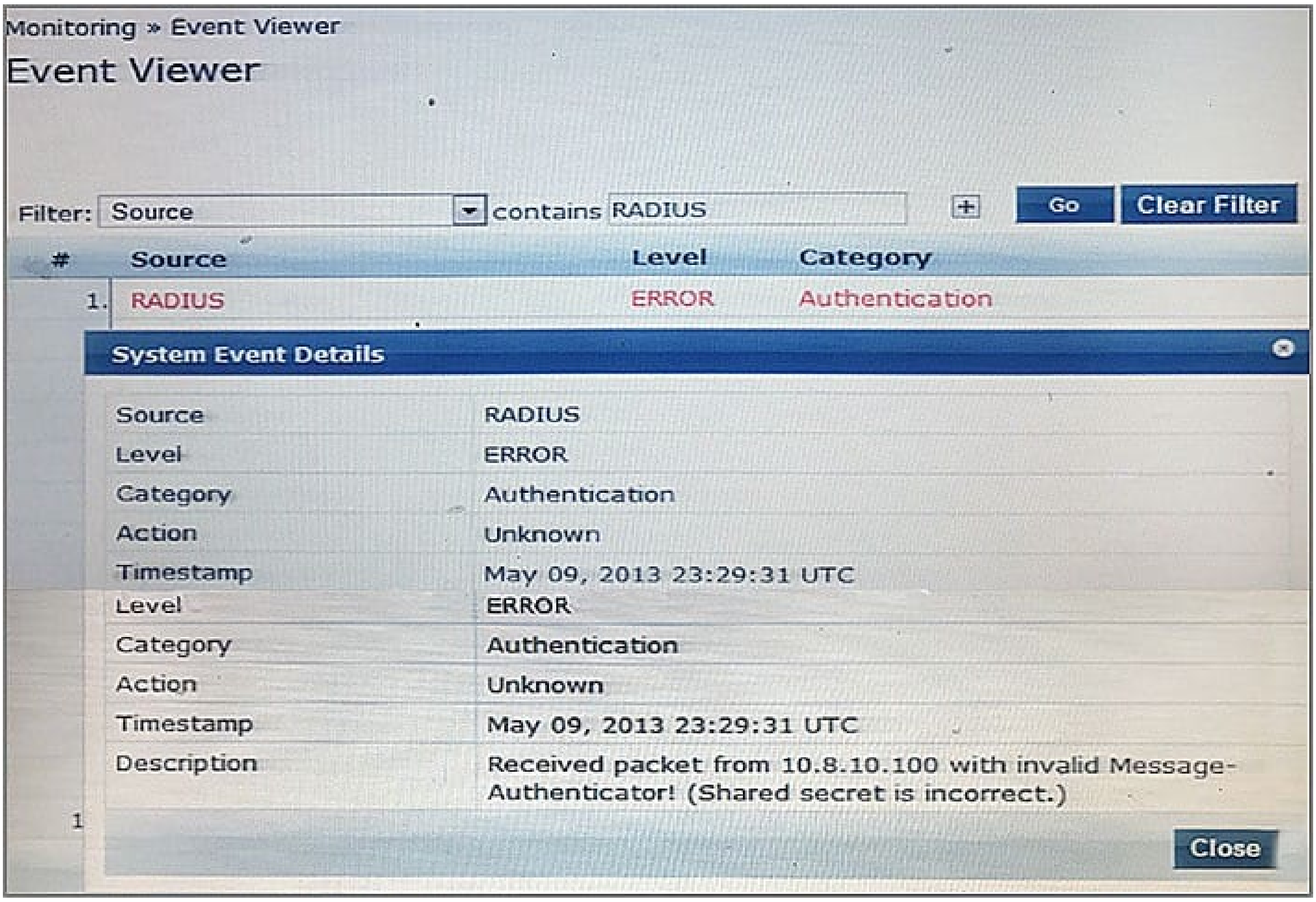
D. It is used by ClearPass to assign TIPS roles to clients during 802.1X authentication

E. To assign different privileges to administrators logging into ClearPass

Correct Answer: C

QUESTION 6

Refer to the exhibit.



Filter: Source contains RADIUS

#	Source	Level	Category
1.	RADIUS	ERROR	Authentication

Source	RADIUS
Level	ERROR
Category	Authentication
Action	Unknown
Timestamp	May 09, 2013 23:29:31 UTC
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.)

The ClearPass Event Viewer displays an error when a user authenticates with EAP-TLS to ClearPass through an Aruba Controller Wireless Network.

What is the cause of this error?

A. The controller\\'s shared secret used during the certificate exchange is incorrect.

B. The NAS source interface IP is incorrect.

C. The client sent an incorrect shared secret for the 802.1X authentication.

D. The controller used an incorrect shared secret for the RADIUS authentication.

E. The client\\'s shared secret used during the certificate exchange is incorrect.

Correct Answer: D

QUESTION 7

A hotel chain deployed ClearPass Guest. When hotel guests connect to the Guest SSID, launch a web browser and enter the address www.google.com, they are unable to immediately see the web login page. What are the likely causes of this? (Select two.)

A. The ClearPass server has a trusted server certificate issued by Verisign.

B. The ClearPass server has an untrusted server certificate issued by the internal Microsoft Certificate server.

C. The ClearPass server does not recognize the client\\'s certificate.

D. The DNS server is not replying with an IP address for www.google.com.

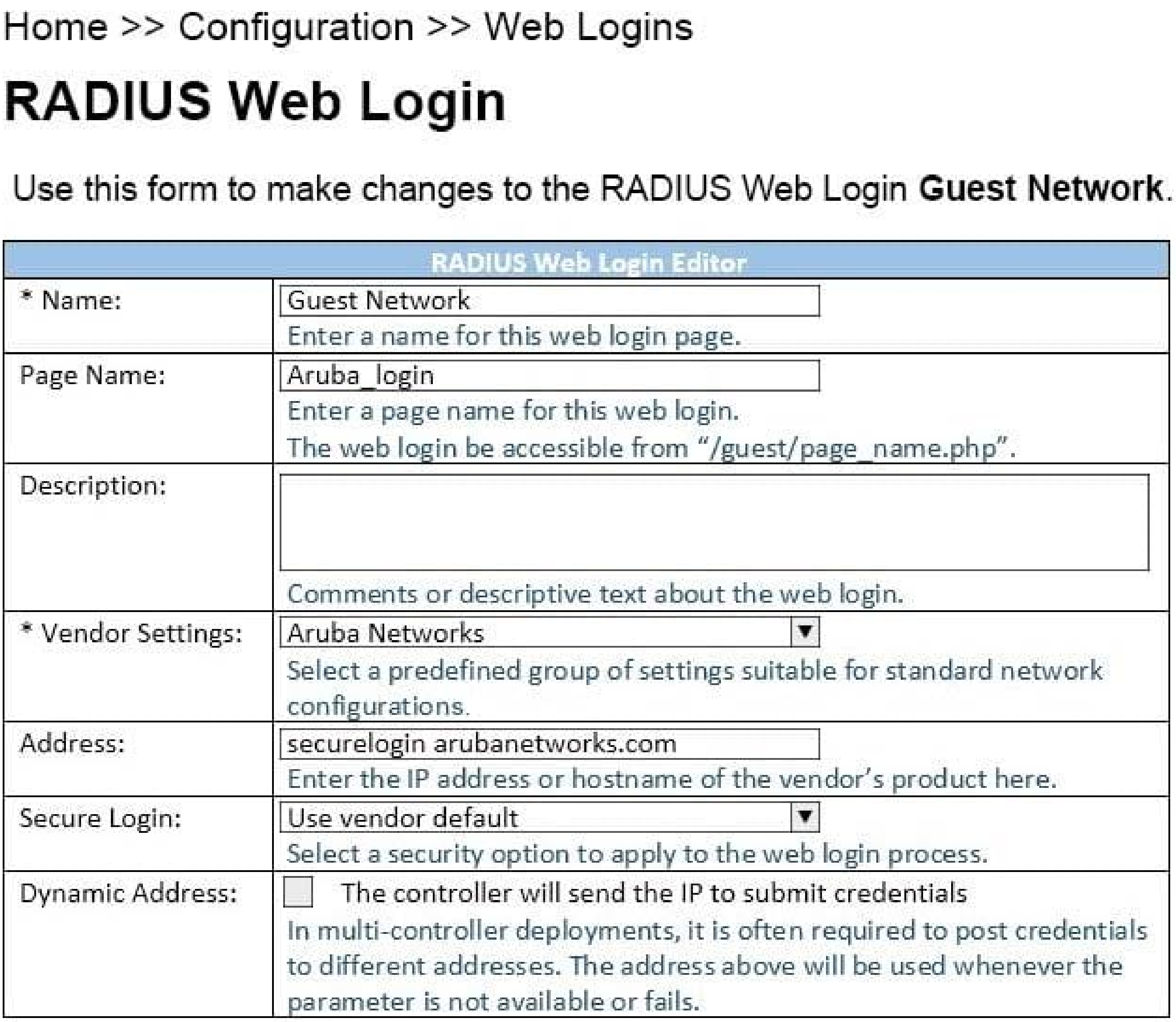
Correct Answer: BD

You would need a publicly signed certificate.

References: http://community.arubanetworks.com/t5/Security/Clearpass-Guest-certificate-error-for-guest-visitors/td-p/221992

QUESTION 8

Refer to the exhibit.



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:	Guest Network Enter a name for this web login page.
Page Name:	Aruba_login Enter a page name for this web login. The web login be accessible from "/guest/page_name.php".
Description:	 Comments or descriptive text about the web login.
* Vendor Settings:	Aruba Networks ▼ Select a predefined group of settings suitable for standard network configurations.
Address:	securelogin arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default ▼ Select a security option to apply to the web login process.
Dynamic Address:	□ The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses. The address above will be used whenever the parameter is not available or fails.

When configuring a Web Login Page in ClearPass Guest, the information shown is displayed. What is the page name field used for?

A. for forming the Web Login Page URL

B. for Administrators to access the PHP page, but not guests

C. for Administrators to reference the page only

D. for forming the Web Login Page URL where Administrators add guest users

E. for informing the Web Login Page URL and the page name that guests must configure on their laptop wireless supplicant.

Correct Answer: A

The Page Name is an identifier page name that will appear in the URL -- for example, "/guest/page_name.php".

References: http://www.arubanetworks.com/techdocs/ClearPass/CPGuest_UG_HTML_6.5/Content/Configuration/CreateEditWebLogin.htm

QUESTION 9

What is the purpose of ClearPass Onboard?

A. to provide MAC authentication for devices that don\\'t support 802.1x

B. to run health checks on end user devices

C. to provision personal devices to securely connect to the network

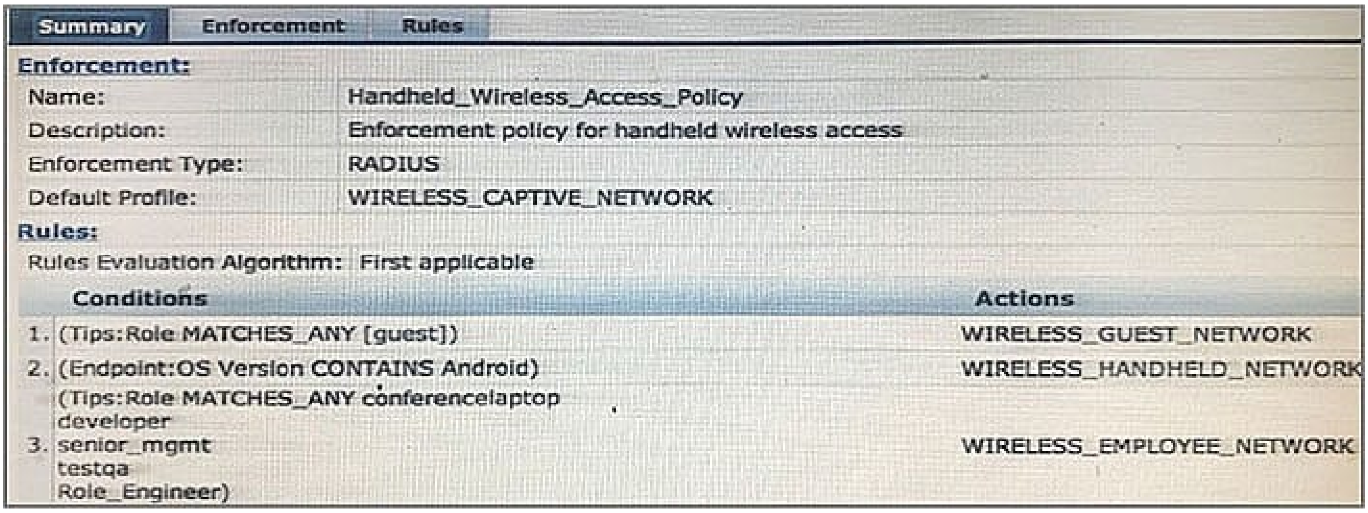
D. to configure self-registration pages for guest users

E. to provide guest access for visitors to connect to the network

Correct Answer: C

QUESTION 10

Refer to the exhibit.



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 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. Which Enforcement Profile is applied?

A. WIRELESS_GUEST_NETWORK

B. WIRELESS_CAPTIVE_NETWORK

C. WIRELESS_HANDHELD_NETWORK

D. Deny Access

E. WIRELESS_EMPLOYEE_NETWORK

Correct Answer: E

MATCHES_ANY: For list data types, true if any of the run-time values in the list match one of the configured values. Example: Tips:Role MATCHES_ANY HR,ENG,FINANCE

References: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/Rules/Operators.htm

QUESTION 11

Which authentication protocols can be used for authenticating Windows clients that are Onboarded? (Select two.)

A. EAP-GTC

B. PAP

C. EAP-TLS

D. CHAP

E. PEAP with MSCHAPv2

Correct Answer: CE

QUESTION 12

Which use cases will require a ClearPass Guest application license? (Select two.)

A. Guest device fingerprinting

B. Guest endpoint health assessment

C. Sponsor based guest user access

D. Guest user self-registration for access

E. Guest personal device onboarding

Correct Answer: CD

QUESTION 13

Why is a terminate session enforcement profile used during posture checks with 802.1x authentication?

A. To send a RADIUS CoA message from the ClearPass server to the client

B. To disconnect the user for 30 seconds when they are in an unhealthy posture state

C. To blacklist the user when they are in an unhealthy posture state

D. To force the user to re-authenticate and run through the service flow again

E. To remediate the client applications and firewall do that updates can be installed

Correct Answer: A

QUESTION 14

An employee provisions a personal smart phone using the Onboard process. In addition, the employee has a corporate laptop provided by IT that connects to the secure network. How many licenses does the employee consume?

A. 1 Policy Manager license, 2 Guest Licenses

B. 2 Policy Manager licenses, 1 Onboard License

C. 1 Policy Manager license, 1 Onboard License

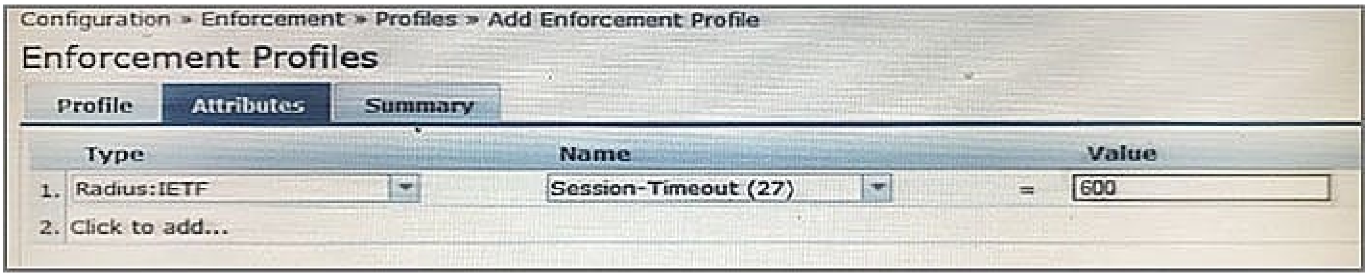
D. 1 Policy Manager license, 1 Guest License

E. 2 Policy Manager licenses, 2 Onboard Licenses

Correct Answer: B

QUESTION 15

Refer to the exhibit.



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

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

An Enforcement Profile has been created in the Policy Manager as shown. Which action will ClearPass take based on the Enforcement Profile?

A. it will count down 600 seconds and send a RADIUS CoA message to the NAD to end the user\\'s session after this time is up

B. it will send the Session-Timeout attribute in the RADIUS Access-Request packet to the NAD and the NAD will end the user\\'s session after 600 seconds

C. it will count down 600 seconds and send a RADIUS CoA message to the user to end the user\\'s session after this time is up

D. it will send the Session-Timeout attribute in the RADIUS Access-Request packet to the user and the user\\'s session will be terminated after 600 seconds

Correct Answer: D

Session Timeout (in seconds) - Configure the agent session timeout interval to re-evaluate the system health again. OnGuard triggers auto-remediation using this value to enable or disable AV-RTP status check on endpoint. Agent re-authentication is determined based on session-time out value. You can specify the session timeout interval from 60 ?600 seconds. Setting the lower value for session timeout interval results numerous authentication requests in Access Tracker page. The default value is 0.

References: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/Enforce/EPAgent_Enforcement.htm