HPE6-A15^{Q&As}

Aruba Certified Clearpass Professional 6.5

Pass HP HPE6-A15 Exam with 100% Guarantee

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

https://www.geekcert.com/hpe6-a15.html

100% Passing Guarantee
100% Money Back Assurance

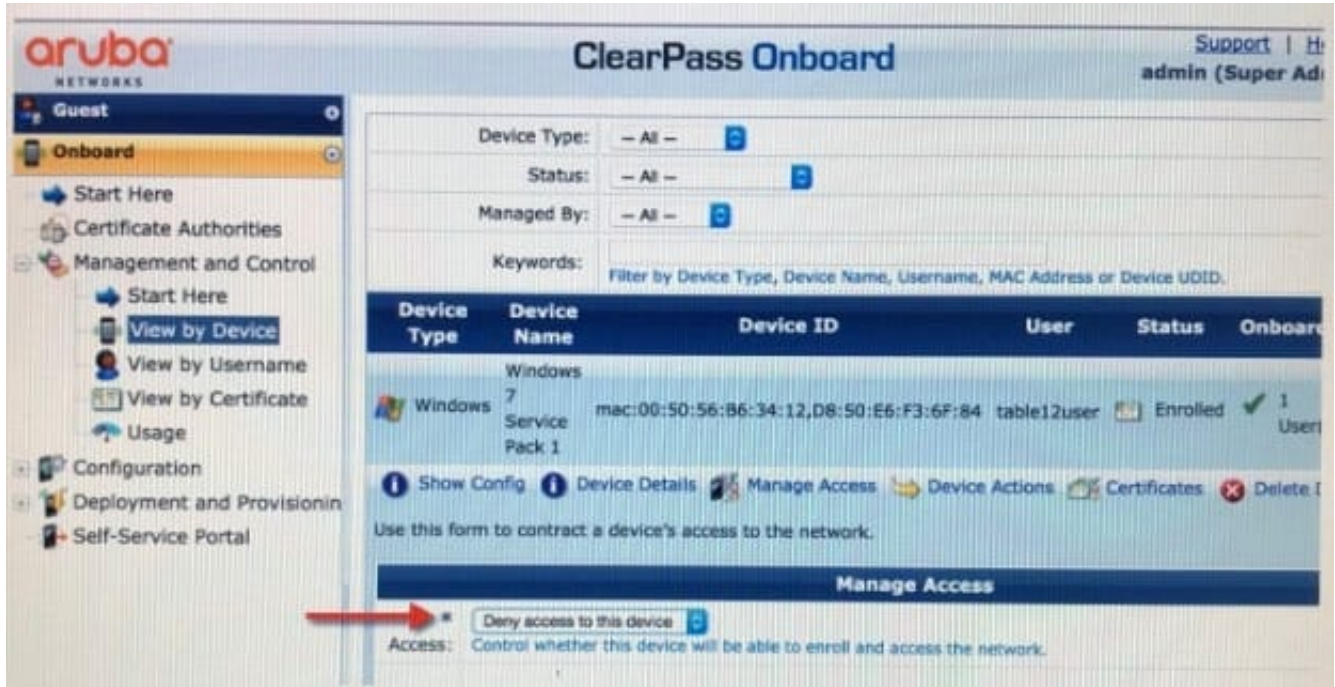Following Questions and Answers are all new published by HP Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

Refer to the exhibit.

Based on the information shown, what will be the outcome when the administrator chooses "Deny Access to this Device? (Select two.)

A. EAP-TLS Authentication will be unaffected

B. The user can Onboard their device again

C. A new device certificate will be automatically pushed out to the device

D. The user cannot Onboard their device again

E. EAP-TLS Authentication will fail

Correct Answer: DE

The Device Management (View by Device) page lists all devices and lets you manage the devices\\' access to the network. For each device, you can allow or deny network access.

When you select the Deny option, a message advises you that any certificates associated with it will be revoked. The device cannot be re-enrolled as long as access is denied. To re-enroll the device, you must use this field to allow access again. References:
http://www.arubanetworks.com/techdocs/ClearPass/6.6/Guest/Content/Onboard/DeviceManagement.htm

QUESTION 2

What is the purpose of RADIUS CoA (RFC 3576)?

A. to force the client to re-authenticate upon roaming to a new Controller

B. to apply firewall policies based on authentication credentials

C. to validate a host MAC address against a whitelist or a blacklist

D. to authenticate users or devices before granting them access to a network

E. to transmit messages to the NAD/NAS to modify a user\'s session status

Correct Answer: E

CoA messages modify session authorization attributes such as data filters. References:
https://tools.ietf.org/html/rfc3576

QUESTION 3

An organization implements dual SSID Onboarding. The administrator used the Onboard service template to create services for dual SSID Onboarding.

Which statement accurately describes the outcome?

A. The Onboard Provisioning service is triggered when the user connects to the provisioning SSID to Onboard their device.

B. The Onboard Authorization service is triggered when the user connects to the secure SSID.

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

D. The device connects to the secure SSID for provisioning.

E. The Onboard Authorization service is never triggered.

Correct Answer: C

QUESTION 4

Refer to the exhibit.

Configuration » Services » Edit - CompanyX Onboard Authorization

Services - CompanyX Onboard Authorization

Summary	Service	Authentication	Roles	Enforcement

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: CompanyX Onboard Authorization Policy ▾ **Modify**   Add new En

Enforcement Policy Details

Description: Sample policy controlling authorization during Onboard provisioning

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: evaluate-all

Conditions	Enforcement Profiles
1. (Date:Day-of-Week *BELONGS_TO* Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	[Allow Access Profile], [Aruba Terminate Session]

Based on the configuration of the Enforcement Profiles in the Onboard Authorization service shown, which Onboarding action will occur?

A. The device will be disconnected from the network after Onboarding so that an EAP-TLS authentication is not performed.

B. The device will be disconnected from and reconnected to the network after Onboarding is completed.

C. The device\\'s onboard authorization request will be denied.

D. The device will be disconnected after post-Onboarding EAP-TLS authentication, so a second EAP-TLS authentication is performed.

E. After logging in on the Onboard web login page, the device will be disconnected form and reconnected to the network before Onboard begins.

Correct Answer: B

QUESTION 5

Which components can use Active Directory authorization attributes for the decision-making process? (Select two.)

A. Profiling policy

B. Certificate validation policy

C. Role Mapping policy

D. Enforcement policy

E. Posture policy

Correct Answer: CD

C: Role Mappings Page - Rules Editor Page Parameters

Parameter	Description
Type	The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context. (Refer to Namespaces.) In the role mapping context, Policy Manager allows attributes from following namespaces: • Application • Application:ClearPass • Authentication • Authorization • Authorization:<authorization_source_instance> - Policy Manager shows each instance of the authorization source for which attributes have been configured to be fetched. (See Adding and Modifying Authentication Sources). Only those attributes that have been configured to be fetched are shown in the attributes drop-down list. • Certificate • Connection • Date • Device • Endpoint • GuestUser • Host • LocalUser • Onboard • TACACS • RADIUS - All enabled RADIUS vendor dictionaries.
Name	Displays the drop-down list of attributes present in the selected namespace.
Operator	Displays the drop-down list of context-appropriate (with respect to the attribute data type) operators. Operators have the obvious meaning; for stated definitions of operator meaning, refer to Operators.
Value	Depending on attribute data type, this may be a free-form (one or many line) edit box, a drop-down list, or a time/date widget.

D: Enforcement Policy Attributes tab Parameters

Attribute	Description
Type:	Select the type of attributes from the drop down list.
Host	See Host Namespaces
Authentication	See Authentication Namespaces
Connection	See Connection Namespaces
Application	See Application Namespace
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda • Radius:Aruba	See RADIUS Namespaces
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

References:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/identity/RoleMappingPolicies.html http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/

CPPM_UserGuide/PolicySim/PS_Enforcement_Policy.htm

HPE6-A15 VCE Dumps   HPE6-A15 Exam Questions   HPE6-A15 Braindumps