



HPE6-A68^{Q&As}

Aruba Certified ClearPass Professional (ACCP) V6.7

Pass HP HPE6-A68 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/hpe6-a68.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.

The screenshot shows the Aruba ClearPass Onboard interface. The left sidebar contains navigation options: Guest, Onboard, Start Here, Certificate Authorities, Management and Control, Start Here, View by Device (highlighted), View by Username, View by Certificate, Usage, Configuration, Deployment and Provisioning, and Self-Service Portal. The main content area is titled 'ClearPass Onboard' and includes filter options for Device Type, Status, and Managed By. A table lists devices with columns for Device Type, Device Name, Device ID, User, Status, and Onboard. A device named 'Windows Service Pack 1' is shown with a status of 'Enrolled'. Below the table, there are action buttons: Show Config, Device Details, Manage Access, Device Actions, Certificates, and Delete. A 'Manage Access' section is visible at the bottom, with a red arrow pointing to the 'Deny access to this device' button. Below this button, it says 'Access: Control whether this device will be able to enroll and access the network.'

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

Refer to the exhibit.



Captive Portal Authentication Profile > default		Show Reference	Save As	Reset
Default Role	guest ▼	Default Guest Role	guest ▼	
Redirect Pause	10 sec	User Login	<input checked="" type="checkbox"/>	
Guest Login	<input type="checkbox"/>	Logout popup window	<input checked="" type="checkbox"/>	
Use HTTP for authentication	<input type="checkbox"/>	Logon wait minimum wait	5 sec	
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %	
Max Authentication failures	0	Show FQDN	<input type="checkbox"/>	
Use CHAP (non-standard)	<input type="checkbox"/>	Login page	/auth/index.html	
Welcome page	/auth/welcome.html	Show Welcome Page	<input checked="" type="checkbox"/>	
Add switch IP address in the redirection URL	<input type="checkbox"/>	Allow only one active user session	<input type="checkbox"/>	
While List	<input type="text"/> <input type="button" value="Delete"/> <input type="button" value="Add"/>	Black List	<input type="text"/> <input type="button" value="Delete"/> <input type="button" value="Add"/>	
Show the acceptable use policy page	<input type="checkbox"/>			

Based on the information shown, which field in the Captive Portal Authentication profile should be changed so that guest users are redirected to a page on ClearPass when they connect to the Guest SSID?

- A. both Login and Welcome Page
- B. Default Role
- C. Welcome Page
- D. Default Guest Role
- E. Login Page

Correct Answer: E

The Login page is the URL of the page that appears for the user logon. This can be set to any URL. The Welcome page is the URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL.

References:

http://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/Captive_Portal/Captive_Portal_Authentic.htm

QUESTION 3



Refer to the exhibit.

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

Enforcement Policies - Onboard Provisioning - Aruba

Summary	Enforcement	Rules
Enforcement:		
Name:	Onboard Provisioning - Aruba	
Description:	Enforcement policy controlling network access for device provisioning	
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	
Rules:		
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	

An employee connects a corporate laptop to the network and authenticates for the first time using EAP-TLS. Based on the Enforcement Policy configuration shown, which Enforcement Profile will be sent?

- A. Onboard Post-Provisioning - Aruba
- B. Onboard Pre-Provisioning - Aruba
- C. Deny Access Profile
- D. Onboard Device Repository

Correct Answer: A

QUESTION 4

In a single SSID Onboarding, which method can be used in the Enforcement Policy to distinguish between a provisioned device and a device that has not gone through the Onboard workflow?

- A. Active Directory Attributes
- B. Network Access Device used
- C. Endpoint OS Category
- D. Onguard Agent used
- E. Authentication Method used

Correct Answer: E

QUESTION 5

When is the RADIUS server certificate used? (Select two.)

- A. During dual SSID onboarding, when the client connects to the Guest network



- B. During EAP-PEAP authentication in single SSID onboarding
- C. During post-Onboard EAP-TLS authentication, when the client verifies the server certificate
- D. During Onboard Web Login Pre-Auth, when the client loads the Onboarding web page
- E. During post-Onboard EAP-TLS authentication, when the server verifies the client certificate

Correct Answer: CD

QUESTION 6

Refer to the exhibit.

Enforcement Policies - Enterprise Enforcement Policy

Summary	Enforcement	Rules
Enforcement:		
Name:	Enterprise Enforcement Policy	
Description:	Enforcement policies for local and remote employees	
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	
Rules:		
Rules Evaluation Algorithm: Evaluate all		
Conditions	Actions	
1. (Tips: Posture Equals HEALTHY (0)) AND (Tips:Role MATCHES ANY Remote Worker Role Engineer testqa) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	[RADIUS] EMPLOYEE_VLAN, [RADIUS] Remote Employee ACL	
2. (Tips:Role EQUALS Senior_Mgmt) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	[RADIUS] EMPLOYEE_VLAN	
3. (Tips:Role EQUALS San Jose HR Local) AND (Tips: Posture EQUALS HEALTHY (0))	HR VLAN	
4. (Tips:Role EQUALS [Guest]) AND (Connection:SSID CONTAINS guest)	[RADIUS] WIRELESS_GUEST_NETWORK	
5. (Tips:Role EQUALS Remote Worker) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	RestrictedACL	

Based on the Enforcement Policy configuration shown, when a user with Role Remote Worker connects to the network and the posture token assigned is quarantine, which Enforcement Profile will be applied?

- A. RestrictedACL
- B. Remote Employee ACL
- C. [Deny Access Profile]
- D. EMPLOYEE_VLAN
- E. HR VLAN

Correct Answer: B

The first rule will match, and the Remote Employee ACL will be used.

**QUESTION 7**

Refer to the exhibit.

Administration > Dictionaries > TACACS+ Services

TACACS+ Services Dictionaries

TACACS+ Service Dictionary Attributes

#	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

Close

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 8

An Android device goes through the single-SSID Onboarding process and successfully connects using EAP-TLS to the secure network. What is the order in which services are triggered?

- A. Onboard Authorization, Onboard Provisioning, Onboard Authorization



- B. Onboard Provisioning, Onboard Pre-Auth, Onboard Authorization, Onboard Provisioning
- C. Onboard Provisioning, Onboard Authorization, Onboard Pre-Auth
- D. Onboard Provisioning, Onboard Authorization, Onboard Provisioning
- E. Onboard Provisioning, Onboard Pre-Auth, Onboard Authorization

Correct Answer: D

QUESTION 9

Refer to the exhibit.

The screenshot shows the 'Provisioning Settings' for a 'Guest Onboard' configuration. The 'Maximum Devices' field is set to 3. The 'Authorization' section is expanded, showing 'Authorization Method' set to 'App Auth - check using Aruba Application Authentication' and 'Configuration Profile' set to 'Default Profile'.

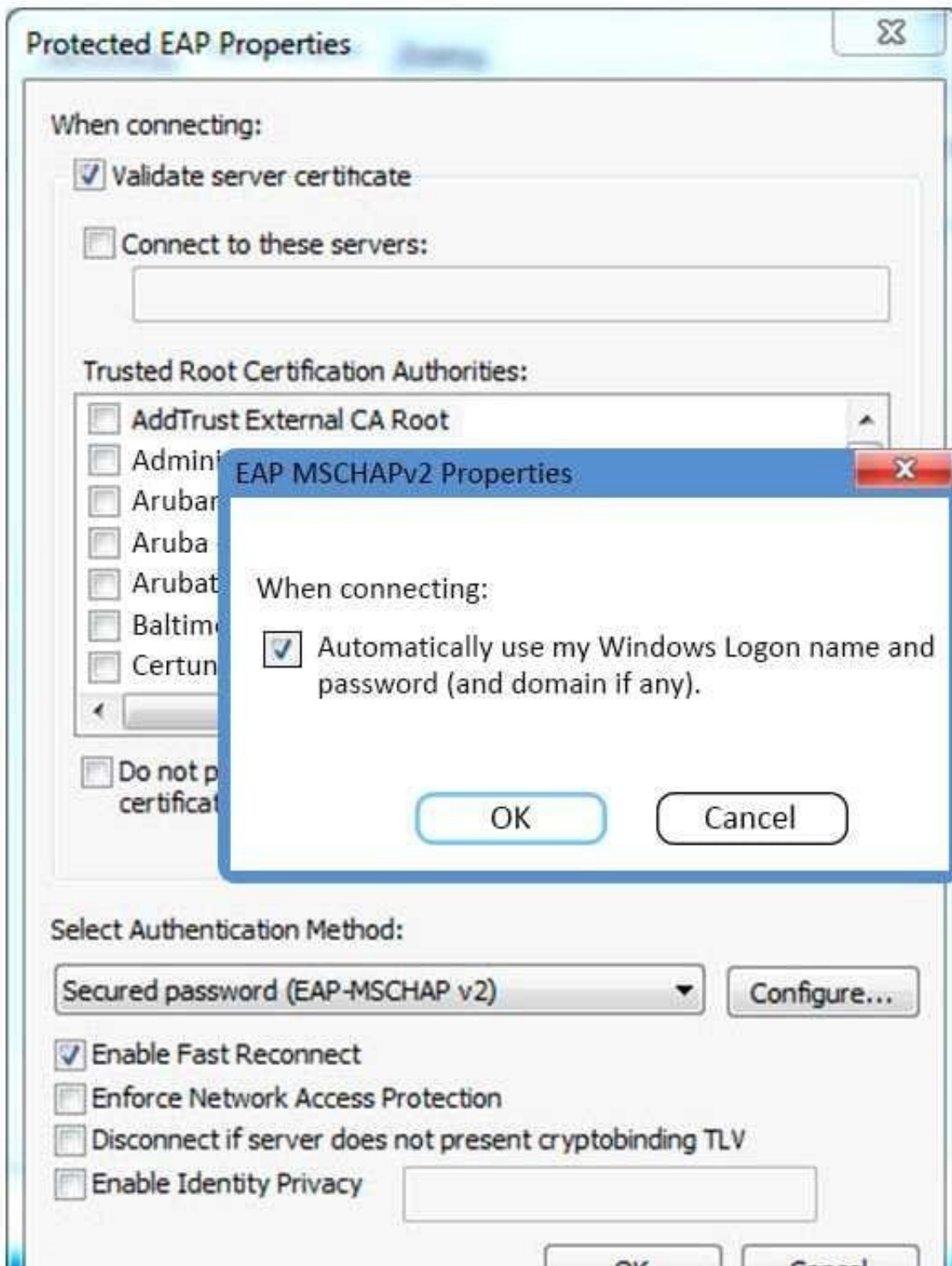
Based on the configuration for `maximum devices` shown, which statement accurately describes its settings?

- A. The user cannot Onboard any devices.
- B. It limits the total number of devices that can be provisioned by ClearPass.
- C. It limits the total number of Onboarded devices connected to the network.
- D. It limits the number of devices that a single user can Onboard.
- E. It limits the number of devices that a single user can connect to the network.

Correct Answer: D

QUESTION 10

Refer to the exhibit.



Based on the configuration of a Windows 802.1X supplicant shown, what will be the outcome when 'Automatically use my Windows logon name and password' are selected?

- A. The client will use machine authentication.
- B. The client's Windows logon username and password will be sent inside a certificate to the Active Directory server.
- C. The client's Windows logon username and password will be sent to the Authentication server.



- D. The client will need to re-authenticate every time they connect to the network.
- E. The client will prompt the user to enter the logon username and password.

Correct Answer: C

QUESTION 11

Which IP address should be set as the DHCP relay on an Aruba Controller for device fingerprinting on ClearPass?

- A. DHCP server IP
- B. Active Directory IP
- C. Switch IP
- D. Microsoft NPS server IP
- E. ClearPass server IP

Correct Answer: E

QUESTION 12

Refer to the exhibit.

The screenshot shows the 'Access Tracker' interface for 'Server: Clearpass6 (10.254.1.176)'. The data filter is set to '[All Requests]' and the date range is 'Last 1 day before Today'. A table of requests is displayed with columns for Server, Type, User, Service Name, Login, and Date. One request is highlighted with a red background, indicating it was rejected. The 'Request Details' pop-up window shows the following information:

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			

What can be concluded from the Access Tracker output shown?

- A. The client used incorrect credentials to authenticate to the network.
- B. ClearPass does not have a service enabled for MAC authentication.

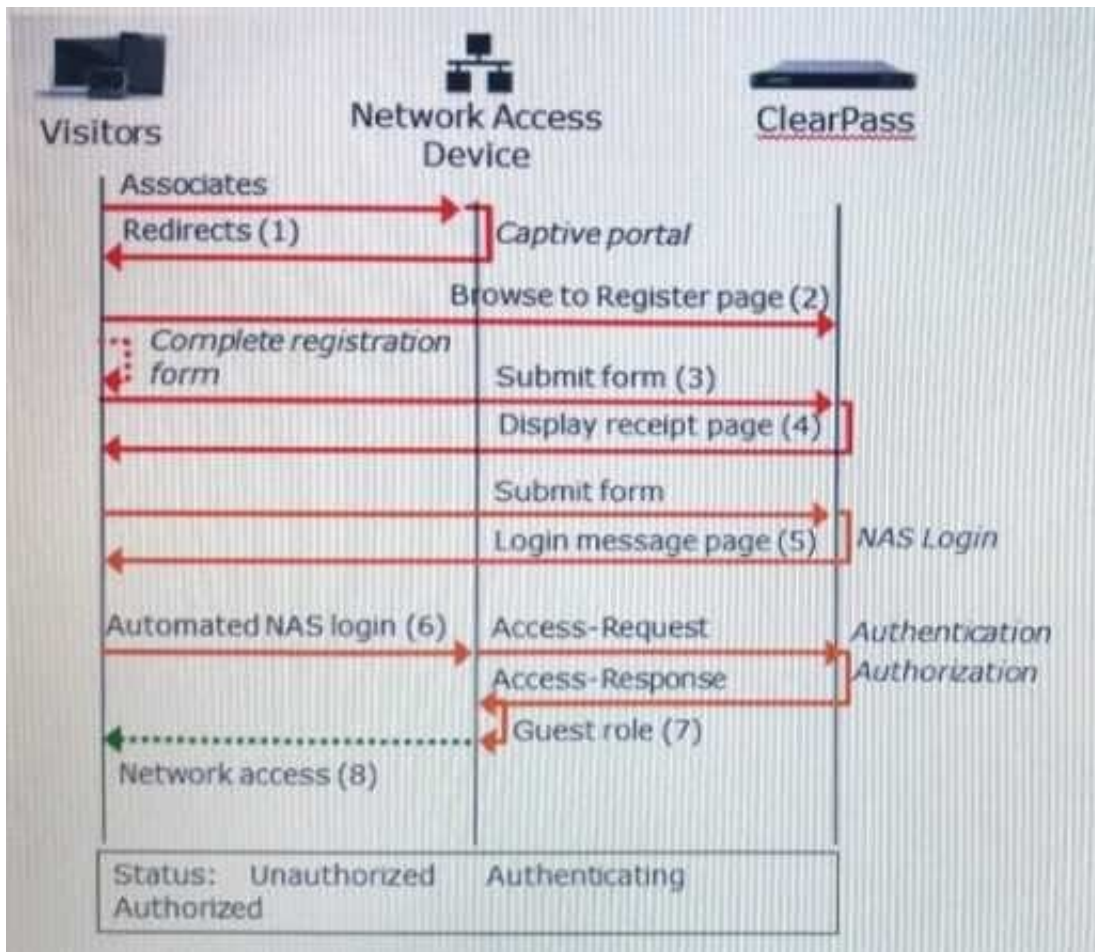


- C. The client MAC address is not present in the Endpoints table in the ClearPass database.
- D. The RADIUS client on the Windows server failed to categorize the service correctly.
- E. The client wireless profile is incorrectly setup.

Correct Answer: B

QUESTION 13

Refer to the exhibit.



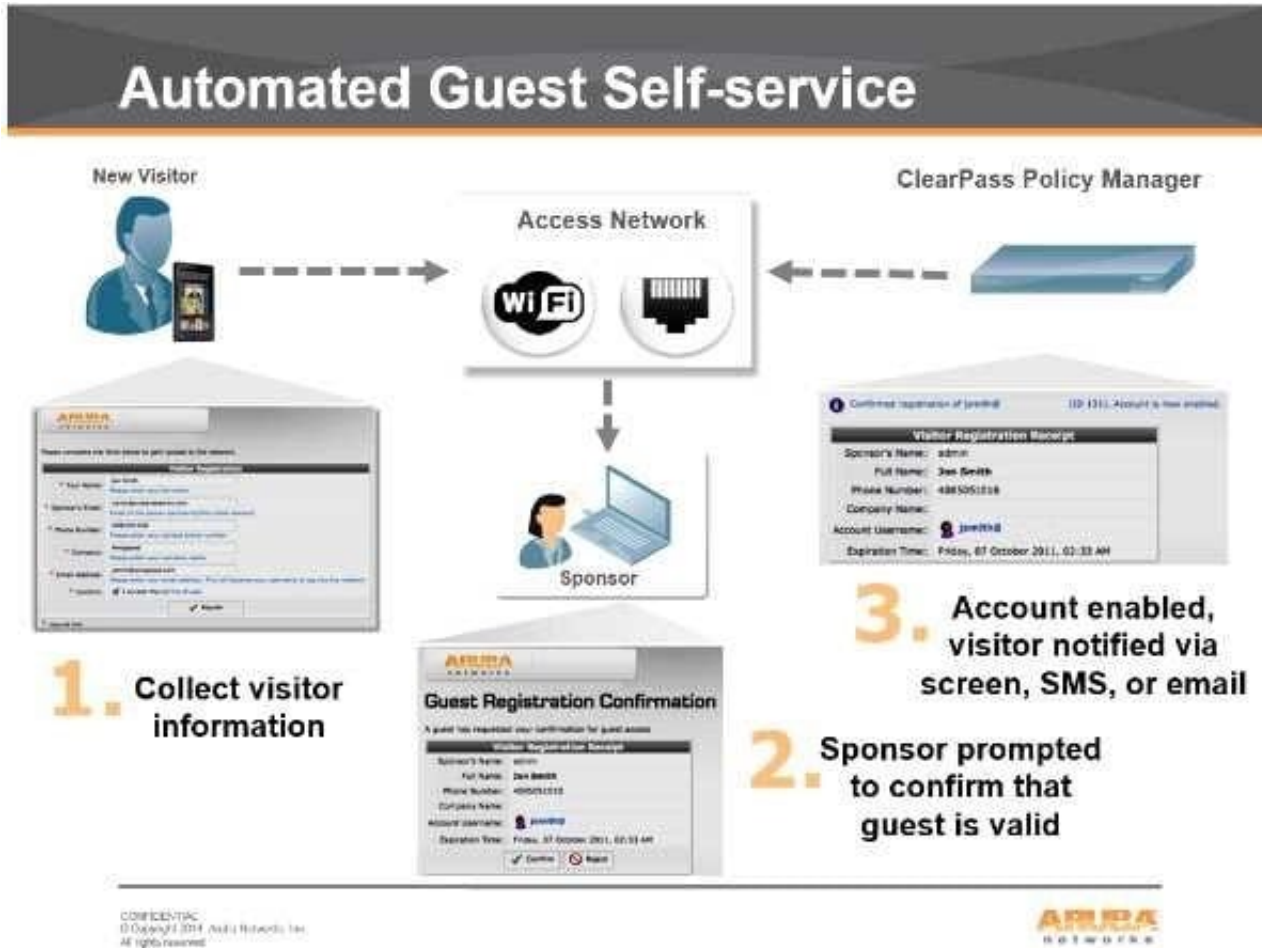
Based on the guest Self-Registration with Sponsor Approval workflow shown, at which stage is an email request sent to the sponsor?

- A. after `Guest Role (7)`
- B. after `Login Message page (5)`
- C. after `Submit form (3)`
- D. after `Automated NAS login (6)`
- E. after `Redirects (1)`



Correct Answer: C

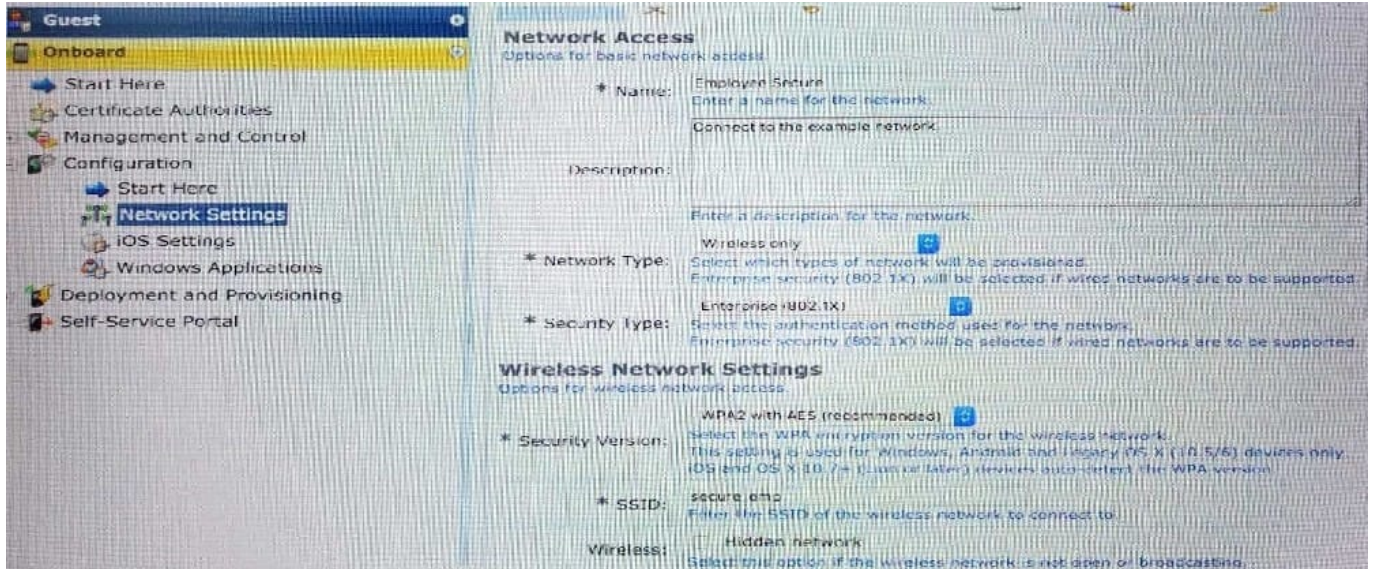
There's the Self Service part of provisioning one's information. Then the sponsor/operator part to confirm that guest is valid. Then the enablement via the sponsor/operator clicking 'confirm'.



References: <https://community.arubanetworks.com/t5/Security/Guest-Captive-Portal-sponsor-approval-architecture/td-p/267625>

QUESTION 14

Refer to the exhibit.



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.

Correct Answer: DE

QUESTION 15

Refer to the exhibit.



Device Provisioning Settings	
General	Web Login
iOS	OS & OS X
Legacy OS X	Windows
Android	Onboard Client
*Name:	Local Device Provisioning <small>Enter a name for this configuration set.</small>
Description:	This is the default configuration set for device provisioning. <small>Enter a description for the configuration set.</small>
*Organization:	Example Organization <small>Enter an organization name for this configuration set. The organization name is displayed by the device during provisioning.</small>
Identity <small>These options control the generation of device credentials</small>	
* Certificate Authority:	Local Certificate Authority <small>Select the certificate authority that will be used to sign profiles and messages.</small>
* Signer:	Onboard Certificate Authority <small>Select the source that will be use to sign TLS client certificates.</small>
* Key Type:	1024-bit RSA - created by device <small>Select the type of private key to use for TLS certificates.</small>
* Unique Device Credentials:	<input checked="" type="checkbox"/> Include the username in unique device credentials <small>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.</small>

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.

Correct Answer: BD

[HPE6-A68 PDF Dumps](#)

[HPE6-A68 VCE Dumps](#)

[HPE6-A68 Practice Test](#)