

## HP.Premium.HPE6-A15.by.VCEplus.105q

Number: HPE6-A15 VCEplus  
Passing Score: 800  
Time Limit: 120 min  
File Version: 3.3



**Exam Code:** HPE6-A15

**Exam Name:** Aruba Certified ClearPass Professional 6.5

**Certification Provider:** HP

**Corresponding Certification:** HP ACCP

**Website:** [www.vceplus.com](http://www.vceplus.com)

**Free Exam:** <https://vceplus.com/exam-hpe6-a15/>

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in HPE6-A15 exam products and you get latest questions. We strive to deliver the best HPE6-A15 exam product for top grades in your first attempt.

**Website:** <https://vceplus.com>

**VCE to PDF Converter:** <https://vceplus.com/vce-to-pdf/>

**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>

**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

## QUESTION 1

Refer to the exhibit.

Summary		Policy	Mapping Rules
<b>Policy:</b>			
Policy Name:	WLAN,role mapping		
Description:			
Default Role:	[Guest]		
<b>Mapping Rules:</b>			
Rules Evaluation Algorithm: First applicable			
Conditions		Role Name	
1.	(Authorization:remotelab AD:Department EQUALS Product Management) OR (Authorization:remotelab AD:UserDN EQUALS Executive)	Executive	
2.	(Authorization:[Endpoints Repository]:OS Family EQUALS IGNORE_CASE Windows)	Vendor	
3.	(Authorization:[Endpoints Repository]:Category CONTAINS SmartDevice) AND (Authorization:[Endpoints Repository]:OS Family EQUALS IGNORE_CASE Apple)	iOS Device	
4.	(Authorization:remotelab AD:Department EQUALS HR) OR (Connection:NAD-IP-Address BELONGS_TO_GROUP HQ) OR (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday) (Host:OSType CONTAINS Fedora)	HR Local	
5.	OR (Host:OSType CONTAINS Redhat) OR (Host:OSType CONTAINS Ubuntu)	Linux User	
6.	(Connection:NAD-IP-Address BELONGS_TO_GROUP Remote NAD)	Remote Employee	

An AD user's department attribute value is configured as "QA". The user authenticates from a laptop running MAC OS X. Which role is assigned to the user in ClearPass?

- A. HR Local
- B. Remote Employee
- C. [Guest]
- D. Executive
- E. iOS Device

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

None of the Listed Role Name conditions are met.

## QUESTION 2

Refer to the exhibit.

Configuration » Authentication » Sources » Add - remotelab AD

Authentication Sources - remotelab AD

Summary	General	Primary	Attributes
Specify filter queries used to fetch authentication and authorization attributes			
Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	dn	UserDN	-
	department	Department	Role, Attribute
	title	Title	Attribute
	company	company	-
	memberOf	memberOf	Role, Attribute
	telephoneNumber	Phone	Attribute
	mail	Email	Attribute

Based on the Attribute configuration shown, which statement accurately describes the status of attribute values?

- A. Only the attribute values of department and memberOf can be used in role mapping policies.
- B. The attribute values of department, title, memberOf, telephoneNumber, and mail are directly applied as ClearPass.
- C. Only the attribute value of company can be used in role mapping policies, not the other attributes.
- D. The attribute values of department and memberOf are directly applied as ClearPass roles.
- E. Only the attribute values of title, telephoneNumber, and mail can be used in role mapping policies.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 3

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

C: Role Mappings Page - Rules Editor Page Parameters



Parameter	Description
Type	<p>The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context. (Refer to <a href="#">Namespaces</a>.)</p> <p>In the role mapping context, Policy Manager allows attributes from following namespaces:</p> <ul style="list-style-type: none"> <li>• Application</li> <li>• Application:ClearPass</li> <li>• Authentication</li> <li>• Authorization</li> <li>• Authorization:&lt;authorization_source_instance&gt; - Policy Manager shows each instance of the authorization source for which attributes have been configured to be fetched. (See <a href="#">Adding and Modifying Authentication Sources</a>). Only those attributes that have been configured to be fetched are shown in the attributes drop-down list.</li> <li>• Certificate</li> <li>• Connection</li> <li>• Date</li> <li>• Device</li> <li>• Endpoint</li> <li>• GuestUser</li> <li>• Host</li> <li>• LocalUser</li> <li>• Onboard</li> <li>• TACACS</li> <li>• RADIUS - All enabled RADIUS vendor dictionaries.</li> </ul>
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 <a href="#">Operators</a> .
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 <a href="#">Host Namespaces</a>
Authentication	See <a href="#">Authentication Namespaces</a>
Connection	See <a href="#">Connection Namespaces</a>
Application	See <a href="#">Application Namespace</a>
<ul style="list-style-type: none"> <li>• Radius:IETF</li> <li>• Radius:Cisco</li> <li>• Radius:Microsoft</li> <li>• Radius:Avenda</li> <li>• Radius:Aruba</li> </ul>	See <a href="#">RADIUS Namespaces</a>
Name	The options displayed for the <b>Name</b> attribute depend on the <b>Type</b> attribute that was selected.
Value	The options displayed for the <b>Value</b> attribute depend on the <b>Type</b> and <b>Name</b> 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/identity/RoleMappingPolicies.html) [http://www.arubanetworks.com/techdocs/ClearPass/Aruba\\_CPPMOnlineHelp/Content/CPPM\\_UserGuide/PolicySim/PS\\_Enforcement\\_Policy.htm](http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/PolicySim/PS_Enforcement_Policy.htm)

#### QUESTION 4

Refer to the exhibit.

Summary	Service	Authentication	Roles	Enforcement
<b>Authentication Methods:</b> <div> [EAP PEAP]  [EAP TLS]  [EAP MSCHAPv2] </div> <div> Move Up  Move Down  Remove  View Details  Modify </div>				
<div>--Select to Add--</div>				
<b>Authentication Sources:</b> <div> [Local User Repository] [Local SQL DB]  remotelab AD [Active Directory] </div> <div> Move Up  Move Down  Remove </div>				

Based on the Authentication sources configuration shown, which statement accurately describes the outcome if the user is not found?

- A. If the user is not found in the remotelab AD but is present in the local user repository, a reject message is sent back to the NAD.
- B. If the user is not found in the local user repository but is present in the remotelab AD, a reject message is sent back to the NAD.
- C. If the user is not found in the local user repository a reject message is sent back to the NAD.
- D. If the user is not found in the local user repository and remotelab AD, a reject message is sent back to the NAD.
- E. If the user is not found in the local user repository a timeout message is sent back to the NAD.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Policy Manager looks for the device or user by executing the first filter associated with the authentication source.

After the device or user is found, Policy Manager then authenticates this entity against this authentication source. The flow is outlined below:

\* On successful authentication, Policy Manager moves on to the next stage of policy evaluation, which collects role mapping attributes from the authorization sources.

\* Where no authentication source is specified (for example, for unmanageable devices), Policy Manager passes the request to the next configured policy component for this service.\* If Policy Manager does not find the connecting entity in any of the configured authentication sources, it rejects the request.

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 134

<https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf>

**QUESTION 5**

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

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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%20Policy%20Manager%206.5%20User%20Guide.pdf>

#### **QUESTION 6**

Which CLI command is used to upgrade the image of a ClearPass server?

- A. Image update
- B. System upgrade
- C. Upgrade image
- D. Reboot
- E. Upgrade software

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



Explanation:

When logged in as appadmin, you can manually install the Upgrade and Patch binaries imported via the CLI using the following commands: \* system update (for patches)

\* system upgrade (for upgrades)

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 564

<https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf>

#### QUESTION 7

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.

**Correct Answer:** AC

**Section:** (none)

**Explanation**



**Explanation/Reference:**

Explanation:

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

#### QUESTION 8

What is the purpose of Operator Profiles?

- 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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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/OperatorProfiles.htm](http://www.arubanetworks.com/techdocs/ClearPass/CPGuest_UG_HTML_6.5/Content/OperatorLogins/OperatorProfiles.htm)

**QUESTION 9**

Refer to the exhibit.

Administration » Dictionaries » RADIUS

### RADIUS Dictionaries

RADIUS Attributes				
Vendor Name:		Aruba (14823)		
#	Attribute Name	ID	Type	In/Out
1.	Aruba-User-Role	1	String	in out
2.	Aruba-User-Vlan	2	Unsigned32	in out
3.	Aruba-Priv-Admin-User	3	Unsigned32	in out
4.	Aruba-Admin-Role	4	String	in out
5.	Aruba-Essid-Name	5	String	in out
6.	Aruba-Location-Id	6	String	in out
7.	Aruba-Port-Id	7	String	in out
8.	Aruba-Template-User	8	String	in out
9.	Aruba-Named-Vlan	9	String	in out
10.	Aruba-AP-Group	10	String	in out

Disable Export Close

In the Aruba RADIUS dictionary shown, what is the purpose of the RADIUS attributes?

A. to gather and send Aruba NAD information to ClearPass

- B. to gather information about Aruba NADs for ClearPass
- C. to send information via RADIUS packets to Aruba NADs
- D. to send information via RADIUS packets to clients
- E. to send CoA packets from ClearPass to the Aruba NAD

**Correct Answer:** C

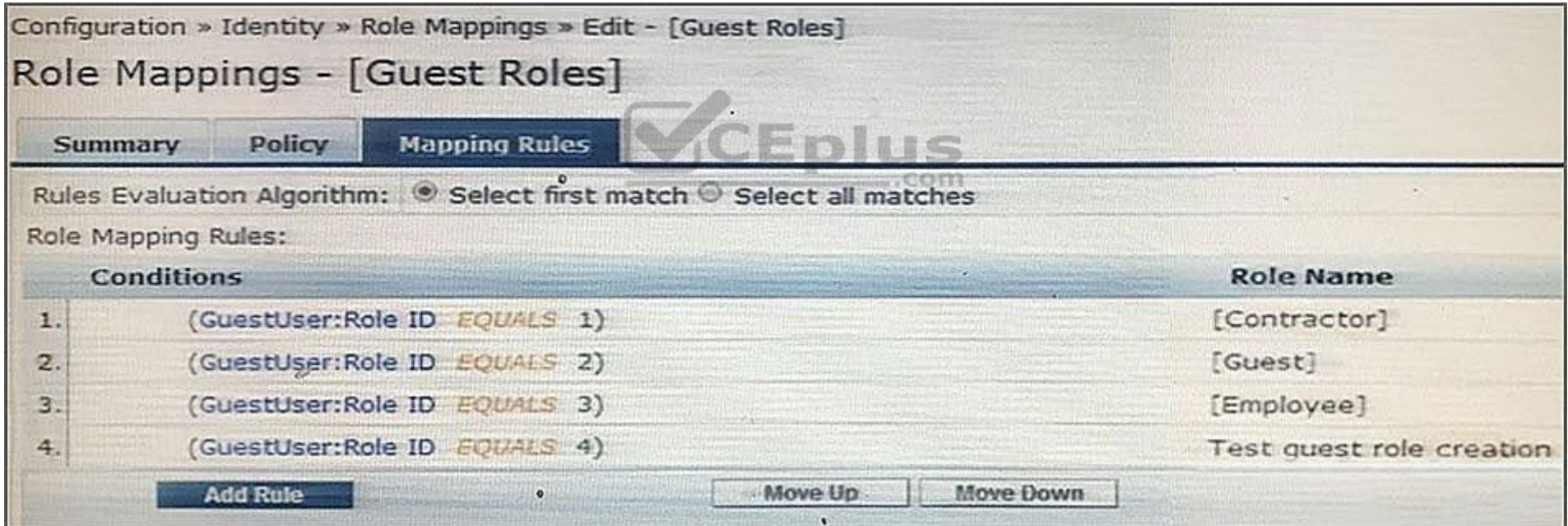
**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 10

Refer to the exhibit.



Configuration » Identity » Role Mappings » Edit - [Guest Roles]

### Role Mappings - [Guest Roles]

Summary Policy **Mapping Rules**

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Role Mapping Rules:

	Conditions	Role Name
1.	(GuestUser:Role ID EQUALS 1)	[Contractor]
2.	(GuestUser:Role ID EQUALS 2)	[Guest]
3.	(GuestUser:Role ID EQUALS 3)	[Employee]
4.	(GuestUser:Role ID EQUALS 4)	Test guest role creation

Add Rule Move Up Move Down

Based on the Guest Role Mapping Policy shown, what is the purpose of the Role Mapping Policy?

- A. to display a role name on the Self-registration receipt page
- B. to send a firewall role back to the controller based on the Guest User's Role ID

- C. to assign Controller roles to guests
- D. to assign three roles of [Contractor], [Guest] and [Employee] to every guest user
- E. to create additional account roles for guest administrators to assign to guest accounts

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 11

A customer wants all guests who access a company's guest network to have their accounts approved by the receptionist, before they are given access to the network. How should the network administrator set this up in ClearPass? (Select two.)

- A. Enable sponsor approval confirmation in Receipt actions.
- B. Configure SMTP messaging in the Policy Manager.
- C. Configure a MAC caching service in the Policy Manager.
- D. Configure a MAC auth service in the Policy Manager.
- E. Enable sponsor approval in the captive portal authentication profile on the NAD.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

A: Sponsored self-registration is a means to allow guests to self-register, but not give them full access until a sponsor (could even be a central help desk) has approved the request. When the registration form is completed by the guest/user, an on screen message is displayed for the guest stating the account requires approval.

Guests are disabled upon registration and need to wait on the receipt page for the confirmation until the login button gets enabled. D. Device Mac Authentication is designed for authenticating guest devices based on their MAC address.

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 94

<https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf>

### QUESTION 12

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:	<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 be accessible from "/guest/page_name.php".
Description:	<div style="border: 1px solid black; height: 40px; width: 100%;"></div> 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 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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

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](http://www.arubanetworks.com/techdocs/ClearPass/CPGuest_UG_HTML_6.5/Content/Configuration/CreateEditWebLogin.htm)

### **QUESTION 13**

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:	<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 be accessible from "/guest/page_name.php".
Description:	<div style="border: 1px solid black; height: 40px; width: 100%;"></div> 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 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 Address field value 'securelogin.arubanetworks.com' used for?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 14**

Refer to the exhibit.



Configuration >> Services >> Edit - MAC Caching - Guest Access With MAC Caching

## Services - MAC Caching - Guest Access With MAC Caching

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results:	Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:	<b>MAC Caching - Guest Access With MAC Caching</b> <a href="#">Modify</a>				<a href="#">Add new Enforcement Policy</a>
<b>Enforcement Policy Details</b>					
Description:	Limits guests to maximum n device for MAC caching purposes				
Default Profile:	[Allow Access Profile]				
Rules Evaluation Algorithm:	first-applicable				
Conditions	Enforcement Profiles				
1. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 2)	[Deny Access Profile]				
2. (Date:Day-of-Week BELONGS TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	MAC Caching - Guest Session Timeout, MAC Caching - Guest Bandwidth Limit, MAC Caching - Guest Session Limit, MAC Caching - Guest MAC Caching (Update Endpoint Known), Mac Caching - Guest Do Expire, Mac Caching - Guest Expire Post Login				

A guest connects to the Guest SSID and authenticates successfully using the guest.php web login page. Based on the MAC Caching service information shown, which statement about the guests' MAC address is accurate?

- It will be visible in the Guest User Repository with Unknown Status
- It will be deleted from the Endpoint table.
- It will be visible in the Guest User Repository with Known Status.
- It will be visible in the Endpoints table with Known Status.
- It will be visible in the Endpoints table with Unknown Status.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 15**

A university wants to deploy ClearPass with the Guest module. The university has two types that need to use web login authentication. The first type of users are students whose accounts are in an Active Directory server. The second type of users are friends of students who need to self-register to access the network. How should the service be set up in the Policy Manager for this network?

- A. Guest User Repository and Active Directory server both as authentication sources
- B. Active Directory server as the authentication source, and Guest User Repository as the authorization source
- C. Guest User Repository as the authentication source, and Guest User Repository and Active Directory server as authorization sources
- D. either the Guest User Repository or Active Directory server should be the single authentication source
- E. Guest User Repository as the authentication source and the Active Directory server as the authorization source

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 16**

An administrator enabled the Pre-auth check for their guest self-registration. At what stage in the registration process in this check performed?

- A. after the user clicks the login button and after the NAD sends an authentication request
- B. after the user self-registers but before the user logs in
- C. after the user clicks the login button but before the NAD sends an authentication request
- D. when a user is re-authenticating to the network
- E. before the user self-registers

**Correct Answer:** C

**Section:** (none)

## Explanation

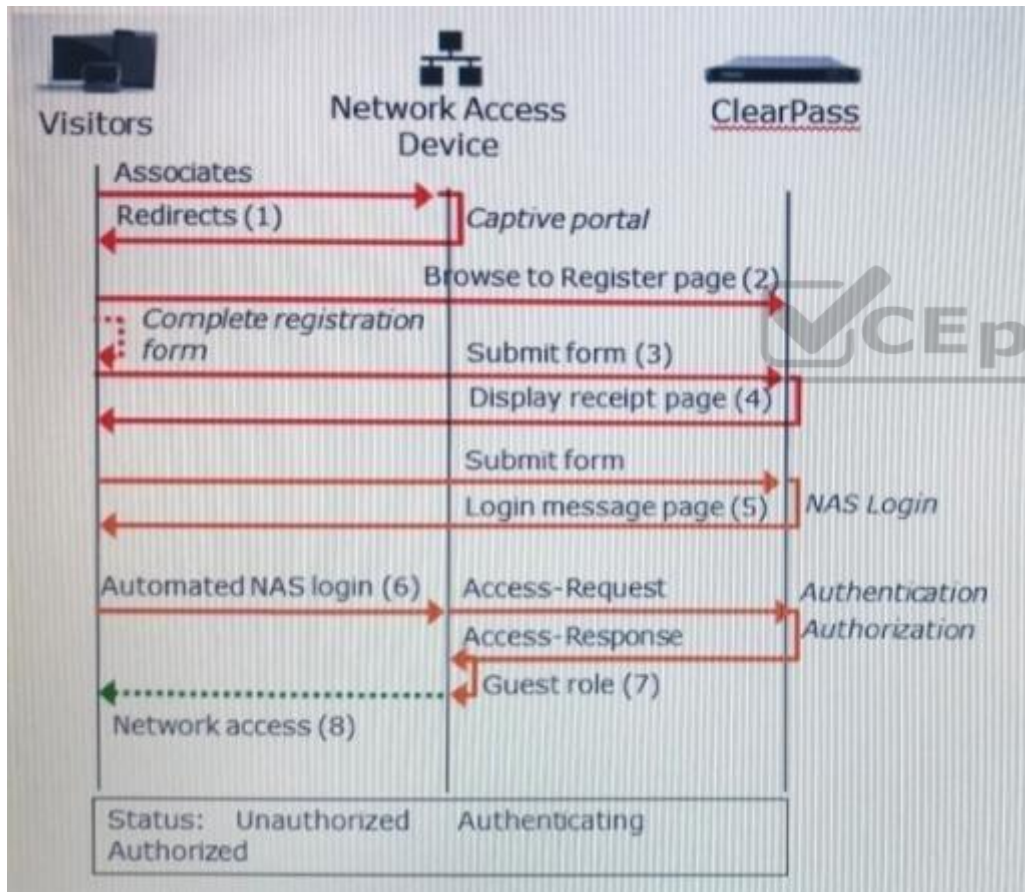
### Explanation/Reference:

Explanation:

The Onboard template is designed for configuration that allows to perform checks before allowing Onboard provisioning for Bring Your Own Device (BYOD) use-cases. This service creates an Onboard Pre-Auth service to check the user's credentials before starting the device provisioning process. This also creates an authorization service that checks whether a user's device can be provisioned using Onboard.

### QUESTION 17

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

There's the Self Service part of provisioning one's information.

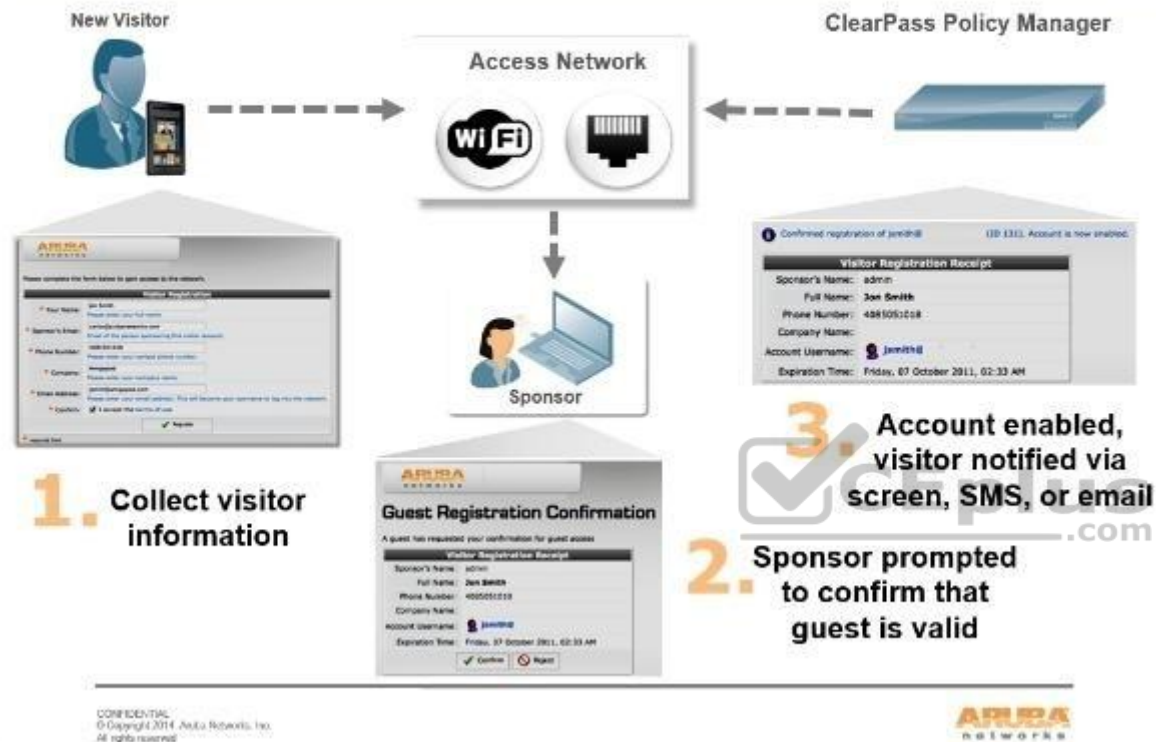
Then the sponsor/operator part to confirm that guest is valid.

Then the enablement via the sponsor/operator clicking 'confirm'.





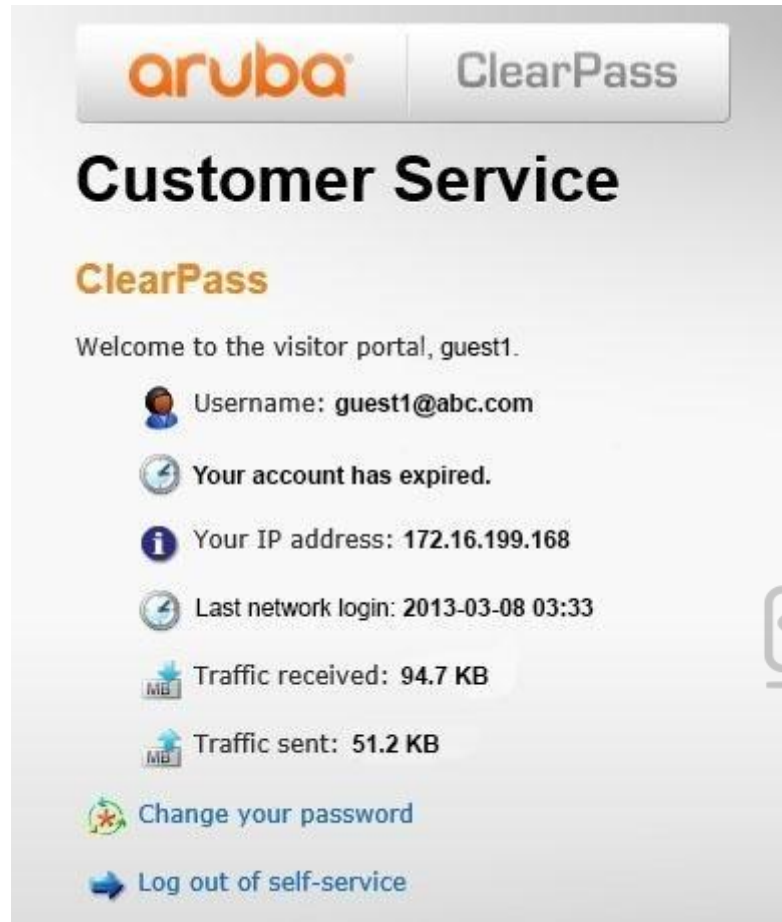
# Automated Guest Self-service



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

## QUESTION 18

Refer to the exhibit.



A user logged in to the Self-Service Portal as shown.  
What do the traffic received and sent statistics present?

- A. the total amount of the traffic the quest transmitted, as seen through RADIUS CoA packets from the client to ClearPass
- B. the total amount of traffic the guest transmitted, as seen through RADIUS accounting messages sent from the NAD to ClearPass
- C. the total amount of traffic the guest transmitted, as seen through RADIUS CoA packets from the NAD to ClearPass
- D. the total amount of traffic the guest transmitted after account expiration, as seen through RADIUS accounting messages sent from the NAD to ClearPass
- E. the total amount of traffic the NAD transmitted to ClearPass, as seen through RADIUS accounting messages from the NAD to ClearPass.

Correct Answer: B

Section: (none)







Explanation

Explanation/Reference:

#### QUESTION 19

Refer to the exhibit.

Use this list view to modify the fields of the form **create\_user**.

Quick Help		Preview Form		
Rank	Field	Type	Label	Description
10	<b>sponsor_name</b>	text	Sponsor's Name:	Name of the person sponsoring this visitor account.
15	<b>sponsor_email</b>	text	Sponsor's Email:	Email of the person sponsoring this visitor account.
20	<b>visitor_name</b>	text	Visitor's Name:	Name of the visitor.
25	<b>visitor_phone</b>	text	Phone Number	The visitor's phone number
 Edit  Edit base field  Remove  Insert before  Insert After  Enable Field				
30	<b>visitor_company</b>	text	Company Name:	Company name of the visitor.
40	<b>email</b>	text	Email Address:	The visitor's email address. This will become their username to log into the network.
50	<b>modify_start_time</b>	dropdown	Account Activation:	Select an option for changing the activation time of this account.

Based on the configuration of the create\_user form shown, which statement accurately describes the status?

- A. The email field will be visible to guest users when they access the web login page.
- B. The visitor\_company field will be visible to operators creating the account.
- C. The visitor\_company field will be visible to the guest users when they access the web login page.
- D. The visitor\_phone field will be visible to the guest users in the web login page.
- E. The visitor\_phone field will be visible to operators creating the account.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

References: <https://community.arubanetworks.com/t5/AAA-NAC-Guest-Access-BYOD/expire-timezone-field-is-not-showing-up-on-the-create-user-form/tap/250230>

#### **QUESTION 20**

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**